Política de Segurança da Informação

Versão	Atualizada em	Responsável
1.0	Setembro/2020	Alexandre Fraga

Sumário

Introdução

O presente documento tem por finalidade determinar as regras e procedimentos relativos à segurança física das instalações, assim como da segurança lógica das informações da Pilotage Investimentos, a serem obrigatoriamente respeitadas e seguidas pela totalidade dos sócios, administradores, colaboradores e funcionários da Pilotage Investimentos.

No decorrer do presente documento, iremos nos referir aos "sócios, administradores, colaboradores e funcionários" indiscriminadamente como "Colaboradores".

Conforme os termos da Instrução CVM nº 558, de 26 de março de 2015, a Pilotage Investimentos adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação à qual um Colaborador tenha acesso, em função da atividade profissional desempenhada, é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

Em anexo é apresentado o "Termo de Responsabilidade" que é assinado por todos os Colaboradores da Pilotage Investimentos, quando do seu ingresso na empresa.

Segregação de Atividades

A Pilotage Investimentos somente utiliza como veículos de investimento, carteiras administradas e fundos de investimento dos quais é gestora, não distribuindo cotas de fundos que não sejam geridos por ela mesma.

Assim, as regras de segregação física e eletrônica restringem-se às áreas responsáveis pela gestão de recursos, de risco e compliance, administrativa e de acesso comum, incluindo visitantes.

Segregação Física

Todos os Colaboradores possuem cartão (pessoal e intransferível) de acesso às instalações físicas, sendo responsáveis pela sua guarda e utilização. Tais cartões permitem o monitoramento de entrada/saída do Colaborador, que poderá ser consultado em caso de necessidade.

As áreas destinadas às atividades de gestão de recursos e de risco e compliance serão fisicamente apartadas das demais áreas comuns da Pilotage Investimentos, como por exemplo, salas de reunião, copa e banheiros.

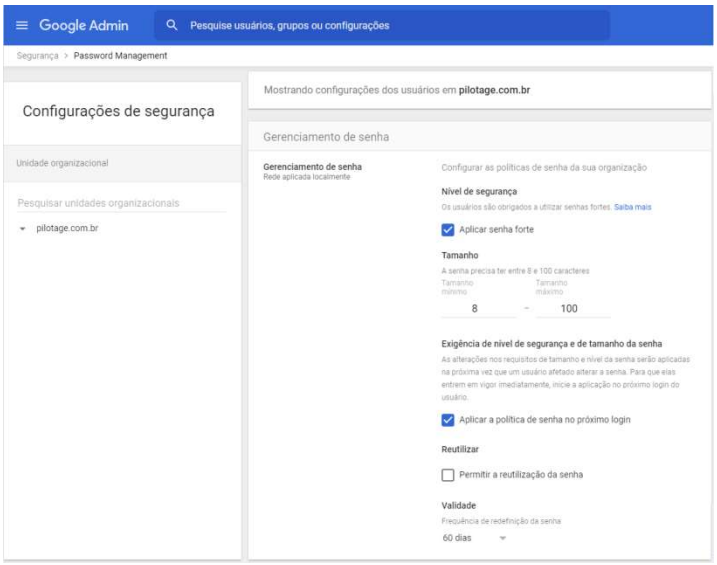
O acesso de pessoas que não fazem parte do quadro de Colaboradores será restrito à recepção e às salas de reunião, exceto mediante autorização da administração e acompanhadas de Colaboradores.

O atendimento a clientes e visitantes nas dependências da Pilotage Investimentos sempre ocorrerá apenas nas salas destinadas para reuniões.

Segregação Eletrônica

Todos os Colaboradores possuem usuário/senha (pessoal e intransferível) de acesso aos equipamentos de informática, bem como aos sistemas, sendo responsáveis pela sua guarda e utilização. Os sistemas possuem trilha de auditoria, que poderá ser utilizada em caso de necessidade.

As regras para definição de senhas no ambiente principal da Pilotage Investimentos são definidas pela Área de Risco e Compliance e são implementadas na plataforma Google Suite Business, conforme figura abaixo.



Concessão e Revisão dos Direitos de Acesso

Em caso de ingresso do Colaborador na Pilotage Investimentos ou mudança de cargo, os direitos de acesso lógico e físico do mesmo devem ser necessariamente revistos e adequados às suas novas atribuições pelo gestor da área onde será alocado.

Caso o Colaborador estiver deixando a organização, seja por iniciativa própria ou não, todos os seus direitos de acesso devem ser removidos tempestivamente. Além disso, o nome dele deve ser removido de listas de e-mail e todos na organização devem ser comunicados sobre o desligamento e orientados a não mais compartilhar informações com essa pessoa.

Término do Vínculo com a Pilotage Investimentos

Complementando o item anterior, deve ser devolvido à organização todo e qualquer ativo que esteja sob posse de um Colaborador cujas atividades foram encerradas. Isso inclui documentos, dispositivos móveis, mídias de armazenamento, softwares, cartões de acesso

etc. E nos casos de informações importantes da organização estarem contidas em dispositivos pertencentes ao Colaborador, essas informações precisam ser copiadas e a seguir apagadas.

Segurança da Informação Confidencial

Em tempos de troca de dados de maneira instantânea usando a internet e com o armazenamento de um volume de informações jamais visto, torna-se ainda muito mais importante classificar e proteger adequadamente os dados da Pilotage Investimentos.

Além disso, a Lei Geral de Proteção de Dados em seu Artigo 46 determina a adoção de medidas para proteger os dados pessoais de acessos não autorizados, conforme descrito abaixo:

- *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*

Assim, os dados utilizados pela Pilotage Investimentos foram mapeados *("data mapping")*, onde foram identificados aqueles que são alvo da LGPD e quais usuários têm acessos aos mesmos (além do nível de permissionamento dado e quem realmente está acessando).

Definição - Classificação de Informações

A Classificação das Informações consiste na identificação da criticidade e na definição de níveis de proteção que cada dado deve receber.

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

Níveis de Classificação das Informações

Conforme recomendado pela norma ISO 27001, as informações devem ser classificadas de acordo com seu valor, requisitos legais, criticidade e sensibilidade.

A norma não determina os níveis necessários, apenas fala que eles devem fazer sentido no contexto da organização. Assim, a Pilotage Investimentos adotou a seguinte classificação para a informação: confidencial, restrita, de uso interno ou pública.

[C3] - Confidencial

É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da Pilotage Investimentos. Devem ser protegidas ao

máximo, como por exemplo, fazendo uso de criptografia para os dados armazenados em meio eletrônico ou cofre, se armazenados em meio físico.

Em caso de e-mail classificado como Confidencial, o mesmo deverá conter a identificação **[C3]** antes da descrição do assunto.

[C2] - Restrita

É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso à uma pasta ou diretório da rede.

Em caso de e-mail classificado como Restrito, o mesmo deverá conter a identificação **[C2]** antes da descrição do assunto.

[C1] - Uso interno

Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

Em caso de e-mail classificado como Uso Interno, a colocação da identificação **[C1]** é facultativa.

[C0] - Pública

São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

No caso de informação classificada como Pública, a colocação da identificação **[C0]** é facultativa.

Rótulo das Informações

Toda vez que uma pessoa receber um documento, um e-mail ou qualquer outro dado, ela precisa saber sobre o seu nível de confidencialidade. O rótulo de um documento da Pilotage Investimentos é colocado em destaque, como feito no cabeçalho deste manual ou na descrição do Assunto de e-mails, como na figura a seguir.

Inventário de Dados – *"Data Mapping"*

A Pilotage Investimentos mantém um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, diretórios, planos de continuidade, entre outros. Ela serve para garantir que nenhum dado seja divulgado indevidamente e que apenas as pessoas que têm direito recebam acesso à informação

Dessa forma, antes de classificar as informações, foram identificados todos os dados necessários à operação da Pilotage Investimentos, os processos e procedimentos pelos quais os dados transitam, o tipo de informação contido nos mesmos (documentos eletrônicos, documentos em papel, etc.), o responsável e se os dados são sensíveis ou não.

O documento *"Mapeamento de Dados e Levantamento de Riscos por Área"* contém essas informações para cada uma das áreas da Pilotage Investimentos.

Prevenção e Proteção

A Pilotage Investimentos sabe não ser possível garantir a total eficácia dos controles de segurança, tanto pela viabilidade técnica quanto pela real necessidade, em função das suas características, tais como porte e complexidade de seu ambiente.

Dessa forma, foi realizada uma análise das lacunas existentes no atendimento às normas e riscos associados ao fluxo de dados pessoais, para estabelecer prioridades e justificativas para a implementação dos controles de segurança específicos para a Pilotage Investimentos, cujo resultado é apresentado no documento *"Mapeamento de Dados e Levantamento de Riscos por Área"*.

Finalidade/Adequação

Todos os dados pessoais utilizados/armazenados pela Pilotage Investimentos seguem estritamente as finalidades para as quais foram coletados, seja por uma necessidade de atendimento a um regulador (CVM, Banco Central do Brasil, etc.) ou ainda pelo consentimento dado pelo Cliente através do "Termo de Consentimento", devidamente assinado por ele.

Os Clientes têm total conhecimento das finalidades comentadas no parágrafo anterior e o Titular dos dados tem como consentir, revogar seu consentimento e verificar quais os consentimentos dados, de maneira inequívoca, a qualquer momento.

Os dados de Clientes são utilizados apenas quando necessário e somente pelos Colaboradores autorizados para tal, conforme descrito na Política de Concessão de Acessos. Os dados são mantidos/armazenados pela Pilotage Investimentos somente pelo tempo necessário à realização das atividades e/ou pelas regras impostas pelos agentes reguladores citados anteriormente.

Compartilhamento de Dados

Alguns dados de clientes são compartilhados com terceiros, para o correto desempenho da atividade de Gestão de Carteiras Administradas, como por exemplo a utilização de plataformas eletrônicas de negociação, o processamento de valoração das operações presentes nas carteiras e com o escritório de contabilidade para a escrituração contábil da Pilotage Investimentos.

Esses parceiros possuem ambientes controlados para garantir a segurança dos dados utilizados e também estabeleceram procedimentos para atendimento às solicitações de Titulares de dados.

A seguir listamos os parceiros da Pilotage Investimentos que têm acesso a dados de clientes:

Parceiro	Tipo de parceria	Dados compartilhados
Genial Investimentos Corretora de Valores S.A. CNPJ nº 27.652.684/0001-62	Plataforma de Negociação Eletrônica	Todos os dados referentes à identificação do Cliente, conforme ICVM 617, além dos ativos que compõem a Carteira de Investimentos do Cliente, bem como os valores financeiros envolvidos

Britech Consultoria e Tecnologia Ltda. CNPJ nº 09.069.233/0001-15	Plataforma de Backoffice, para registro e valoração das operações da Carteira dos Clientes	Todos os dados referentes à identificação do Cliente, conforme ICVM 617, além dos ativos que compõem a Carteira de Investimentos do Cliente, bem como os valores financeiros envolvidos
Adm Fernandes Organizacao Contabil CNPJ nº 03.280.212/0001-68	Escritório de Contabilidade	Dados básicos do Cliente para emissão de Nota Fiscal de Serviços de Administração de Carteira de Valores Mobiliários

Livre Acesso

A Pilotage Investimentos sabe que uma das premissas principais da LGPD diz respeito ao consentimento e ao livre acesso dos Titulares desses dados.

Dessa forma, o mapeamento de dados realizado pela Pilotage Investimentos está documentado e deixa claro quais os dados pessoais são utilizados, quem os acessa e sua forma de armazenamento nas dependências da Instituição.

No caso dos parceiros, a Área de Tecnologia da Pilotage Investimentos considerou adequados os recursos de segurança implantados e assim estabeleceu com esses parceiros um termo de compromisso, assegurando ao Titular dos dados o livre acesso aos mesmos.

Impressão e Cópias

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis no ambiente da Pilotage Investimentos e circulem em ambientes externos à Pilotage Investimentos com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas 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 Pilotage Investimentos 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.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Pilotage Investimentos.

Descarte de Informações

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, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, usando preferencialmente uma trituradora, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar hard drives, pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Pilotage Investimentos.

Restrições Comportamentais

Em nenhuma hipótese um Colaborador pode emitir opinião em nome da Pilotage Investimentos, ou utilizar material, marca e logotipos da Pilotage Investimentos para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno 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 Pilotage Investimentos.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Pilotage Investimentos. Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos.

A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

Monitoramento

A Pilotage Investimentos 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 Pilotage Investimentos para a atividade profissional de cada Colaborador.

Todas os documentos são armazenados no provedor de serviços em nuvem da Pilotage Investimentos, o Google Suíte Business. Nesse servidor, as informações são segregadas por área e respeitando os acessos individuais de cada colaborador, contando com as políticas de segurança e backup contratados da plataforma.

Em caso de divulgação indevida de qualquer informação confidencial, o Diretor de Compliance apurará o responsável por tal divulgação, sendo certo que poderá verificar quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

Em caso de vazamento, perda, furto ou roubo de quaisquer materiais ou equipamentos que contenham informações confidenciais, o Colaborador deverá notificar imediatamente o Diretor de Compliance sobre tal evento, por telefone, e-mail ou mensagem de texto.

Plano de Resposta a Incidentes de Segurança da Informação

É fundamental estar pronto e saber como agir diante de um incidente de segurança da informação.

Assim, os Colaboradores da Pilotage Investimentos devem estar preparados para responder ao incidente e saber como atuar num episódio dessa natureza, já que a resposta dada ao incidente e a reação da equipe são elementos importantes no estabelecimento das sanções e na sua quantificação.

Dado que esse ponto merece uma atenção especial, ainda mais levando-se em conta a entrada em vigor da Lei Geral de Proteção aos Dados (LGPD), a Pilotage Investimentos optou por criar um documento dedicado apenas a este assunto, destacando ainda o tratamento de incidentes envolvendo dados pessoais de clientes *("PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM DADOS PESSOAIS")*.

Testes Periódicos de Segurança

Além do tratamento dos alertas emitidos pela plataforma do Google Suite Business, são realizados testes de segurança para os sistemas de informações de duas plataformas externas utilizados pela Pilotage Investimentos, em periodicidade no mínimo anual, para garantir a efetividade dos controles internos mencionados neste documento, especialmente as informações mantidas em meio eletrônico.

Essas plataformas contam com protocolos seguros, que fazem uso de criptografia, assim como assinaturas e certificados digitais, para desempenhar suas atividades – a plataforma de negociação da Genial Investimentos, onde as operações envolvendo valores mobiliários são

realizadas e a plataforma de backoffice da Britech S/A, onde as operações realizadas na plataforma Genial são registradas e gerenciadas.

Como exemplo de relatório de teste dessas plataformas, temos:

Relatório de Resultados

Scan Full de Aplicação (SFA)
saas.britech.com.br
março 2020

Resumo gerencial

Dados Principais

URL	saas.britech.com.br
Data do scan	março 2020
ID do scan	c4f1020c-7b11-4f33-95e2-9f6c17437911
Tipo de scan	Scan Full de Aplicação (SFA)

Informativo

A exibição do Selo Site Blindado é proveniente da não existência de vulnerabilidades críticas no alvo analisado.

Em caso de apontamento de vulnerabilidades críticas, é imprescindível que as mesmas sejam corrigidas no período de 72 horas para que o Selo Site Blindado não deixe ser exibido.

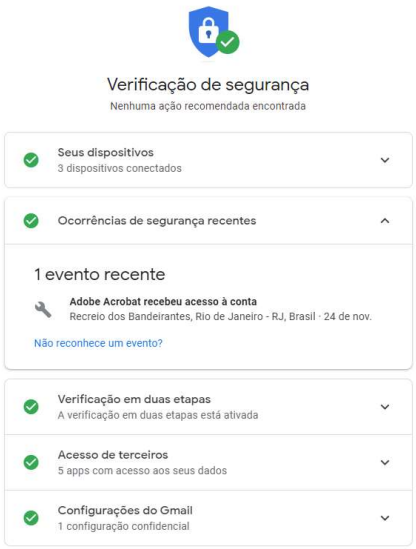
Riscos à Aplicação

O gráfico abaixo representa os apontamentos realizados neste scan e seus respectivos níveis de risco.

No caso das contas mantidas na plataforma Google, mensalmente é feita a verificação de ocorrências nas Contas de Usuários, relatando ações importantes, como:

- logins em novos dispositivos;
- mudanças de senha;
- mudanças nas informações de recuperação;
- pedidos para fazer o download dos seus dados.

Se houver uma ou mais dessas ações em uma conta, o Google enviará um alerta de segurança usando métodos como e-mail e notificações para os usuários e também poderão ser consultadas no endereço https://myaccount.google.com/security, como apresentado no exemplo abaixo:



Esse resultado será armazenado como evidência da realização do acompanhamento das contas de usuários, registradas no domínio *pilotage.com.br*.

Segurança Cibernética

A Segurança Cibernética é um conjunto de ações sobre pessoas, tecnologias e processos contra ataques cibernéticos, tendo como objetivo tratar e proteger os dados confidenciais armazenados em meio eletrônico.

Em tempos de troca de dados de maneira instantânea usando a internet e com o armazenamento de um volume de informações jamais visto, torna-se ainda muito mais importante classificar e proteger adequadamente os dados da Pilotage Investimentos.

Ataques Cibernéticos

É importante que todos tenham conhecimento sobre os principais tipos de ataques cibernéticos (ações executadas por criminosos, que usam vulnerabilidades de rede para atacar e roubar os dados confidenciais), que podem causar grandes danos à Pilotage Investimentos.

Sendo assim, os principais mecanismos utilizados pelos criminosos e que devem demandar especial atenção dos Colaboradores, são:

Vírus

O vírus é um programa ou código de código usado para danificar o computador, corromper os arquivos do sistema e destruir dados, ficando inativo na máquina até que seja executado,

podendo contaminar outros computadores da rede, roubar senhas e dados, corromper arquivos, encaminhar spam para contatos de e-mail ou, até mesmo, controlar o computador.

Worms

São mais antigos que vírus, chegando como anexos de mensagens. O que o torna tão devastador é sua capacidade de se espalhar sem ação direta do usuário.

Adware

É uma forma de software que exibe anúncios e coleta informações sobre o comportamento do usuário, podendo redirecionar a navegação para páginas da web parecidas com outras promoções de produtos.

Esse tipo de ataque tem como objetivo obter informações como: a localização, detalhes de senhas de acesso (palavras-passe) e endereços IP do computador ou correio eletrônico.

Ransomware

Também conhecido como "sequestrador digital", é um software malicioso que infecta o computador e exibe mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar. Essa classe de malware é um esquema de lucro criminoso, que pode ser instalado por meio de links enganosos em uma mensagem de e-mail, mensagens instantâneas ou sites.

Cavalo de Tróia

O *Trojan Horse*, ou Cavalo de Tróia, é um malware que se oculta em programas que parecem inofensivos ou tentam enganar o usuário para que o mesmo faça a instalação. Esse tipo de malware não se multiplica ou infecta outros arquivos - ele fica oculto coletando informações ou configurando brechas na segurança do sistema. Além disso, a infecção pode controlar o computador e bloquear o acesso do usuário a ele.

Spyware

É um software de espionagem praticamente invisível que funciona em segundo plano, sem ser notado, enquanto coleta dados ou fornece acesso remoto para o invasor.

É um dos malwares mais perigosos, visto que não causa danos somente ao dispositivo, mas também procura a identidade pessoal do usuário. Durante um ataque hacker, o spyware é útil na coleta de informações financeiras, como senhas, contas bancárias e dados de cartão de crédito.

Antivírus e Firewall

Todos os equipamentos utilizados pelos Colaboradores da Pilotage Investimentos contam com a proteção de software antivírus e firewall pessoal nativos do sistema operacional Windows *(Windows Defender)*.

Além disso, as plataformas externas utilizadas (Google Suite Business, Britech e Genial) também contam com proteção de antivírus e firewall.

Responsável pela Segurança da Informação

O sócio-diretor Alexandre França Fraga é o responsável designado para tratar de todos os assuntos relacionados à Segurança da Informação na Pilotage Investimentos.

Mensalmente, o responsável pela Segurança da Informação gera um relatório listando a ocorrência ou não de incidentes, bem como os planos de ação adotados para a mitigação dos mesmos, que é encaminhado para os membros do Comitê de Segurança da Informação.

Comitê de Segurança da Informação

O Comitê de Segurança da Informação atualmente é composto pelos sócios-diretores da Pilotage Investimentos, a saber:

- Alexandre França Fraga – Diretor de Risco e Compliance
- Marcelo Saddi Castro – Diretor de Gestão de Recursos
- Fábio de Aguiar Faria – Diretor Executivo

Competências do Comitê de Segurança da Informação

Compete ao Comitê de Segurança da Informação:

- elaborar propostas de normas e políticas de uso dos recursos de informação da Pilotage Investimentos.
- rever a Política de Segurança da Informação e normas relacionadas, no período máximo de 02 (dois) anos, e sugerir alterações;
- estabelecer diretrizes e definições estratégicas para as ações e projetos relacionados à Segurança da Informação;
- dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação e em normas relacionadas;
- propor e acompanhar planos de ação para aplicação da Política de Segurança da Informação, assim como campanhas de conscientização dos usuários;

- receber comunicações de descumprimento das normas referentes à Política de Segurança da Informação, instruí-las com os elementos necessários à sua análise e acompanhar os procedimentos para a sua correção;
- solicitar, quando necessário, a realização de auditorias, relativamente ao uso dos recursos de tecnologia da informação no âmbito da Pilotage Investimentos;
- elaborar relatório anual de suas atividades, disponibilizado para todos os Colaboradores da Pilotage Investimentos.