PGC – PLANO DE GERENCIAMENTO DE CRISE

Complemento a Plano de Continuidade de Negócio

v.2.0 | *Revisão* 2025

A.S

ALMEIDA SANTOS

ADVOGADOS

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: PGC – Plano de Gerenciamento de Crise					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	01/06/2023	01/06/2026	Anual	17.06
Nome do arquivo: PGC – Plano De Gerenciamento De Crise.Docx					

Sumário

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: PGC – Plano de Gerenciamento de Crise					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	01/06/2023	01/06/2026	Anual	17.06
Nome do arquivo: PGC – Plano De Gerenciamento De Crise.Docx					

Objetivo

Estabelecer o plano de gerenciamento de crise no âmbito da **Almeida Santos**, elencando procedimentos e protocolos a serem adotados quando em situação de crise ou de ameaça de crise. Os procedimentos e protocolos aqui abordados englobam o acionamento do Comitê de Segurança da Informação de Segurança da Informação, gerenciamento da crise propriamente dito, e o pós-crise.

Termos e Definições

- Crise: situação caracterizada pela materialização de um evento de risco ou série de eventos que culminam no rompimento significativo das operações normais, podendo gerar consequências graves às operações e/ou à imagem da **Almeida Santos**, demandando medidas extraordinárias para restabelecer as operações.

- Comitê de Segurança da Informação de Segurança da Informação: Comitê de Segurança da Informação instaurado em situações de crise ou de ameaça de crise, com o objetivo de coordenar o monitoramento e a resposta à situação de crise.

- Incidente Crítico: evento ou série de eventos que podem desencadear ameaças ao funcionamento e/ou que tenham impacto desastroso na reputação da empresa.

- Informação Privilegiada: toda informação relacionada à empresa ou às seus clientes que possa influir de modo significativo na negociação dos acordos.

- Matriz de riscos: documento que apresenta os riscos mapeados para a **Almeida Santos**, com seus respectivos cenários de crise e severidade.

- Plano de Continuidade de Negócio: conjunto de medidas de contenção e remediação de um evento ou série de eventos, com o objetivo de manter a normalidade da operação, ou minimizar os impactos de tais eventos.

- Plano de Resposta a Incidente: conjunto de medidas destinadas à identificação da origem de um evento que cause qualquer tipo de impacto às operações e de rápido restabelecimento de sua normalidade.

- Plano de Gerenciamento de Crise: plano que visa estabelecer procedimentos e protocolos a serem adotados, pelas áreas acionadas pelo Comitê de Segurança da Informação de Segurança da Informação, quando em situação de crise ou de ameaça de crise.

- Protocolo de atuação em crise: documento que retrata as ações a serem adotadas quando instaurado o cenário de crise.

- Matriz de Riscos de Crise: apresenta os eventos de materialização de riscos que podem desencadear uma crise para a **Almeida Santos**, com seus respectivos cenários de crise e severidade.

- Sociedades Controladas: as sociedades nas quais a empresa, diretamente ou através de outras sociedades, é titular de direitos de sócia que lhe assegurem, de modo permanente, preponderância nas deliberações sociais e o poder de eleger a maioria dos administradores.

Atribuições e Responsabilidade

Equipes	Responsável por:
Comitê da Segurança da Informação (CSI)	Avaliar e aprovar a presente Política; Avaliar a eficácia e efetividade dos planos de contingências propostos frente às situações reais.
Diretoria Operacional	Participar / liderar o Comitê de Segurança da Informação de Segurança da Informação; Assegurar que todos os recursos necessários para o acionamento dos planos de contingência estejam disponíveis; Conhecer e assegurar a implantação e a aplicação desta Política; Identificar potenciais cenários de materialização de risco que possam desencadear uma crise em suas respectivas diretorias; Elaborar os respectivos planos de contingência para os riscos de impacto alto e que possam desencadear crises consideradas graves; Assegurar que todos os colaboradores sejam informados e treinados nos planos de contingência.
Planejamento e Controle	Monitorar a efetividade da aplicação da presente Política; Propor, quando necessário, ações preventivas e/ou corretivas a fim de garantir a eficácia dos planos de contingência; Esclarecer dúvidas acerca da aplicabilidade da presente política.
Tecnologia da Informação	Elaborar planos de contingência para eventuais incidentes de segurança da informação; Acionar o Comitê de Segurança da Informação; Garantir o correto acionamento do plano de contingência definidos para os incidentes de segurança da informação; Comunicar e notificar os times de tecnologia impactados por eventuais problemas na infraestrutura de tecnologia.
Comitê de Segurança da Informação de Riscos	Acompanhar com a Diretoria a identificação e classificação dos riscos e dos cenários de crise e elaboração dos respectivos planos de contingência; Avaliar o possível impacto do incidente na reputação da empresa; Acionar os processos de monitoramento da repercussão do incidente na mídia e redes sociais; Definição da estratégia de comunicação com os públicos de interesse internos e externos e na escolha e preparação do porta-voz.

Diretrizes Gerais

A **Almeida Santos** define e adota plano de contingência para todos os cenários de crise considerados graves, ou seja, todos os eventos que possam impactar de forma relevante a imagem e as operações da **Almeida Santos**, bem como comprometer a sua credibilidade.

Os nossos processos da gestão de crises têm como objetivo estabelecer padrões estruturados para auxiliar nas respostas a possíveis situações que caracterizem uma crise grave, conforme abaixo:

- Obter o controle da situação o mais breve possível;
- Comunicar as partes internas e externas;
- Definir papéis e responsabilidades;
- Desenvolver um processo de tomada de decisão claro e testado;
- Garantir pessoas com competência em papéis específicos de gestão de crises, por meio de treinamentos, exercícios e avaliações de seu conhecimento, habilidades e experiência;
- Manter registros e rastreabilidade de todas as decisões tomadas;
- Estabelecer um Comitê de Segurança da Informação para gestão da crise;
- Aprender com os erros e efetuar mudanças para evitar sua recorrência.

Nenhum colaborador, em hipótese alguma, poderá conversar a respeito da situação de crise instaurada com qualquer pessoa que não esteja envolvida no Comitê de Segurança da Informação, bem como fazer qualquer comentário em redes sociais ou com colegas.

Nota 1: Ao ser abordado por um jornalista, outro colaborador, parceiro, acionista, amigo ou familiar, limite-se a dizer que não está autorizado a comentar a respeito do assunto e direcione o contato para o time de comunicação.

1. Diretrizes Específicas

1.1. Cenários de Crise

- Ocorrências que possam gerar externalidades negativas aos nossos colaboradores, parceiros e clientes;
- Eventos que tenham impacto significativo ao meio ambiente;
- Eventos de desastre natural que impacte diretamente as operações;
- Eventos relacionados a interrupções relevantes dos sistemas de telecomunicações e internet;
- Eventos de saúde pública, como pandemias;
- Interrupção de serviços prestados por terceiros que impactem de forma relevante em nossas operações;
- Incêndio no escritório;
- Pane no sistema logístico que impacte massivamente na entrega de encomendas;
- Acusações de favorecimento comercial, cartel, fiscal/lavagem de dinheiro, corrupção ou acusação de improbidade administrativa ou de assédios cometidas pela alta administração;
- Operações de busca e apreensão de documentos (por exemplo, pela PF – Polícia Federal);
- Decisões judiciais desfavoráveis que gerem ônus financeiro relevante ou risco reputacional;
- Acusações pública de racismo, homofobia, transfobia ou qualquer outro tipo de preconceito;

- Incidentes sérios de segurança da informação (vazamento de informações, invasão de sistemas que ocasionem paradas de sistemas ou rupturas de serviços);
- Campanhas de marketing "polêmicas" não aceitas pelo público.

1.2. Orientações para elaboração de planos de contingência

- Identificar todos os públicos que podem ser afetados pela crise;
- Identificar possíveis formas de evitar que a crise se instaure;
- Identificar áreas envolvidas no Plano de Contingência;
- Avaliar necessidade de recursos financeiros para a implantação do Plano de Contingência;
- Elaborar um passo-a-passo para acionamento do Plano de Contingência: quem deve ser informado, o que deve ser dito, responsabilidades das partes envolvidas;
- Aprovar o Plano de Contingência nas instâncias aplicáveis;
- Divulgar o Plano de Contingência para o público interessado;
- Treinar o público interessado, sempre que possível, por meio de simulação de situações reais.
-

2. Da atuação do Comitê de Segurança da Informação

O Comitê de Segurança da Informação somente deve ser acionado em situações necessárias e extremas e devem ter poderes de decisão enquanto durar o problema.

No gerenciamento de qualquer crise, o Comitê deve nortear sua atuação nas seguintes diretrizes:

- Informar o Conselho de Administração sobre a crise instaurada e, se possível, já comunicar as tratativas que serão adotadas;
- Identificar todos os públicos que podem ser afetados pela crise, informando que o problema foi detectado, que está sendo sanado e, quando possível, falar sobre as tratativas;
- Comunicar somente o que pode ser confirmado com absoluta certeza. Não comente situações hipotéticas;
- Manter-se acessível e não negar informações passíveis de serem divulgadas;
- Comunicar, se possível, todas as más notícias de uma única vez;
- Deixar um canal de comunicação aberto com o público de interesse;
- Registrar todas as ações adotadas;
- Monitorar e avaliar a situação da crise;
- Não deixar de se comunicar no momento certo;
- Tomar decisões baseadas em informações técnicas e em fatos reais;
- Expor os problemas e apontar soluções de forma tempestiva;
- Atender aos públicos interno e externo e a imprensa, sempre que possível, a fim de evitar ilações sem fundamentos acerca da incidente.

O Comitê de Segurança da Informação deve definir um porta-voz experiente, informado, que fale com clareza e não se sinta intimidado diante dos públicos de interesse envolvidos na crise.

Política de Consequências a Violação

Qualquer violação a presente política será passível de penalização, que poderá ser desde advertência verbal até demissão por justa causa e, no caso de ocorrência de danos, reparação do eventual dano causado.

As medidas de consequências adotadas pela **Almeida Santos**, seja no âmbito interno, ou seja, por meio de adoção de medida judicial cabível, serão aplicadas após a avaliação da gravidade do caso concreto e dos impactos causados pela violação.

Compete ao Comitê de Segurança da Informação apurar os casos relatados e deverá, em casos graves, ratificar a sua decisão junto a Diretoria.

Das Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da **Almeida Santos**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela empresa.

Controle de Atualização

Versão	Data	Alterações
01	01/06/2023	Versão Inicial
02	01/06/2025	Versão Revisada