POLÍTICA DE GERENCIAMENTO DE CRISE

1. Introdução

O Grupo ISG é uma holding que atua nos setores de prestação de serviços e nos segmentos educacional, inovação e tecnologia. A continuidade dos negócios é essencial para garantir a resiliência e sustentabilidade das operações, protegendo os ativos, investidores, clientes, colaboradores e parceiros comerciais. Reconhecendo que incidentes podem ocorrer a qualquer momento, o Grupo ISG prepara-se para responder eficazmente e recuperar rapidamente as atividades.

Esta Política de Gerenciamento de Crise estabelece diretrizes e procedimentos para identificar, avaliar e mitigar riscos que possam comprometer a continuidade das operações do Grupo ISG. Além disso, assegura que todas as empresas do Grupo fiquem prontas para enfrentar crises, minimizando interrupções e preservando a reputação corporativa. Esta Política abrange desde a análise de impacto nos negócios até a implementação de planos de recuperação e estratégias de comunicação, promovendo um ambiente de negócios seguro, transparente e confiável.

2. Objetivo

O objetivo desta política é definir um conjunto de ações e responsabilidades que garantam a continuidade dos negócios do Grupo ISG, abrangendo todas as empresas que integram a holding. Pretende assegurar a capacidade de resposta a incidentes, minimizar interrupções operacionais e proteger os interesses da empresa incluindo a preservação da imagem diante dos acionistas, fornecedores, clientes, parceiros e colaboradores.

3. Escopo

Esta Política aplica-se a todos os colaboradores, terceiros, fornecedores e parceiros de negócios do Grupo ISG e abrange todas as operações e atividades críticas da empresa.

4. Diretrizes gerais

As diretrizes para a Política de Gerenciamento de Crise estabelecem os princípios fundamentais e procedimentos para garantir que o Grupo ISG possa continuar operando durante e após eventos disruptivos. A continuidade dos negócios é essencial para manter

a confiança dos clientes, proteger os ativos da empresa e garantir a viabilidade a longo prazo. Para isso deve-se observar as seguintes diretrizes:

4.1 Desenvolver e implementar planos de resiliência que permitam a rápida recuperação das operações essenciais após um incidente disruptivo.

4.2 Proteger os dados sensíveis e garantir a continuidade dos sistemas de informação e tecnologia, minimizando os riscos de perda de dados e interrupções tecnológicas.

4.3 Implementar estratégias para preservar e proteger a imagem e reputação do Grupo ISG durante e após crises, garantindo a confiança dos investidores, acionistas, clientes, colaboradores e parceiros comerciais.

4.4 Assegurar que todos os membros da equipe de resposta estejam devidamente treinados sobre situações que podem ocorrer durante crise e preparados para agir rapidamente e eficazmente em situações de urgência.

4.5 Garantir uma comunicação clara e transparente com todas as partes interessadas durante e após incidentes, fornecendo informações precisas e oportunas para mitigar rumores e preservar a confiança.

4.6 Revisar e atualizar regularmente os planos de continuidade de negócios para refletir mudanças nos riscos, operações e ambiente de negócios, incorporando feedback de exercícios e incidentes reais.

4.7 Assegurar que todos os processos de continuidade de negócios estejam em conformidade com normas e regulamentos nacionais e internacionais aplicáveis, como a NBR ISO 22301:2020.

4.8 Minimizar os impactos financeiros resultantes de interrupções nas operações, implementando estratégias de mitigação de riscos e planos de recuperação eficientes.

4.9 Promover a sustentabilidade operacional a longo prazo, garantindo que todas as operações possam ser mantidas e recuperadas de forma eficiente em qualquer cenário de crise.

4.10 Estabelecer procedimentos claros e eficazes para a recuperação e reconstrução de operações afetadas, assegurando que a holding possa voltar a operar normalmente o mais rápido possível após um incidente.

4.11 Promover uma cultura organizacional que valorize a resiliência e a continuidade dos negócios, incentivando todos os colaboradores a participar ativamente dos processos de planejamento e recuperação.

4.12 Implementar um sistema contínuo de monitoramento e avaliação de riscos, permitindo a identificação precoce de ameaças e a adoção de medidas preventivas adequadas.

4.13 Priorizar a saúde e segurança dos colaboradores durante incidentes, assegurando que os planos de continuidade incluam medidas adequadas de proteção e bem-estar.

4.14 Garantir que as atividades de todas as Unidades de Negócios do Grupo ISG possam continuar sem interrupções significativas, promovendo a adaptação ao trabalho a fim de não interromper as atividades.

4.15 Alinhar os planos de continuidade de negócios com a estratégia corporativa do Grupo ISG, garantindo que as ações tomadas em momentos de crise suportem os objetivos de longo prazo da holding.

5. Análise de impacto nos negócios

5.1 Cada empresa do grupo deve identificar seus processos críticos e avaliar o impacto de possíveis interrupções.

5.2 Realizar uma avaliação de riscos para identificar vulnerabilidades e ameaças que possam comprometer a continuidade dos negócios da holding.

6. Planos de continuidade de negócios (PCNs) deve conter:

6.1 Estando em crise, cada Unidade de Negócio deve desenvolver e manter um Plano de Continuidade de Negócios, alinhado com os objetivos estratégicos do Grupo ISG.

6.2 Incluir procedimentos detalhados para resposta a incidentes, recuperação de desastres e comunicação durante crises.

6.3 Estabelecer uma equipe dedicada à continuidade de negócios, responsável por coordenar as atividades de planejamento, resposta e recuperação.

6.4 Definir claramente os papéis e responsabilidades de todos os colaboradores envolvidos nos PCNs.

7. Diretrizes específicas

7.1 Desenvolver estratégias para garantir a continuidade das atividades acadêmicas, incluindo a transição para o ensino a distância em caso de interrupções.

7.2 Implementar medidas de proteção e recuperação de dados a respeito das empresas e dos atendimentos.

7.3 Assegurar a resiliência dos sistemas tecnológicos, incluindo redundância de infraestrutura e backup regular de dados.

7.4 Fortalecer a segurança cibernética para proteger contra ameaças que possam comprometer a continuidade dos serviços tecnológicos.

7.5 Implementar medidas para assegurar a disponibilidade contínua dos sistemas de inteligência artificial, incluindo arquiteturas redundantes e planos de failover.

7.6 Plano de *failover* é o processo de alternar automaticamente para um sistema redundante ou backup quando o sistema primário falha. Isso é feito para garantir que os serviços e operações continuem sem interrupções perceptíveis ou com o mínimo de tempo de inatividade. A implementação de planos de failover é muito importante para:

7.6.1 Garantir a disponibilidade contínua de serviços críticos.

7.6.2 Minimizar o tempo de inatividade durante falhas inesperadas.

7.6.3 Proteger contra perdas de dados e impactos negativos nas operações comerciais.

7.6.4 Manter a confiança dos clientes e a reputação da empresa.

7.7 Estabelecer processos contínuos de monitoramento e manutenção dos sistemas de IA para prever e mitigar falhas antes que causem interrupções significativas.

7.8 Conduzir testes regulares de resiliência para avaliar a capacidade dos sistemas de IA de resistir e se recuperar de incidentes disruptivos.

8. Gestão de dados e inovação

8.1 Garantir a segurança e integridade dos dados em geral utilizados e gerados pelos sistemas de IA implementando criptografia, backups regulares e medidas de proteção contra perda de dados.

8.2 Assegurar que a gestão dos dados permaneça em conformidade com normas e regulamentos aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).

8.3 Desenvolver processos que permitam a rápida adaptação e integração de novas tecnologias e inovações nos sistemas de IA garantindo que o Grupo ISG permaneça na vanguarda tecnológica.

8.4 Investir continuamente em pesquisa e desenvolvimento para melhorar a robustez e a eficiência dos sistemas de IA incluindo o uso de tecnologias emergentes como aprendizado de máquina e big data.

8.5 Estabelecer parcerias estratégicas com outras organizações e instituições de pesquisa para fortalecer as capacidades de inovação e garantir a continuidade dos avanços tecnológicos.

9. Mapa estratégico e Avaliação de Desempenho

9.1 Criar um mapa estratégico que alinhe os objetivos de continuidade de negócios com a missão e visão do Grupo ISG, facilitando a comunicação e execução das estratégias.

9.2 Definir objetivos e metas específicas para a continuidade de negócios, baseados em uma análise detalhada dos riscos e impactos potenciais.

9.3 Estabelecer indicadores para monitorar e avaliar a eficácia dos planos de continuidade de negócios, tais como tempo de recuperação, disponibilidade dos sistemas e número de incidentes.

9.4 Utilizar ferramentas de avaliação para acompanhar o progresso e identificar áreas de melhoria.

10. Ferramentas de gestão e plano de recuperação

10.1 Implementar softwares específicos para gestão de continuidade de negócios que auxiliem na criação, manutenção e execução dos PCNs.

10.2 Utilizar plataformas de comunicação robustas para garantir a rápida disseminação de informações críticas durante incidentes.

10.3 Definir objetivos claros para a recuperação das operações, priorizando os processos críticos e minimizando os impactos negativos.

10.4 O plano deve incluir estratégias de recuperação, recursos necessários, cronogramas e responsabilidades específicas.

11. Implementação e execução

11.1 Realizar testes e exercícios regulares para validar a eficácia do plano de recuperação e ajustar conforme necessário.

11.2 Revisar e atualizar o plano de recuperação periodicamente para refletir mudanças nas operações, tecnologia e ambiente de negócios.

12. Comunicação e treinamento

12.1 Desenvolver um plano de comunicação detalhado para informar todas as partes interessadas sobre os passos de recuperação e status das operações.

12.2 Realizar treinamentos periódicos para garantir que todas as equipes estejam familiarizadas com os procedimentos de recuperação e possam agir prontamente em caso de incidentes.

13. Gestão da imagem e reputação

13.1 Reconhecer que o processo de recuperação judicial pode afetar não apenas a reputação da empresa, mas também a confiança de fornecedores, clientes e parceiros comerciais.

13.2 Implementar estratégias de comunicação eficazes para gerenciar a percepção pública e proteger a imagem corporativa durante e após incidentes disruptivos.

13.3 Garantir que a recuperação dos negócios esteja devidamente preparada para atuar em diversas frentes, prevenindo ou mitigando impactos negativos à imagem do Grupo ISG.

14. Criação de um Comitê de Gerenciamento de Crise

Deve ser criado um Comitê de Gerenciamento de Crise, formado por pelo menos quatro integrantes e o Diretor de Compliance. Esse Comitê é responsável pela supervisão e implementação desta Política. Suas responsabilidades incluem:

14.1 Desenvolvimento e manutenção do Plano de Continuidade de Negócios (PCN).

14.2 Revisão e atualização periódica da Política e dos Planos.

14.3 Coordenação de testes e exercícios de continuidade.

14.4 Comunicação desta Política e procedimentos a todos os colaboradores.

15. Gerentes de Unidades de Negócios

Os Diretores Executivos de Unidade de Negócios são responsáveis por:

15.1 Identificar e avaliar os riscos que podem afetar suas áreas/empresas de sua responsabilidade.

15.2 Implementar procedimentos específicos de continuidade de negócios.

15.3 Participar de testes e exercícios de continuidade.

16 Colaboradores são responsáveis por:

16.2 Estar cientes e seguir as diretrizes de continuidade de negócios.

16.3 Participar de treinamentos e exercícios de continuidade.

16.4 Relatar quaisquer incidentes que possam comprometer a continuidade dos negócios.

17 Proibições para todos os colaboradores

Para garantir a eficácia e a integridade do Plano de Gerenciamento de Crise do Grupo ISG, é essencial que todos os colaboradores sigam rigorosamente as diretrizes estabelecidas. As seguintes ações são estritamente **proibidas:**

17.2 Divulgar informações confidenciais relacionadas ao Plano de Gerenciamento de Crise a pessoas não autorizadas, incluindo, mas não se limitando a concorrentes, fornecedores e familiares.

17.3 Não devem utilizar os recursos, ferramentas e informações fornecidas pelo Grupo ISG para fins pessoais ou não autorizados. Isso inclui o uso de equipamentos de comunicação, software e dados corporativos.

17.4 Os colaboradores não podem tentar acessar áreas restritas, sistemas ou informações que não estejam diretamente relacionados às suas funções e responsabilidades.

17.5 Qualquer modificação no Plano de Gerenciamento de Crise deve ser aprovada pela alta administração. Colaboradores não estão autorizados a fazer alterações ou ajustes no Plano sem a devida autorização.

17.6 Negligenciar ou ignorar os procedimentos estabelecidos no Plano Gerenciamento de Crise, especialmente durante uma situação de crise ou emergência.

17.7 Divulgar informações incorretas, incompletas ou enganosas sobre a situação de continuidade dos negócios, tanto interna quanto externamente, é estritamente proibido.

17.8 Devem evitar qualquer situação em que haja um conflito de interesse que possa comprometer a integridade do Plano de Gerenciamento de Crise. Qualquer potencial conflito deve ser imediatamente comunicado à administração.

17.9 Desviar ou contornar os protocolos de segurança estabelecidos. Isso inclui, mas não se limita a falhas na utilização de senhas seguras, proteção de dados e manutenção da integridade dos sistemas de TI.

17.10 É obrigatório reportar qualquer incidente que possa impactar a continuidade dos negócios. A omissão de tais relatórios é considerada uma violação grave desta política.

17.11 É obrigatória a participação em treinamentos, exercícios de simulação e outras atividades relacionadas à continuidade dos negócios, sendo vedada a ausência sem justificativa.

18 Treinamento e conscientização

O Grupo ISG deve fornecer treinamento regular e programas de conscientização para todos os colaboradores, garantindo que todos estejam familiarizados com seus papéis e responsabilidades em relação à continuidade de negócios.

19 Revisão e atualização da Política

Esta Política deve ser revisada e, se necessário, atualizada anualmente ou após qualquer incidente significativo que revele a necessidade de mudanças. As atualizações devem ser comunicadas a todos os colaboradores.

20 Conformidade e auditoria

A conformidade com esta política será monitorada por meio de auditorias regulares. Não conformidades devem ser corrigidas prontamente e medidas corretivas devem ser implementadas pela Diretoria de Compliance.

21 Aprovação

Esta Política de Continuidade de Negócios foi aprovada pela Alta Gestão e entra em vigor a partir da data de sua assinatura.

22 Referências Normativas

Esta política foi elaborada em conformidade com as seguintes normas:

ABNT NBR ISO 22301:2020 - Gestão de Continuidade de Negócios.

ABNT NBR ISO 31000:2018 - Gestão de Riscos.

ABNT NBR ISO 37001:2016 - Sistemas de Gestão Antissuborno.

ABNT NBR ISO 37301:2021 - Sistemas de Gestão de Compliance.