POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SISTEMA CREDISIS

CrediSIS
Sistema de Crédito Cooperativo

www.credisis.com.br

FICHA-CONTROLE

Título:	**Política de Segurança da Informação do Sistema CrediSIS**
Autoria	Segurança da Informação
Status	Aprovada
Órgão Homologador	Conselho de Administração - CONSAD
Data da Homologação	24/04/2024
Classificação do Documento	Interno

HISTÓRICO DE VERSIONAMENTO

Versão	Descrição	Responsável	Aprovação
1.0	Versão Inicial do Documento	Infraestrutura de TI, Sistemas e Proteção de Dados	Reunião Extraordinária do CONSAD de 03/05/2019
2.0	Revisão	Infraestrutura de TI, Sistemas e Proteção de Dados	Reunião Ordinária do CONSAD de 29/04/2021
3.0	Revisão	Infraestrutura de TI, Sistemas e Proteção de Dados	Reunião Ordinária do CONSAD de 26/01/2022
4.0	Revisão	Proteção de Dados	Reunião Extraordinária do CONSAD de 03/05/2019
5.0	Revisão	Segurança da Informação	Reunião Extraordinária do CONSAD de 24/04/2024

SUMÁRIO

1. OBJETIVO

Art. 1º A Política de Segurança da Informação ("Política") tem como objetivo estabelecer conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança da informação, em especial sobre a segurança cibernética, visando preservar a confidencialidade, integridade e disponibilidade das informações sob responsabilidade do Sistema CrediSIS.

2. ABRANGÊNCIA

Art. 2º Esta Política tem abrangência sistêmica, ou seja, aplica-se à CrediSIS Central e a todas as suas Cooperativas Filiadas.

3. CONCEITOS E DEFINIÇÕES

Art. 3º Para inteira compreensão desta Política, ficam estabelecidos os seguintes conceitos e definições:

I. **Recursos:** Qualquer ativo, tangível ou intangível, pertencentes a serviço ou sob responsabilidade da CrediSIS Central, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem ou não, sistemas e processos;

II. **Ameaça:** Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais;

III. **Colaborador:** Entende-se como colaborador qualquer pessoa que trabalhe para o CrediSIS, quer seja funcionário com registro em carteira de trabalho, estagiário ou aprendiz;

IV. **Controle:** Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros;

V. **Gestor:** Colaborador que exerce cargo de liderança como: diretor, gerente, coordenador, líder ou chefe de seção;

VI. **Alta Administração:** Presidente, Vice-Presidente e membros do Conselho de Administração;

VII. **Informação:** Dados ou conjunto de dados que possuam algum propósito e valor para o CrediSIS, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem;

VIII. **Princípios de Privilégio Mínimo e Necessário Saber:** do Inglês "*Least Privilege e Need to know*", estes são princípios que devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de privilégios para executar a atividade necessária (Privilégio Mínimo) a quem realmente tenha a necessidade de acesso (Necessário Saber);

IX. **Risco:** Qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e sua estratégia de negócios ou, conforme a ISO 31000, o efeito da incerteza nos objetivos;

X. **Segurança da Informação (SI):** é a proteção das informações, sendo caracterizada pela preservação de:

a) **Confidencialidade:** garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;

b) **Integridade:** garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade;

c) **Disponibilidade:** garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;

XI. **Segurança Cibernética:** Conjunto de tecnologias, processos e práticas, projetados para proteger redes, computadores, sistemas e dados, de ataques, danos, acidentais ou não, e acessos não autorizados, visando proteger somente assuntos relacionados ao digital;

XII. **Nuvem (*Cloud*):** Infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e irrestrita;

XIII. ***On Premise***: É uma abordagem em tecnologia da informação e software, na qual os sistemas, servidores e aplicativos são implantados e mantidos localmente, dentro das instalações físicas de uma organização;

XIV. ***IDS e IPS*:** Sigla de *Intrusion Detection System e Intrusion Prevention System*, são sistemas de detecção e prevenção a intrusão. A finalidade do IDS é identificar atividades anômalas na infraestrutura de redes ou de dispositivos, já o IPS que é um complemento não obrigatório aos IDS, tem por finalidade a execução automática de ações já previstas nas políticas do sistema ou em outras bases de referência internas e/ou externas;

XV. ***Malware:*** termo que se refere a *softwares*/códigos maliciosos utilizados para infectar dispositivos ou sistemas com intuito de causar danos, alterações, roubo de informações, entre outros. São exemplos de *malware*: vírus*, trojan* e *worm*;

XVI. ***Active Directory (AD):*** É um sistema da Microsoft usado principalmente em ambientes de rede de computadores para gerenciar e armazenar informações sobre usuários, computadores, impressoras e outros ativos;

XVII. **VLAN:** Sigla de *Virtual Local Area Network (Rede Local Virtual)*, que permite separar fisicamente uma rede em múltiplas redes lógicas independentes;

XVIII. **NAT:** Sigla de *Network Address Translation (Tradução de Endereço de Rede)*, é uma técnica utilizada para permitir que vários dispositivos em uma rede compartilhem um único endereço IP público para se conectar à internet;

XIX. **SSID:** Sigla de *Service Set Identifier (Identificador do conjunto de serviços)* É um identificador exclusivo que roteadores e pontos de acesso sem fio usam para identificar e distinguir suas redes;

XX. **MDM:** Sigla de *Mobile Device Management* (Gerenciamento de Dispositivos Móveis) refere-se a um conjunto de técnicas e ferramentas utilizadas para monitorar, gerenciar e controlar dispositivos móveis;

XXI. NDA: Sigla de *Non Disclosure Agreement* (Acordo de Não Divulgação.) É um documento vinculativo entre duas partes com o objetivo de não compartilhar informações

4. PAPÉIS E RESPONSABILIDADES

Art. 4º É responsabilidade de todos que se relacionem com as informações do CrediSIS, seguir as orientações de Políticas específicas, inclusive esta, Manual do Colaborador, Código de Ética e Conduta, Regimento Interno, Manual Operacional e demais normativos existentes que possam endereçar a segurança da informação, inclusive promover uma cultura de segurança na instituição, adotando comportamentos seguros nas suas rotinas e ações.

Art. 5º Todos os setores também possuem minimamente uma corresponsabilidade quanto ao levantamento de informações e evidências mediante a condução de auditorias internas, externas ou validações de conformidade acerca de segurança da informação, devendo contribuir e colaborar de forma transparente, honesta e sincera com as respostas durante todo o processo.

Art. 6º São responsabilidades da **ALTA ADMINISTRAÇÃO**:

I. Garantir aderência à Política de Segurança da Informação de acordo com os objetivos, estratégias e propósito do negócio do CrediSIS;

II. Seguir e aplicar as diretrizes de segurança previstas nas Políticas Específicas, Regimento Interno e no Estatuto Social da CrediSIS Central e suas singulares;

III. Tomar decisões de alto nível relacionadas à segurança da informação, incluindo, mas não se limitando, a alocação de orçamento, investimentos significativos em recursos e tecnologia, aprovação de iniciativas estratégicas;

IV. Aderir, assim como todos do sistema, as diretrizes, premissas e regras de segurança, bem como disseminá-las, demonstrando compromisso visível com a segurança em suas ações e decisões;

V. Apoiar ações e programas de conscientização em Segurança da Informação do Sistema CrediSIS.

Art. 7º São responsabilidades dos **COLABORADORES**:

I. Utilizar de modo seguro, responsável, moral e ético, todos os equipamentos, serviços e sistemas de TI;

II. Seguir as normas, procedimentos e Políticas do Sistema CrediSIS;

III. Notificar o setor de Segurança da Informação sobre as violações da Política de Segurança da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;

IV. Definir o valor da informação sob sua responsabilidade, seguindo as diretrizes da Política de Classificação da Informação;

V. Participar das ações e programas de conscientização e treinamento em segurança da informação.

Art. 8º São responsabilidades dos **GESTORES**:

I. Apoiar e incentivar o estabelecimento da Política de Segurança da Informação no CrediSIS;

II. Garantir que seus liderados tenham acesso e conhecimento desta Política e demais normas e padrões de segurança cibernética e da informação;

III. Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos colaboradores que violarem o Código de Ética e Conduta, a Política de Segurança da Informação e as normas da CrediSIS Central;

IV. Estabelecer controles de acessos a sistemas e dados de seus colaboradores;

V. Facilitar que seus colaboradores atuem em conjunto, quando pertinente, em processos de resposta a incidentes de segurança da informação;

VI. Antes de efetuar qualquer contratação de sistemas, aplicações, serviços ou soluções tecnológicas, submeter aos setores de Segurança da Informação e Riscos Não-Financeiros para efetuar a análise de fornecedor e classificação de relevância, garantindo assim o cumprimento de normas vigentes e processos internos;

Art. 9º São responsabilidades do **SETOR DE INFRAESTRUTURA DE TI**:

I. Gerir adequadamente os ativos e acessos de infraestrutura de TI, sejam eles internos ou em nuvem;

II. Manter atualizada a infraestrutura tecnológica, de acordo com a Política de Gestão de Ativos de TI;

III. Manter o processo para correção de vulnerabilidades, conforme descrito na Política de Gestão de Vulnerabilidades;

IV. Informar imediatamente o setor de Segurança da Informação, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos de TI da CrediSIS Central;

V. Manter padrões e configurações de segurança em servidores, firewalls, redes e demais ativos de TI sob sua gestão;

VI. Implementar e manter procedimentos de backup, garantindo a disponibilidade e integridade das informações em casos de incidentes de segurança ou desastres;

VII. Programar e executar testes de recuperação de desastres previstos nos escopos de continuidade de negócios.

Art. 10. São responsabilidades das **COOPERATIVAS FILIADAS**:

I. Seguir todas as diretrizes desta Política e das mencionadas;

II. Notificar o setor de Segurança da Informação sobre as violações da Política de Segurança da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;

III. Manter o processo para correção de vulnerabilidades, conforme descrito na Política de Gestão de Vulnerabilidades;

IV. Colaborar com a CrediSIS Central na implantação dos requisitos de tecnologia descritos nas políticas;

V. Implementar, manter ou contribuir com os procedimentos de backup da cooperativa, garantindo a disponibilidade e integridade das informações em caso de incidentes ou desastres;

VI. Facilitar que seus colaboradores atuem em conjunto, quando pertinente, em processos de resposta a incidentes de segurança da informação;

VII. Contribuir com os setores de tecnologia da Central nos diversos aspectos que se remetem a segurança da informação e cibernética, garantindo uma abordagem integrada e consistente de segurança.

Art. 11. São responsabilidades do **SETOR DE OPERAÇÕES**:

I. Implementar processos, recursos e tecnologia que visem garantir a disponibilidade das aplicações e sistemas do CrediSIS;

II. Colaborar com as demais áreas de tecnologia, em especial com as áreas de Infraestrutura de TI, Desenvolvimento e Segurança da Informação na resposta a incidentes, correções de vulnerabilidades, aplicação de patches de atualização, visando minimizar o impacto ao negócio;

III. Implementar processos de gestão de mudanças para execução de mudanças planejadas em sistemas, aplicações e serviços da operação de TI.

Art. 12. São responsabilidades do **SETOR DE DESENVOLVIMENTO**:

I. Tratar os riscos e vulnerabilidades conforme diretrizes da Política de Gestão de Vulnerabilidades;

II. Implementar práticas de segurança no desenvolvimento de soluções, adotando padrões e diretrizes de segurança de mercado conforme exigido na Política de Desenvolvimento Seguro;

III. Controlar alterações nos sistemas e serviços mantidos pela área, mantendo o alinhamento adequado com demais áreas, em especial o setor de Operações, para garantir que não ocorram impactos adversos na operação da empresa ou em sua segurança;

IV. Utilizar técnicas que visem garantir a proteção de dados pessoais e sensíveis durante processamento, armazenamento e transmissão dos mesmos em processos de desenvolvimento.

Art. 13. São responsabilidades do **SETOR DE GESTÃO DE PESSOAS**:

I. Garantir que o processo formal de avaliação dos candidatos às vagas de emprego inclua a verificação adequada de antecedentes e referências do candidato de acordo com a ética, leis e normativos vigentes, em especial a política de recrutamento e seleção da CrediSIS Central;

II. Garantir que a Política, Normas e Procedimentos desta Política sejam divulgados no processo de admissão/integração de novos colaboradores;

III. Promover, juntamente com o setor de Segurança da Informação, capacitação e programas de conscientização de segurança e desta política para todos os colaboradores;

IV. Notificar as áreas sobre contratações, afastamentos, férias ou desligamento de colaboradores para execução adequada de controle de acessos.

Art. 14. São responsabilidades dos **FORNECEDORES, TERCEIROS E PARCEIROS DE NEGÓCIO**:

I. Cumprir as determinações da Política, Normas e Procedimentos publicados pela CrediSIS Central e suas singulares;

II. Cumprir com o NDA (*Non Disclosure Agreement*) do CrediSIS;

III. Fornecer informações a CrediSIS Central durante processos de análise e diligência prévia;

IV. Notificar prontamente a instituição contratante sobre qualquer incidente de segurança que possa afetar seus dados e sistemas, incluindo violações de segurança, acessos autorizados ou outras atividades suspeitas;

V. Cooperar com auditorias e avaliações de segurança conduzidas pela organização ou por terceiros designados.

Art. 15. São responsabilidades do **SETOR DE SEGURANÇA DA INFORMAÇÃO**:

I. Elaborar e conduzir os processos de revisão desta Política;

II. Conduzir a resposta aos Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos

fatos ocorridos, conforme Plano de Resposta a Incidentes de Segurança da Informação;

III. Orientar e coordenar as ações de segurança da informação e cibernética necessárias para a CrediSIS Central e cooperativas filiadas;

IV. Conduzir o processo de gestão de vulnerabilidades, de acordo com as diretrizes estabelecidas na política relacionada a este tema;

V. Definir um plano ou programa para ações de disseminação e conscientização da cultura de Segurança da Informação;

VI. Apoiar nas diretrizes e avaliação de riscos de segurança da informação e cibernética;

VII. Fazer a gestão dos certificados da CrediSIS Central através de solução tecnológica específica para essa finalidade.

5. TRATAMENTO E CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 16. Dados e Informações consideradas críticas e essenciais para a continuidade dos negócios do Sistema CrediSIS deverão ter cópia de segurança em local físico distinto, devidamente protegido para essa finalidade ou outro meio eficiente para permitir sua pronta recuperação em caso de perda ou danos.

Art. 17. Os equipamentos que contiverem informações do CrediSIS, somente poderão ser deslocados para venda ou doação, após serem submetidos ao processo de sanitização.

Parágrafo único. As cooperativas singulares são responsáveis por executar o processo de sanitização dos equipamentos ou por encaminhá-los ao setor de Operações da Central, para que esta execute o processo, garantindo registros e evidências de todo o processo para fins de auditoria e controle.

Art. 18. No caso da não utilização de processos de sanitização, o disco rígido deverá ser armazenado em local seguro ou destruído.

Art. 19. Em caso de terceirização deste serviço, como descarte de equipamentos eletrônicos através de alguma empresa, eles devem garantir o cumprimento do disposto nesta Política.

Art. 20. As informações contidas em material ou dispositivos que se tornarem passíveis de descarte, deverão ser preferencialmente destruídas, conforme descrito na Política de Gestão, Retenção e Descarte de Dados e Documentos.

Art. 21. Dados e Informações deverão ser classificadas quanto a sua relevância, seguindo as diretrizes da Política de Classificação da Informação.

6. DA GESTÃO DE ACESSOS

Art. 22. Deve ser definido um processo formal de registro para cancelamento e provisionamento de acessos de usuários, permitindo a atribuição adequada de direitos de acesso.

Art. 23. O processo supracitado deve garantir minimamente que:

I. Registros formais sejam definidos para solicitação de concessão e revogação de acessos;

II. Cada colaborador deve possuir suas próprias credenciais de usuário, não sendo permitido o uso compartilhado do mesmo;

III. O bloqueio dos acessos deve ser realizado ou, quando não for possível, a alteração imediata da senha deve ser realizada durante períodos de férias e afastamento;

IV. Em caso de desligamento do colaborador, os acessos devem ser revogados imediatamente;

V. Os proprietários dos ativos de TI, sistemas, aplicações e plataformas têm a responsabilidade por provisionar ou revogar acessos pertinentes a sua responsabilidade e garantir que o nível de acesso concedido atende as práticas de privilégio mínimo;

VI. Adaptar os direitos de acesso de um usuário mediante a mudanças de função e atividades;

VII. Implementar revisões periódicas, ao menos anualmente, dos usuários e acessos concedidos aos ambientes de sua propriedade e responsabilidade.

Parágrafo único: Exceções para liberação de acesso serão avaliadas e liberadas somente com autorização do superior imediato, informando o período e com justifica plausível.

Art. 24. Os colaboradores do setor de Infraestrutura de TI possuem permissão de administrador e acesso autorizado em todos os ativos de TI gerenciados pela CrediSIS Central, bem como, desktops e notebooks.

Art. 25. Os colaboradores dos setores de Desenvolvimento e Operações terão acesso permitido aos servidores dos quais possuem aplicações e serviços (internos ou em nuvem) sob sua gestão.

Art. 26. Os colaboradores de Banco de Dados terão acesso restrito aos servidores onde os serviços de banco de dados estão em execução.

Parágrafo único. Os acessos dos ambientes de banco de dados devem respeitar as diretrizes descritas na Política de Banco de Dados.

Art. 27. Toda cooperativa que possui uma equipe de TI local ou terceirizada, assessorada pela CrediSIS Central, terá acessos privilegiados na infraestrutura local da cooperativa, devendo obrigatoriamente cumprir com os itens desta política, termo de responsabilidade e as normas estipuladas pela CrediSIS Central.

Parágrafo único. O termo de responsabilidade citado no Art. 27 consta Anexo à Circular CrediSIS nº 045/2019.

Art. 28. Os acessos aos serviços de gestão e controle tecnológicos como: Active Directory, Servidores de aplicações e serviços, Plataforma colaborativa de e-mail, ambientes de virtualização, *Cloud*, Malha e Ferramentas de segurança (firewall e

outras soluções) e demais ferramentas desse escopo, são de administração exclusiva da CrediSIS Central.

Art. 29. Os colaboradores não devem efetuar tentativas de obter acesso às informações e/ou utilizar credenciais que não lhe são permitidas, devendo solicitar acesso à informação ao respectivo proprietário.

Art. 30. A elaboração das normas e procedimentos de acesso deverá levar em consideração os riscos do acesso e alteração não autorizados, divulgação indevida e indisponibilidade dos dados, que tem por consequência às fraudes, problemas legais, perdas de negócios, danos à imagem e dificuldade na recuperação da informação.

7. ACESSO REMOTO

Art. 31. O acesso remoto só deverá ocorrer mediante autorização do usuário da estação de trabalho, com acesso supervisionado, com exceção de manutenções agendadas fora do horário de expediente.

Art. 32. O acesso remoto de terceiros nos ativos de TI na CrediSIS Central, só deverá ocorrer mediante autorização e com acesso supervisionado.

§1º O acesso remoto deverá ser feito através de software adquirido e licenciado pela CrediSIS Central para atendimento/suporte aos colaboradores da singular.

§2º Só será permitido o acesso remoto por outro software caso o principal esteja indisponível ou a empresa prestadora de serviços não possua licenciamento, podendo utilizar outro software mediante solicitação através da ferramenta de registro de chamados para o setor de Operações da CrediSIS Central, a ser avaliado pelo setor de Segurança da Informação.

8. POLÍTICA DE SENHAS

Art. 33. As senhas são de uso pessoal e intransferível, não devem ser compartilhadas e nem anotadas em meios físicos, sendo obrigatório utilizar a ferramenta disponibilizada pela central para armazenamento de senhas.

Art. 34. As senhas devem ser alteradas sempre que existir qualquer indicação de comprometimento ou vazamento.

Art. 35. Os sistemas e plataformas utilizadas devem possuir requisitos que atendam senhas com no mínimo 8 caracteres entre letras maiúsculas, minúsculas, números e caracteres especiais.

Art. 36. As senhas de acesso a e-mail, usuário de máquina (Active Directory) e CrediSIS ERP devem ser renovadas automaticamente a cada 90 dias, não podendo ser utilizadas as últimas 3 senhas, ficando como recomendado seguir os mesmos requisitos para demais plataformas, principalmente considerando sua criticidade.

Art. 37. Após no máximo 5 tentativas errôneas a senha e usuário devem ser bloqueados, fazendo-se necessário uma solicitação para sua redefinição e desbloqueio.

9. SEGURANÇA FÍSICA

Art. 38. O acesso físico ao Data Center da CrediSIS Central deve ser restrito apenas aos colaboradores devidamente autorizados.

Parágrafo único. Caso seja necessário conceder acesso a outros colaboradores, a solicitação deve ser feita formalmente via chamado com justificativa plausível, cabendo análise por parte da gerência de Infraestrutura de TI e Diretoria.

Art. 39. Os equipamentos instalados nos Data Centers da CrediSIS Central, que atualmente operam os serviços e aplicações mais críticas para o funcionamento dos negócios, devem possuir contingência adequada que garanta a continuidade das

operações sem prejuízo ao funcionamento da CrediSIS Central e Cooperativas Filiadas ao Sistema CrediSIS.

Art. 40. As salas devem ser fechadas com uso de chaves, fechaduras eletrônicas ou biometria, restringindo o acesso apenas a pessoas autorizadas, onde na Central deve obrigatoriamente ser com fechadura eletrônica ou biometria para controle eficaz que permita registro e rastreabilidade dos acessos.

§ 1º Na impossibilidade de implementar controle de acessos eletrônicos, os registros de acesso devem ser realizados utilizando a planilha do Anexo I como modelo.

§ 2º Em caso de acessos de terceiros ou prestadores de serviços devem conter o nome da empresa, CNPJ, nome do funcionário da empresa e CPF

Art. 41. A estrutura para manter a segurança física dos equipamentos deve obedecer aos padrões de segurança gerais do sistema CrediSIS e adequar-se, no mínimo, às especificações dispostas na Política de Abertura de PA e Política de Terminais de Autoatendimento (ATM).

Art. 42. Toda manutenção a ser efetuada no Data Center ou CPD deve ser agendada e comunicada com antecedência mínima de 02 (dois) dias úteis.

§ 1º Para manutenções nas cooperativas que possuem equipe de TI Local ou Terceirizada, esta deve ser comunicada e obrigatoriamente deve informar com antecedência à equipe da CrediSIS Central, para apoiar em processos geridos pela mesma de forma centralizada.

§ 2º O setor de Infraestrutura de TI ou Operações, que normalmente acompanham e apoiam as manutenções, se notificadas sem a antecedência mínima poderão cancelar o acompanhamento da manutenção por conta do impacto que o não planejamento ou comunicação antecipada podem ocasionar.

Art. 43. Demais detalhes sobre rede elétrica, cabeamentos, *nobreaks*, equipamentos de rede, climatização das salas de CPD e Data Center, extintores ou sistemas de combate a incêndio, dentre outros, devem ser consultados na Política de Abertura de PA.

Art. 44. Para mais detalhes, consultar a Política de Segurança Física do Sistema CrediSIS.

10. DA SEGURANÇA DA REDE CORPORATIVA

Art. 45. Devem possuir ferramentas e processos que registrem e monitorem atividades, incluindo serviços de redes como autenticação, encriptação e controles de conexões.

Art. 46. Devem existir equipamentos de *firewall* de nova geração capazes de, além de controlar o tráfego de entrada e saída, possuir também inspeção profunda do tráfego de rede *(deep inspection*), detecção e prevenção a intrusão (IDS/IPS), filtro de conteúdo WEB, filtro de DNS, VPN, SD-WAN, permitir controle centralizado por meio das ferramentas utilizadas pela CrediSIS Central para gerência, orquestração e coleta de logs e integração com Active Directory.

Art. 47. Os equipamentos devem estar devidamente licenciados para permitir suporte e garantia do fabricante e o funcionamento de todos os recursos necessários.

Parágrafo único. Não é permitido a utilização de firewalls que estejam em desacordo com esta Política

Art. 48. Para aprimoramento dos recursos de segurança e segregação da rede corporativa, recomenda-se a utilização de switches gerenciáveis que permitam a utilização de VLAN na rede da CrediSIS Central e cooperativas.

Art. 49. Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS capaz de detectar e responder a uma

tentativa externa, mal-intencionada e suficientemente grave que possa ameaçar os recursos do sistema de informações.

Parágrafo único. O setor de Segurança da Informação deve avaliar os eventos de IDS/IPS e intervir, quando necessário, otimizando os processos de bloqueio.

11. SEGURANÇA DE REDES WI-FI

Art. 50. Toda rede WIFI possui acesso à internet fornecido por um provedor, o qual é contratado pela CrediSIS Central ou Cooperativa, portanto o seu uso deve ser minimamente controlado, visto que a responsabilidade por essa internet é exclusivamente de quem a contratou, sendo essencial possuir controles de registros, logs ou acessos para fins de auditoria.

Art. 51. A rede Wi-Fi corporativa deve garantir a autenticação dos usuários por meio do Active Directory, utilizando métodos e protocolos de segurança reconhecidos, a fim de assegurar a integridade e confidencialidade das conexões.

Art. 52. Na utilização de redes Wi-Fi corporativa, é obrigatório a utilização de um switch gerenciável.

Art. 53. A rede Wi-Fi corporativa só deve ser acessada por notebooks/desktops corporativos.

Art. 54. O tráfego da rede Wi-Fi corporativa deve ser inspecionado pelo firewall gerido pela CrediSIS Central, sem a utilização de *Network Address Translation* (NAT) entre o firewall e a estação de trabalho.

Art. 55. A rede Wi-Fi de visitantes não deve ter comunicação com as redes corporativas e deve ser restrita apenas para acesso à internet.

Art. 56. Fica a critério da CrediSIS Central e de cada Cooperativa liberar o uso da rede Wi-Fi de visitante para seus colaboradores.

Parágrafo único: A rede Wi-Fi de visitantes destina-se à conexão de dispositivos móveis de colaboradores, cooperados, terceiros, entre outros.

Art. 57. Os pontos de acesso Wi-Fi utilizados para disseminação das redes corporativa e de visitantes devem suportar múltiplos SSIDs, permitindo a segregação lógica das redes.

Art. 58. É vedado o uso de redes abertas (sem exigência de autenticação), ou com senha genérica.

12. USO ACEITÁVEL DOS ATIVOS DE TI

Art. 59. Os colaboradores do Sistema CrediSIS devem fazer uso dos ativos de TI concedidos pela própria instituição com o objetivo específico de desenvolverem suas atividades profissionais, sendo expressamente proibida a utilização para fins particulares.

Art. 60. A alteração e/ou a manutenção de qualquer equipamento de propriedade da CrediSIS Central é uma atribuição específica dos profissionais de tecnologia da CrediSIS Central que, a seu exclusivo critério, poderá delegar formalmente a outro responsável.

Parágrafo único. Demais colaboradores são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos.

Art. 61. Os equipamentos da CrediSIS Central devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado.

Art. 62. O desligamento da estação de trabalho deverá ser efetuado após o colaborador encerrar a sua jornada diária.

Art. 63. O bloqueio de tela das estações de trabalho deverá ser ativado sempre que o usuário se afastar do computador que estiver utilizando.

Art. 64. Todos os dispositivos removíveis (pen drive, hd externo, micro SD e similares), serão bloqueados por meio da solução antivírus. Para a liberação, é necessário a abertura de um chamado ao setor de Operações e este será avaliado posteriormente pelo setor de Segurança da Informação.

Art. 65. A CrediSIS Central emprega uma solução de MDM dedicada exclusivamente a smartphones. Essa abordagem garante o controle preciso e a gestão remota eficiente dos dispositivos, que permita, mas não limitar-se-á:

I. Efetuar a limpeza remota de dados corporativos ou de todo o dispositivo;

II. Efetuar bloqueio remoto de dispositivo;

III. Definir aplicativos autorizados para os aparelhos.

Parágrafo único. Todas as cooperativas singulares filiadas à CrediSIS Central deverão possuir a solução de MDM instalado em seus dispositivos móveis corporativos, concordando com as regras e políticas estabelecidas, para garantir a segurança dos dispositivos, onde estas serão geridas pelo setor de Infraestrutura de TI alinhados às estratégias de negócio da CrediSIS Central.

Art. 66. Os smartphones disponibilizados para colaboradores com autorização para uso externo devem possuir termo de responsabilidade devidamente assinado pelo colaborador e gestor responsável.

Art. 67. Em casos de roubo ou furto de equipamentos, deve ser imediatamente comunicado ao gestor e registrado boletim de ocorrência em órgão competente.

13. LICENÇA DE SOFTWARES

Art. 68. Todo equipamento deverá ter o seu sistema operacional devidamente licenciado, obedecendo os termos de utilização do fabricante.

Art. 69. É terminantemente proibido a utilização de *softwares* piratas, não licenciados, que podem acarretar em riscos de segurança da informação e multas por parte dos fabricantes.

Parágrafo único. Se identificado fato que se enquadre no descrito acima, o setor de Segurança da Informação emitirá notificação para regularização. Se houver reincidência do processo, sanções (cooperativas) ou medidas disciplinares (colaborador) poderão ser aplicadas.

Art. 70. Solicitações para instalação de novos softwares nas estações de trabalho do sistema CrediSIS, dependendo de sua natureza, devem passar por uma análise de segurança cibernética para garantir que a solução é minimamente segura e não possui registros de vazamentos na internet. O mesmo deve ser levado em consideração para plugins e extensões de navegadores, respeitando sempre os princípios de segurança da informação, em especial o de confidencialidade.

14. CONSCIENTIZAÇÃO E DIVULGAÇÃO DA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTIVA

Art. 71. Esta política, deve ser amplamente divulgada no processo de admissão e integração de novos Colaboradores, tanto pelo setor de Gestão de Pessoas quanto pelos Gestores.

Art. 72. Programas de conscientização, divulgação e reciclagem do conhecimento desta política ou de seus temas devem ser estabelecidos e praticados regularmente, para garantir que todos que tenham relação com informações de responsabilidade do CrediSIS saibam as diretrizes e as responsabilidades relacionadas à sua segurança.

Art. 73. Esta Política deverá ser compartilhada com terceiros, em versão com nível de detalhamento adequado, conforme determina a Resolução n° 4.893/21.

15. DAS PRÁTICAS DE MESA LIMPA E TELA LIMPA

Art. 74. A mesa limpa deve ser estendida para outros conceitos como “tela limpa” e “lixo limpo”, reduzindo acessos não autorizados a informações durante e fora do horário normal de trabalho.

Parágrafo único: Para otimizar o processo de tela limpa, deve evitar ser armazenado documentos na área de trabalho e configurar para todas as estações de trabalho do CrediSIS o bloqueio de tela automático após, no máximo, 15 minutos de inatividade.

Art. 75. Os locais de armazenamento e arquivamento de documentos devem prover mecanismos que dificultem o acesso à informação classificada em qualquer nível mais sigiloso que público, inclusive arquivamento físico em gavetas, armários, entre outros.

Art. 76. Documentos impressos que possuem informações de qualquer classificação mais sigilosa que público, principalmente se conter dados pessoais ou sensíveis, devem ser retirados das impressoras imediatamente e armazenados de forma adequada.

Art. 77. Recomenda-se sempre que possível, ao final do dia, organizar sua área de trabalho, removendo de sua mesa, papéis impressos que possam conter informações de âmbito confidencial ou restrito apenas ao setor.

16. DO USO DE E-MAIL CORPORATIVO

Art. 78. Todos os colaboradores que necessitam de um e-mail corporativo, devem ter um endereço de e-mail corporativo nominal, no formato padrão de “nome” sequenciado de “sobrenome”.

Parágrafo único. É proibido o uso de e-mails genéricos ou de cargo/função a serem utilizados por colaboradores, para garantir a devida rastreabilidade e auditoria de todo o processo de uso da solução.

Art. 79. O uso de e-mail corporativo deve ser restrito apenas para assuntos pertinentes ao sistema CrediSIS e seus relacionamentos como ferramenta de formalização e comunicação, sendo expressamente proibido sua utilização para tratar assuntos de cunho pessoal que não fazem parte dos negócios do sistema CrediSIS.

Art. 80. O uso indevido do e-mail corporativo assim como o uso de e-mail pessoal para âmbito corporativo, quando comprovado, acarretará em medidas disciplinares para o colaborador.

Art. 81. O compartilhamento de informações pelo *e-mail* corporativo ou ferramentas correlatas como chat, serviço de armazenamento (*Drive*), entre outros, devem respeitar as diretrizes desta Política e da Política de Classificação da Informação.

17. USO DE DISPOSITIVOS MÓVEIS PESSOAIS

Art. 82. Para colaboradores contratados em regime de CLT é proibido o uso de dispositivos pessoais para execução de suas rotinas e atividades.

Art. 83. Profissionais contratados em regime de Pessoa Jurídica que fazem uso de dispositivos pessoais para execução de suas rotinas e atividades, devem utilizar VPN para conexão aos recursos do CrediSIS.

Art. 84. Os profissionais contratados sob o regime de Pessoa Jurídica devem utilizar um VDI exclusivo e individual para acessar o ambiente e os recursos da CrediSIS Central, sendo estritamente proibido o compartilhamento de acesso.

18. USO DE APLICATIVOS DE COMUNICAÇÃO

Art. 85. O uso de aplicativos de comunicação ou mensagens instantâneas populares, mas não corporativos e sem gerenciamento centralizado, deve ser proibido, principalmente nas estações de trabalho.

Art. 86. A utilização fora das estações de trabalho deve ser feita única e exclusivamente em aparelho corporativo, adquirido pela instituição e cedido

adequadamente mediante termo de responsabilidade, com solução de MDM conforme especificado no Art. 65, devidamente configurada para minimamente garantir que possui acesso e controle do dispositivo.

Art. 87. A opção pela utilização de tais aplicativos nas estações de trabalho deve ser precedida preferencialmente junto com a aquisição de ferramentas que garantam a capacidade de gerar a rastreabilidade, auditoria e histórico de conversas das comunicações, garantindo monitoração e controle adequado do processo, além de ser aplicado bloqueios evitando tráfego de arquivos que possam acarretar na execução indevida de códigos maliciosos.

19. REGISTROS DE AUDITORIA

Art. 88. A CrediSIS Central deverá registrar eventos em logs de auditoria, no mínimo, mas não limitando-se aos bancos de dados de produção, ERP CrediSIS, servidores de arquivos, ambientes virtuais, Active Directory, ambientes de *backup*, ambientes em *cloud*, dispositivos de rede como *firewall* e roteadores pertencentes ao CrediSIS.

Art. 89. Os registros devem conter ao menos informações de identificação de usuário (quando aplicável), data, hora e as ações do evento.

Art. 90. As trilhas de auditoria (*logs*) dos bancos de dados de Produção e do ERP CrediSIS, deverão ser mantidas por um período mínimo de 01 ano e demais logs de eventos dos dispositivos citados no Art. 108º por pelo menos 30 dias, ambos fora da infraestrutura principal, em local centralizado e protegido contra acessos não autorizados.

Art. 91. Os dispositivos de terceiros conectados à rede do CrediSIS, (desconsiderando as estações de trabalho), devem armazenar seus registros de log de acordo com o Art. 89, respeitando o prazo estipulado pelo Art. 90.

Art. 92. As falhas nos registros das trilhas de auditoria (*logs*) devem ser registradas, analisadas e devem ser tomadas providências para correção imediata.

20. CONTROLES CRIPTOGRÁFICOS

Art. 93. Deve ser feito uma avaliação considerando os critérios definidos na Política de Classificação da Informação, para definir o nível de proteção ou criptografia das informações.

Art. 94. Todos os notebooks corporativos configurados para uso na rede do CrediSIS devem possuir criptografia de disco habilitada.

Art. 95. Deve ser definido um ciclo de vida de certificados e chaves criptográficas, para o devido monitoramento e controle.

Art. 96. Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves.

21. GESTÃO DE VULNERABILIDADES

Art. 97. A gestão de vulnerabilidades possui uma política específica que estabelece diretrizes para identificação, análise, tratamento e monitoramento contínuo de vulnerabilidades nos ativos de TI mais críticos do ambiente CrediSIS, suas cooperativas filiadas, bem como suas aplicações e sites Web. Ela visa garantir a segurança e integridade do ambiente de TI, bem como o tratamento eficaz das vulnerabilidades para mitigar riscos e proteger os ativos da instituição.

Art. 98. O processo inclui a realização periódica de varreduras na rede para identificar vulnerabilidades, seguida pela classificação e priorização com base em critérios como gravidade, impacto no negócio e exposição do ativo de TI.

Art. 99. As vulnerabilidades identificadas são formalmente registradas e comunicadas, sendo os responsáveis informados com detalhes sobre as vulnerabilidades e as recomendações para mitigação.

Art. 100. As correções são testadas em ambiente controlado, sempre que possível, sendo adotados controles alternativos caso a correção não seja viável.

Art. 101. As vulnerabilidades sem correção ou patch são registradas em uma carta de aceitação de risco, contendo contexto, classificação de risco, possíveis impactos, ações mitigatórias (se houver) e justificativa para aceitação do risco.

Art. 102. Para maiores detalhes, consultar a Política Gestão de Vulnerabilidades.

22. PROTEÇÃO CONTRA *MALWARES*

Art. 103. A proteção contra *malwares* possui uma política específica que estabelece diretrizes para garantir a segurança dos ativos de TI da instituição, onde inclui a instalação e atualização regular de sistemas de antivírus em notebooks, desktops, servidores e estações de trabalho virtualizadas definindo ainda que procedimentos de detecção, prevenção e combate a *malware* devem ser estabelecidos, e qualquer problema deve ser relatado às equipes técnicas para as devidas tratativas, possuindo um monitoramento constante com relatórios periódicos para verificar a proteção dos ativos de TI onde, em casos excepcionais, uma análise de risco pode ser realizada para determinar a necessidade de medidas alternativas de segurança.

Art. 104. Para maiores detalhes, consultar a Política de Proteção Contra Malware.

23. DESENVOLVIMENTO SEGURO

Art. 105. Nas diferentes fases do desenvolvimento de sistemas como Projeto, Desenvolvimento, Testes, Aprovação e Implementação e Manutenção, devem conter verificações de Segurança da Informação.

Art. 106. Aplicar medidas e controles de segurança no repositório de código-fonte e configuração como restrição de acesso e controle de versão, levando em conta as ferramentas e linguagem utilizadas.

Art. 107. Implementar rotinas de testes durante o ciclo de desenvolvimento, levando em conta não somente as funcionalidades e desempenho, mas considerar requisitos de segurança.

Art. 108. Devem haver controles que garantam a segurança de informações sensíveis ao longo de todo o processo de desenvolvimento.

Art. 109. Sistemas da informação desenvolvidos ou adquiridos devem contar com atributos e funcionalidades de segurança que protejam adequadamente as informações, conforme definido na Política de Desenvolvimento Seguro.

24. DA GESTÃO DE FORNECEDORES

Art. 110. O processo de gestão de fornecedores seguirá os requisitos e diretrizes definidas na Política de Compras e Contratação de Serviços da CrediSIS Central.

Art. 111. Antes de qualquer aprovação de contratação de solução, ferramenta ou serviço de processamento, armazenamento de dados e de computação em nuvem, uma análise de fornecedor deve ser feita pelos setores de Segurança da Informação e Riscos Não-Financeiros para que algumas informações e requisitos sejam definidos e também seja feita uma análise de classificação de relevância deste fornecedor, avaliando a necessidade de notificação junto ao órgão regulador.

Parágrafo único. Se na análise do setor de Segurança da Informação o fornecedor obter um risco alto, automaticamente a recomendação é não avançar com a contratação, exceto se houver um compromisso do fornecedor de se adequar durante um período pré-acordado com a área contratante e em comum acordo com o setor de Segurança da Informação, e seja comunicado à diretoria, cabendo a ela levar ao conhecimento do conselho. Demais níveis de risco serão informados, com os respectivos pontos de atenção, cabendo a decisão de contratação por parte da área contratante

Art. 112. Uma classificação de relevância também será efetuada para avaliar a necessidade de notificação desta contratação junto ao órgão regulador conforme exigido na resolução 4.893 do Banco Central.

25. DO SERVIÇO DE NUVEM

Art. 113. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada ao Banco Central do Brasil.

Parágrafo único. Para esta contratação também deve ser considerada análises e classificação de relevância descritos no capítulo de gestão de fornecedores.

Art. 114. Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles *software* como serviço (SaaS) ou armazenamento de base de dados devem possuir acesso seguro através de interfaces HTTPS, bem como a autenticação segura e em ambientes segregados.

Art. 115. Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

Art. 116. A comunicação entre os serviços alocados nos Data centers físicos da CrediSIS Central com a cloud deve ser, preferencialmente, através de uma VPN, garantindo a criptografia dos dados em trânsito.

Art. 117. Assim como na infraestrutura *On Premise,* deve existir monitoramento contínuo dos serviços em nuvem, em especial aspectos de segurança.

26. DA CONTINUIDADE DE NEGÓCIOS

Art. 118. Devem ser elaborados, no tocante a continuidade de negócios, cenários de incidentes de segurança da informação, especialmente de segurança cibernética, que avaliem os procedimentos e controles aplicados, observando como diretrizes:

I. O possível impacto aos negócios;
II. A tendência do cenário de ameaças.

Parágrafo único. Deverão ser considerados como cenários de incidentes, para os testes de continuidade de negócios, as falhas citadas no Plano de Recuperação de Desastres Infraestrutura de TI, bem como os escopos previstos no Plano de Resposta a Incidentes.

27. *BACKUP*

Art. 119. Toda informação proveniente de servidores, bancos de dados e storages que estejam sob responsabilidade da área de Infraestrutura de TI, deverão ser considerados para avaliação de inclusão nos processos de backup.

Art. 120. A periodicidade dos backups pode variar, atendendo a particularidades, de acordo com o serviço ou origem da informação.

Art. 121. Os processos de backup possuem retenções diferentes, considerando os tipos de mídias e informações utilizadas.

Art. 122. Para maiores detalhes, consultar a Política de *Backup*.

28. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 123. Os colaboradores do Sistema CrediSIS devem ser capacitados minimamente para identificar eventos e incidentes de segurança e reportar desvios na operação que possam caracterizar um incidente de segurança cibernética.

Art. 124. O processo de gestão de incidentes de segurança da informação começa com a detecção. Incidentes podem ser identificados de várias maneiras e através de diversas fontes, dependendo da sua origem ou natureza.

Art. 125. Para maiores detalhes, consultar a Política de Gestão de Incidentes de Segurança da Informação.

29. PROTEÇÃO DE DADOS PESSOAIS

Art. 126. A estrutura de Proteção de Dados para o Sistema CrediSIS está organizada de maneira centralizada tanto em relação à Instituição, quanto ao organograma da CrediSIS Central, vinculado à Diretoria de Riscos e Supervisão.

Art. 127. A CrediSIS Central mantém em sua estrutura organizacional um Encarregado de Proteção de Dados, que é responsável pelas atribuições legalmente estabelecidas na LGPD e por coordenar as diretrizes e operações do tema.

Art. 128. A proteção de dados é parte integrante da responsabilidade dos colaboradores e terceiros CrediSIS e, portanto, deve ser tratada conforme diretrizes da Política de Proteção de Dados Pessoais.

30. DAS EXCEÇÕES

Art. 129. Ocorrências relacionadas ao funcionamento da Política, não contempladas neste documento, serão levadas para conhecimento da Diretoria que avaliará a necessidade de encaminhar para deliberação do Conselho de Administração da Instituição.

31. DAS PENALIDADES

Art. 130. O colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções e medidas disciplinares.

32. REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 131. Esta Política deverá ser revista e atualizada, ao menos anualmente, com vistas a se manter em sintonia com as regras de negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

33. DAS REFERÊNCIAS

Art. 132. Para um entendimento mais abrangente sobre a Política de Segurança da Informação, deve-se consultar os documentos abaixo referenciados:

I. **ABNT NBR ISO/IEC 27001:2022**: Segurança da Informação, Cibersegurança e Proteção de Privacidade;

II. **ABNT NBR ISO/IEC 27002:2022**: Segurança da Informação, Cibersegurança e Proteção de Privacidade - Controles de Segurança da Informação;

III. NIST 800-30;

IV. Resolução CMN nº 4893/21;

V. **CrediSIS:** Política gestão de Incidentes de Segurança da Informação;

VI. **CrediSIS:** Plano de Resposta a Incidentes de Segurança da Informação;

VII. **CrediSIS:** Plano de Recuperação de Desastres Infraestrutura de TI;

VIII. **CrediSIS:** Política Gestão de Vulnerabilidade;

IX. **CrediSIS:** Política Gestão de Ativos de TI;

X. **CrediSIS:** Política Proteção contra Malware;

XI. **CrediSIS:** Política de Backup;

XII. **CrediSIS:** Política Desenvolvimento Seguro;

XIII. **CrediSIS:** Política de Classificação da Informação;

XIV. **CrediSIS:** Política de Recrutamento e Seleção da Credisis;

XV. **CrediSIS:** Política de Banco de Dados;

XVI. **CrediSIS:** Política Abertura de PA;

XVII. **CrediSIS:** Política Terminais de Autoatendimento (ATM);

XVIII. **CrediSIS:** Política de Teletrabalho do Sistema Credisis;

XIX. **CrediSIS:** Política de Compras e Contratação de Serviços da Credisis Central;

XX. **CrediSIS:** Política de Gestão, Retenção e Descarte de Dados e Documentos.

34. DAS DISPOSIÇÕES FINAIS

Art. 133. Esta Política foi aprovada na Reunião Extraordinária do Conselho de Administração da CrediSIS - Central de Cooperativas de Crédito, realizada em 03 de maio de 2019 com o nome de “Política de Segurança Cibernética e da Informação” e a nova nomenclatura de “Política de Segurança da Informação” foi ajustada na primeira revisão realizada na Reunião Ordinária Conselho de Administração do dia 29 de abril de 2021, posteriormente, em segunda revisão, foram realizadas atualizações na Reunião Ordinária do Conselho de Administração de 26 de janeiro de 2022, a terceira revisão foi aprovada em Reunião Extraordinária do Conselho de Administração de 26 de outubro de 2022 e, a quarta revisão, aprovada na Reunião Extraordinária do Conselho de Administração, realizada em 24 de abril de 2024.

35. ANEXOS

- **Anexo I - Controle de acessos CPD/Data Center:** https://drive.google.com/file/d/1gp6YMxI2ervjbq8uCVDWcSRmKVSQsC4z/view?usp=sharing