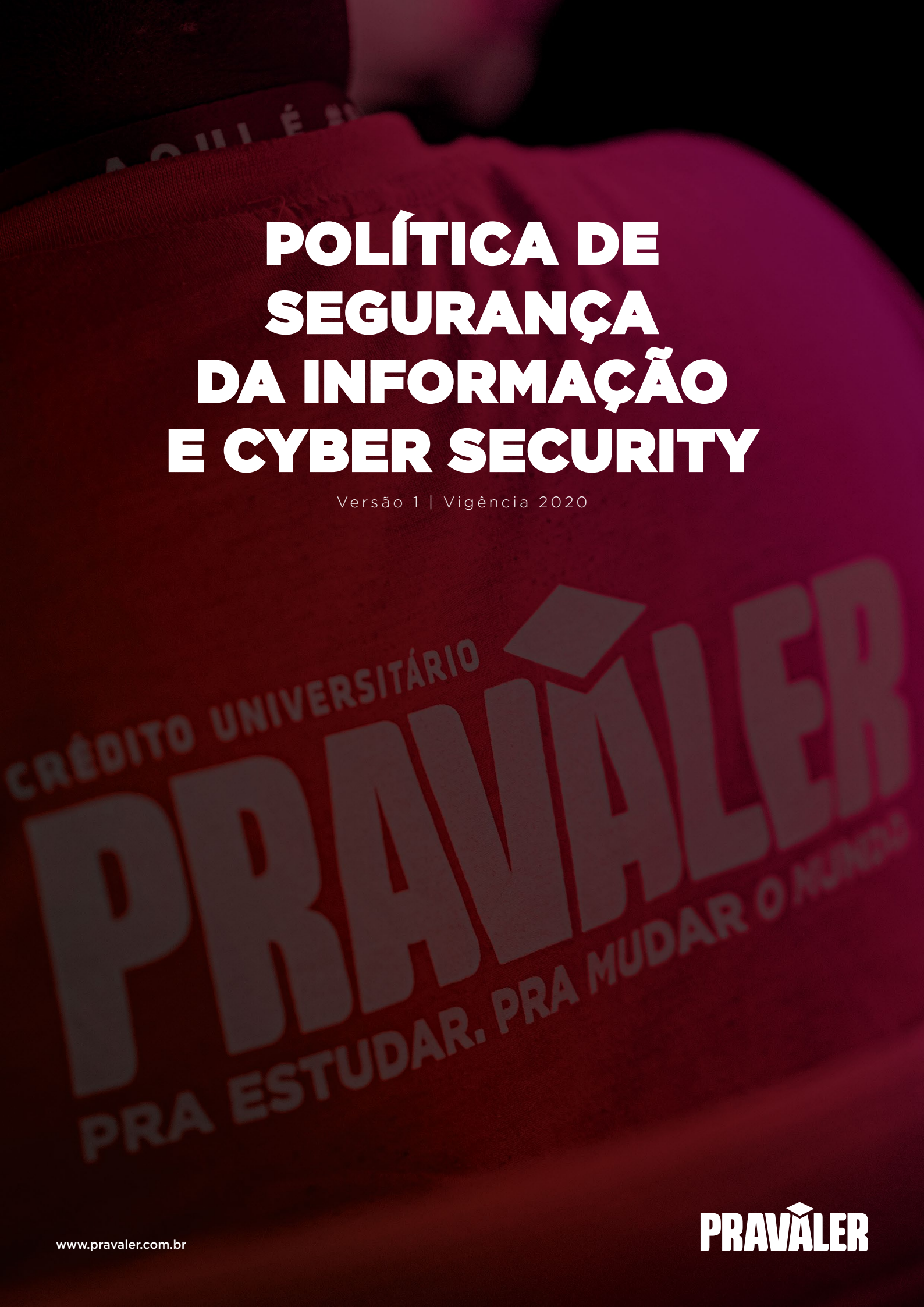
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

Versão 1 | Vigência 2020



www.pravaler.com.br

PRAVALER

INTRODUÇÃO

Aqui no PRAVALER desenvolvemos soluções simples e totalmente digitais para facilitar a concessão de crédito estudantil para alunos que precisam de ajuda para pagar as mensalidades. Assim, elaboramos esta Política de Segurança da Informação e Cyber Security (Política) para reafirmar o compromisso que temos com a adoção das melhores práticas de segurança da informação e proteção dos dados de nossos clientes.

OBJETIVO

O objetivo desta Política é formalizar os conceitos e as diretrizes da Segurança da Informação e Cyber Security do PRAVALER que visam à proteção dos ativos de informação, de modo garantir a confidencialidade, integridade e disponibilidade das informações.

DEFINIÇÕES

Para os fins desta Política, serão adotadas as seguintes definições:

- **Informação:** reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;
- **Segurança da Informação:** conjunto de ações e controles com objetivo de garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos do PRAVALER;
- **Confidencialidade:** as informações somente devem ser divulgadas a indivíduos, entidades ou processos autorizados;
- **Integridade:** salvaguarda da exatidão da informação e dos métodos de processamento;
- **Disponibilidade:** sempre que necessário, as pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes;
- **Conformidade:** cumprimento de um requisito legal ou regulatório relacionado à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração do PRAVALER;
- **Incidente de Segurança da Informação:** evento decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;
- **Risco de Segurança da Informação:** riscos associados à violação da confidencialidade, integridade e disponibilidade das informações do PRAVALER nos meios físicos e digitais.

PÚBLICO-ALVO

Esta Política destina-se a todos os PRAVALENTES, parceiros, fornecedores e prestadores de serviços do PRAVALER.

DIRETRIZES GERAIS

O PRAVALER visa estabelecer princípios e diretrizes para assegurar a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados. Tais medidas garantem, também, a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança.

REGRAS BÁSICAS DE SEGURANÇA DA INFORMAÇÃO

Esta Política está disponível para consulta a todos que queiram e eventuais desvios deverão ser reportados à Diretoria de Tecnologia da Informação.

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

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

I. Confidencialidade: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

II. Integridade: garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.

III. Disponibilidade: permite que a informação seja utilizada sempre que necessário, estando ao alcance de seus usuários.

CICLO DE VIDA DA INFORMAÇÃO

Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

I. Manuseio: é a etapa onde a informação é criada e manipulada.

II. Armazenamento: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.

III. Transporte: ocorre quando a informação é transportada para algum local, não importando o meio no qual ela está armazenada.

IV. Descarte: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações deve ser avaliada em razão do teor do conteúdo, relevância do conhecimento externo e pelos elementos intrínsecos do documento. O acesso, divulgação e tratamento do documento (físico ou digitalizado), dado ou informação do PRAVALER, são restritos aos PRAVALENTES que tenham necessidade de conhecê-los em razão de suas atividades profissionais, pautados pela regulamentação existente e pelos princípios de pertinência, utilidade e relevância.

Toda informação de uso corporativo deve ser classificada de acordo com o grau de sigilo para o negócio da empresa, considerando-se os três níveis descritos a seguir:

I. Confidencial: É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

II. Restrito: São informações específicas para uso interno, com circulação exclusiva e irrestrita dentro da empresa. Estas informações podem estar disponíveis a todos os PRAVALENTES e prestadores de serviços, devendo ser utilizadas somente para as atividades do PRAVALER. Essas informações, mesmo sendo de circulação livre dentro das empresas, não devem ser divulgadas para entidades externas sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela alçada responsável pela informação ou documento em questão.

III. Público: São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Incidente de segurança será qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da segurança da informação.

SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

O Sistema de Gestão da Segurança da Informação (SGSI) é um conjunto de disciplinas, deveres e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação visando a coordenação de ações em quatro grandes frentes de atuação:

I. Governança das políticas e procedimentos de segurança da informação;

II. Recursos e componentes de segurança da informação;

III. Monitoramento contínuo do ambiente de tecnologia da informação;

IV. Gestão de crises e continuidade de negócios.

CONTROLES INTERNOS DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

1. IDENTIFICAÇÃO/AVALIAÇÃO DE AMEAÇAS E VULNERABILIDADES

Caberá ao Departamento de Segurança da Informação do PRAVALER a identificação e avaliação dos riscos a que os processos e ativos relevantes estejam sujeitos em virtude das vulnerabilidades e possíveis cenários de ameaça atribuídos a cada processo ou ativo.

No que tange às empresas prestadoras de serviços e fornecedores que manuseiem dados ou informações sensíveis, as quais sejam relevantes para a condução de suas atividades operacionais, elaboramos cláusulas contratuais obrigatórias para que se adequem ao disposto na Resolução CMN 4658/2018.

2. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Sem prejuízo de ações específicas para proteção e prevenção de riscos identificados e avaliados pela área responsável, serão adotadas pelo PRAVALER, por meio do Departamento de Segurança da informação, rotinas padronizadas de prevenção e proteção dos processos e ativo, conforme previsto em norma interna, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

Destacando a execução periódica de testes de ataque e invasão, visando monitorar a eficiência de seu sistema de proteção a vulnerabilidades cibernéticas, realizamos no PRAVALER testes tanto em ambiente interno (na modalidade Gray Box) como no externo (na modalidade Black Box).

3. MONITORAMENTO E TESTES

Devem ser implementados controles internos efetivos para proteção dos RTICs (Recursos de Tecnologia da Informação e Comunicação) do PRAVALER, garantindo a sua confidencialidade, integridade, disponibilidade e norteado por esta política, com as melhores práticas de mercado e regulamentações vigentes.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre os ambientes de produção, homologação e teste. As ameaças cibernéticas devem ser analisadas em conjunto com as vulnerabilidades detectadas pelo SGSI nos ativos de informação e devem possuir monitoramento proativo.

4. PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Os incidentes de segurança da informação devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades aos quais estamos suscetíveis, respeitando o nível de exposição a risco aceito e definido pelo PRAVALER.

4.1. COMUNICAÇÃO DE INCIDENTES

Os intervenientes devem comunicar imediatamente os casos de incidentes ao Gestor de Segurança da Informação. Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causas-consequências, riscos envolvidos, partes envolvidas e planos de respostas. A avaliação deverá ser direcionada ao Diretor de Tecnologia da Informação para decisão das ações iniciais a serem tomadas. Classificada a relevância do incidente, o PRAVALER emitirá, tempestivamente, comunicado às partes envolvidas informando a situação ocorrida e ações definidas, ainda que preliminares, informando/notificando as atividades posteriores pertinentes. O Gestor de Segurança da Informação deve elaborar e divulgar ao Conselho de Administração relatório anual sobre os planos de ação e de resposta aos incidentes.

4.2. TENTATIVA DE BURLAR

A mera tentativa de burlar às diretrizes e controles estabelecidos pelo PRAVALER, quando constatada, deve ser tratada como uma violação.

4.3. TRATAMENTO DE VULNERABILIDADES IDENTIFICADAS

O tratamento e correções proativas das principais fragilidades ou fraquezas dos ativos de informação a serem utilizados devem estar registrados, sendo necessário avaliar o risco residual e ser sustentado pelos intervenientes indicados no plano.

4.4. CONFLITOS DE INTERESSE

Possuímos um processo de concessão de acessos que utiliza critérios claros e objetivos para identificar os conflitos de interesse aos quais decorrem de limitações técnicas ou de situações devidamente autorizadas. Há devido monitoramento das atividades dos intervenientes e das ameaças cibernéticas.

4.5. ELABORAÇÃO DE PLANO DE AÇÃO

O Plano de Ação deverá ser elaborado pelo Departamento de Segurança da Informação, podendo ser envolvidos outros departamentos caso necessário para implementação das soluções para administração de eventuais contingências. Tal plano deve contar com definição expressa dos papéis e responsabilidades na solução do impasse, prevendo acionamento dos PRAVALENTES-chaves e contatos externos relevantes, caso aplicáveis. Deverão ser levados em consideração os cenários de ameaças previstos na avaliação de risco, havendo critérios para classificação dos incidentes, por severidade. O Plano de Ação deverá, ainda, prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.

4.6 COMUNICAÇÃO AOS ÓRGÃOS REGULADORES

Conforme determinado na Resolução CMN 4.658/18, o PRAVALER efetuará comunicação tempestiva das ocorrências de incidentes relevantes e interrupções de serviços relevantes que configurem uma situação de crise, bem como as providências adotadas para o reinício dessas atividades.

5. PROGRAMA DE CAPACITAÇÃO, CONSCIENTIZAÇÃO E REVISÃO DOS NORMATIVOS

O PRAVALER possui e mantém um programa de revisão/atualização que visa garantir que todos os requisitos técnicos e legais de segurança implementados estão sendo cumpridos, atualizados e em conformidade com a legislação vigente. O programa também inclui a revisão periódica dos planos de ação, sua adesão a iniciativas de compartilhamento de informações sobre incidentes cibernéticos com outras instituições financeiras e/ou entidades de classe em que haja foros de tratamento do tema.

Os PRAVALENTES são informados sobre a importância da Segurança da Informação e Cyber Security através da plataforma WorkPlace.

RESPONSABILIDADES

As questões de segurança de informação e segurança cibernética, deverão ser endereçadas ao Diretor responsável pela Política de Segurança Cibernética (Resolução CMN 4.658/18 e Circular 3909/18).

CORRELAÇÃO COM LEGISLAÇÃO E REGULAMENTAÇÃO

Elaboramos esta Política em consonância com os seguintes normativos:

- Resolução CMN 4.658/18;
- Circular 3909/18.

DOCUMENTOS RELACIONADOS

- Código de Conduta Ética

DESCRIÇÃO RESUMIDA DA REVISÃO

Não se aplica.

ANEXOS

Não se aplica.

INFORMAÇÕES DE CONTROLE

Código do Documento:	Área:	Status:	Confidencialidade:	Versão:
POL.INST.0005	T.I.	APROVADO	PÚBLICO	1