Política de Segurança da Informação da Aggrandize

Políticas corporativas

AGGRANDIZE TECNOLOGIA DA INFORMAÇÃO LTDA

E-mail: contato@aggrandize.com.br
Telefone: +55 (53) 3307-0304
Site: www.aggrandize.com.br

Pelotas Parque Tecnológico
Av. Domingos de Almeida, 1785, Sala 08
Areal, Pelotas - RS, 96085-470

Controle de Versão

Versão	Data	Autor	Descrição das alterações	Revisado por
0.1	13/09/2023	Fladhimyr Castello	Criação do documento inicial	Dartagnan Farias
0.2	31/05/2024	Dartagnan Farias	Adição de controles de acordo com RFP Consolidada	Fladhimyr Castello
0.3	19/06/2024	Dartagnan Farias	Ajustes de numeração de seções; Inclusão de competências CISO, Comitê de segurança; Inclusão de competências noc & soc; Ajuste de competências colaboradores.	Fladhimyr Castello
0.4	03/07/2024	Dartagnan Farias	Remoção do termo de compromisso.	Fladhimyr Castello
0.5	09/08/2024	Fladhimyr Castello	Redistribuição das responsabilidades do CISO, Comitê de segurança, Diretoria e Sócios.	Dartagnan Farias

Tabela1. Controle de versão do documento.

Política de Segurança da Informação da Aggrandize

Políticas corporativas

1. Disposições preliminares

A Política de Segurança da Informação da Aggrandize (PSIA) define diretrizes e atribuições a serem seguidas pelos Colaboradores da Aggrandize na execução de suas as atividades no tocante a segurança dos dados e informações.

Para os fins desta política, são considerados Colaboradores da Aggrandize todos os funcionários integrantes do quadro de pessoal, os estagiários, os sócios, os diretores e demais prestadores de serviço. Também são considerados colaboradores, aqueles que estejam em licença, férias ou por outro motivo afastado.

2. Recursos computacionais

Entende-se por recursos computacionais todos e quaisquer recursos de software ou hardware utilizados para acesso a dados, informações e sistemas de informações.

A Aggrandize disponibiliza seus recursos computacionais, em comodato, a seus colaboradores[1], como ferramenta para que estes conduzam seu trabalho de forma profissional e ética. Espera-se que os colaboradores acessem unicamente as informações e sistemas de informação necessários para exercer as atividades e responsabilidades a eles atribuídas para as suas funções e/ou prestação de serviços.

Os recursos computacionais não devem ser utilizados para a propagação de e-mail ou documentos com conteúdo inapropriado que promova, incite ou instrua ações e atitudes, tais como: crime, roubo, violência, terrorismo, difamação, calúnia, preconceito de qualquer tipo ou classe, drogas e pornografia.

O acesso a qualquer site da internet através de equipamentos da Aggrandize está restrito às atividades necessárias ao bom desempenho profissional. A Aggrandize se reserva o direito de, sem aviso prévio, monitorar o uso da internet pelo Colaborador.

É proibido instalar, nos computadores da Aggrandize, softwares para os quais não se tenha a licença de uso correspondente.

Para colaboradores que utilizem equipamentos próprios espera-se que os mesmos cuidados sejam observados.

3. Objetivos

São objetivos desta política:

[1] Exclui-se na política estagiários e prestadores de serviços, que são casos tratado individualmente.

I. Estimular um ambiente corporativo de fluidez e segurança das informações.
II. Orientar os Colaboradores da Aggrandize quanto às práticas de segurança da informação.

4. Papéis e responsabilidades

Compete a todos os Colaboradores:

I. Comprometer-se com a observância, aplicação e efetividade das diretrizes da Política de Segurança da Informação, inclusive participando dos treinamentos disponibilizados pela Aggrandize.
II. Proteger a integridade, a disponibilidade, a privacidade e a confidencialidade dos dados e informações da Aggrandize e de qualquer pessoa física ou jurídica que mantenha relações comerciais com a Aggrandize.
III. Utilizar, de forma responsável, profissional, ética e legal todos os recursos computacionais disponibilizados pela Aggrandize, conforme descrito no Código de Ética e conduta Aggrandize.
IV. Não copiar, instalar ou alterar software e/ou configurações de software e hardware sem autorização formal do NOC & SOC.
V. Comunicar à área ao NOC & SOC qualquer incidente que possa comprometer a segurança das informações.
VI. Aos usuários de notebooks é permitido o acesso às redes de terceiros, desde que respeitadas as regras desta política bem como a política de segurança de informação dos terceiros.
VII. Caso haja utilização de equipamentos comodatos os colaboradores necessitam atuar em conformidade com as cláusulas do Contrato de Comodato de Equipamentos Aggrandize.
VIII. Caso haja utilização de equipamentos de propriedade pessoal os colaboradores necessitam atuar em conformidade com a Política de Segurança BYOD da Aggrandize;

Compete aos Sócios:

IX. Supervisionar a implementação e a execução das atividades destinadas à segurança das informações;

Compete à Diretoria:

X. Estabelecer uma cultura organizacional pautada pela livre circulação segura de informações na Aggrandize;
XI. Aprovar e supervisionar a implementação do Plano de Continuidade de Negócios e do Plano de Recuperação de Desastres;
XII. Aprovar a Política de Segurança das Informações e suas revisões, observando as disposições legais.

Compete ao Comitê de Segurança da Informação:

XIII. Revisar a Política de Segurança da Informação e outras políticas relacionadas, garantindo que estejam alinhadas com os objetivos estratégicos da Aggrandize e com as regulamentações aplicáveis.
XIV. Monitorar e garantir que a Aggrandize esteja em conformidade com todas as leis, regulamentações e normas aplicáveis, como a ISO/IEC 27001, LGPD e outras.
XV. Revisar a implementação dos Planos de Continuidade de Negócios e de Recuperação de Desastres, garantindo que sejam testados e atualizados regularmente.
XVI. Revisar a implementação dos Planos de Continuidade de Negócios e de Recuperação de Desastres, garantindo que sejam testados e atualizados regularmente.
XVII. Promover uma cultura organizacional que valorize a segurança da informação, incentivando boas práticas e a adesão às políticas de segurança entre todos os colaboradores.
XVIII. Coordenar e conduzir auditorias internas de segurança da informação para assegurar a conformidade com as políticas e procedimentos estabelecidos.

Compete ao NOC & SOC:

XIX. Criar processos e procedimentos para zelar os recursos computacionais da Aggrandize.
XX. Desenvolver e manter um book de acesso com perfis definidos para onboarding de usuários ou movimentação interna.
XXI. Desenvolver um padrão de segregação de função documentado para sistemas e informações.
XXII. Realizar revisões periódicas de acessos privilegiados.
XXIII. Autorizar e/ou conceder permissão para que os Colaboradores tenham acesso aos recursos computacionais.
XXIV. Adotar medidas emergenciais para preservar a segurança dos recursos computacionais, dados e informações, incluindo a suspensão, bloqueio ou alteração de contas e senhas.
XXV. Efetuar e/ou autorizar qualquer tipo de alteração e reparo interno ou externo nos recursos computacionais da Aggrandize.
XXVI. Implementar ferramentas de contenção automatizada de ataques.
XXVII. Implementar processos automatizados para criação, movimentação e revogação de acessos.
XXVIII. Estabelecer metodologias para coleta de indicadores de acesso aos sistemas.
XXIX. Realizar avaliações periódicas de vulnerabilidades e gerir incidentes de segurança.
XXX. Gerenciar o ciclo de vida dos ativos de TI, incluindo a substituição de equipamentos e sistemas obsoletos.
XXXI. Monitorar a capacidade e o desempenho da infraestrutura de TI e garantir a escalabilidade necessária.
XXXII. Garantir que todos os softwares instalados possuam licenças válidas.
XXXIII. Implementar e monitorar o uso de segundo fator de autenticação para acessos aos sistemas.
XXXIV. Monitorar eventos de segurança em regime 24x7.
XXXV. Definir indicadores de segurança e monitorar periodicamente os acessos de usuários, incluindo os acessos privilegiados;
XXXVI. Realizar análises regulares de riscos de segurança da informação, identificando ameaças, vulnerabilidades e impactos, e recomendando medidas de mitigação.

XXXVII. Realizar revisões periódicas de acessos privilegiados.
XXXVIII. Implementar os planos de mitigação de riscos aprovados pelo Comitê de Segurança.
XXXIX. Desenvolver e executar programas de treinamento e conscientização em segurança da informação para todos os colaboradores

Compete ao CISO (Chief Information Security Officer):

XL. Desenvolver e executar a Política de Segurança da Informação e outras políticas relacionadas, alinhando-a com os objetivos de negócios da Aggrandize.
XLI. Desenvolver os planos de mitigação de riscos.
XLII. Garantir a conformidade operacional com as normas e regulamentações de segurança aplicáveis (por exemplo, ISO/IEC 27001), conforme orientado pelo Comitê de Segurança.
XLIII. Supervisionar a criação, atualização e implementação de políticas, procedimentos e padrões de segurança da informação, conforme aprovado pelo Comitê de Segurança.
XLIV. Gerenciar a resposta a incidentes de segurança, incluindo a investigação, a análise pós-incidente e a implementação de ações corretivas.
XLV. Monitorar e relatar regularmente ao Comitê de Segurança da Informação o estado da segurança da informação, incluindo riscos, incidentes e eficácia dos controles implementados.
XLVI. Trabalhar com outras áreas de negócio para integrar a segurança da informação em todos os processos, promovendo a cooperação e a coordenação através do Comitê de Segurança da Informação.
XLVII. Liderar a equipe de segurança da informação, promovendo o desenvolvimento contínuo de habilidades e capacidades da equipe.
XLVIII. Avaliar e recomendar novas tecnologias e soluções de segurança para proteger os ativos de informação da Aggrandize.
XLIX. Desenvolver e atualizar processo de descarte de informações sensíveis.
L. Desenvolver o Plano de Continuidade de Negócios e o Plano de Recuperação de Desastres.
LI. Planejar e coordenar a implementação de controles de segurança da informação, incluindo controles técnicos, administrativos e físicos.
LII. Avaliar continuamente a eficácia dos controles de segurança da informação e recomendar melhorias.
LIII. Supervisionar a resposta a incidentes de segurança, garantindo uma resposta eficaz e a recuperação rápida dos sistemas afetados, além de coordenar a análise pós-incidente e a implementação de ações corretivas.
LIV. Desenvolver e implementar programas de treinamento e conscientização em segurança da informação para todos os colaboradores da Aggrandize.
LV. Informar regularmente à diretoria sobre o estado da segurança da informação, incluindo riscos, incidentes, conformidade e a eficácia dos controles implementados.

5. Disposições finais

Esta política deve ser objeto de atualização periódica, no mínimo a cada 2 anos, objetivando refletir as alterações ocorridas nos ambientes interno e externo da Aggrandize.