# Política de Segurança da Informação

***Segurança da Informação***

**2022**

# ÍNDICE

## APRESENTAÇÃO

*A política de segurança da informação possibilita a implementação das melhores práticas de segurança da informação, com a finalidade em atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades e promover uma cultura educativa organizacional de segurança da informação e a proteção de dados à informação do PRAVALER, de clientes, fornecedores e de parceiros.*

## OBJETIVO

*Essa política tem como objetivo estabelecer as diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações a fim de preservar as informações quanto aos seguintes princípios:*

- *Integridade: garantia de que a informação seja mantida em seu estado original, exata e completa;*
- *Confidencialidade: garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados;*
- *Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.*

*O PRAVALER considera em suas políticas de segurança da informação o processo contínuo no qual os riscos são identificados, analisados, avaliados, tratados e reduzidos a um nível aceitável.*

## APLICABILIDADE

*A política de segurança da informação se aplica a todos os colaboradores do PRAVALER, identificados nessa política como: Pravalentes, independente do cargo ou função que ocupem.*

## DOCUMENTOS RELACIONADOS

*NBR ISO IEC 27001: 2022*
*NBR ISO IEC 27002: 2022*

# DIRETRIZES

## CONTROLE DE ACESSO

*Os dispositivos de identificação e senhas devem proteger a identidade do colaborador, de forma a evitar e prevenir que um usuário se passe por outro perante o PRAVALER ou terceiros.*
*Os dispositivos de identificação utilizados no PRAVALER, como o número de registro do colaborador, o crachá, o adesivo identificador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos devem estar associados a uma pessoa física e atrelados aos seus documentos oficiais reconhecidos pela legislação brasileira.*
*O colaborador, vinculado a tais dispositivos identificadores, é responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Os acessos são pessoais e intransferíveis, não devendo ser compartilhados com qualquer outro colaborador.*
*Deverá constar nos contratos do PRAVALER com colaboradores, cláusula de confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pelo PRAVALER.*
*O acesso à informação e às funções dos sistemas de aplicação devem ser restringidos por meio de controle de acesso.*
*Os colaboradores devem possuir nível de permissão definido de acordo com seu cargo e função, estabelecidos pelo seu gestor imediato e solicitados via chamados na ferramenta homologada.*
*Os acessos a documentos devem ser protegidos por lista de controle de acesso.*
*O PRAVALER deve manter um inventário de contas administrativas atualizadas, desativar contas não associadas ou inativas e controlar os acessos com base no mínimo privilégio.*
*Habilitar o bloqueio automático de sessões da estação de trabalho após um determinado período de inatividade.*
*Os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, quando houver demissão, afastamento médico, licenças e/ou outros tipos de suspensão do contrato de trabalho.*
*A revisão de acesso será executada a cada de 6 meses. Além de quando o profissional for promovido ou houver troca de área.*

## SENHAS DE ACESSO

*Ao realizar o primeiro acesso ao equipamento, o colaborador deverá trocar imediatamente a sua senha conforme as orientações apresentadas a seguir:*

- *As senhas de acesso devem ter, no mínimo, 9 caracteres.*

*A senha deve respeitar os 4 critérios de complexidade abaixo:*

- *Uma ou mais letras minúsculas;*
- *Pelo menos 1 letra maiúscula;*
- *Pelo menos 1 caractere numérico;*
- *Pelo menos 1 caractere especial (! @, #, $, %, %, &, ,*).*

*Como boas práticas recomendamos que evite, na composição de sua senha:*

- *Utilização de números sequenciais (12345);*
- *Utilização de letras sequenciais do teclado (qwert);*
- *Utilização de datas comemorativas e especiais;*
- *Utilização de números de telefone, endereço ou placa de veículos;*
- *Utilização de combinações contendo PRAVALER: (ex: PRAVALER@2022)*

*As senhas de acesso devem ser trocadas em intervalos máximos de 90 dias, em caso de suspeitas de comprometimento ou em qualquer momento que o colaborador desejar.*
*O colaborador será notificado 8 dias antes do prazo máximo para alteração da referida senha. Caso não troque, o acesso será bloqueado automaticamente.*
*Durante a renovação da senha, não serão aceitas as últimas 5 senhas já registradas.*
*Em caso de digitação errônea por 3 vezes consecutivas da senha de acesso, a conta será bloqueada.*
*O colaborador deve utilizar a autenticação de duplo fator (MFA) nos sistemas que possuem este recurso.*
*As senhas não devem ser expostas, compartilhadas ou reveladas a outras pessoas.*
*O colaborador não deve transcrever a senha em papel ou outros meios.*
*Em caso de descoberta da senha por terceiros, esquecimento da senha ou bloqueio de conta, a equipe de identidade e gestão de acesso deve ser acionada por meio de um processo formal.*

## CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

*A definição do grau de sensibilidade para a informação deve possibilitar:*

- *A determinação de medidas mínimas para proteger tais informações;*
- *A garantia da continuidade operacional de processamento destas informações.*

*As informações documentadas devem ser identificadas, armazenadas, transmitidas e descartadas de acordo com sua classificação.*
*Ativos tecnológicos devem ter controles aplicados para a proteção da informação que armazena, processa e manuseia, com o tratamento apropriado à sensibilidade e criticidade operacional, conforme classificada.*

*O grau de sensibilidade da informação deve ser avaliado quanto à necessidade de proteger a CID - Confidencialidade, Integridade, Disponibilidade da informação.*

*Classificação da informação quanto ao sigilo:*

| *Classificação* | ***PÚBLICA*** | ***CORPORATIVA*** | ***CONFIDENCIAL*** |
|---|---|---|---|
| *Impacto quanto à perda de Confidencialidade* | *Inexistente* | *Baixo* | *Alto* |
| *Definição* | *Pode ser divulgada a qualquer pessoa sem que haja implicações ao PRAVALER.*<br>*O conhecimento desta informação pelo público não expõe a organização a prejuízo financeiro, constrangimento, tampouco compromete a segurança dos ativos.* | *São restritas ao âmbito do PRAVALER.*<br>*Porém, se ocorrer divulgação externa das informações ou comprometimento, as consequências não são críticas.* | *Informações que o PRAVALER ou seus contratados têm a obrigação legal, regulamentar ou social de proteger.*<br>*Divulgação não autorizada teria um impacto adverso à organização.*<br>*Dado Pessoal é confidencial.*<br>*Dado de Cliente é confidencial.* |

## USO DOS ATIVOS

*O PRAVALER disponibiliza para seus colaboradores equipamentos exclusivamente para o desempenho de suas atividades profissionais, portanto, o uso inadequado desses equipamentos e para fins que não sejam os delineados pelo PRAVALER, é proibido.*
*O colaborador deve zelar pelo bom uso dos ativos a ele disponibilizados não removendo, alterando ou adicionando, qualquer tipo de componente interno de hardware ou software. Todos os ativos de hardware e software são monitorados, inventariados e auditados com objetivos de manter os padrões de segurança estabelecidos pela empresa.*
*Os equipamentos devem ser inspecionados antes da reutilização ou descarte para averiguar quanto à existência de informação sensível armazenada. Caso o equipamento inspecionado em questão contenha informação sensível, deve ser sobrescrita de forma segura antes da reutilização ou descarte.*

*O uso das mídias removíveis deve ser bloqueado e liberado conforme necessidade. É imprescindível, o uso de criptografia ao armazenar em mídia removível autorizada, informação de classificação confidencial.*
*Documentos necessários para as atividades do PRAVALER devem ser salvos no ambiente do Sharepoint ou OneDrive corporativo. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador. Não sendo de responsabilidade da área de tecnologia recuperar os dados perdidos.*
*É vedada a conexão de quaisquer equipamentos que não sejam de propriedade do PRAVALER ou homologados pelo PRAVALER, em sua rede corporativa, especialmente os notebooks, já que comprometem a segurança da informação e a qualidade dos serviços.*
*O PRAVALER tem propriedade legal sobre todos os arquivos produzidos em seus computadores, reservando-se o direito de manter, a seu critério, histórico de acessos e transações realizadas através das conexões Internet ou Intranet, quando considerado necessário, por motivos de segurança ou para fins de auditoria.*
*No caso de furto ou roubo de um ativo fornecido pelo PRAVALER, notificar imediatamente a equipe de suporte técnico e procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência.*
*Para informações adicionais como critérios para disponibilização de dispositivos, manutenção e reparos ou devolução de dispositivos, o PRAVALER disponibiliza a Política de dispositivos de trabalho, localizada na biblioteca do conhecimento.*

## MESA E TELA LIMPAS

*O colaborador deve conhecer as regras para utilização da informação de forma segura, evitando expor qualquer informação que possa prejudicar o PRAVALER, clientes e parceiros.*
*As informações críticas do negócio devem ser guardadas em lugar seguro quando não em uso, principalmente quando o local de trabalho estiver desocupado.*
*As mesas de trabalho devem estar organizadas, visando a redução do risco de acesso não autorizado, perda, furto e dano da informação em papéis e mídias de armazenamento removíveis que contenham informações do PRAVALER.*
*As áreas de trabalho dos computadores devem estar limpas de arquivos que contenham informações críticas do negócio. Estes arquivos devem estar armazenados apropriadamente no Sharepoint.*
*O computador deve ser desligado ou bloqueado quando não utilizado ou quando o colaborador se ausentar da mesa de trabalho. Como configuração padrão, o sistema operacional deve fazer o bloqueio automático de tela a partir de 5 minutos de inatividade.*

## TRANSFERÊNCIA DE INFORMAÇÕES

*Os requisitos para confidencialidade da informação estão descritos em contratos através de cláusulas de confidencialidade.*
*Os colaboradores devem ser cautelosos na utilização de quaisquer meios de comunicação (web, e-mail, telefone etc.), ficando proibida qualquer troca de informações com o meio exterior sobre informações com mais alto grau de criticidade ao negócio, sem autorização.*
*Os colaboradores devem usar navegadores e clientes de e-mail homologados e autorizados pela equipe de Tecnologia da Informação.*
*O correio eletrônico corporativo fornecido pelo PRAVALER deve ser utilizado para fins das atividades corporativas.*
*É expressamente proibido:*

- *O envio de material obsceno, ilegal ou não ético, propagandas, mensagem do tipo "corrente", discriminatórias, preconceituosas ou ofensivas no que se refere à nacionalidade, raça, orientação sexual, religião, opinião política e conteúdo que ferem os valores do PRAVALER.*
- *A inserção ou disseminação de arquivos que contenham vírus ou qualquer espécie de programas nocivos;*
- *Divulgar conteúdo que viole quaisquer direitos autorais, patentes, marcas registradas, marcas de serviço, nomes comerciais, segredos comerciais ou outros direitos de propriedade intelectual de terceiros;*
- *Forjar quaisquer das informações do cabeçalho do remetente.*

## TRABALHO REMOTO

*O trabalho remoto à rede do PRAVALER somente é permitido por meio do acesso via VPN – Virtual Private Network.*
*O trabalho remoto é parte da estratégia da Diretoria de Tecnologia do PRAVALER.*
*Os acessos são realizados em sistema de Plataforma como Serviço.*
*Acessos a documentos, correio eletrônico, sistemas são realizados através de credencial única utilizando Múltiplos fatores de autenticação.*
*O trabalho remoto será feito de forma individual, sendo os colaboradores responsáveis por seus acessos, bem como, por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os colaboradores devem adotar medidas de cautela, para que terceiros não tenham acesso, sem autorização, ao ambiente tecnológico do PRAVALER.*
*Os equipamentos fornecidos pelo PRAVALER devem ser utilizados no trabalho remoto exclusivamente para as atividades de trabalho.*

## USO E INSTALAÇÃO DE SOFTWARE

*O uso de software pirata pode acarretar prejuízos para o PRAVALER.*

*É proibida a instalação de software, sem que estejam devidamente identificados, licenciados e homologados pela equipe de infraestrutura do PRAVALER.*
*Para fazer a solicitação de download de softwares, que passaram pelo processo de licença e homologação, o PRAVALER disponibiliza um canal no sistema Orquestra.*
*Não é permitido o download de software, programas, jogos, executáveis da Internet ou de quaisquer outros meios para os computadores do PRAVALER sem o devido processo formal, evitando assim, qualquer contaminação por vírus que pode comprometer os sistemas e informações do PRAVALER ou problemas com a legislação de direitos autorais.*

## BACKUP

*O PRAVALER adota soluções e estratégias de Backup para proteger os seus dados contra perdas. A Política de Backup e Restore objetiva estabelecer os critérios, responsabilidades, procedimentos a serem seguidos para a gestão de Cópias de Segurança e Restauração.*
*O backup das estações de trabalho será realizado apenas para as pastas área de trabalho e meus documentos diretamente no Onedrive.*
*Testes periódicos de restauração são programados e realizados com o intuito de atestar a integridade do backup, averiguar os processos de backup e estabelecer melhorias.*

## PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

*O PRAVALER possui soluções de proteção contra malware, com medidas de detecção e de prevenção. Listadas no tópico de Prevenção e Detecção de Invasão.*
*Os servidores e estações de trabalho do PRAVALER possuem sistema de identificação e prevenção instalado, ativado e atualizado sistematicamente.*
*Os colaboradores são responsáveis pela prevenção de contaminação da rede e em caso de identificação ou suspeita de vírus, deve solicitar análise pela equipe de suporte técnico por meio de abertura de chamado.*
*Os colaboradores não devem interromper a verificação periódica pelos sistemas de proteção contra malware existentes em suas estações de trabalho.*

## GESTÃO DE VULNERABILIDADES TÉCNICAS

*As vulnerabilidades técnicas são identificadas por meio de um scanner de vulnerabilidades específico para este fim e por meio de programa de testes de invasão. Listado no tópico de Prevenção e Detecção de Invasão.*
*As ações requeridas para o tratamento das vulnerabilidades técnicas são de acordo com a criticidade de cada vulnerabilidade.*

*São realizados testes e avaliações nas correções antes de serem implementadas, para assegurar a efetividade da solução.*

## PREVENÇÃO E DETECÇÃO DE INVASÃO

*O PRAVALER possui controles para identificar ações de um atacante. As tecnologias utilizadas no momento são:*

- *Antivírus EDR – Windows Defender*
- *Firewall - Fortinet*
- *Detecção e resposta extendidas – Wazuh*
- *Identificação de Vulnerabilidades – Qualys*
- *Correlação de Logs – Octupus*
- *AntiSpam – Microsoft*
- *Secure Command Center – Google*
- *Data Loss Prevention – Microsoft*
- *Controle de Acesso – Octupus & Office365*
- *Web Application Firewall - CloudFlare*

*As ações requeridas para o tratamento de um incidente de segurança são de acordo com a criticidade de cada vulnerabilidade.*
*Adicionalmente somos monitorados 24x7, tanto pelas tecnologias informadas quando pelo SOC, hoje contratado pela Clavis.*

## SEGURANÇA EM REDES

*As responsabilidades e os procedimentos para gerenciar os ativos de rede devem ser definidos a fim de conceder apenas os acessos necessários à atividade e minimizar danos causados por falha na operacionalização ou manutenção.*
*Soluções de segurança em rede devem ser implementadas de forma a manter configurações de segurança padrão para os dispositivos de rede, fazendo uso de tecnologias ou ferramentas adequadas para todos os ativos da empresa.*
*As conexões à rede do PRAVALER devem ocorrer exclusivamente por meio de acesso autenticado.*
*As redes são segregadas do ambiente de desenvolvedores, homologação e produção.*
*O acesso à rede de visitantes do PRAVALER será liberado somente para fins de acesso à internet, por meio de um processo de cadastro.*
*Os ativos de tecnologia da informação devem ser sincronizados a partir de uma origem de tempo confiável para que os registros contenham informação de data/hora consistente.*

## RELACIONAMENTO COM TERCEIROS

*Um processo formal para gestão de terceiros deve ser estabelecido, incluindo cláusulas de confidencialidade.*
*Aplica-se aos terceiros a Política de Segurança Cibernética de Terceiros, disponível na Biblioteca do Conhecimento, que será monitorada sistematicamente pelo PRAVALER.*
*Os colaboradores sob controle do terceiro com acesso aos dados pessoais do PRAVALER estão sujeitos a assinatura do termo de confidencialidade.*
*Conforme Política de Segurança Cibernética de Terceiros, estes devem utilizar medidas técnicas de segurança adequadas, como antivírus, firewall, Múltiplo Fator de Autenticação, criptografia e medidas de conscientização de segurança da informação.*
*Além de, adotar medidas de segurança para lidar com riscos, a fim de evitar destruição acidental, alteração, divulgação ou acesso não autorizado.*
*As credenciais de acesso dos terceiros devem ser seguras, sendo de sua responsabilidade qualquer incidente em decorrência de uso indevido. É proibido o compartilhamento de usuários e senhas entre os prestadores de serviço.*
*O acesso a rede interna será monitorado e auditado pelo setor de Segurança da Informação quando julgar necessário.*
*Na hipótese de suspeita de incidente de segurança, o acesso físico aos ativos deve ser imediatamente interrompido.*

## CONFORMIDADE COM REQUISITOS LEGAIS E CONTRATUAIS

*Os requisitos legais, regulamentares e contratuais aplicáveis ao PRAVALER devem ser identificados, documentados e atualizados, bem como os responsáveis diretos pela conformidade com estes requisitos.*
*Devem ser implementados controles para que requisitos legais, regulamentares e contratuais relativos aos direitos de propriedade intelectual sejam atendidos:*

- *Por meio da Política para uso e instalação de software;*
- *Por meio de conscientização para que o PRAVALER não copie livros, documentos ou outros materiais, quando não permitido pela lei de direito autoral.*

## REGISTROS E MONITORAMENTO

*O PRAVALER possui controles que visam registrar logs de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação que sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.*

*Os registros de eventos estabelecem o fundamento para os sistemas de monitoramento automatizados, os quais são capazes de gerar relatórios consolidados e alertas na segurança do sistema.*

## GESTÃO E RESPOSTAS A INCIDENTES DE SEGURANÇA DE INFORMAÇÃO

*Incidentes de segurança da Informação se caracterizam por violar o CID (Confidencialidade, Integridade e Disponibilidade).*
*O time de Segurança da Informação deve garantir a identificação, proteção, detecção, respostas e recuperação de maneira eficaz. Todo incidente de segurança da informação deve ser comunicado.*
*Deve-se manter um processo de respostas a incidentes, mapeado através de uma análise de riscos, e amplamente divulgado às partes interessadas, a fim de aplicar as medidas necessárias durante o ciclo de vida de um incidente.*
*Qualquer comunicação relacionada a segurança da informação junto às autoridades e órgãos oficiais, tais como entidades reguladoras, entidades de conformidade, governo, entre outras, devem ser previamente autorizadas pelo CTO ou responsável.*

## TREINAMENTO E CONSCIENTIZAÇÃO

*Os colaboradores, devem receber e realizar o treinamento obrigatório, com finalidades educativas e de conscientização, relacionados à Segurança da Informação.*
*A equipe de Segurança da Informação tem como responsabilidade a promoção dos planos de conscientização e treinamento. Deve assegurar que os treinamentos serão executados dentro do prazo estabelecido.*
*O Treinamento Obrigatório em Segurança da Informação será realizado nos primeiros 30 dias após a contratação do colaborador e está disponível na Universidade Pravalentes. Para melhor aproveitamento e atualização dos colaboradores este curso deverá ser realizado anualmente.*
*Campanhas para a conscientização sobre segurança da informação serão publicadas quinzenalmente no formato de "Pílulas". Ou seja, pequenos textos, com temas pertinentes a área, serão disponibilizados no canal General do Slack.*
*No mês de novembro, as campanhas de treinamento e conscientização serão intensificadas, em decorrência ao dia Internacional da Segurança da Informação, com Palestras e outras atividades em cronograma que será divulgado aos colaboradores.*
*Como exercício de simulação e avaliação de colaboradores, serão lançadas campanhas de simulação de Phishing, o planejamento e cronograma será realizado de forma sigilosa pelo departamento de Segurança da informação.*

# GESTÃO DE CONTINUIDADE DE NEGÓCIOS

*A Gestão de Continuidade de Negócios (GCN) trata da capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções dos negócios, mantendo suas operações em um nível previamente definido pelos gestores, por meio da Análise de Impacto nos Negócios (BIA).*

*O Plano de Continuidade de Negócios (PCN), é a ferramenta de gestão que reconhece ameaças potenciais à organização e analisa o impacto que elas podem ter nas operações do dia a dia. Também fornece uma maneira de mitigar essas ameaças, colocando em prática uma estrutura a qual permite as funções-chave do PRAVALER continuem.*

*O PRAVALER possui mecanismos de acionamento dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional.*

*Para os testes contínuos em sistemas, o PRAVALER utiliza o ciclo Plan-Do-Check-Act (PDCA).*

- *Plan (Planejar e estabelecer) - Esta parte do ciclo busca planejar e estabelecer uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimentos pertinentes para a melhoria da continuidade de negócios de forma a ter resultados alinhados com os objetivos e políticas gerais da organização.*

- *Do (Implementar e operar) - Esta parte do ciclo busca implementar e operar a política de continuidade de negócios, controles, processos e procedimentos. É fundamental manter um programa de exercícios controlados para os casos contemplados no Sistema de Gestão de Continuidade de Negócios, de forma a garantir tanto sua execução correta em situações reais quanto as possibilidades de avaliação de melhorias.*

- *Check (Monitorar e revisar) - Esta parte do ciclo busca monitorar e revisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, definir e autorizar ações de melhorias e correções. Isso deve ser realizado através de avaliações de desempenho realizadas após cada exercício controlado ou situação real, contemplados pelo Sistema de Gestão de Continuidade de Negócios.*

- *Act (Manter e melhorar) - Esta parte do ciclo busca manter e melhorar o Sistema de Gestão de Continuidade de Negócios tomando ações corretivas e*

*preventivas, baseadas nos resultados das avaliações de desempenho e da análise crítica da direção e reavaliando o escopo do Sistema de Gestão de Continuidade de Negócios e as políticas e objetivos de continuidade de negócios. O Sistema de Gestão de Continuidade de Negócios deve sempre se manter alinhado com essas políticas e objetivos.*

- *Solicitações de Acesso - Todas as solicitações de acesso para aplicações, infraestrutura de datacenter físico ou em nuvem, será necessário abrir uma solicitação via orquestra (atual ferramenta de chamados). Para solicitação ao edifício e ao escritório físico do PRAVALER deverá ser reservado via Deskbee (ferramenta atual). Somente após a resposta a autorização do gerente diretor ou gestor, o acesso será concedido ou negado, com resposta no mesmo canal utilizado na abertura da solicitação. Para acessos já mapeados a função, não é necessária a autorização.*

*Maiores informações sobre Gestão de Continuidade de Negócio estão nas Instruções Gerais de Continuidade de Negócio, localizado na pasta de Tecnologia, na Biblioteca do Conhecimento PRAVALER.*

## CRIPTOGRAFIA

*As informações do PRAVALER devem ser criptografadas de modo a garantir sua confidencialidade, disponibilidade e integridade. As equipes de Dev Experience e SRE e DBRE são responsáveis por gerenciar as chaves criptográficas empregadas ou que deverão ser empregadas nos sistemas de informações do PRAVALER, tais como:*

- ***Criptografia de Dados em Trânsito** – São dados enviados ou recebidos através das redes corporativas e internet. Todas as aplicações internas ou externas do PRAVALER utilizam de protocolos seguros de comunicação como HTTPS (Hyper Text Transfer Protocol Secure) com certificado TLS 1.2 (versão mínima).*
- ***Criptografia de Dados em Repouso** – São dados armazenados em Banco de Dados, HD Externos e arquivos armazenados em sistemas de nuvem por exemplo. O PRAVALER utiliza o Google Cloud, onde os dados são criptografados automaticamente e o Cloud SQL tem as certificações SSAE 16, ISO 27001 e PCI DSS, além de conformidade com a HIPAA.*
- ***Criptografia em Armazenamento** – São dados armazenados em Servidores, Notebooks, Desktops e Discos Removíveis (Ex: Todos os armazenamentos disponibilizados pelo PRAVALER devem ser protegidos com o sistema de Criptografia).*

*Toda infraestrutura tecnológica do PRAVALER em nuvem deve ser igualmente criptografada de acordo com as melhores práticas dos provedores de serviços em nuvem.*

## PROCESSO DISCIPLINAR

*É obrigatório que o colaborador cumpra esta política, caso não ocorra, será considerada uma infração.*
*O PRAVALER, por meio da Gestão de Segurança da Informação, exercerá seu poder para determinar sanções aos infratores. A infração será classificada em 3 níveis de incidentes: Leve, Médio e Grave.*
*Diante da constatação de um incidente já devidamente classificado, as seguintes sanções serão aplicadas aos colaboradores internos:*

- *Advertência Verbal: Aplicada na constatação de incidente leve. Esta advertência será comunicada diretamente ao colaborador, pelo processo 'Gestão de Pessoas';*
- *Advertência Escrita: Aplicada na constatação de incidente médio ou grave. Informado ao processo 'Gestão de Pessoas' para aplicação desta advertência conforme legislação pertinente;*
- *Suspensão: Aplicada após o recebimento de 3 advertências pelo mesmo motivo de forma consecutiva;*
- *Demissão: Aplicada na constatação de incidente grave. Informado ao processo 'Gestão de Pessoas' para aplicação desta penalidade conforme legislação pertinente.*

*A pena de demissão por justa causa será aplicada nos casos legais e após regular apreciação por meio do processo disciplinar.*
*Diante da constatação de um incidente já devidamente classificado, no caso de colaboradores terceirizados, será solicitado à empresa prestadora da respectiva mão de obra, o afastamento temporário ou definitivo do funcionário, conforme a falta cometida podendo em último caso, o PRAVALER solicitar a rescisão do contrato de prestação de serviço.*
*A aplicação destas sanções não isenta o colaborador de sofrer outras penalidades previstas em contratos, ou mesmo de sofrer processos penais por crimes de condescendência criminosa, de violação de sigilo funcional entre outros, estabelecidos no código penal.*

## REVISÕES E ATUALIZAÇÕES

*Esta política estará sob constante revisão e atualização. Para fins de conformidade com as boas práticas, estipula-se o prazo de 6 meses para revisão completa de seus tópicos.*

## PAPÉIS E RESPONSABILIDADES

| *NOME* | *RESPONSABILIDADES* |
|---|---|
| ***Colaborador*** | *É da responsabilidade de cada colaborador, o prejuízo ou dano que vier a sofrer ou causar ao PRAVALER ou a terceiros em decorrência da não obediência às diretrizes desta política.*<br>*Caso identificado, o colaborador deverá notificar a equipe de segurança da informação os incidentes, fragilidades ou ainda, suspeitas de fragilidades de segurança da informação observadas no PRAVALER.* |
| ***Diretoria de Tecnologia / Área de Plataforma & Segurança*** | *Segregar as funções administrativas e operacionais; Monitorar e auditar o ambiente tecnológico, através da implantação de sistemas de monitoramento de servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede; Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança da informação estabelecidos nesta política.* |
| ***Comitê de Segurança da Informação*** | *Tratar de questões, propor soluções, metodologias e processos específicos de segurança da informação. Neste contexto, é responsável por analisar criticamente a política de segurança da informação. O Comitê de Segurança da Informação é multidisciplinar, composto por representantes da Assessoria Jurídica, do Encarregado pela Proteção de Dados Pessoais, da Gestão de Pessoas, da Tecnologia da Informação e de, pelo menos uma das áreas: Qualidade, Processos ou Projetos.* |
| ***Alta Direção e Gerência*** | *Promover entre os colaboradores a cultura da Segurança da informação; Autorização e apoio na execução das atividades.* |

## INFORMAÇÕES DE CONTROLE

| Data | Mudança | Responsável | Versão |
|---|---|---|---|
| *Jul/2022* | *Elaboração da Política* | *Marcos Pereira* | *0.1* |
| *Jul/2022* | *Versão Revisada* | *Fernando Tralci* | *0.2* |
| *Jul/2022* | *Versão Revisada* | *Marcelo Malcher* | *0.3* |
| *Ago/2022* | *Versão Revisada* | *Anderson Xavier* | *0.3* |
| *Ago/2022* | *Revisão Jurídico* | *Larissa Barbosa* | *0.4* |
| *Ago/2022* | *Versão final – Segurança da Informação* | *Marcos Pereira* | *1.0* |
| *Set/2022* | *Atualização da Política* | *Anderson Xavier* | *2.0* |
| *Mar/2023* | *Versão Revisada* | *Fernanda Mara Cruz* | *2.1* |
| *Mar/2023* | *Versão final* | *Marcos Pereira* | *3.0* |