POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS PESSOAIS

VALORA
INVESTIMENTOS

Versão vigente: 09/10/2024
Versão anterior: Jun.22

Sumário

1. Escopo

Nossas informações são valiosas para os nossos processos de negócio, projetos e serviços. Por isso, precisamos estar atentos pela forma como qual manipulamos esta informação durante todo o ciclo de vida, com a devida segurança desde a coleta até o descarte.

Assim, o escopo desta Política consiste em apresentar a relevância da segurança da informação, segurança cibernética e proteção de dados pessoais para as Gestoras do Grupo Valora, as medidas necessárias, as políticas relacionadas e como manter a governança.

2. A quem se destina

Deverá ser implementada internamente e revista pelo Comitê da Lei Geral de Proteção de Dados e pelo Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer* - DPO).

3. Documentos relacionados

Este documento se relaciona com a:

- Política de gestão de acessos e identidades;
- Política de redes seguras;
- Política de segurança física e do ambiente;
- Política de segurança física;
- Política de criptografia;
- Política de cloud;
- Política de anonimização;
- Política de antivírus e antimalware;
- Política de redes sociais e mensagens eletrônicas;
- Política de classificação da informação;
- Política de BYOD;
- Política de home office seguro.

4. Referências

- Guia de Cibersegurança - ANBIMA, Edição 3 | 2021;
- Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H. Fundamentos de Segurança da Informação: com base na ISO 27001 e ISO 27002. Brasport, 1ª edição, 2018;
- Os Pilares da Segurança da Informação: Ian Ramone (Security Account Manager N&DC);
- LEI GERAL DE Proteção de Dados – Lei 13.709/18
- PROJETO ABNT PE-451.01 - Certificação de Sistemas de Gestão da Proteção e Privacidade de Dados Pessoais
- PROJETO ABNT NBR ISO/IEC 27001
- PROJETO ABNT NBR ISO/IEC 27701
- REGULAMENTO EUROPEU GDPR

- MARCO CIVIL DA INTERNET

5. Responsabilidades: O compromisso com a segurança da informação

Todos do Grupo Valora devem ter responsabilidade com a segurança das informações: as diretrizes estabelecidas nas políticas de segurança deverão ser seguidas por todos os colaboradores e se aplicam a todas as informações sob qualquer meio, eletrônico e físico.

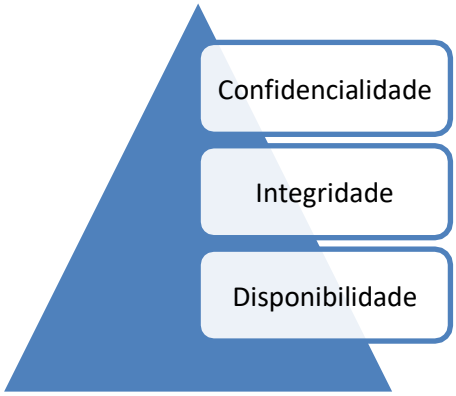
Todos na execução de suas tarefas devem ter a missão de cuidar da segurança das informações e não esperar que esta seja uma responsabilidade exclusiva da área de Tecnologia. Devem colaborar e cuidar para que somente pessoas autorizadas tenham acesso às informações e que os controles implementados sejam levados à sério no dia a dia.

Será de responsabilidade dos colaboradores:

- Proteger as informações do Grupo Valora e seus clientes: zelar para que as informações confidenciais, não caiam na mão de quem não deveria ter acesso;
- Cuidado redobrado para que não haja divulgação, perda, modificação ou destruição não autorizada;
- Descartar *("dia da faxina")* as informações que não há mais necessidade e finalidade, para continuar armazenando. O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.
- Se presenciar qualquer violação das políticas de segurança, deve imediatamente adotar as medidas presentes no PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA.

6. Os pilares da segurança da informação

São os três principais critérios de segurança da informação: Confidencialidade, Integridade e Disponibilidade (CID).



6.1. Confidencialidade

A confidencialidade é o grau em que o acesso às informações é restrito a um grupo definido e autorizado a ter esse acesso.

A troca de informações entre os colaboradores deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de compliance deve ser acionada previamente à revelação.

Nesse sentido, todas as mensagens enviadas/recebidas dos computadores disponibilizados pelo Grupo Valora permitem a identificação do seu remetente/receptor.

Garantir que a informação não esteja disponível ou revelada a indivíduos ou processos que não deveriam ter acesso, que não estão autorizados.

6.2. Integridade

A integridade garante que a informação não sofra uma alteração indevida; que a informação está exata e completa.

6.3. Disponibilidade

A disponibilidade garante que temos a informação disponível quando precisamos dela.

Além do CID (confidencialidade, integridade e disponibilidade), temos mais dois pilares complementares que são de extrema importância e relevância:

6.4. Autenticidade

A autenticidade garante que nada se perca no meio do caminho no processo de comunicação, os remetentes não passem por terceiros e nem que a mensagem sofra alterações.

6.5. Legalidade

A legalidade garante que as informações foram produzidas respeitando toda a legislação vigente.

7. Classificação da Informação

Consulte a política de classificação das informações para verificar todas as informações produzidas e armazenadas pelo Grupo Valora**.**

8. Home office seguro

O home office e o trabalho remoto se tornaram algo muito comum no Grupo Valora e para isto, devemos ter cuidado redobrado com a segurança.

Verifique a política de home office seguro para consultar todas as medidas de segurança que devem ser adotadas.

9. Política de gestão de acessos e identidades

Devemos levar em consideração o ciclo de vida das identidades dos colaboradores, desde o momento da admissão, no qual diversas contas e acessos são disponibilizados, observadas as barreiras de informação e potenciais conflitos de interesse eventualmente existentes. Verifique esta política para compreender as medidas eficazes para gestão dos acessos, senhas e autorizações, que devem fazer parte do nosso dia a dia.

10. Utilização da rede e dos equipamentos fornecidos pela Valora Gestão de Investimentos

Atenção: As considerações sobre o que podemos visualizar, fazer, navegar e utilizar, se aplicam tanto para o cenário do home office, quanto presencial, no escritório da empresa, ou outros locais.

Todos os colaboradores e terceiros, devem ler com atenção:

- a política de BYOD, que traz todas a medidas de segurança;
- a política de redes seguras;
- a política de home office seguro.

Ressaltamos abaixo, alguns pontos de atenção principais que estão explicados nas políticas supracitadas, bem como no nosso Código de Ética e Conduta:

- As máquinas, equipamentos de propriedade do Grupo Valora e a rede wi-fi, devem ser utilizados com a finalidade restrita à realização de atividades de trabalho;

- Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade do Grupo Valora**,** que pode analisar, monitorar, se necessário, com o objetivo de detectar e prevenir a execução de programas maliciosos, integridade da rede, dos dados etc. Podemos, ainda, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação que não esteja de acordo com as nossas políticas de segurança.

- A Internet disponibilizada pelo Grupo Valora aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, porém desde que não prejudique o andamento das suas atividades e entregas. Liberdade com responsabilidade!

- É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e restritas em listas de discussão, repositórios públicos, redes sociais, sites, fóruns, WhatsApp ou qualquer outra tecnologia correspondente, podendo se aplicar as penalidades previstas nas legislações correspondentes e procedimentos internos, em caso de divulgação e/ou compartilhamento indevido.

- O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo Grupo Valora**.**

- Os colaboradores não poderão, em hipótese alguma, utilizar os recursos do Grupo Valora para fazer download ou distribuição de *softwares piratas.*

- Como regra geral, materiais de cunho sexual, difamatório, apologia ao tráfico de drogas, pedofilia, materiais ofensivos e discriminatórios, são expressamente proibidos. Não poderão de maneira alguma serem acessados, expostos, armazenados, compartilhados ou gravados, por meio de qualquer recurso, ressaltando que, em caso de descumprimento dessas regras, podem ser aplicadas as penalidades previstas nas legislações correspondentes e procedimentos internos.

- Os colaboradores não poderão usar os recursos do Grupo Valora para propagar qualquer tipo de vírus e de malware. Verifique nossa política de antivírus e antimalware. Consulte as medidas para manter seu acesso seguro, na política de BYOD e Home office seguro.

11. Redes sociais e uso do e-mail

Apenas colaboradores devidamente autorizados podem falar em nome do Grupo Valora nos meios de comunicação, redes sociais e afins. As redes sociais e o uso de mensagens eletrônicas fazem parte do nosso dia a dia, por isso, leia com muita atenção a política de redes sociais e mensagens eletrônicas.

12. Notebooks

Deve fazer parte das responsabilidades do colaborador cuidar do seu equipamento, zelar e manter em boas condições. Somente pessoas autorizadas, devem realizar instalações, ajustes e reparações.

É de responsabilidade do colaborador tudo que for executado na sua máquina, portanto, todos devem ter muita atenção com o que acessam, compartilham, divulgam e armazenam.

Todos devem ler com muita atenção a política de BYOD e aplicar as medidas de segurança.

13. Plano de continuidade e backup

Devemos ter atenção com a gestão da continuidade e precisamos cuidar da integridade das informações para evitar as perdas e indisponibilidade.

Para isso, o Grupo Valora deve preparar, manter e testar o plano de backup e continuidade, que inclua:

- recuperação (restaurar) de todos os seus dados de forma íntegra, caso um incidente de perda de dados venha a ocorrer;
- cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da empresa;
- backups devem ser automatizados;
- infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados;

Testes regulares de back-up serão conduzidos para garantir a integridade e a eficácia dos procedimentos de recuperação.

A contratação de serviços de processamento e armazenamento de dados e de computação em nuvem deverá observar as regras e procedimentos descritos na Política de Seleção, Contratação e Monitoramento dos Prestadores de Serviço adotada internamente, cujo processo de due diligence será coordenado pela equipe de Compliance com apoio das áreas interessadas.

É importante estar ciente das diretrizes apontadas em nossa Política de Contingência.

14. Riscos Cibernéticos

Considerando a atividade de gestão profissional de recursos de terceiros desempenhada pelo Grupo Valora são essenciais todos os recursos tecnológicos necessários ao processo de análise, investimento e desinvestimento, tais como: (i) compra e venda de ativos para as carteiras sob gestão; (ii) conferência e liberação das carteiras; e (iii) acesso aos sistemas de informação.

Diante da possibilidade de invasores utilizarem (i) *Malware*, (ii) Engenharia social; (iii) Ataques de DDos (*distributed denial of services*) e *botnets*; e (ix) Invasões (*advanced persistent threats*), o Grupo adota as seguintes ações de prevenção e proteção:

AÇÕES DE PREVENÇÃO E PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS E SEGURANÇA CIBERNÉTICA
Acesso Escalonado do Sistema
O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance, Risco e PLD e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores. O Grupo Valora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede do Grupo Valora necessária ao exercício de suas atividades. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas do Grupo Valora em caso de violação.

Senha e Login
A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas **semestralmente**, conforme aviso automático, programado no e-mail pela área de informática. Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.
Uso de Equipamentos e Sistemas
Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. A utilização dos ativos e sistemas do Grupo Valora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional. Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Diretor de Compliance, Risco e PLD.
Acesso Remoto
O Grupo Valora permite o acesso remoto pelos Colaboradores ao e-mail, rede e diretório, conforme requisição por estes e autorização pelo responsável da área.
Controle de Acesso
O acesso de pessoas estranhas ao Grupo Valora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da respectiva Gestora. Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, as Gestoras monitoram a utilização de tais meios.
Firewall, Software*, Varreduras e *Backup
As Gestoras utilizam um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance, Risco e PLD é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede). As Gestoras mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras **diárias** para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede das Gestoras.

As Gestoras utilizam um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance, Risco e PLD é responsável por patches regulares nos sistemas das Gestoras.

As Gestoras mantêm e testam regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance, Risco e PLD. As informações das Gestoras são atualmente objeto de backup **diário** com o uso de computação na nuvem.

São mantidos inventários atualizados de *hardware* e *softwares* utilizados pelo Grupo Valora. Em tempo real são realizadas verificações, a fim de identificar elementos estranhos, tais como computadores não autorizados ou softwares não licenciados.

Sempre que houver alteração relevante na estrutura tecnológica serão realizadas análises de vulnerabilidade.

Os colaboradores devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade no Grupo Valora.

15. Gestão de incidentes

Qualquer evento que possa impactar na segurança da informação, inclusive o vazamento de informações confidenciais, deve ser reportado como um incidente de segurança e seguir o Plano de Resposta a Incidentes a seguir apresentado.

Todos os incidentes devem ser detectados, analisados e tratados. Da mesma forma, as medidas para resolução devem ser registradas na base de conhecimento e compartilhadas como lições aprendidas e melhoria contínua da segurança.

O Diretor de Compliance, Risco e PLD responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos das Gestoras de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão das

Gestoras, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
(vii) Determinação do responsável (ou seja, às Gestoras ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, Risco e PLD, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

16. Regulamentos, legislações e processos disciplinares

O Grupo Valora se mantém em conformidade com as legislações e diretrizes pertinentes à sua área de atuação, com a devida atenção à segurança e as boas práticas do mercado.

Em caso de não cumprimento ou violação desta política, bem como, das demais regulamentações, por quaisquer pessoas, essas poderão ser passíveis de processos disciplinares, responsabilização cível, administrativa ou penal.

17. Tratamento de Dados Pessoais

Em relação ao tratamento de dados pessoais, devemos estar atentos e manter nossos processos em conformidade com a Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018.

O tratamento de Dados Pessoais e Dados Pessoais Sensíveis consiste em toda e qualquer operação realizada com tais dados, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

As atividades de tratamento de Dados Pessoais e Dados Pessoais Sensíveis deverão observar a boa-fé e os seguintes princípios:

(i) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(ii) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

(iii) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

(iv) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;

(v) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vi) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(vii) segurança: utilização de medidas 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 difusão;

(viii) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;

(ix) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

(x) responsabilização e prestação de contas: demonstração, pelo Grupo Valora, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

O tratamento de Dados Pessoais e Dados Pessoais Sensíveis só será realizado nas seguintes hipóteses:

(i) para o cumprimento de obrigação legal ou regulatória pelo Grupo Valora;

(ii) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

(iii) quando necessário para atender aos interesses legítimos do Grupo Valora ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais e Dados Pessoais Sensíveis;

(iv) mediante o fornecimento de consentimento pelo titular por escrito ou outro meio que demonstre a manifestação de vontade do titular; ou

(v) para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

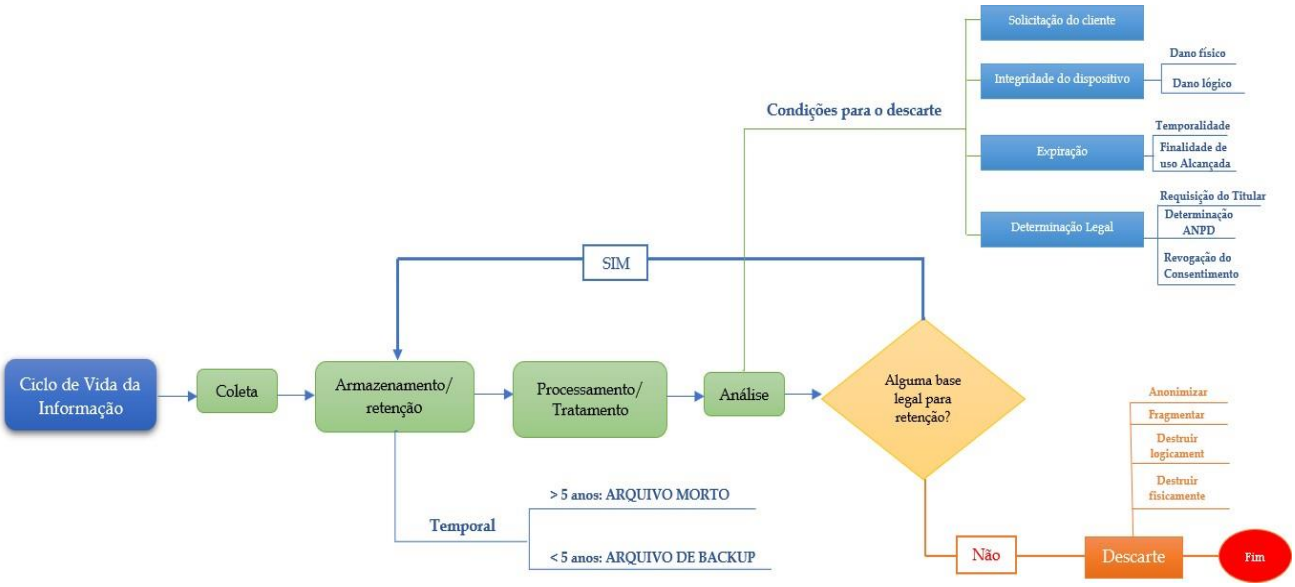
O Grupo Valora manterá registro das operações de tratamento de Dados Pessoais e Dados Pessoais Sensíveis que realizar, especialmente quando baseado no seu legítimo interesse.

Em caso de dúvidas, consulte nosso aviso de privacidade ou procure o Encarregado de Proteção de Dados através do e-mail: dpo@valorainvest.com.br .

18. Ciclo de Vida da Informação

Toda a informação tem um ciclo estabelecido e os processos que a cercam devem observar e seguir as fases de seu ciclo de vida de acordo com o seu estado de utilização.

Segue o fluxograma com as principais fases do ciclo de vida da informação:



19. Segurança física e dos ambientes

Devemos manter os ambientes do Grupo Valora protegidos contra acessos não autorizados. O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros. Todas as medidas que devem ser seguidas estão descritas na Política de Segurança Física e do Ambiente.

20. Comunicação

Esta política deve ser disseminada e compartilhada por todos no Grupo Valora**,** fazendo parte da nossa cultura de privacidade e proteção de dados, afinal: *"A segurança da informação é o berço da proteção de dados".*

Todas as medidas de segurança da informação, segurança cibernética e proteção de dados devem ser reforçadas periodicamente nas ações de comunicação interna e treinamentos contínuos.

O treinamento levará em consideração o tratamento das informações confidenciais e, no que se refere ao tratamento de Dados Pessoais e Dados Pessoais Sensíveis, abordará aspectos como: (i) natureza; (ii) escopo; (iii) finalidade; (iv) probabilidade e a gravidade de riscos; (v) benefícios decorrentes do tratamento de dados.

Os procedimentos e rotinas definidos na presente Política serão abordados em treinamento anual, coordenado pelo Diretor de Compliance ou terceiro contratado para esta finalidade, visando a sua disseminação entre a equipe.

Revisão:

A presente política deverá ser revisada anualmente com atualizações que se julguem necessárias para a garantia da segurança da informação.

QUADROS DE APROVAÇÃO E DE CONTROLE DE MANUTENÇÃO DA POLÍTICA

Data Atualização	Responsável	Aprovação
09/10/2024	MP	DP
20/06/2022	MP	DP
28/01/2019	MP	DP
10/01/2018	MP	DP
24/02/2017	MP	DP
27/08/2015	MP	DP

ANEXO

ACESSOS E PROCEDIMENTOS ADICIONAIS

Mapeamento dos Diretórios:
Perfil de acesso por área;
Definição de usuário por área.

Sistemas Internos:

Anima
Advice
Totvs
OrderBy
Phibra
Bloomberg
Economática
Comdinheiro

Sistemas Externos:

Bradesco Net Empresas;
Bradesco Custódia;
BTG Extranet;
Santander custódia;
SMA BNY Mellon;
Salesforce.

Issues:

1) Solicitar aos gestores a separação das pessoas em grupos de acesso para a definição dos acessos como somente leitura ou leitura e gravação.

ANEXO

TERMO DE COMPROMISSO E RESPONSABILIDADE –
POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Declaro ter conhecimento, estar de pleno acordo e comprometo-me a respeitar as regras consubstanciadas na Política de Segurança de Informação, Segurança Cibernética e Proteção de Dados Pessoas do Grupo Valora, dedicando especial cuidado aos seguintes aspectos:

1) Atentar para o fato de que os produtos e serviços do Grupo Valora são sua propriedade, e a contribuição que os colaboradores dão ao desenvolvimento e implementação de tais produtos e serviços, durante seu período empregatício, faz com que os mesmos sejam propriedade do Grupo Valora e continuarão a sê-lo, mesmo se o Colaborador deixar o Grupo;
2) Não violar a Política de Segurança de Informação, Segurança Cibernética e Proteção de Dados Pessoais ou tentar "acessos não autorizados" à rede do Grupo Valora;
3) Utilizar de forma adequada e correta os equipamentos de informática, sistemas e telefonia disponibilizados para a execução do meu trabalho;
4) Não divulgar ou facilitar o uso de minha senha pessoal de acesso à rede de computadores do Grupo Valora e a seus aplicativos;
5) Não praticar ou permitir que terceiros pratiquem atos que possam trazer danos potenciais ao Grupo Valora, como vírus ou acessos indevidos à rede de computadores;
6) Não discutir informações confidenciais de trabalho em ambientes públicos (tais como restaurantes, aeroportos...)

Autorização:
Autorizo o Grupo Valora a efetuar a gravação, reprodução, divulgação, e escuta de minhas conversas telefônicas efetuadas no escritório, bem como das mensagens eletrônicas (MSN) trocadas dentro do Grupo Valora, a monitorar o uso da internet e correio eletrônico e a tomar as devidas providências, caso constate violação da política de segurança da informação.

Vigência e Formalização:
O presente Termo vigorará por tempo indeterminado e permanecerá válido mesmo após o meu desligamento da Valora Gestão de Investimentos, podendo ser utilizado caso o Termo aqui assinado seja quebrado por algum motivo.

Para tanto, assino o presente Termo de Compromisso e Responsabilidade, declarando-me ciente de que a displicência ou descumprimento de quaisquer normas estabelecidas na Política de Segurança de Informação, Segurança Cibernética e Proteção de Dados Pessoais poderá acarretar punições disciplinares, além da obrigação de ressarcir o Grupo Valora de eventuais prejuízos decorrentes das falhas ou omissões por mim cometidas.

São Paulo,_____de_____20___

_____
Nome: