## 1 OBJETIVO

Esta Política de Segurança da Informação estabelece o direcionamento e o compromisso da Alta Direção, através de Diretrizes, Princípios e Responsabilidades voltados à proteção das informações e ativos tecnológicos da IntelCav Tecnologias e Cartões S.A, contra ameaças internas e externas, intencionais ou acidentais, que possam comprometer os negócios da organização.
Nosso compromisso é garantir a confidencialidade, integridade e disponibilidade das informações de nossos clientes, parceiros e colaboradores, bem como assegurar a conformidade com os requisitos legais e contratuais aplicáveis.

## 2 ESCOPO

Esta política se aplica a todos os Colaboradores, Terceirizados, Estagiários, Prestadores de serviço e qualquer outro agente que tenha acesso aos ativos de informação da IntelCav, independentemente da forma de vínculo.

## 3 TERMOS E DEFINIÇÕES

**Ativos:** são elementos que manipulam os processos da informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada. Figuram como ativos, além da informação, pessoas, microcomputadores e seus acessórios, notebooks, impressoras, servidores, dispositivos de armazenamento de dados, sistemas de informática, dispositivos e meios de transmissão de dados ou quaisquer outros dispositivos que venham a processar informação ou prover acesso aos recursos de tecnologia.

**Classificação da Informação:** é o processo de programar um controle para identificar a informação gerada pela ou para a empresa, assegurando o nível de proteção adequado do valor gerado ao negócio da organização.

**Comprometimento:** é qualquer situação em que a segurança, integridade, confidencialidade ou disponibilidade de dados é violada ou colocada em risco.

**Confidencialidade:** é o princípio de Segurança da Informação que define como toda informação deve ser protegida de acordo com o grau de sigilo do seu conteúdo, controlando o seu acesso e uso, disponibilizando a informação apenas aos indivíduos responsáveis por ela.

**Credencial:** é a forma como é conferido ao Usuário, acessos a áreas e sistemas nas dependências da IntelCav.

**Criptografia:** técnica pela qual a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas pelo proprietário ou seu destinatário.

**Dado Pessoal:** qualquer Informação relativa a uma pessoa física identificada ou razoavelmente identificável e registrada em qualquer formato, como: Nome; Endereço; Número da Identidade; entre outras.

**Dado Pessoal Sensível:** qualquer Dado Pessoal que, além de identificar uma pessoa natural, também defina origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso; filosófico ou político; dado referente à saúde ou à vida sexual; dado genético ou biométrico; quando vinculado a uma pessoa natural.

**Disponibilidade:** é o princípio da Segurança da Informação que define que toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos necessitarem, para o melhor desempenho de suas atribuições e/ou funções.

**Dupla Custódia:** é a forma segura de controlar o acesso ou armazenar informação através do compartilhamento de responsabilidades entre dois ou mais usuários. Sendo recomendável, quando possível, entres usuários de departamentos diferentes.

**Incidentes de Segurança da Informação:** é um evento ou série de eventos adversos, indesejados ou inesperados; confirmados ou sob suspeitas, relacionados à Segurança da Informação que têm uma probabilidade significativa de comprometer as operações do negócio e ameaçar a Segurança da Informação.

**Informação:** é um conjunto de dados gerados, processados, transportados, armazenados, manipulados e organizados que podem transmitir uma ideia, conhecimento e valor.

**Integridade:** é o princípio da Segurança da Informação que define que toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

**Login:** é o processo de identificação e autenticação de um usuário com prévio cadastramento através de identificador único, para acessar um sistema, aplicativo, site ou rede, de modo a garantir a individualização do seu proprietário.

**Segregação de Função:** é um princípio de controle interno que consiste em dividir responsabilidades e tarefas críticas entre diferentes pessoas, para reduzir o risco de erro, fraude ou abuso de poder.

**Titular de Dados:** pessoa natural a quem se referem os Dados Pessoais.

**Usuário:** é o funcionário, prestador de serviços, terceiro ou qualquer outro indivíduo, independente do vínculo, que utiliza informações da IntelCav para suas tarefas profissionais.

## 4 DIRETRIZES GERAIS

A Política de Segurança da Informação da IntelCav está alinhada com:

**Estratégia do Negócio:** a Segurança da Informação é parte integrante do Planejamento Estratégico da IntelCav, apoiando a continuidade dos serviços, a confiança dos Clientes e a reputação da Organização.

**Legislação, Regulamentações e Contratos:** a IntelCav cumpre integralmente os requisitos legais, normativos e contratuais aplicáveis, como: Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18); PCI CPP (Payment Card Industry Card Production and Provisioning); demais órgãos reguladores; se aplicável e Contratos com Clientes e Parceiros.

**Ambiente de Ameaças Atual e Futuro:** a IntelCav realiza avaliação contínua do cenário de ameaças, riscos emergentes e tendências tecnológicas, adotando medidas preventivas e reativas adequadas.

## 5 REGRAS GERAIS

O conhecimento dos requisitos de Segurança da Informação adotados pela IntelCav deve ser constantemente difundido, a conscientização dos funcionários é requisito imprescindível para o negócio da empresa.

### 5. 1 Propriedade da Informação

Toda informação gerada internamente pela IntelCav que não contenha dados de Clientes é considerada propriedade intelectual da empresa. Essa informação deve ser tratada em conformidade com o que estabelece a Diretriz de Classificação da Informação e demais normas relacionadas.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.013 - Classificação da Informação.

### 5. 2 Classificação da Informação

Todas as informações sob responsabilidade da IntelCav, independentemente do formato, meio de armazenamento ou forma de compartilhamento, devem ser devidamente classificadas de acordo com sua sensibilidade e criticidade.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.013 - Classificação da Informação.

### 5. 3 Segregação de Funções e Dupla Custódia

Práticas de segregação de funções e dupla custódia devem ser adotadas sempre que necessário, visando garantir a integridade dos ativos da organização e a segurança dos processos.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.009 – Concessão de Acessos,
- PO-GRI.009 – Concessão de Acessos,
- PO-GRI.001 – Concessão de Acessos Físicos,
- PO-GRI.014 – Concessão de Acessos Lógicos
- IT-GRI.015 – Revogação e Concessão de Acessos Lógicos.

### 5. 4 Atualização e Conscientização dos Usuários

Todos os colaboradores devem manter-se constantemente atualizados quanto às políticas, normas e diretrizes aplicáveis às suas atividades. Em caso de dúvidas sobre o tratamento adequado de informações, é obrigatória a consulta ao gestor imediato, ao Gestor de Segurança da Informação ou ao Encarregado de Proteção de Dados (DPO).

Esse item é atendido conforme estabelecido nos documentos:
- FI-GRI.042–Termos de Ciência da Política de Segurança da Informação,
- FI-GRI.071–Termo de Responsabilidade – Terceiros,
- FI-GRI.073–Termo de Responsabilidade – Funcionários,
- FI-GRI.074–Termo de Responsabilidade – Terceiros.

### 5. 5 Gestão de Mudanças em Infraestrutura e Redes

Qualquer proposta de alteração nos domínios ou infraestrutura de redes da empresa deverá ser submetida à análise e aprovação formal do Comitê de Gestão de Mudanças, conforme procedimentos estabelecidos.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.011 – Gestão de Mudança,
- IT-GRI.019 – Gestão de Mudança

### 5. 6 Responsabilidade sobre Confidencialidade e Integridade

É dever de cada usuário preservar a confidencialidade e a integridade das informações acessadas, tomando precauções quanto ao seu compartilhamento, seja ele interno ou externo. Deve-se sempre considerar a classificação da informação conforme as Diretrizes vigentes.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.013 - Classificação da Informação,
- FI-GRI.073–Termo de Responsabilidade – Funcionários,
- FI-GRI.074–Termo de Responsabilidade – Terceiros,
- FI-GRI.099 – Termo Responsabilidade – Designado de Segurança

### 5. 7 Compromissos no Ato de Contratação

Todos os colaboradores devem, no momento de sua contratação, ler, compreender e assinar o Termo de Confidencialidade e o Termo de Responsabilidade referentes à Segurança da Informação.

Esse item é atendido conforme estabelecido nos documentos:
- FI-GRI.062-Termo de confidencialidade para visitanes,
- FI-GRI.068-Termo de Confidencialidade de Segurança
- FI-GRI.073–Termo de Responsabilidade – Funcionários,
- FI-GRI.074–Termo de Responsabilidade – Terceiros,
- FI-GRI.099 – Termo Resposnabilidade – Designado de Segurança

### 5. 8 Compromissos de Terceiros

Prestadores de serviços contratados devem obrigatoriamente assinar Termos de Confidencialidade e Responsabilidade antes do início de qualquer atividade dentro da empresa.

Esse item é atendido conforme estabelecido nos documentos:
- FI-GRI.062-Termo de confidencialidade para visitantes,
- FI-GRI.068-Termo de Confidencialidade de Segurança

- FI-GRI.069 – Termo de Confidencialidade de Security Officer
- FI-GRI.070 – Termo de Confidencialidade e não Divulgação
- FI-GRI.072 – Termo de Ciência da Política de Segurança da Informação
- FI-GRI.074–Termo de Responsabilidade – Terceiros,
- FI-GRI.099 – Termo Responsabilidade – Designado de Segurança

### 5. 9 Credenciais de Acesso

As credenciais eletrônicas (login e senha) são de uso pessoal, exclusivo e intransferível. O usuário é o único responsável pelas ações realizadas com sua identificação nos sistemas da empresa.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.002 - Usuário

### 5. 10 Concessão de Acessos

Os acessos concedidos aos usuários devem ser estritamente limitados às funções necessárias para o desempenho de suas atividades profissionais, respeitando o princípio do menor privilégio.

Esse item é atendido conforme estabelecido nos documentos:
- PO-GRI.001 - Concessão de Acessos Físicos
- PO-GRI.014 - Concessão de Acessos Lógicos
- PO-GRI.016 - Revogação de Acessos Lógicos
- IT-GRI.015 - Revogação e concessão de acessos lógicos.

### 5. 11 Impressão de Documentos

Todo documento enviado à impressão deve ser retirado imediatamente da impressora, evitando o extravio ou exposição indevida de informações.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.002 - Usuário

### 5. 12 Uso da Internet

A utilização da internet deve estar alinhada às atividades profissionais.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.005 – Acesso à Internet

### 5. 13 Controle de Ativos de Terceiros

Ativos de propriedade de prestadores de serviço devem ser devidamente inventariados, identificados por número de série e controlados quanto à sua entrada e saída das dependências da empresa, conforme a Diretriz de Ativos.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.003 – Utilização de Ativos
- DO-TEI.002 - Política Tecnologia da Informação

### 5. 14 Segurança da Informação para Ativos em Nuvem

A IntelCav declara que, atualmente, não utiliza ativos hospedados em ambientes de computação em nuvem para suportar seus processos operacionais, administrativos ou de Segurança da Informação. Todas as informações e recursos tecnológicos são mantidos em infraestrutura própria e controlada internamente.

### 5. 15 Gerenciamento de Ativos

Ativos portáteis devem ser registrados, configurados e transportados de acordo com as regras definidas na Diretriz de Ativos.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.003 – Utilização de Ativos
- DO-TEI.002 - Política Tecnologia da Informação

### 5. 16 Uso de Softwares

É expressamente proibida a instalação ou uso de softwares não licenciados ou não homologados pela área de Tecnologia da Informação nos equipamentos da IntelCav.

Esse item é atendido conforme estabelecido nos documentos:
- DO-TEI.002 - Política Tecnologia da Informação

### 5. 17 Gestão de Riscos

Todos os Riscos identificados devem possuir um plano de tratamento, contendo as ações necessárias para sua mitigação, aceitação, transferência ou eliminação. Além disso, os riscos devem ser classificados conforme seu nível de criticidade, de forma a estabelecer a prioridade de tratamento, garantindo que os riscos mais relevantes à operação e à segurança da informação sejam endereçados com maior urgência.

Esse item é atendido conforme estabelecido nos documentos:
- Mapeamento de Processo de cada área
- IT-GRI-096 – Analise de Risco - BIA

### 5. 18 Incidentes de Segurança

Qualquer incidente de segurança da informação deve ser imediatamente comunicado à área de Segurança da Informação e/ou Gestão de Riscos, para que sejam tomadas as ações corretivas cabíveis.

Esse item é atendido conforme estabelecido nos documentos:
- PO-GRI.013 – Gestão de Incidentes
- IT-GRI.004 – Gestão de Incidentes

### 5. 19 Política de Senhas

As senhas devem obedecer a critérios mínimos de complexidade conforme Diretriz vigente.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.024 – Política de Senhas

### 5. 20 Descarte Seguro de Informações

A eliminação de documentos físicos ou digitais deve ser feita de forma segura e irreversível, evitando qualquer possibilidade de recuperação, total ou parcial.

Esse item é atendido conforme estabelecido nos documentos:
- FI-GRI.012 - Eliminação de dados e mídias de Armazenamento

### 5. 21 Política de Mesa e Tela Limpa

A prática de mesa e tela limpa deve ser adotada por todos os departamentos da organização e seguida por todos os colaboradores, com o intuito de evitar a exposição de documentos, mídias removíveis ou informações sensíveis a acessos não autorizados. Além disso, é essencial que estações de trabalho e consoles de servidores sejam bloqueados ou desligados sempre que não estiverem em uso, garantindo a proteção das informações e dos sistemas.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.027 - Mesa Limpa

### 5. 22 Plano de Continuidade de Negócios

Devem ser mantidos planos de continuidade operacional para os sistemas e serviços críticos que sustentam as operações da IntelCav, visando reduzir impactos e assegurar a retomada das atividades em situações de indisponibilidade de recursos de informação. Tais planos devem ser constantemente atualizados e testados, no mínimo, uma vez a cada 12 (doze) meses, de forma a garantir sua eficácia diante de cenários adversos.

Esse item é atendido conforme estabelecido nos documentos:
- IT-GRI.021 – Plano de Continuidade de Negocio SP
- IT-GRI.033 – Plano de Continuidade de Neogcio RS

### 5. 23 Privacidade

A IntelCav reafirma seu compromisso com a privacidade e proteção de dados pessoais, estando plenamente alinhada à Lei Geral de Proteção de Dados (Lei nº 13.709/18 - LGPD) e demais regulamentações aplicáveis. Com o objetivo de atender às exigências da LGPD no que se refere à formalização de boas práticas de governança e à transparência no tratamento de dados pessoais, a IntelCav estabelece diretrizes claras por meio de suas Políticas de Privacidade. Dessa forma, todo colaborador ou terceiro que utilize ativos tecnológicos fornecidos pela empresa, ao tratar dados pessoais, deve seguir não apenas as diretrizes desta Política de Segurança da Informação, mas também cumprir integralmente as disposições da LGPD, das Políticas de Privacidade da IntelCav e da

Legislação aplicável, garantindo a adoção de medidas técnicas e administrativas eficazes para proteger os dados pessoais contra acessos indevidos, perda, destruição, alterações ou qualquer outra forma de tratamento inadequado ou ilegal.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.026 – Política de Privacidade

## 5. 24 Controle de Acesso

Os controles asseguram que apenas pessoas autorizadas possam acessar informações, sistemas e recursos tecnológicos conforme suas responsabilidades funcionais. Todos os acessos devem ser concedidos com base no princípio do menor privilégio e revistos periodicamente. É obrigatória a revogação imediata de acessos quando houver alteração de função, desligamento ou encerramento de contrato.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.005 - Acesso a Internet
- DO-GRI.009 - Concessão de Acessos
- DO-GRI.025 -Acesso Remoto
- PO-GRI.001 - Concessão de Acessos Físicos
- PO-GRI.014 - Concessão de Acessos Lógicos
- PO-GRI.016 - Revogação de Acessos Lógicos
- IT-GRI.012 - Auditoria de Acessos - Active directory
- IT-GRI.015 - Revogação e concessão de acessos lógicos
- IT-GRI.040- Acesso Remoto - I.T

## 5. 25 Segurança Física e do Ambiente

A IntelCav possui medidas de Segurança Física para proteger as instalações, equipamentos e informações contra acesso, danos ou interferências não autorizadas. O controle de entrada e saída de pessoas, visitantes e prestadores de serviço é realizado por meio de registros e/ou credenciais, conforme Procedimentos.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.009 - Concessão de Acessos
- DO-GRI.018 - Visitantes
- DO-GRI.025 - Acesso Remoto
- PO-GRI.001 - Concessão de Acessos Físicos
- PO-GRI.003 – Agendamento e Recebimento de Visitantes
- PO-GRI.014 - Concessão de Acessos Lógicos
- PO-GRI.016 - Revogação de Acessos Lógicos
- IT-GRI.012 - Auditoria de Acessos - Active directory
- IT-GRI.015 - Revogação e concessão de acessos lógicos
- IT-GRI.040- Acesso Remoto - I.T

## 5. 26 Gestão de Ativos

Todos os ativos de Informação, incluindo hardware, software, documentos e mídias, são devidamente identificados, registrados e classificados de acordo com sua importância e sensibilidade. A propriedade e a responsabilidade sobre cada ativo devem ser formalmente atribuídas, garantindo que seu uso e descarte sigam as Diretrizes da IntelCav.

Esse item é atendido conforme estabelecido nos documentos:

- DO-TEI.002 - Política Tecnologia da Informação

### 5. 27 Transferência de Informações

A transferência de informações, seja por meio eletrônico, físico ou verbal, é realizada de forma segura, garantindo a confidencialidade, integridade e rastreabilidade dos dados. Sempre que possível, os canais de comunicação devem utilizar mecanismos criptográficos adequados e ser autorizados pela área de Tecnologia da Informação.

### 5. 28 Configuração e Manuseio Seguros de Dispositivos Endpoint do Usuário

Todos os dispositivos de usuário (como notebooks, desktops e smartphones corporativos) são configurados conforme padrões de segurança definidos pela IntelCav. Utilizamos antivírus, atualizações automáticas, bloqueio de tela e mecanismos de autenticação forte. O manuseio desses dispositivos fora das dependências corporativas deve seguir as mesmas práticas de segurança.

Esse item é atendido conforme estabelecido nos documentos:

- DO-GRI.003 – Utilização de Ativos
- DO-TEI.002 - Política Tecnologia da Informação

### 5. 29 Backup

A IntelCav mantém rotinas de backup periódicas de todos os sistemas e informações críticas, assegurando a restauração de dados em caso de incidentes. Os backups são armazenados de forma segura, em local protegido e com controle de acesso restrito.

Esse item é atendido conforme estabelecido nos documentos:

- DO-GRI.008 – Cópias de Backup
- PO-GRI.017 – Transporte de Backup
- IT-GRI.016 – Transporte de backup
- IT-GRI.022 – Backup e restore de chaves criptográficas
- IT-TEI.038 – Backup Veeam

### 5. 30 Criptografia e Gerenciamento de Chaves

A criptografia deve ser utilizada para proteger informações classificadas como sensíveis ou confidenciais, tanto em trânsito quanto em repouso. As chaves criptográficas são gerenciadas de forma segura, com controle de ciclo de vida, segregação de funções e registros de uso, conforme Diretrizes e Procedimentos estabelecidos.

Esse item é atendido conforme estabelecido nos documentos:

- DO-GRI.007 – Utilização de Chaves Criptográficas

### 5. 31 Gestão de Vulnerabilidades Técnicas

A IntelCav mantém um processo contínuo de identificação, avaliação e correção de vulnerabilidades técnicas em sistemas, aplicações e equipamentos. As correções são aplicadas de forma controlada, priorizando vulnerabilidades críticas e observando os prazos definidos pela Segurança da Informação.

Esse item é atendido conforme estabelecido nos documentos:
- DO-GRI.007 – Utilização de Chaves Criptográficas
- IT-GRI.011 - Descarte seguro de informações.
- IT-GRI.003 - Scans de Vulnerabilidades

### 5. 32 Desenvolvimento Seguro

Os processos de Desenvolvimento de Sistemas e aplicações seguem princípios de segurança desde a concepção até a implantação. São adotadas práticas de codificação segura, revisões de código, testes de segurança e controle de versões, assegurando que eventuais vulnerabilidades sejam identificadas e tratadas antes da liberação em ambiente produtivo.

Esse item é atendido conforme estabelecido nos documentos:
- PO-P&D.008 – Desenvolvimento Seguro
- IT-P&D.010 – Desenvolvimento Seguro

### 5. 33 Sansões

Todos os colaboradores, internos ou externos, da IntelCav devem proteger adequadamente as informações, sejam físicas ou digitais, conforme seu grau de sensibilidade e criticidade. É responsabilidade de cada indivíduo assegurar a confidencialidade, integridade e segurança dos dados utilizados, assim como dos recursos e ativos relacionados à informação. O não cumprimento das diretrizes estabelecidas nesta Política, ou o uso indevido de informações, poderá acarretar medidas disciplinares e administrativas. Dependendo da gravidade da infração, as penalidades podem incluir advertências verbais ou escritas, suspensão temporária, rescisão contratual ou desligamento definitivo. Em situações mais graves, poderão ser aplicadas também as sanções previstas na legislação vigente.

Esse item é atendido conforme estabelecido nos documentos:
- DO-DRH.002 – Código de Ética e Conduta

### 5. 34 Solicitações de exceção à esta Politica

Toda situação que inviabilize, de forma temporária ou permanente, o cumprimento das diretrizes estabelecidas nesta Política deve ser formalizado por meio de registro de Desvio ou Concessão. Esse registro deve ser submetido ao Gestor de Segurança da Informação e Gestão de Riscos da IntelCav, contendo o período de vigência da exceção e demais informações necessárias para sua devida avaliação. Durante o processo de revisão desta Política, todos os registros de exceção serão analisados, a fim de verificar sua relevância e considerar possíveis ajustes na nova versão deste documento.

### 5. 35 Conscientização e Cultura de Segurança

A disseminação contínua dos requisitos de segurança da informação é essencial para o ambiente corporativo. A conscientização dos colaboradores é considerada fator crítico de sucesso para a proteção dos ativos da IntelCav.

### 5. 36 Encerramento de Vínculo

No encerramento do vínculo com a IntelCav, o usuário deve devolver imediatamente quaisquer ativos (materiais, documentos, mídias, dispositivos e etc.) que contenham dados sensíveis, informações sigilosas, metodologias, estratégias ou conteúdo de propriedade da empresa, em qualquer formato.

Esse item é atendido conforme estabelecido nos documentos:

- PO-GRI.016 – Revogação de Acessos Lógicos
- IT-GRI.009 – Declaração de Concessão de Revogação de Chave
- IT-GRI.015 – Revogação e Concessão de acesso lógicos

### 5. 37 Auditorias de Segurança da Informação (Externa)

A IntelCav mantém um processo estruturado para a realização de auditorias independentes de Segurança da Informação, em conformidade com o controle A.5.35 da ISO/IEC 27001:2022.

Para garantir a imparcialidade, a objetividade e a eficácia da avaliação do Sistema de Gestão de Segurança da Informação (SGSI), a empresa contrata uma organização terceirizada especializada para a condução de auditorias externas independentes e testes de segurança bianuais, incluindo, quando aplicável, avaliações técnicas como testes de intrusão, revisão de configurações, análise de vulnerabilidades e verificação da conformidade dos controles implementados.

## 6 ESTRATIFICAÇÃO DA POLÍTICA

| Política de Segurança da Informação | | Indicador | Fonte | Período | Meta |
|---|---|---|---|---|---|
| *Confidencialidade das informações* | ***Proteger dados de clientes, parceiros e colaboradores contra acessos não autorizados*** | Número de incidentes de acesso não autorizado | Segurança da Informação | Mensal | 0 |
| *Integridade das informações* | ***Garantir que todas as informação e dados tratados pela organização permaneçam corretos, consistentes e confiáveis*** | Percentual de falhas ou inconsistências nos arquivos | Segurança da Informação | Mensal | 0% |
| *Disponibilidade das informações e sistemas* | ***Manter sistemas críticos operacionais e disponíveis*** | Tempo médio de indisponibilidade (HSM; Processamento; Auditoria) | Tecnologia da Informação | Mensal | 95% |
| *Conformidade legal e contratual (LGPD, Contratos)* | ***Garantir conformidade regulatória*** | Número de notificações no cumprimento aos requisitos legais | Qualidade/ RH e Contabilidade | Mensal | 0 |
| *Conscientização e treinamento* | ***Capacitar colaboradores e terceiros em SI e LGPD*** | % de colaboradores treinados | Segurança da Informação e RH | Mensal | 90% |
| *Melhoria contínua do SGI* | ***Implementar ações corretivas e preventivas para reduzir riscos*** | % de ações corretivas implementadas no prazo | Qualidade e Segurança da Informação | Mensal | 70% |

# 7 PRINCIPAIS RESPONSABILIDADES

## 7.1 Usuários

- Usar crachá visível nas dependências da empresa.
- Não compartilhar credenciais de acesso.
- Manter o ambiente de trabalho organizado.
- Zelar pelos ativos sob sua responsabilidade.
- Preservar a confidencialidade e integridade das informações.
- Respeitar direitos autorais e de propriedade intelectual.
- Conhecer e seguir a Política de Segurança da Informação.
- Apoiar na divulgação da Diretriz de Segurança da Informação.
- Reportar incidentes ou usos indevidos à Segurança da Informação.
- Participar dos treinamentos de Segurança promovidos pela empresa.

## 7.2 Área de Redes

- Garantir a confidencialidade, integridade e disponibilidade das informações.
- Manter domínios e estações atualizados com antivírus ativos.
- Sugerir treinamentos para usuários, conforme necessidade.
- Monitorar violação de lacres em equipamentos e agir conforme o caso.
- Avaliar a necessidade de contingência de ativos de informática.
- Configurar sistemas conforme a Diretriz de Segurança da Informação.

## 7.3 Recursos Humanos

- Coordenar treinamentos em segurança da informação e uso de recursos.
- Apoiar treinamentos e eventos externos da equipe de segurança.
- Garantir assinatura dos Termos de Responsabilidade na contratação.
- Apoiar a divulgação da Política de Segurança da Informação.

## 7.4 Gestores (Diretores, Gerentes, Supervisores, Coordenadores)

- Apoiar e divulgar a Diretriz de Segurança da Informação.
- Identificar necessidades de treinamentos em suas equipes.
- Garantir o cumprimento das Diretrizes de segurança.
- Analisar processos e identificar riscos potenciais.

## 7.5 Segurança da Informação

- Utilizar informações com ética e foco nos interesses da empresa.
- Garantir confidencialidade e integridade das informações.
- Manter Diretrizes e Procedimentos para prevenção de perdas ou vazamentos.
- Informar à Alta Gestão incidentes relevantes.
- Avaliar conformidade com a Diretriz de Segurança.
- Registrar atividades e auditorias realizadas.
- Auditar backups, logs e acessos (usuários, firewall, etc.).
- Promover seminários e ações de conscientização anuais.
- Revisar acessos e identificar irregularidades.

## 7.6 Administradores de Chaves Criptográficas

- Gerar, armazenar, controlar e destruir chaves com segurança.
- Informar riscos ou falhas relacionadas a chaves imediatamente.
- Documentar todas as atividades com chaves.
- Seguir e preservar os Procedimentos estabelecidos.

- Evitar qualquer divulgação não autorizada.
- Garantir que os Custódios conheçam suas responsabilidades.

### 7.7 Custódios de Chaves Criptográficas

- Manter sigilo sobre informações e atividades sob sua guarda.
- Não repassar dados a terceiros, mesmo superiores ou suplentes.
- Informar ao Comitê responsável em caso de qualquer ocorrência de Incidentes.

### 7.8 Projetos

- Considerar riscos de Segurança em todas as fases dos projetos.
- Incluir requisitos de segurança e LGPD desde o planejamento.
- Garantir testes de Segurança antes da implantação.
- Documentar projetos com controle de acesso adequado.
- Colaborar com a área de Segurança na validação de controles.

### 7.9 Desenvolvimento de Sistemas

- Adotar práticas seguras de programação.
- Incluir segurança e LGPD no Desenvolvimento desde o início.
- Separar ambientes de desenvolvimento, teste e produção.
- Proteger dados sensíveis com criptografia ou mascaramento.
- Documentar alterações e participar de auditorias técnicas.

### 7.10 Produção

- Aplicar controles físicos e lógicos conforme Políticas, Diretrizes, Procedimentos estabelecidos.
- Restringir o acesso às áreas críticas apenas a colaboradores autorizados.
- Praticar dupla custódia e segregação de funções.
- Controlar e rastrear materiais sensíveis.
- Relatar incidentes e falhas de Segurança imediatamente a área de Segurança.
- Participar dos treinamentos obrigatórios da área.

## 8 REVISÕES

A Política de Segurança da Informação deverá ser revisada ao menos uma vez por ano, ou de acordo com a necessidade.