POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA CACTVS

1. OBJETIVO

A Política de Segurança da Informação e Cibe segurança, tem como objetivo estabelecer os princípios, diretrizes e atribuições que norteiam a definição de procedimentos que visam proteger sistemas, infraestrutura de tecnologia, ativos de informação, bem como assegurar a confidencialidade, a integralidade e a disponibilidade dos dados e dos sistemas de informação utilizados.

A presente política se aplica ao Grupo Cactvs, portanto sempre que citado “Cactvs” leia-se todas as empresas do Grupo Cactvs, quais sejam: Cactvs Instituição de Pagamento S.A, Cactvs Corretora de Seguros S.A, Cactvs Marketplace de Alimentação e Refeição Ltda.

2. DEFINIÇÕES

Segurança da Informação: Desenvolvimento integrado das ações para a gestão inteligente de proteção orientada a recursos humanos, ativos físicos e à infraestrutura tecnológica da informação.

Cibe segurança: Conjunto de processos e tecnologias que visam proteger sistemas, ativos de informação, rede e dados de eventuais cibernéticos, intrusão ilícita e vazamento de dados sigilosos.

Usuários: Quem irá se utilizar de informações para empreender atividades pertinentes ao Grupo Cactvs. Para esta Política, consideram-se usuários os profissionais celetistas, diretores, menores aprendizes, estagiários e terceiros que acessam

qualquer tipo de informação para execução de atividades profissionais no Grupo Cactvs.

3. INTRODUÇÃO

A informação é um dos principais bens da instituição. Assim, o Grupo Cactvs define a estratégia de segurança da Informação e Cibe Segurança para proteger a integridade, disponibilidade e confidencialidade da informação.

Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital do Grupo Cactvs.

Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada, em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde a coleta até o descarte.

4. DIRETRIZES

Todas as políticas de segurança da informação devem estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.

As políticas de segurança da informação irão ser revisadas com periodicidade anual pelo Grupo Cactvs com aplicação no Brasil e no exterior.

A inclusão de diretrizes ou exceções por requisito regulatório e a publicação nas unidades do exterior, serão identificadas pelo responsável por segurança da informação do GRUPO CACTVS, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para o Departamento de Compliance para revisão e à aprovação pela Diretoria.

A adesão à essa Política e eventuais desvios, são reportados periodicamente pela Diretoria ao Departamento de Compliance, à Auditoria Interna e de demais comitês de risco.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente.

As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

5. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações do Grupo Cactvs, clientes, e público em geral está fundamentado nos seguintes princípios:

• **Confidencialidade:** garantir que o acesso à informação seja obtido somente por pessoas autorizadas;

• **Disponibilidade:** garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;

• **Integridade:** garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

6. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, o Grupo Cactvs adota os seguintes processos:

a) Gestão de Ativos

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos

(p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário e serem protegidos contra acessos indevidos. A proteção pode ser, física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou hardening, patch management, autenticação e autorização).

Os ativos do Grupo Cactvs, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, devendo ser identificados, inventariados e protegidos de acesso indevido. Devendo possuir documentação e rotinas de manutenção atualizados promovendo o uso adequado e prevenindo exposição indevida das informações.

b) Classificação e Segurança da Informação

As informações devem ser classificadas de acordo com a confidencialidade, conforme Critérios para Classificação e Gestão da Informação para o Brasil, definidos em política interna e Diretrizes de Segurança da Informação.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

Prevendo assim as melhores práticas para governança de Segurança no que diz respeito às políticas, processos, regulações, auditorias e demais controles

c) Gestão de Acessos

As concessões, revogações, transferência, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos do Grupo Cactvs.

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

d) Segurança Ofensiva

Entende-se por Segurança Ofensiva a forma de detectar vulnerabilidades e se precaver de ataques cibernéticos de forma proativa, por meio da aplicação de técnicas e ferramentas.

e) Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos do Grupo Cactvs para que sejam recomendadas as proteções adequadas.

Princípios de plano de Gestão de Vulnerabilidade:

- Inventariar os ativos de tecnologia da informação;
- Verificar e avaliar a vulnerabilidade nos Ativos de TI
- Avaliar o Risco Potencial;
- Definir a Remediação;
- Verificar Efetividade de Remediação;
- Validar a Solução final ou acompanhar o seu plano de ação

No que tange aos Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura do Grupo Cactvs, parceiros ou prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

e) Gestão de Riscos em Prestadores de Serviços

O prestador de serviços passará por avaliação de risco, que pode incluir a validação in loco dos controles de SI, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços.

Os prestadores de serviços devem informar os incidentes relevantes, relacionados às informações do Grupo Cactvs armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

f) Tratamento de Incidentes de Segurança da Informação e Cyber Segurança

A área de Cyber Segurança monitora a segurança do ambiente tecnológico do Grupo Cactvs, analisando os eventos e alertas para identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pelo Grupo Cactvs. Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro.

Incidentes classificados como relevantes devem ser comunicados ao Regulador.
Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação etc.

Informações sobre incidentes que possam impactar outras instituições financeiras e de Pagamento no Brasil, devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares.

A área de T.I. elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Departamento de Compliance e a Diretoria, conforme determinações legais e regulamentares.

Visando aprimorar a capacidade de resposta a incidentes, o Grupo Cactvs realiza testes de continuidade de negócios simulando cenários de incidentes críticos de Cyber Security, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e na mitigação dos riscos relacionados à segurança da informação.

g) Conscientização em Segurança da Informação e Cyber Segurança

O Grupo Cactvs promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação.

Periodicamente, serão disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, telemídias ou redes sociais aos colaboradores e clientes.

h) Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de segurança da informação**.**

i) Segurança Física do Ambiente

O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes.

j) Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas deve garantir a aderência aos documentos Diretrizes de Segurança da Informação e boas práticas de segurança da instituição.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

k) Gravação de Logs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

Essas informações devem ser protegidas contra modificações e acessos não autorizados.

l) Programa de Cyber Segurança

O Programa de Cyber Segurança do Grupo Cactvs é norteado pelos seguintes fatores:

• Regulamentações vigentes;
• Melhores práticas;
• Cenários mundiais;
• Análises de risco da própria instituição.

Conforme sua criticidade, as ações do programa dividem-se em:

• **Críticas:** Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;

• **Sustentação:** Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;

• **Estruturantes:** Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o banco para o futuro.

m) Proteção de perímetro

Para proteção da infraestrutura do Grupo Cactvs contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de DDoS, Spam, Phishing, APT/Malware, invasão de dispositivos de rede e servidores, ataques a aplicação e scan externos.

Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares ou não homologados.

n) Propriedade Intelectual

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Pertencem exclusivamente ao Grupo Cactvs todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou realizados pelo colaborador ao Grupo Cactvs, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho ou contrato de estágio do colaborador. Quaisquer informações e conteúdos cuja propriedade intelectual pertença ao Grupo Cactvs, ou tenham sido por ele disponibilizado, inclusive informações e conteúdo que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da instituição não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa do Grupo Cactvs.

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual do Grupo Cactvs.

o) Declaração de Responsabilidade

Periodicamente os colaboradores do Grupo Cactvs devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com o Grupo Cactvs devem possuir cláusula que assegure a confidencialidade das informações.

7. DEMANDAS E PROJETOS:

As demandas e projetos de negócio, serviços de retaguarda ou tecnologia devem estar em conformidade com as diretrizes, processos e arquitetura corporativa de segurança da informação. As demandas e projetos devem ser submetidos aos checklists de Segurança da Informação aplicados pela área de Governança de TI do Grupo Cactvs, garantindo a sua aderência às melhores práticas e normativos de segurança.

8. SEGURANÇA DEFENSIVA

Entende-se como Segurança Defensiva a estratégia de defesa, que possui o objetivo de prevenção, identificação e resposta de possíveis incidentes de Segurança.

Os controles de Segurança adotados referente a criptografia, rastreabilidade de operações transacionais, segmentação de redes e manutenção de cópias de segurança são detalhados nos normativos NP 08.003 Norma de Controle de Acesso e Autenticação e NP 08.004 Norma de Uso de Recursos de TI.

9. PAPÉIS E RESPONSABILIDADES

As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionadas pela Diretoria de T.I. e Segurança Corporativa.

- **Auditoria Interna**

Os papéis e responsabilidades da Auditoria Interna estão descritos na Política de Auditoria Interna e Externa.

- **Controles Internos**

Os papéis e responsabilidades de Controles Internos estão descritos na Política de Gerenciamento Integrado de Risco Operacional e Política de Controles Internos.

10. SEGURANÇA CORPORATIVA

• Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;
• Proteger a informação de ameaças buscando garantir a continuidade do negócio e minimizar os riscos ao negócio;
• Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação (SGSI).
• Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com a Diretoria de T.I. e Segurança da Informação.
• Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pela Diretoria Executiva, envolvendo as áreas responsáveis.
• Estabelecer e disseminar uma cultura de segurança da informação.
• Propor o investimento para a segurança da informação.
• Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.

Diretoria de T.I. e Segurança da Informação

Aprovar a estratégia, objetivos, orçamento e ações necessárias para a mitigação dos riscos dos processos de segurança da informação e manter o parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

Auditoria Interna

Supervisionar os processos de segurança da informação.

Área de Negócio

Proteger as informações do Grupo Cactvs sob sua responsabilidade.

11. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O objetivo da gestão de incidentes de segurança da informação é documentar as ações necessárias para resposta quando da ocorrência de incidentes ou em momentos de crise, sendo que os incidentes classificados como relevantes serão objeto de registro por meio do relatório anual e de reporte tempestivo ao Banco Central do Brasil.

Adicionalmente, são disponibilizados canais de comunicação para que qualquer usuário possa reportar incidentes de Segurança da Informação de forma a possibilitar a análise e tratamento adequado do incidente.

O reporte pode ser realizado através contatar através dos canais de Serviço de Atendimento ao Cliente – SAC 0800 9540 404, e-mail: sac@cactvs.com.br, chat: (11) 91139-8261, disponíveis em nosso site: www.cactvs.com.br.

12. RELATÓRIO ANUAL

Anualmente, será elaborado relatório de Incidentes de Segurança da Informação abordando os seguintes aspectos:

▪ A efetividade da implementação das ações para adequar a estrutura organizacional e operacional do Grupo Cactvs aos princípios e às diretrizes da presente política;

▪ O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

▪ Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

▪ Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

Os relatórios estarão à disposição do Banco Central do Brasil pelo prazo de cinco anos, podendo ele fazer uso das informações a qualquer momento.

13. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE OS INCIDENTES RELEVANTES

O Grupo Cactvs compromete-se com o compartilhamento de informações sobre incidentes relevantes com as demais instituições do Mercado financeiro como forma de contribuir com o mapeamento de vulnerabilidades e ameaças envolvendo a segurança cibernética, bem como desenvolver mecanismos para sua mitigação.

14. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Visa garantir que existam planos de continuidade de negócios e recuperação de desastres que contemplem alocação de profissionais, os principais processos e ativos de tecnologia e negócio do Grupo Cactvs.

15. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem é realizada através de processos que contemplam:

▪ A adoção de práticas de governança proporcionais a relevância do serviço a ser contratado;
▪ A avaliação da capacidade do fornecedor em assegurar o cumprimento da legislação vigente, o acesso da instituição aos dados e informações a serem processados ou armazenados pelo prestador de serviço, a confidencialidade, a integridade a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço;
▪ Identificar o local de armazenamento de dados e suas especificidades para aderência regulatória;
▪ Controles de acesso voltados a proteção de dados;
▪ Os critérios de decisão quanto terceirização de serviços relevantes.

Todos os contratos com empresas que armazenam dados em nuvem contemplam cláusulas que asseguram o armazenamento e processamento seguro, seu local exato de armazenamento, bem como a disponibilização dos dados para o Grupo Cactvs quando da necessidade de auditoria pelo Banco Central.

16. TERMO DE RESPONSABILIDADE

É exigido um termo de responsabilidade e ciência em que os Colaboradores e Fornecedores se comprometem a agir de acordo com os padrões de confidencialidade e disponibilidade dos dados do Grupo Cactvs. Este termo é assinado no ato da contratação.

17. SANÇÕES DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas nas políticas internas e na legislação vigente onde as empresas estiverem localizadas.

18. DOCUMENTOS RELACIONADOS

Esta Política Segurança da Informação e Cybersegurança é complementada por procedimentos específicos de Segurança da Informação em conformidade com os aspectos legais e regulamentares e aprovadas pela diretoria do Grupo Cactvs.

Regulamentações:

Resolução 4.658 do Banco Central
Circular 3.909 do Banco Central
Resolução 4.752 do Banco Central

19. DISPOSIÇÕES FINAIS

O Grupo Cactvs se reserva o direito de monitorar, inspecionar ou auditar o acesso e o uso de aplicativos e informações de sua propriedade ou sob sua guarda com ou sem o consentimento, presença ou conhecimento dos Usuários, mas respeitando aspectos legais.

Nenhum software utilizado pelo Grupo Cactvs para controle e proteção de suas informações pode ser alterado ou desabilitado pelos Usuários.

Esta Política será revisada com a periodicidade mínima anual ou sempre que houver alteração no processo e/ou regulatória.

20. GLOSSÁRIO

APT (*Advanced Persintent Threat*): ataques avançados persistentes.

Cyber Security: é o termo que designa o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição de informações.

Parque tecnológico: conjunto de ativos de infraestrutura e sistemas de tecnologia.

Segregação de funções: consiste na separação das atividades entre áreas e pessoas potencialmente conflitantes ou que possuem informações privilegiadas, na qual, o colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

Grupo Cactvs: inclui a Cactvs Instituição de Pagamento S.A, a Cactvs Corretora de Seguros S.A., Cactvs Marketplace de Alimentação e Refeição LTDA.