Assunto: Política de Segurança da Informação

1. Objetivo

A Política de Segurança da Informação é um conjunto de diretrizes que objetiva proteger as informações da instituição, sejam elas, impressas, verbais e/ou sistêmicas; bem como, o controle de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas estabelecem uma proteção adequada para qualquer empresa.

2. Legislação

A presente política dispõe de procedimentos que tem por finalidade estabelecer as regras que orientam a execução e controle das atividades/operações em conformidade com os dispostos na Resolução CMN nº 4.893/21 e Resolução CVM nº 21/21, alterada pelas resoluções 162/22, 167/22 e 179/23.

3. Princípios de Segurança da Informação

A Política de Segurança da Informação visa garantir a proteção das informações de diversos tipos de ameaças, de forma consistente visando a minimização aos danos e maximização do retorno dos investimentos e das oportunidades de negócio.

A Segurança da Informação é aqui caracterizada pela preservação da:

- Confidencialidade, que é a garantia de que a informação é acessível somente às pessoas com acesso autorizado;
- Integridade, que é a salvaguarda da exatidão e o conteúdo da informação e dos métodos de processamento;
- Disponibilidade, que deve ser divulgada a todos os Funcionários/Colaboradores e disponibilizadas de maneira que seu conteúdo possa ser consultado a qualquer momento; e
- Acesso controlado, significa que os Funcionários/Colaboradores terão controle sobre as informações a serem identificadas e processadas de forma a mitigar ameaças à segurança da informação ou possíveis quebras da confidencialidade das mesmas.

Para assegurar esses princípios, as atividades de segurança da informação devem ser adequadamente gerenciadas e protegidas contra roubos, fraudes, espionagem, perda não intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os Funcionários/Colaboradores adotem a ação de “comportamento seguro e consistente” com a finalidade de proteção das informações, devendo assumir atitudes proativas e engajadas.

Campanhas contínuas de conscientização de segurança da informação serão utilizadas para monitoração e controle desses princípios.

Atribuições e Responsabilidades na Gestão de Segurança da Informação

Responsável pela área de Tecnologia
A área de Tecnologia deve:
- Planejar, implantar e gerenciar o uso dos recursos de informática da instituição, em linha com os planos estratégicos de negócios e operacionais, adotando tecnologias e métodos que melhor se adequem a este objetivo e garantam o cumprimento dos requisitos legais, dentre outros.
- Garantir o processamento das transações, visando a qualidade, integridade e rapidez das informações produzidas.
- Definir os padrões de hardware e software e recomendar a aquisição de recursos de informática.
- Administrar os recursos de informática e prover as tecnologias e meios necessários para que os mesmos sejam devidamente utilizados.
- Assegurar a capacitação ao nível adequado do pessoal de tecnologia sobre o entendimento dos negócios da instituição.
- Analisar viabilidade técnica/financeira de utilização de recursos de informática (software, sistemas, aplicativos, hardware e outros) próprios ou de terceiros.
- Elaborar guias de desenvolvimento e gerenciamento de projetos de informática e coordenar o treinamento do pessoal envolvido nos mesmos.
- Garantir a adequada proteção e integridade dos dados, tais como armazenamento, transmissão, backup, antivírus, gerenciamento de “senhas”, segregação de funções entre outros.
- Prestar suporte à Auditoria referente às trilhas de auditoria que possam ser verificadas, a fim de garantir o nível de controles internos da organização.

Responsável pela área de Compliance
A área de Compliance deve:
- Desenvolver e acompanhar a implantação dos controles internos, bem como promover testes periódicos incentivando a realização de provas e verificação de dados.
- Realizar em conjunto com a área de Tecnologia a avaliação quanto ao desempenho dos procedimentos de controles executados, exposição dos riscos e situação dos planos de ação desenvolvidos.
- Avaliar periodicamente os canais de comunicação, verificando se as informações estão disponíveis a todos os Funcionários/Colaboradores, de acordo com o seu nível de atuação, de forma confiável e compreensível, desde que relevantes para suas tarefas e responsabilidades.
- Participar dos treinamentos e testes de segurança da informação.

Demais Gerências e Diretoria(s)
As demais Gerências/Diretoria(s) deverão:
- Garantir uma ativa participação dos Usuários nos processos de planejamento, desenvolvimento e implantação dos projetos de Tecnologia e de
- segurança da informação.
- Garantir que o uso dos recursos de informática contribua para a melhora da rentabilidade, controles e otimizações de processos da organização.

- Garantir que estejam adequadamente definidas as solicitações para a área de Tecnologia.
- Aprovar/homologar dentro dos prazos acordados no plano de trabalho de cada um dos projetos que impactam a área, os produtos a serem entregues em cada uma de suas fases, assegurando que revisões sejam efetuadas por pessoas apropriadas e de responsabilidade comprovada.
- Criar as condições necessárias, em termos de recursos humanos e materiais, para o uso adequado dos recursos de informática, assegurar que os mesmos sejam aceitos e bem utilizados pelos Usuários.
- É de responsabilidade da área em questão que estiver interessada em inscrever algum Funcionário/Colaborador em cursos externos de informática, realizar a solicitação para a análise e/ ou indicação da área de Tecnologia.
- Assegurar que estão sendo tomadas medidas de proteção das informações que circulam pela sua(s) área(s) de responsabilidade, garantir que os acessos estejam adequados e identificar riscos e exposições.

Usuários

Os Usuários deverão:

- Participar ativamente nos processos de planejamento, desenvolvimento e implantação de novas ferramentas tecnológicas para racionalização e otimização das rotinas operacionais e de segurança da informação.
- Garantir que os dados de sua propriedade sejam protegidos contra acessos não autorizados.
- Respeitar as normas internas e externas de segurança, proteção à informação e outros.
- Somente utilizar software, sistemas aplicativos ou hardware registrados e homologados pela área de Tecnologia.
- Manter todos os dados de uso nos diretórios da rede, para que não haja perdas de informações.

Áreas de Tecnologia e de Compliance

Cabe às duas áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta; prover todas as informações de gestão de segurança da informação.

Estrutura Tecnológica

Entende-se por “recursos tecnológicos” os recursos utilizados para o tratamento de informações, incluindo computadores, equipamentos, sistemas, softwares, redes de comunicações, base de dados, acessos, dados armazenados em meios magnéticos e outros.

Como também a implantação da “Plataforma de Gestão” através de ferramentas para a redução de vulnerabilidade local e nas nuvens, que tem por finalidade processar as rotinas de backup e recuperação de informações; assim como os registro e tratamento das incidências.

A empresa ***PLANUS – Cloud, Networking & Services*** foi contratada para o fornecimento desses recursos através dos serviços de Interconexão e Conectividade, Data Center e Colocation; como também, soluções de infraestrutura em Cloud e recuperação de desastres, com monitoramento 24x7; operação e suporte; estrutura de back-up entre outros.

Recursos contratados

Item	Descrição (Produto)	Quantidade
AD	Core (vCPU)	2
	Memória (GB)	2
	Disco Alta Performance (GB)	100
	Proteção Anti-Malware VM´s (VM Windows)	1
TS	Core (vCPU)	6
	Memória (GB)	12
	Disco Alta Performance (GB)	200
	Proteção Anti-Malware VM´s (VM Windows)	1
FS	Core (vCPU)	2
	Memória (GB)	2
	Disco Alta Performance (GB)	1.000
	Proteção Anti-Malware VM´s (VM Windows)	1
Item	**Descrição (Produto)**	**Quantidade**
Licenciamento	SO Windows Server 2012 R2 Datacenter Edition (vCPU)	10
	CAL Terminal Services	03
	CAL Office Standard	03
	Exchange	03
Item	**Descrição (Produto)**	**Quantidade**
GESTÃO	Monitoramento e NOC 24x7 (item monitorado - VM, Link, etc)	3
	Gestão e suporte de S.O. 24x7 (VM S.O. Linux ou Windows)	3

Item	Descrição (Produto)	Quantidade
Backup 7 dias em Disco	Veam Backup & Replication Enterprise	3
	Backup Espaço Provisionado (GB)	1.300
	Gestão de Backup (por servidor)	3
Item	**Descrição (Produto)**	**Quantidade**
IP	IP Público	1
BANDA INTERNET	Banda Internet (1 Mbps)	5

Recursos/sistemas/ferramentas contratadas

- Módulos antivírus – compatíveis com Panda® AVG® __Norton® _ ou Avast®
- Módulos de limpeza de *spywares* – Ad-Aware®, Spyboot®
- Módulos de comunicação VoIP – Skype®; e,
- Sistema operacional: Windows 2010® / service pack 4
- Aplicativos da Microsoft Office
- *Sistema de Controle de Carteiras - Posição Clientes*

- *Sistema de Controle de Carteiras - Posição Administrador*
- *Front End - Boletagem e Transmissão Operações*
- *NEXUS: limites, controle e enquadramento das operações por produto*
- *Provedor de Dados: ANBIMA, Reuters, Bloomberg entre outros*

Procedimentos

1. Classificação da Informação

As informações que transitam pela ***4i Capital*** são classificadas em quatro padrões distintos, conforme o disposto na Política Código de Ética e Conduta, a saber: Informações Públicas, Informações Internas, Informações Confidenciais e Informações Restritas.

Informações Públicas: Aquelas destinadas à disseminação fora da instituição. Possuem caráter informativo geral e são direcionadas ao público externo.

Informações Internas: São aquelas destinadas ao uso dentro da instituição. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a ***4i Capital*** ou seus Investidores e Funcionários/Colaboradores. Essas informações não exigem proteções especiais, salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional.

Informações Confidenciais: Também se destinam ao uso interno da instituição. Entretanto, se diferem das informações de natureza interna, na medida em que sua eventual divulgação poderia afetar significativamente os negócios da ***4i Capital***, seus Investidores e Funcionários/Colaboradores. Exemplos: registros de empregados, planos salariais e informações sobre Investidores. Sua divulgação é proibida, salvo se solicitada pelo órgão fiscalizador competente, situação na qual deverá ser prestada, mediante autorização da área em questão ou da área de Compliance.

Informações Restritas: Correspondem às informações cuja divulgação não autorizada provavelmente provocaria danos substanciais, constrangimentos e/ou penalidades a instituição, seus Investidores e Funcionários / Colaboradores. Consideram-se informações de natureza confidencial todas as informações às quais os Funcionários / Colaboradores venham a ter acesso, em decorrência do desempenho de suas funções, inclusive por meio dos sistemas e arquivos disponibilizados para tanto, que não sejam notória e comprovadamente de domínio público. As pessoas designadas para o trato e uso de tais informações têm a responsabilidade de garantir que elas sejam devidamente protegidas e seguramente armazenadas quando não estiverem em uso.

Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o Funcionário/Colaborador deve, previamente à sua divulgação, consultar o responsável pela área de Compliance para obter orientação adequada.

2. Obtenção de Senhas e Acesso a Rede e E-mail

Senhas

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos.

Todos os equipamentos/computadores da ***4i Capital*** possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

As senhas são de caráter sigiloso, pessoal e intransferível e serão fornecidas aos Funcionários/Colaboradores através de liberação/acesso através de aplicativo específico. Em nenhuma hipótese as senhas deverão ser transmitidas a terceiros.

Os Usuários e Senhas são cadastrados e gerenciados pelo aplicativo Active Diretory da Microsft. Tais senhas devem ser substituídas a cada 45 (quarenta e cinco) dias.

Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada.

As senhas são criadas pelos Usuários respeitando as políticas de administração de rede, controlada através da ferramenta Microsoft Active Directory:, conforme definição:

- ✓ Mínimo de 8 caracteres;
- ✓ Utilize alguma regra para criar sua senha e memorizar;
- ✓ Troque letras por números ou caracteres especiais. Por exemplo: i=1, s=5, a=@, t=7, o=0.

Acesso à rede via WI-FI

O acesso à rede interna via Wi-Fi é permitido para todos os Funcionários/Colaboradores e Visitantes. Esta rede permite acesso apenas a internet e serviços nela disponíveis. O acesso é restrito a sites pertinentes ao ambiente corporativo, ou seja, conforme item abaixo - **Internet.**

Os acessos, mesmo pela rede de Visitantes, podem ser monitorados e controlados.

Não é permitido através do Wi-Fi o acesso à rede de computadores da corporação; como também, do Data Center e servidores.

A rede Wi-Fi possui acesso restrito para administração do ambiente, e é de uso exclusivo da equipe de Tecnologia, com controle de senhas e permissões já descritos acima.

Internet

Os Funcionários/Colaboradores deverão utilizar os recursos de acesso à internet apenas para assuntos corporativos, sendo a utilização para fins particulares tratadas como exceção. Para

preservar esses recursos, a ***4i Capital*** se reserva o direito de controlar e monitorar seus conteúdos e formas de utilização.

Como qualquer outro material de trabalho, as páginas da Internet também devem ser usadas preferencialmente para fins profissionais. Para uma utilização eficiente e produtiva algumas regras devem ser obedecidas:

- não é permitido visitar sites que contenham materiais obscenos, lascivos, preconceituosos ou outro tipo de material repreensível;
- não é permitido enviar ou receber material obsceno ou difamatório ou cujo objetivo seja aborrecer, assediar ou intimidar terceiros;
- não é permitido utilizar os computadores da instituição objetivando práticos de atos ilícitos;
- não é permitido apresentar opiniões pessoais como se fossem da ***4i Capital***.

É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, atividades de hacker e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento das áreas de Tecnologia e/ou Compliance.

Por padrão são bloqueados acesso a redes sociais, streaming de mídia, armazenamento em nuvem, fóruns de discussão e download de softwares e arquivos (FTP, Torrent e demais meios de compartilhamento de arquivos). A solicitação de acesso a estes tipos de sites deve ser formalizada junto a área de Tecnologia e a concessão do acesso só é fornecida com a aprovação por e-mail do gestor imediato do Funcionário/Colaborador.

Utilizamos um equipamento do tipo “Next Generation Firewall”, que realiza o controle de acesso a aplicações e sites, conforme descrição. Este equipamento realiza o registro do log de acesso e bloqueio, ficando disponível por um período de 6 meses.

Uso do E-mail

Como se trata de ferramenta de trabalho, o e-mail poderá ser rastreado, monitorado, gravado e/ou inspecionado, sem prévio aviso, com objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta.

Os Funcionários/Colaboradores, com a aceitação dos termos e condições das Políticas da instituição, estão cientes de que as informações transmitidas e recebidas em sua conta de e-mail poderão ser monitoradas, ficando cientes de que o uso indevido ou não autorizado os sujeitará a punições.

Os e-mails serão controlados pelos softwares Exchange e Active Diretory da Microsoft onde são cadastrados os Funcionários/Colaboradores da ***4i Capital*** conforme solicitação da área de Recursos Humanos (“RH”).

Quando da contratação ou desligamento do Funcionário/Colaborador cabe a área contratante através de comunicação ao RH, informar do evento de forma que o acesso ao(s) sistema(s)/aplicativo(s), e-mail, internet, pastas e arquivos da rede, entre outros seja liberado ou bloqueado.

A ***4i Capital*** se reserva o direito de controlar e monitorar seus conteúdos e formas de utilização.

3. Acompanhamento e Controles de Recursos

Gravação Telefônica

A Central Telefônica registra todas as ligações recebidas e efetuadas de todos os ramais e linhas instaladas; no entanto, em função de obrigatoriedade normativa, algumas áreas da instituição podem ter seus ramais ligados a sistema de gravação de voz. Estas gravações serão verificadas, a cada 24 meses, pela área de Compliance. A escuta por outro Funcionário / Colaborador só poderá ser realizada com a aprovação do Gestor responsável, através de autorização escrita justificando a medida.

Política de Backup

Todos os documentos arquivados pelos Funcionários/Colaboradores na rede, ou seja, nos servidores são objeto de back-up diário com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

O backup é feito diariamente e mantido em arquivo físico (quando aplicável) pelo período de 30 dias. Após este prazo os documentos são classificados, separados e enviados para uma empresa especializada na guarda de documentos. O prazo de arquivamento é estabelecido por tipo de documento/legislação vigente - Política de Guarda de Documentos - Informações.

Instalação de Softwares/Aplicativos

Todos os programas/aplicativos utilizados pelos Funcionários/Colaboradores devem ter sido previamente aprovados e autorizados pela área de Tecnologia.

Os sites de downloads conhecidos são bloqueados, não sendo permitido a baixa de softwares/aplicativos; a exceção são os softwares definidos pelos órgãos reguladores das atividades objeto da instituição, com o acompanhamento da área de Tecnologia.

Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos equipamentos para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

A cópia de arquivos e instalação de programas devem ser executadas apenas pela área de Tecnologia da ***4i Capital;*** bem como, deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

Todos os sistemas/aplicativos eletrônicos utilizados pela instituição estão sujeitos à revisão, monitoramento e gravação a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

Vírus

A atualização das definições de vírus é realizada de forma automática, pelo menos uma vez por dia. Esta definição é enviada a todos os equipamentos e garante que os vírus “lançados” mais recentemente sejam detectados e removidos. Além destas definições, esta ferramenta possui módulo de detecção de comportamento, o que permite que um vírus ou software malicioso, mesmo não mapeado pelo fabricante, seja bloqueado e eliminado.

A detecção de vírus é monitorada automaticamente pelo software antivírus, sendo assim, no caso da detecção de vírus o usuário, a princípio, não precisa realizar nenhuma interação com o software. Compete à área de Tecnologia monitorar as ações tomadas pelo software em questão.

São realizadas semanalmente ações proativas para detecção de falhas da ferramenta e, se necessário atualização ou reinstalação, garantindo que nenhum computador ou servidor fique sem o software em pleno funcionamento.

Temos em nosso Firewall e AntiSpam um módulo de detecção de vírus, “*spyware e ransonware*”; sendo assim, caso ocorra a tentativa de recebimento ou download de algum item malicioso, o bloqueio e a comunicação a área de Tecnologia, se darão automaticamente. Outro módulo em nosso firewall é o IPS, que trabalha na prevenção de intrusões, seja por ferramentas ou manualmente.

4. Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios da ***4i Capital*** consiste no uso de sistemas/aplicativos/arquivos “na nuvem” e equipamentos em ambiente alternativo, facilitando o deslocamento para outros sites, caso necessário.

O processo de Continuidade de Negócio estabelece as estruturas de proteção e os procedimentos operacionais em situação emergencial em casos de incidência de falhas/indisponibilidade dos recursos existentes.

Temos como contingência posições de trabalho contratadas com a empresa Planus Cloud, Networking and Services, localizada em São Paulo. Seu uso pode ser feito com base em agendamento prévio via chamado e acionamento do colaborador com o cargo de SLM na empresa contratada.

A sala será preparada conforme premissas do contrato, sendo disponibilizadas vinte estações de trabalho, ramais e uma impressora.

Para contingência de nosso Data Center principal, temos replicação dos arquivos e bancos de dados e sistemas para um data center do tipo “Disaster Recovery”, localizado em São Paulo. O acionamento deste site deve ser feito via chamado, decretando o desastre e a necessidade de subida dos serviços. Deverá ser registrado chamado e acionado o colaborador SLM da empresa contratada. Toda a ativação do site de desastre deverá ser acompanhada pela equipe de Tecnologia e Compliance para as devidas configurações.

São realizados testes semestrais para ambos os ambientes, validando o plano e corrigindo eventuais falhas ou documentando novas demandas.

5. Identificação de Riscos

A instituição conta com ferramentas como o Antivírus, *Firewall* com IPS e IDS e AntiSpam que geram relatórios automáticos contendo informação de riscos do ambiente, podendo inclusive identificar tentativa de acesso ou comportamento de usuário e serviço potencialmente perigoso. A partir daí a equipe de TI avalia qual a real necessidade e qual ação deverá ser tomada.

6. Avaliação de Riscos, Correções e Mitigação de Falhas

Semestralmente a ***4i Capital*** irá contratar empresa especializada em testes de intrusão, avaliação de ambiente e detecção de riscos no ambiente e recursos tecnológicos. Esta avaliação completa é acompanhada da área de Tecnologia.

O documento final desta avaliação é um detalhamento de todos os problemas, falhas e riscos encontrados, bem como as devidas soluções.

Com base neste documento é realizado um planejamento para correção dos problemas ou mitigação no caso de problemas encontrados, mas sem solução ou suporte pelo Prestador dos serviços; podendo-se optar inclusive pela migração dos serviços caso não exista uma solução definitiva à falha.

Estas empresas especializadas em segurança da informação, bem como a consultoria que temos contrato firmado, são responsáveis por apontar novas descobertas de falhas, conforme boletim informativo dos fabricantes ou empresas especializadas, em itens utilizados em nosso ambiente.

As ações para correção serão tomadas assim que publicada as ferramentas para isso e até lá são decididas ações para mitigação.

7. Plano de Ação e de Resposta a Incidentes

Caberá a área de Tecnologia definir os recursos a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da Política de Segurança da Informação quanto a:

- Definição de processos, testes e trilhas de auditoria;
- Definição de métricas e indicadores adequados; e
- Identificação e a correção de eventuais deficiências.

Com base nessas premissas, o Plano deve detalhar:

✓ A ferramenta de controle para registro de ocorrência de incidente seja para a correção de alguma funcionalidade, correção de algum erro de tratamento e/ou correções em conteúdo de dados;

✓ Pontos de controle: realização periódica de auditoria de melhores práticas, segurança e pontos falho.

✓ Correções e melhorias: atualização/manutenção da(s) ferramenta(s) com novas funcionalidades, controles e recursos tecnológicos.

- ✓ Registro, divulgação e orientação do posicionamento quanto à Segurança Cibernética a todos os Funcionários/Colaboradores da ***4i Capital***; como também, aos órgãos reguladores.

A área de Tecnologia através de seus Funcionários/Colaboradores e a ***PLANUS – Cloud, Networking & Services*** compõem a equipe para dar as respostas / correções aos incidentes.

Em caso de crise, a Diretoria Executiva é quem deve decidir as ações a fim de impactar o mínimo possível os negócios.

Responsabilidade

A Diretoria Executiva da ***4i Capital*** se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes.

A Política deve ser revisada e/ou atualizada anualmente, de forma a evidenciar a sua apreciação, discussão e reformulação através de Ata de Reunião.

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente através de e-mail ao seu Superior e/ ou a área de Compliance.

Canal de Comunicação*: E-mail:* compliance@4icapital.com.br

ANEXO

Termo de Responsabilidade de Segurança da Informação

Atesto ter recebido, lido e compreendido os princípios e diretrizes da Política de Segurança da Informação da ***4i Capital Ltda***, comprometendo-me a observá-la integralmente e comunicar ao meu Superior e/ou a área de Compliance sobre qualquer inconformidade que venha a ser de meu conhecimento.

Declaro ter pleno conhecimento que o descumprimento da Política e deste Termo pode implicar em demissão, inclusive por justa causa, sem prejuízo de apuração dos danos que tal descumprimento possa causar a Instituição.

Data: _____/_____/_____

Assinatura:_____

Nome:

RG:

Cargo: