FORPUS
CAPITAL

Política de Sigilo da Informação e Segurança Cibernética

Válido a partir de	Novembro de 2025
Área Responsável	Compliance
Destinatários	Público em Geral

Sumário

Introdução

A Forpus Capital, enquanto Gestora de Recursos de Terceiros, possui acesso a informações internas e de terceiros que não estão disponíveis ao público, algumas destas informações, inclusive, podendo possuir caráter confidencial.

Nos últimos anos houve um aumento significativo nas ameaças cibernéticas, que englobam, além de uma maior quantidade de ameaças, uma maior sofisticação nos mecanismos utilizados. Diante deste cenário, a Forpus Capital está comprometida a zelar pela segurança de seus negócios, registros e informações contra riscos e, também, ataques cibernéticos.

Todos os colaboradores da Forpus Capital têm a responsabilidade de proteger a segurança e integridade dos arquivos, especialmente aqueles que contenham dados sensíveis ou confidenciais, contra vazamento de informações, formando uma primeira camada de proteção às ameaças cibernéticas e acessos não-autorizados. Para que isto seja possível, é primordial que a Forpus Capital esteja alinhada de forma permanente às melhores práticas de cibersegurança e segurança da informação.

Objetivo

A presente política tem como objetivo estabelecer medidas tomadas pela Forpus Capital que garantam a segurança cibernética, bem como o constante aprimoramento da segurança da informação e segurança cibernética da Gestora, por meio do estabelecimento de regras internas para o tratamento de informações confidenciais e sensíveis, da identificação e prevenção de contingências e desenvolvimento de um plano de resposta a incidentes.

Os protocolos de segurança cibernética adotados pela Forpus Capital, foram elaborados utilizando como base as melhores práticas vigentes no mercado, bem como observando as diretrizes estabelecidas pela Anbima.

1. Segurança e Sigilo da Informação

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Forpus Capital, que não a necessitem ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Serão consideradas Informações Sensíveis aquelas que possuam relevante potencial estratégico bem como detenham capacidade, de caso expostas, realizar prejuízos de grande porporção (“Informações Sensíveis”). Este tipo de dado somente deverá ser compartilhada com um grupo seleto de pessoas pré-ordenadas, mediante aprovação do O Diretor de *Compliance,* Risco, PLDFT e LGPD.

Já as Informações Confidenciais serão compreendidas aquelas em que é possível o compartilhamento com um espectro maior de colaboradores, mas que ainda possuem informações pessoais de clientes, e que são capazes de provocar prejuízos relevantes (“Informações Confidenciais”).

Poderá ser interpretado também como Informação Confidencial qualquer informação sobre a Forpus Capital e suas atividades, bem como de seus sócios e clientes ou colaboradores, que for obtida em decorrência do desempenho das atividades normais do Colaborador, que só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Cliente, quando envolvido, e pelo Diretor de *Compliance*, Risco, PLDFT e LGPD.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Forpus Capital e circulem em ambientes externos à Forpus Capital com estes arquivos, uma vez que tais arquivos contêm Informações Confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Forpus Capital e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade, bem como deverá informar ao Diretor de *Compliance,* Risco, PLDFT e LGPD da impressão e, após a utilização, de seu descarte.

Ainda, qualquer impressão de documentos deve ser imediatamente conservada pelo Colaborador responsável pela impressão, pois podem conter informações restritas e confidenciais, inclusive para outros Colaboradores da Forpus Capital.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração à presente política e a Forpus Capital poderá, através de seu O Diretor de *Compliance,* Risco, PLDFT e LGPD e quando cabível, procurar as medidas judiciais, caso o(s) responsável(eis) ocasione(m) qualquer dano ou prejuízo à própria Gestora, aos seus clientes e Colaboradores.

O descarte de documentos físicos que contenham Informações Confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

A utilização de mídia removível (tais como pen-drives, discos flexíveis, cartões de memória e similares) ficará vedada e os dispositivos desabilitados. O Diretor de *Compliance,* Risco, PLDFT e LGPD poderá aprovar exceções a esta vedação, mediante email, documento por escrito ou outro tipo de formalização que apresente exigências, obrigações e prazos para a utilização deste tipo de mídia.

É proibida a conexão de equipamentos na rede da Forpus Capital que não estejam previamente autorizados pela área de informática e pela área de compliance. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos e materiais que estão sob sua responsabilidade.

Não obstante, o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é, também, terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Forpus Capital, seus clientes e Colaboradores.

Em nenhuma hipótese um Colaborador poderá emitir opinião por e-mail em nome da Forpus Capital, ou utilizar material, marca e logotipos da Forpus Capital para assuntos não corporativos ou após o rompimento do seu vínculo com a Gestora, salvo se expressamente autorizado pelo Diretor de *Compliance*, Risco, PLDFT e LGPD.

A Forpus Capital se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Forpus Capital para a atividade profissional de cada Colaborador. O Diretor de *Compliance*, Risco, PLDFT e LGPD poderá, a qualquer momento, analisar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente pelo Diretor de *Compliance*, Risco, PLDFT e LGPD, com registro em ata.

2. Programa de Cibersegurança da Forpus Capital

2.1. Avaliação de Risco (*Risk Assessment)*

Como primeiro passo a ser dado na identificação de possíveis ameaças cibernéticas e mitigação de riscos, a Forpus Capital realiza uma avaliação de risco, cuja primeira etapa é a identificação de motivações para possíveis ataques cibernéticos.

Dentre as diversas razões para a realização desses ataques, as principais costumam ser:

- Obtenção de ganho financeiro;

- O Roubo, a manipulação e/ou a adulteração de informações;
- Obtenção de vantagens competitivas e informações confidenciais de empresas concorrentes;
- Fraudar, sabotar ou expor a instituição invadida;
- Promoção de ideias políticas e/ou sociais; e
- Promoção do terror e disseminação do pânico.

Diante desse cenário, os invasores podem valer-se de vários métodos para a realização de um ataque cibernético. Os mais comuns são:

- *Malware – softwares* desenvolvidos para corromper computadores e redes:
    - Vírus: *software* que causa danos a máquina, rede, *softwares* e banco de dados;
    - Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
    - *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
    - *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
    - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
    - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
    - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
    - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
    - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

As ameaças cibernéticas podem variar, ainda, em função da natureza, vulnerabilidade e informações/bens de cada organização.

2.2. Ações de Prevenção e Proteção

Visando mitigar e minimizar a concretização dos riscos identificados, a Forpus Capital adota medidas que busquem impedir previamente a ocorrência de um ataque cibernético, como:

- Controle do acesso aos ativos da Gestora, por meio de identificação, autenticação e autorização dos usuários e a utilização de sistema específico para a autenticação e acesso aos dados, que ficam armazenados em sistema online.

- Estabelecimento de regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede – complexidade, periodicidade e autenticação de múltiplos fatores – em função da relevância do ativo acessado;

- Segregação de senhas entre serviços;

- Limitação do acesso, uma vez concedido, a apenas recursos relevantes para o desempenho das atividades. A concessão de acesso será implementada de forma a ser revogada rapidamente quando necessário;

- O acesso aos dados é restringido conforme o grau de permissão, tendo acesso aos dados sensíveis somente quem detém responsabilidade e necessita de fato utilizar os dados para o desempenho de suas funções.

- Os eventos de login e alteração de senhas na Forpus Capital são auditáveis e rastreáveis;

- Ao incluir novos equipamentos e sistemas em produção, a Forpus Capital garante que serão feitas configurações seguras de seus recursos;

- Restrição ao acesso físico às áreas com informações críticas/sensíveis;

- Criação de logs e trilhas de auditoria sempre que os sistemas permitirem;

- Realização de diligência na contratação de serviços de terceiros, inclusive serviços em nuvem, com adequação a questões jurídicas, incluindo cláusulas de confidencialidade, proteção de dados pessoais e exigência de controles de segurança na própria estrutura dos terceiros;

- Implementação de segurança de borda, nas redes de computadores, por meio de *firewalls* e outros mecanismos de filtros de pacotes;

- Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoal, atualmente sendo empregado o software Sophos, reconhecido como um dos mais seguros existentes.

- Implementação de segregação de serviços sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamentos relevantes;

- Impedimento à instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*); e

Todas as informações do servidor da Forpus Capital, do banco de dados dos clientes e os modelos dos analistas são armazenados em sistema de armazenamento de nuvem[1], o qual possui todas as certificações internacionais de Compliance necessárias (HDPR, HIPAA, ITAR dentre outras), tendo como segurança sistemas de *data leak prevention*, *zero trust security*, e dados devidamente criptografados.

O acesso aos documentos que se consideram sigilosos, Informações Confidenciais e Informações Sensíveis será somente possível por colaboradores da Forpus Capital que detenham competência para os manusear, uma vez que estes arquivos possuem distinção quanto aos níveis de acesso possíveis, sendo acessíveis somente pelo setor de Risco, Compliance e Trading e Comercial, quando definidos a correlação com a área a tratar os dados.

[1] www.box.com

2.3. Monitoramento e Testes

Conforme recomendado pela Anbima, a Forpus Capital faz uso de mecanismos para monitoração de seus sistemas. A seguir, estão elencadas algumas das medidas tomadas:

- Criação de mecanismos de monitoramento de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade;
- Manutenção de inventários atualizados de *hardware* e *software*, bem como verificação destes com frequência para identificar elementos estranhos à instituição;
- Manutenção dos sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas;
- Monitoramento diário das rotinas de *backup*; e
- Realização de análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

2.4. Plano de Resposta a Incidentes (PRI)

A Forpus desenvolveu um Plano de Resposta à Incidentes ("PRI") que endereça vários estágios relacionados à um Incidente de Segurança da Informação, sendo eles:

- Preparação, por meio de medidas para monitorar certos usos de informações e sistemas;
- Detecção de acessos não autorizados ou outras brechas em potencial;
- Após, proceder com análise de forma a determinar o tipo de incidente que ocorreu, a informação acessada (caso tenha ocorrido) e a extensão da perda relatada;
- Contenção do incidente, por meio da definição de papéis e responsabilidades aos colaboradores, conforme o caso;
- Erradicação, determinando se e quais sistemas devem ser desconectados ou desabilitados;
- Recuperação e/ou restauração dos serviços que tenham sido impactados; e

- Acompanhamento pós-incidente, por meio da notificação de todas as partes envolvidas e do fornecimento de suporte para a mitigação dos danos ocorridos pelo incidente em questão.

3. Reciclagem e Revisão

A atual política será revisada periodicamente pela Forpus Capital, a fim de que nossos protocolos se mantenham sempre atualizados e alinhados às melhores práticas de proteção.

4. Atualização

Versão	Motivo da Alteração	Data de Aprovação	Autor
1	Implementação	31/08/2021	Diretor de Compliance, Risco, PLDFT e LGPD
2	Revisão Periódica	16/11/2022	Diretor de Compliance, Risco, PLDFT e LGPD
3	Revisão Periódica	06/12/2023	Diretor de Compliance, Risco, PLDFT e LGPD
4	Revisão Periódica	13/11/2024	Diretor de Compliance, Risco, PLDFT e LGPD
5	Revisão Periódica	26/11/2025	Diretor de Compliance, Risco, PLDFT e LGPD