Conteúdo

HISTÓRICO DE ALTERAÇÕES 4
APROVAÇÕES 4
Objetivo 5
Responsabilidades 5
Responsabilidades da Diretoria 5
Responsabilidades das Gerências 5
Responsabilidades dos Colaboradores 5
Responsabilidades do Comitê Gestor da Política de Segurança 5
Comitê Gestor da Política de Segurança: 6
Conceitos 6
Acordo de Confidencialidade 6
Ambiente de Desenvolvimento 6
Ambiente de Teste 6
Ambiente de Produção 6
Aplicativo 6
Arquivo de log 6
Ativo 6
Colaborador 6
Componentes de Rede 6
Configuração 6
Gestor 6
Usuário 7
Normas Gerais 7
Documentação de Referência 8
Política de Segurança Física e de Ambiente 8
Quanto à Contratação e Gestão de Pessoas 8
Quanto à Segurança Patrimonial 9
Quanto ao Controle de Acesso Físico 9
Quanto à Gestão Ambiental 9
Política de segurança de redes e da plataforma de Contact Center 9
Quanto aos Meios Lógicos e Físicos 9
Quanto à Monitoração 10
Quanto à Documentação 10
Quanto ao Controle de Acesso Lógico 10

Política de segurança em sistemas e aplicativos. 11
Quanto aos Aplicativos.....11
Quanto aos Sistemas Operacionais, Softwares Básicos e Dados.....11
Protocolo de recebimento e leitura.....13

HISTÓRICO DE ALTERAÇÕES

Versão	Descrição	Data
1	Criação do documento	26/09/2023

APROVAÇÕES

Nome	Cargo
Rogério Barreto Rodrigues	CEO
Danilo Nader	CTO

Objetivo

A Política de Segurança da Informação tem por objetivo, orientar as ações e procedimentos que garantam a continuidade dos negócios da Proa.AI, que com suas ações pioneiras e inovadoras vem buscando e aperfeiçoando sua visão sobre a Política de Segurança interna, e a partir deste instrumento, institucionaliza a aplicação das estratégias e diretrizes de segurança da informação que será amplamente divulgada e aplicada a todos os seus funcionários, colaboradores, parceiros, fornecedores e clientes.

Responsabilidades

Responsabilidades da Diretoria

- Assegurar os recursos necessários para implementação da Política de Segurança.
- Garantir o cumprimento da Política de Segurança definida neste documento.
- Promover atualização periódica da Política de Segurança da Proa.AI.
- Aprovar as Ações de Segurança e Plano de Continuidade dos Negócios da Proa.AI.
- Aprovar os Planos de Auditoria.
- Definir e decidir quanto às medidas a serem tomadas no caso de violação da Política de Segurança, e aplicá-las quando de direito.
- Garantir a continua divulgação da Política de Segurança da Informação, através de campanhas de conscientizações, programas de capacitação e outros instrumentos de sensibilização.

Responsabilidades das Gerências

Implementar as Ações de Segurança definidas pela empresa, através de Normas e Procedimentos.

Garantir que os colaboradores sob sua supervisão compreendam e desempenhem a obrigação de proteger os ativos da Empresa.

Responsabilidades dos Colaboradores

- Cumprir a Política de Segurança da Informação da Proa.AI.
- Comunicar formalmente ao Órgão Gestor de Segurança qualquer irregularidade ou desvio de segurança.
- Cada funcionário, estagiário, terceirizado, prestador de serviços, colaborador ou cliente que possuir chaves de acesso (login - UserID) e senha, será responsável pelo seu uso correto, pelo sigilo e confidencialidade do seu código. Fica vedada a divulgação de senhas de acesso mesmo em caráter temporário. É considerada falta gravíssima a divulgação ou compartilhamento de senhas de acesso.

Responsabilidades do Comitê Gestor da Política de Segurança

- Elaborar Planos de Ação para implementação da Política de Segurança.
- Gerenciar o cumprimento da Política de Segurança.
- Revisar periodicamente a Política de Segurança, sugerindo ações que se façam necessárias.
- Elaborar Planos de Auditoria com bases nas diretrizes estabelecidas pela direção da Proa.AI.

Comitê Gestor da Política de Segurança:

Rogério Barreto Rodrigues	CEO
Danilo Nader	CTO

Conceitos

Acordo de Confidencialidade
Cláusulas ou instrumentos contratuais que contém e especifica responsabilidades, direitos e deveres dos contratados (colaboradores), tais como práticas e leis de direito autorais ou de proteção de dados, bem como a extensão da responsabilidade para fora das dependências da organização e após a rescisão do vínculo contratual.

Ambiente de Desenvolvimento
Instalações de processamento de dados cuja plataforma tecnológica destina-se ao uso exclusivo dos técnicos desenvolvedores de aplicativos.

Ambiente de Teste
Instalações de processamento de dados cuja plataforma tecnológica (segregada) destina-se exclusivamente a testes de execução dos aplicativos, compreendendo também a homologação.

Ambiente de Produção
Instalações de processamento de dados cuja plataforma tecnológica destina-se exclusivamente ao armazenamento e execução dos aplicativos.

Aplicativo
Arquivos de programas executáveis em computadores, autônomo, para realização de tarefas específicas.

Arquivo de log
Registro detalhado de todas as transações efetuadas durante a utilização de um aplicativo ou sistema operacional e necessário ao rastreamento do seu uso.

Ativo
Patrimônio composto por bens e direitos da Proa.AI.

Colaborador
Pessoa que presta serviços seja através de Contrato Individual de Trabalho, ou por vínculo a um Contrato de Prestação de Serviço.

Componentes de Rede
Equipamentos empregados nas redes (LAN/MAN/WAN...), incluindo sua infra-estrutura para comunicação, gerência e supervisão, compostos por hardware e software.

Configuração
Conjunto de características físicas e funcionais de hardware e software necessárias ao seu adequado funcionamento.

Gestor
Gerente ou Administrador.

Usuário

Pessoa autorizada a utilizar os serviços prestados pela infra-estrutura tecnológica da Proa.AI.

Normas Gerais

Todo conjunto de normas e procedimentos, além dos planos de ação para implementação das medidas de segurança serão desenvolvidos à luz destas orientações, sempre visando o estrito atendimento destas.

Todas as falhas, incidentes ou desvios de regras de segurança, sob suspeita ou devidamente identificadas, devem ser prontamente comunicadas ao gerente ou superior e ao help desk, ao qual caberá informar ao gestor de TI local, que avaliará a situação e encaminhara o problema ao "Grupo de Resposta a Incidentes" e também aos integrantes do Comitê de Ética, Privacidade e Segurança, para a tomada de medidas efetivas.

Todos os departamentos, setores e usuários de sistemas informatizados, são responsáveis por manter os procedimentos de cópia de segurança de suas estações de trabalho, que deverão ser realizados nas pastas apropriadas do servidor de arquivos centralizado. Os discos rígidos locais não possuem sistemas automáticos de backup portando, dados de clientes estão proibidos nessa área e para garantir essa norma auditoria interna e externa poderão ser aplicadas sem prévio aviso, estando os infratores sujeitos as sanções cabíveis.

Todo contrato de prestação de serviços diversos, internos ou externos, as instalações da Proa.AI que inclua previsão de manipulação de informações corporativas, deve conter cláusulas que garantam o cumprimento da Política de Segurança da Informação da Proa.AI, bem como, os controles de acesso lógico e físico devem estar vinculados ao período de vigência do contrato de serviço.

Gerentes, diretores e demais cargos executivos são diretamente responsáveis pela implementação da Política de Segurança da Informação da Proa.AI, de sua divulgação as demais unidades da organização, com base em normas e procedimentos, gerenciando o contínuo risco de segurança das informações e a garantia de aderência de todo o seu quadro de funcionários, estagiários, prestadores de serviços e fornecedores.

A Política de Segurança da Informação da Proa.AI deve ser divulgada para toda a sua comunidade usuária, que deve ser formal e expressamente comunicada sobre suas responsabilidades.

Toda informação deve ser alvo de classificação quanto à sua confidencialidade.

As pessoas contratadas devem ser treinadas e mantidas atualizadas para o pleno exercício de suas funções sobre a Política de Segurança da Informação da Proa.AI e sobre os procedimentos organizacionais.

A realização de serviços solicitados por clientes só deverá ocorrer com autorização formal, após a análise do impacto sobre a segurança das informações, nos ambientes da Proa.AI.

Todos os elementos necessários para a plena continuidade do negócio devem ter sua operacionalidade garantida.

Todo Plano de Ação decorrente da Política de Segurança da Informação da Proa.AI deve ser elaborado considerando os aspectos de economicidade.

Todos os procedimentos devem estar documentados e atualizados, de acordo com as metodologias adotadas pela Proa.AI.

A Proa.AI deverá possuir sistemática de administração, custeio e conhecimento do seu patrimônio (tangível e intangível).

A guarda, circulação e descarte de informações, nas suas diversas mídias, devem ser disciplinadas por procedimentos formalmente estabelecidos.

O ambiente operacional e tecnológico devem estar protegidos contra elementos ou softwares que possam causar danos.

A incorporação de novas tecnologias deve ocorrer garantindo a sua segurança sem comprometer os níveis de segurança já estabelecidos.

O ambiente tecnológico deve ser mantido atualizado, para atender aos níveis de segurança e qualidade requeridos pelo negócio.

Documentação de Referência

- ABNT- NBR ISO/IEC 17799:2005 (Brasil). Tecnologia da Informação. Código de prática para a gestão da segurança da informação.
- NBR 11515/2007 Critérios de segurança física, relativos ao armazenamento de dados.
- ISO/IEC GUIDE 73:2009
- NIST SP 800-61 Computer Security Incident Handling Guide, April 2021
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems, July 2008
- NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems, July 2021
- NIST SP 800-45 Guidelines on Electronic Mail Security, February 2007
- NIST SP 800-44 Guidelines on Securing Public Web Servers, September 2002
- NIST SP 800-42 Guideline on Network Security Testing, October 2003
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy, September 2009
- NIST SP 800-40 Procedures for Handling Security Patches, July 2013
- NIST SP 800-35 Guide to Information Technology Security Services, October 2003
- NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, April 2021
- NIST SP 800-30 Risk Management Guide for Information Technology Systems, September 2012

Política de Segurança Física e de Ambiente

Quanto à Contratação e Gestão de Pessoas

A contratação de pessoas deverá observar a legislação específica e considerar referências de caráter pessoal, profissional e acadêmica, com base nas diretrizes já praticadas pela Proa.AI.

Os gestores serão orientados a observar o comportamento e desempenho dos seus contratados, identificando problemas de ordem pessoal que possam comprometer a segurança da organização.

A contratação de pessoas, materiais, equipamentos e serviços devem contemplar dispositivos que garantam o pleno cumprimento do Acordo de Confidencialidade, das normas e procedimentos de segurança em vigor prevendo sanções em caso de descumprimento ou negligência na sua aplicação.

Quando do desligamento de colaboradores, devem ser revogados todos os seus dispositivos de acesso, físico e lógico, e o seu ingresso nas instalações da empresa deve obedecer aos mesmos critérios definidos para visitantes.

Medidas e procedimentos que eliminem os riscos de acessos não autorizados, perda e ou danos às informações que possam comprometer a segurança, devem ser definidos e divulgados entre os colaboradores, através de normas e instrumentos de comunicações formais.

Quanto à Segurança Patrimonial

Os perímetros de segurança das instalações físicas da Proa.AI serão definidos e protegidos de acessos não autorizados.

Os recursos de processamento de dados devem estar abrigados em instalações apropriadas, sendo o seu acesso restrito a pessoas autorizadas.

Os ambientes físicos, internos e externos, da Proa.AI serão classificados quanto ao grau de riscos e ameaças, com o intuito de disciplinar as ações de proteção.

Os projetos de novas instalações, construção e reformas devem atender às normas de segurança vigentes.

A Proa.AI deverá possuir planos de conservação e sustentabilidade de suas instalações e edificações.

A infra-estrutura e insumos necessários à continuidade do negócio devem ser protegidos e ter sua disponibilidade garantida.

Quanto ao Controle de Acesso Físico

Na alienação ou reutilização de equipamentos será assegurada a remoção de informações neles depositadas, classificadas como confidenciais e restritas.

Reparos ou recuperação de dados em disco rígido, mídias removíveis ou outros dispositivos deverão ser unicamente realizados por técnico da Proa.AI tem ambiente controlado sob a supervisão de um responsável de TI.

Quanto à Gestão Ambiental

A preservação do meio ambiente natural, no tocante à conservação das áreas internas e circunvizinhas, deve ser garantida.

O descarte de materiais tóxicos ou poluentes, utilizados na manutenção ou limpeza das instalações, deve ser formalmente disciplinado conforme as melhores práticas internacionais.

Política de segurança de redes e da plataforma de Contact Center

Quanto aos Meios Lógicos e Físicos

Todos os componentes de rede serão classificados de acordo com sua criticidade para a continuidade do negócio e preservados quanto às ameaças físicas e ambientais.

Os computadores e os serviços da rede interna e externa de comunicação de dados empregados pela Proa.AI são de responsabilidade desta e sua aplicação / utilização dependerá das necessidades departamentais, dos requerimentos dos clientes e das funções exercidas por seus

colaboradores, portanto esses recursos serão dedicados para uso exclusivo e para os propósitos de negócios da organização.

Toda a aquisição de hardware, softwares, acessórios e suprimentos relativos às tecnologias da informação, deverão seguir os padrões de segurança e de homologação definidos por TI.

Todos os recursos de informática da Proa.AI deverão ser inventariados e plenamente controlados pela área de tecnologia da informação. Dessa forma, nenhum colaborador, independentemente de seu cargo ou função, terá o direito de instalar ou desinstalar hardwares, softwares ou acessórios sem a prévia autorização formal e acompanhamento dos representantes de TI ou designados.

As informações que trafegam no ambiente de rede devem ter garantida a integridade e confidencialidade, em conformidade com sua classificação.

Os ativos de rede serão liberados para uso após efetiva homologação, realizada em ambiente distinto do de produção e devidamente documentados.

As intervenções no ambiente de rede serão permitidas mediante autorização formal e acompanhadas de supervisão.

Quanto à Monitoração

O ambiente de rede poderão ser monitorados, e as ações serão obrigatoriamente documentadas.

A responsabilidade quanto à execução e análise crítica da documentação gerada na monitoração será do CSO (o mesmo que executa por seus designados).

As informações geradas por sistemas internos, clientes, funcionários, prestadores de serviços, terceirizados, fornecedores, parceiros ou colaboradores da Proa.AI, serão consideradas sigilosas e de uso interno, sendo algumas classificadas como confidenciais a partir de especificações contratuais ou não.

A utilização pública de qualquer informação do âmbito da Proa.AI deve ser sempre previamente autorizada pela alta direção responsável pelo conteúdo em questão.

Quanto à Documentação

A documentação referente à descrição da rede, suas conexões externas, inventários e configuração de seus ativos são confidenciais, e deverão ser mantidas sempre atualizadas, preservando os registros históricos.

Quanto ao Controle de Acesso Lógico

Todos os acessos aos sistemas de informações devem ser controlados, e possuírem as devidas autorizações definidas, para as necessidades específicas de trabalho ao qual o colaborador esteja vinculado. A disponibilização de acesso é realizada através de uma chave de usuário (Login) e uma senha pessoal e intransferível, que deverá ser mantida secreta e é de responsabilidade exclusiva do possuidor. Sansões disciplinares (internas e judiciais) serão aplicadas caso seja identificado qualquer desvio das diretrizes de segurança estabelecidas.

O acesso lógico à rede deve ser controlado de forma centralizada, através de procedimentos formais e a partir do perfil de cada usuário no qual estará definido seu nível de autorização. A Proa.AI adota os princípios de menor privilégio em todos os níveis hierárquicos.

Todo serviço de rede não autorizado será rastreado, bloqueado, desabilitado, documentado e auditado.

Todas as transações na rede estarão obrigatoriamente protegidas através de mecanismos de segurança.

A criação de conta de acesso lógico para uso coletivo não é permitida em nenhuma hipótese.

Política de segurança em sistemas e aplicativos.

Quanto aos Aplicativos

Todos os sistemas ou aplicações que manipularem informações críticas e estejam alojados nos servidores de rede da organização, deverão possuir controles e serem avaliados pelo Comitê de Ética, Privacidade e Segurança da Proa.AI.

Os gestores dos aplicativos serão identificados e terão suas responsabilidades definidas formalmente em documentação, conforme a sensibilidade de cada negócio.

Para cada aplicativo será desenvolvido um plano de segurança, incluindo o contingenciamento.

A documentação das aplicações será mantida atualizada.

Os acessos aos aplicativos serão gerenciados objetivando controle de permissões e rastreamento, de acordo com as definições de perfis de usuários por funcionalidade.

Ambientes distintos serão definidos para desenvolvimento, teste e produção dos aplicativos.

Os aplicativos e suas versões serão disponibilizados em produção devidamente homologados, com o registro de sua análise de impacto sobre a segurança das informações.

As versões de desenvolvimento e de produção serão controladas e armazenadas com suas respectivas configurações de ambiente tecnológico.

A Proa.AI deverá estabelecer mecanismos formais (documentos/contratos) de proteção de direitos autorais sobre os aplicativos desenvolvidos por ela ou sob encomenda.

Os aplicativos serão desenvolvidos adotando ferramentas e metodologias padronizadas pela Proa.AI.

Todos os registros de ocorrência, tais como arquivos de logs e notificações, previstos pelo perfil do aplicativo, serão obrigatoriamente mantidos de forma que permita a plena recuperação de informações em caso de falhas e auditorias de violação de segurança.

Quanto aos Sistemas Operacionais, Softwares Básicos e Dados

Todos os softwares estarão em conformidade com os termos de licenciamento e com os direitos autorais de propriedade material e intelectual.

Todo o acervo de softwares e dados mantidos pela Proa.AI, em conformidade com seu perfil de utilização e especificidades, deve ser passível de recuperação a partir de cópias de segurança.

A instalação de softwares no ambiente de Produção será formalmente aprovada pelos gestores de TI e pelo CSO da Proa.AI.

O ambiente operacional será monitorado, registrando as ocorrências necessárias para contabilização do uso de recursos, recuperação de informações em situações de falhas,

auditorias e rastreamento de tentativas de violação, sendo mantido preservadas as evidências para uso interno e judicial.

Protocolo de recebimento e leitura

Declaro ter recebido da Proa.AI o documento Política de Segurança da Informação e ter tomado conhecimento de seu teor, através da leitura de seu conteúdo.

Assumo a responsabilidade de questionar a Proa.AI imediatamente, para esclarecimentos, sobre qualquer conteúdo cuja clareza não tenha conseguido identificar.

Local e Data:	
Nome Completo:	
CPF:	
Assinatura	