PLANO DE CONTINUIDADE DE NEGÓCIOS

Sumário

1. Objetivo 3
2. Público-Alvo e Abrangência 3
3. Estrutura Documental da Gestão de Continuidade de Negócios 4
4. Atribuições e Responsabilidades 4
5. Análise de Impacto nos Negócios (BIA) 5
6. Cenários de Ameaça 7
7. Critérios e Procedimentos de Ativação 8
8. Estratégias de Recuperação 10
9. Terceiros e Fornecedores Críticos 11
10. Testes, Exercícios e Simulações 11
11. Comunicação de Crise 12
12. Contatos de Emergência 12
13. Indicadores de Desempenho 12
14. Sanções Disciplinares 13
15. Normativos de Referência 13
16. Revisão 13
17. Aprovação 14

Informação para uso interno

PLANO DE CONTINUIDADE DE NEGÓCIOS

1. Objetivo

Este Plano de Continuidade de Negócios ("PCN") integra o arcabouço normativo de segurança da informação do Grupo ASA, em conformidade com a Política Corporativa de Segurança da Informação e Cibersegurança (PSI/PSC) e com os marcos regulatórios e referenciais descritos na Seção 29 da PSI/PSC.

O PCN tem por objetivo:

- Estabelecer as diretrizes, responsabilidades e princípios que norteiam a Gestão de Continuidade de Negócios (GCN) do Grupo ASA, garantindo a capacidade de responder, resistir e recuperar-se de incidentes, falhas, crises ou desastres que possam comprometer a prestação de serviços essenciais;
- Assegurar que os processos críticos, sistemas tecnológicos, infraestruturas de suporte e recursos humanos estejam preparados para lidar com interrupções, por meio de planos, estratégias e testes que assegurem a resiliência operacional;
- Garantir o cumprimento dos objetivos de tempo de recuperação (RTO) e ponto de recuperação (RPO) definidos na Análise de Impacto nos Negócios (BIA);
- Assegurar a continuidade das operações dentro de níveis aceitáveis de risco e em conformidade com os requisitos regulatórios aplicáveis.

2. Público-Alvo e Abrangência

O PCN aplica-se a todas as áreas organizacionais, unidades de negócio, produtos, canais e plataformas tecnológicas do Grupo ASA, incluindo filiais, parceiros estratégicos, prestadores de serviço e fornecedores críticos cujas atividades estejam diretas ou indiretamente relacionadas à entrega de serviços essenciais.

O PCN abrange:

- Os processos críticos identificados na Análise de Impacto nos Negócios (BIA);
- As infraestruturas de suporte físico e lógico que compõem o ambiente operacional, incluindo ambientes de produção, contingência e nuvem;
- Os sistemas, aplicações e serviços tecnológicos classificados como críticos ou de alta disponibilidade;
- Os recursos humanos, comunicações e instalações físicas necessários à operação em modo de contingência.

Todos os colaboradores, gestores, terceiros e parceiros são responsáveis por observar as diretrizes aqui estabelecidas.

Informação para uso interno

3. Estrutura Documental da Gestão de Continuidade de Negócios

A Gestão de Continuidade de Negócios do Grupo ASA é composta pelos seguintes documentos, que se complementam e devem ser mantidos atualizados:

Documento	Propósito	Nível / Alcance
PCN	Diretrizes, governança, critérios de ativação, estratégias de recuperação e gestão de crise.	Estratégico e operacional - todo o Grupo ASA.
BIA	Identificação de processos críticos, dependências, impactos de indisponibilidade e definição de RTO/RPO.	Analítico - por processo de negócio e sistema.
DRP	Procedimentos técnicos de *failover*, *restore* de backups, ativação de site alternativo e recuperação de infraestrutura.	Técnico - TI e Infraestrutura.
PCC	Plano de Comunicação de Crise: fluxos de comunicação interna e externa, porta-vozes, modelos pré-aprovados de comunicação.	Comunicação - Diretoria, Compliance, Jurídico.

O presente documento (PCN) estabelece as diretrizes gerais. O BIA, o DRP e o PCC são documentos complementares que detalham respectivamente a análise de impacto, os procedimentos técnicos de recuperação e os fluxos de comunicação de crise.

4. Atribuições e Responsabilidades

4.1. Diretoria Executiva / Board of Directors

- Garantir os recursos humanos, financeiros e tecnológicos necessários à implementação e manutenção da Gestão de Continuidade de Negócios (GCN);
- Assegurar que a GCN esteja integrada à estrutura de governança, riscos e conformidade do Grupo ASA;
- Monitorar periodicamente os indicadores de desempenho da continuidade de negócios, avaliando resultados de testes, planos de ação e auditorias;
- Deliberar sobre a ativação do Comitê de Crise em situações de indisponibilidade severa;
- Garantir o reporte tempestivo aos reguladores aplicáveis, conforme o *Playbook* de Notificações Regulatórias e a Seção 15.2 da PSI/PSC.

4.2. CISO e/ou área responsável pela Gestão de Continuidade de Negócios

- Manter e aprimorar o Programa de Gestão de Continuidade de Negócios (PGCN);
- Conduzir as Análises de Impacto nos Negócios (BIA) e avaliações de riscos operacionais e tecnológicos;

Informação para uso interno

- Coordenar o desenvolvimento, a execução e o teste dos planos de continuidade (PCN, DRP e PCC);
- Garantir que incidentes que afetem serviços críticos sejam tratados e reportados conforme os procedimentos de gestão de crises e a Seção 15 da PSI/PSC;
- Promover programas de conscientização e treinamento contínuo sobre continuidade de negócios;
- Manter documentação atualizada, evidências de testes e relatórios de auditoria;
- Avaliar periodicamente a eficácia do programa, propondo melhorias contínuas.

4.3. Áreas de Negócio e Donos de Processo

- Identificar processos críticos, dependências e recursos necessários à continuidade operacional;
- Garantir a execução dos planos específicos de continuidade de suas áreas e reportar desvios ou falhas;
- Participar ativamente dos testes e simulações de contingência;
- Colaborar na atualização dos documentos e planos sob sua responsabilidade.

4.4. Área de Tecnologia e Infraestrutura

- Assegurar a disponibilidade dos ambientes de produção e contingência, conforme os RTO e RPO estabelecidos no BIA;
- Executar e documentar testes periódicos de *Disaster Recovery* (DRP);
- Implementar e manter controles de redundância, backup e restauração;
- Garantir que os sistemas críticos contem com monitoramento contínuo e alertas automáticos.

4.5. Colaboradores, Terceiros e Parceiros

- Conhecer e cumprir as diretrizes deste Plano de Continuidade de Negócios;
- Reportar imediatamente qualquer incidente ou evento que possa comprometer a continuidade das operações;
- Participar de treinamentos e testes quando convocados;
- Cumprir as obrigações contratuais e normativas relacionadas à continuidade de serviços.

5. Análise de Impacto nos Negócios (BIA)

A Análise de Impacto nos Negócios (*Business Impact Analysis* — BIA) é o instrumento que identifica e classifica os processos críticos do Grupo ASA, suas dependências, os impactos de indisponibilidade e os objetivos de recuperação.

O BIA deve ser revisado ao menos anualmente e sempre que houver mudança material nos processos de negócio, na infraestrutura tecnológica ou no ambiente regulatório.

Informação para uso interno

O BIA deve contemplar, no mínimo:

- Identificação e priorização dos processos críticos de negócio;
- Mapeamento de dependências (sistemas, infraestrutura, terceiros, recursos humanos, comunicações);
- Avaliação de impacto financeiro, operacional, regulatório e reputacional da indisponibilidade;
- Definição de RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*) por processo e sistema crítico;
- Identificação de níveis mínimos de serviço (operação degradada) durante a contingência.

5.1. Classificação de Processos e RTO/RPO de Referência

Os parâmetros abaixo constituem referência corporativa inicial e não substituem os valores formais definidos e aprovados no BIA:

Criticidade	Descrição	RTO Máximo	RPO Máximo
Crítica	Processos cuja indisponibilidade gera impacto financeiro, regulatório ou reputacional imediato e severo.	≤ 4 horas	≤ 1 hora
Alta	Processos cuja indisponibilidade gera impacto significativo em até 24 horas.	≤ 8 horas	≤ 4 horas
Média	Processos cuja indisponibilidade é tolerável por até 72 horas com impacto gerenciável.	≤ 24 horas	≤ 12 horas
Baixa	Processos cuja indisponibilidade é tolerável por mais de 72 horas.	≤ 72 horas	≤ 24 horas

O BIA completo, com o detalhamento por processo, sistema e área responsável, consta de documento interno específico mantido pela área de Segurança da Informação / Gestão de Continuidade de Negócios.

Informação para uso interno

6. Cenários de Ameaça

O PCN deve contemplar, no mínimo, os seguintes cenários de ameaça, conforme exigido pela Seção 16 da PSI/PSC:

#	Cenário	Descrição	Estratégia Primária
C1	Ataque de *Ransomware*	Criptografia maliciosa de dados e sistemas, com ou sem exfiltração. Indisponibilidade total ou parcial.	Isolamento de rede, restore de backups off-line, ativação do IRP (Seção 15 PSI/PSC).
C3	Interrupção de Provedor de Nuvem	Indisponibilidade prolongada de provedor crítico ou SaaS essencial.	Ativação de ambiente alternativo, operação degradada, contato com provedor.
C4	Falha de Infraestrutura Crítica	Falha de energia, telecomunicações, rede ou hardware crítico sem redundância.	Ativação de redundância, UPS/gerador, links alternativos.
C5	Pandemia / Indisponibilidade de Pessoal	Ausência massiva de colaboradores por pandemia, greve ou evento externo.	Operação remota, cross-training, priorização de processos críticos.
C6	Comprometimento de Terceiro Crítico	Indisponibilidade ou violação de segurança em prestador de serviço essencial.	Ativação de provedor alternativo, operação manual temporária.
C7	Incidente Cibernético (não-ransomware)	Ataque DDoS, comprometimento de credenciais, exfiltração de dados.	Contenção, ativação IRP, failover se necessário.

Os cenários devem ser revisados anualmente e atualizados conforme a evolução do ambiente de ameaças e os resultados de avaliações de risco.

Informação para uso interno

7. Critérios e Procedimentos de Ativação

7.1. Critérios de Ativação do PCN

O PCN deve ser ativado quando um ou mais dos seguintes critérios forem atendidos:

- Indisponibilidade confirmada ou iminente de processo ou sistema classificado como crítico no BIA;
- Incidente cibernético de alta severidade que comprometa a integridade, disponibilidade ou confidencialidade de sistemas críticos;
- Indisponibilidade do data center primário ou de provedor de nuvem crítico;
- Evento que comprometa a capacidade operacional do Grupo ASA (desastre natural, pandemia, indisponibilidade de pessoal);
- Determinação da Diretoria Executiva, do CISO ou do Comitê de Crise.

7.2. Fluxo de Escalonamento e Ativação

O fluxo de ativação segue as seguintes etapas:

Etapa	Ação	Responsável
1. Detecção	Identificar o evento e avaliar impacto preliminar. Registrar em ferramenta de incidentes.	Equipe de Monitoramento / SOC / Área afetada.
2. Escalonamento	Escalonar ao CISO e ao gestor da área afetada. Avaliar critérios de ativação do PCN.	CISO / Head de Segurança da Informação / Tecnologia da Informação / Áreas de Negócio.
3. Ativação	Ativar o PCN e convocar o Comitê de Crise. Notificar Diretoria, Jurídico e Compliance.	CISO / CTO / Diretoria Executiva.
4. Execução	Executar estratégias de recuperação (DRP), operação degradada e comunicação de crise (PCC).	TI / Infraestrutura / Áreas de Negócio.
5. Monitoramento	Monitorar a recuperação, avaliar progresso em relação ao RTO/RPO. Atualizar stakeholders.	CISO / Comitê de Crise.
6. Normalização	Confirmar restabelecimento completo. Desativar o PCN formalmente. Registrar timeline.	CISO / Diretoria.
7. Pós-incidente	Conduzir análise pós-incidente (*lessons learned*). Atualizar PCN, BIA, DRP conforme necessário.	CISO / Segurança da Informação / Tecnologia da

Informação para uso interno

		Informação / Áreas de Negócio.

Informação para uso interno

8. Estratégias de Recuperação

O Grupo ASA deve manter as seguintes estratégias de recuperação, proporcionais à criticidade dos processos e sistemas:

8.1. Redundância e Alta Disponibilidade

- Sistemas críticos devem contar com infraestrutura redundante, geograficamente segregada, de forma a permitir failover automático ou manual em tempo compatível com o RTO definido;
- Ambientes de nuvem devem utilizar configurações multi-região ou multi-zona de disponibilidade para sistemas críticos.

8.2. Backup e Restauração

- Todos os dados e sistemas críticos devem possuir política de backup documentada, com frequência compatível com o RPO definido;
- Backups devem ser armazenados em localização fisicamente segregada do ambiente de produção;
- Deve ser mantido ao menos uma cópia de backup off-line ou imutável, como proteção contra-ataques de ransomware;
- Testes de restauração de backup devem ser realizados ao menos semestralmente, com documentação dos resultados.

8.3. Operação em Modo Degradado

- Para cada processo crítico, deve estar definido o nível mínimo de serviço aceitável durante a contingência (operação degradada);
- Procedimentos manuais ou alternativos devem estar documentados para os casos em que a recuperação automática não seja possível dentro do RTO;
- Priorização de restauração por criticidade;
- Procedimentos manuais alternativos por processo, quando aplicável.

8.4. Site Alternativo

- O Grupo ASA deve manter capacidade de operação a partir de site alternativo (físico ou virtual), com acesso aos sistemas críticos, comunicações e dados necessários;
- O site alternativo deve ser testado ao menos semestralmente como parte dos exercícios de continuidade.

Informação para uso interno

9. Terceiros e Fornecedores Críticos

Os contratos com terceiros e fornecedores críticos devem conter requisitos mínimos de continuidade, incluindo:

- SLAs de disponibilidade e desempenho, com penalidades definidas;
- RTO e RPO compatíveis com os requisitos do Grupo ASA;
- Canais de acionamento em caso de crise ou indisponibilidade;
- Obrigação de participação em testes integrados, quando aplicável;
- Manutenção de contatos de escalonamento de crise atualizados;
- Obrigação de manutenção de planos próprios de continuidade e *disaster recovery*;
- Direito de auditoria e verificação periódica dos controles de continuidade do terceiro;
- Obrigação de comunicação tempestiva de incidentes que possam afetar os serviços prestados ao Grupo ASA.

Esses requisitos devem estar alinhados com a Seção 17 (TPRM) da PSI/PSC.

10. Testes, Exercícios e Simulações

O Grupo ASA deve realizar testes de continuidade e recuperação com periodicidade mínima semestral, conforme a Seção 16 da PSI/PSC, incluindo:

Tipo de Teste	Descrição	Frequência Mínima
Tabletop Exercise	Simulação baseada em cenário, com discussão dos fluxos de escalonamento, decisão e comunicação.	Semestral.
Teste de Failover / DRP	Teste técnico de failover para ambiente de contingência, com medição de RTO/RPO real.	Semestral.
Teste de Restore de Backup	Restauração efetiva de dados a partir de backup, validando integridade e tempo de recuperação.	Semestral.
Simulação de Crise Completa	Exercício abrangente envolvendo múltiplas áreas, com ativação real ou simulada do PCN.	Semestral.

Os resultados de todos os testes devem ser documentados, incluindo: timeline de execução, RTO/RPO efetivamente atingidos, falhas identificadas, ações corretivas e oportunidades de melhoria.

O PCN, o BIA e o DRP devem ser revisados após cada teste ou incidente relevante.

Informação para uso interno

11. Comunicação de Crise

O Grupo ASA deve manter Plano de Comunicação de Crise (PCC) formalizado, contemplando:

- Definição dos porta-vozes autorizados para comunicação interna e externa;
- Fluxos de comunicação com colaboradores, clientes, parceiros, reguladores e imprensa;
- Modelos pré-aprovados de comunicação pré-aprovados para diferentes cenários;
- Canais de comunicação alternativos para uso em caso de indisponibilidade dos canais primários;
- Alinhamento com o *Playbook* de Notificações Regulatórias (Seção 15.2 da PSI/PSC) para garantia de cumprimento dos prazos de notificação aplicáveis.

Somente pessoas expressamente autorizadas podem comunicar-se externamente sobre incidentes ou crises, conforme designação no PCC.

12. Contatos de Emergência

O Grupo ASA deve manter lista atualizada de contatos de emergência, incluindo, no mínimo:

Categoria	Exemplos	Responsável pela Atualização
Comitê de Crise	CEO, CISO, Diretor Jurídico, Diretor de Compliance, Head de TI.	CISO / RH.
Reguladores	NYDFS, Bacen, ANPD, SEC, NY AG, Florida OFR.	Compliance / Jurídico.
Provedores Críticos	Provedores de nuvem, data center, telecomunicações, segurança.	TI / Infraestrutura.
Assessorias Externas	Escritório de advocacia, perícia forense, comunicação de crise, seguros.	Jurídico / CISO.

A lista de contatos deve ser mantida em local seguro, acessível off-line, em local resiliente e atualizada ao menos trimestralmente.

13. Indicadores de Desempenho

O desempenho do Programa de Continuidade de Negócios deve ser monitorado por meio dos seguintes indicadores mínimos:

- Percentual de processos críticos cobertos por planos de continuidade;
- Percentual de testes de continuidade realizados versus planejados;
- RTO e RPO efetivamente atingidos nos testes versus os definidos no BIA;
- Tempo médio de ativação do PCN em testes e incidentes reais;

Informação para uso interno

- Percentual de ações corretivas concluídas no prazo após testes;
- Percentual de planos revisados no prazo;
- Percentual de terceiros críticos testados/validados, quando aplicável.
- Percentual de terceiros críticos com evidências de planos de continuidade próprios.

Os indicadores devem ser reportados periodicamente ao CISO e à Diretoria Executiva.

14. Sanções Disciplinares

As violações a este Plano estão sujeitas às medidas disciplinares, contratuais e legais cabíveis, conforme previsto na Seção 26 da PSI/PSC do Grupo ASA e na legislação aplicável em cada jurisdição.

15. Normativos de Referência

Este Plano deve ser interpretado em conjunto com os seguintes normativos e referenciais:

- Política Corporativa de Segurança da Informação e Cibersegurança (PSI/PSC) do Grupo ASA - especialmente as Seções 15 (Resposta a Incidentes), 16 (Continuidade de Negócios) e 17 (TPRM);
- Playbook de Notificações Regulatórias;
- Análise de Impacto nos Negócios (BIA) do Grupo ASA;
- Plano de Recuperação de Desastres (DRP) do Grupo ASA;
- Plano de Comunicação de Crise (PCC) do Grupo ASA;
- ISO 22301:2019 - Business Continuity Management Systems, quando aplicável;
- ISO/IEC 27031:2022 - ICT Readiness for Business Continuity, quando aplicável;
- NIST SP 800-34 - Contingency Planning Guide for Federal Information Systems;
- NYDFS 23 NYCRR Part 500;
- GLBA / FTC Safeguards Rule (16 CFR Part 314).

16. Revisão

Este Plano entra em vigor na data de sua aprovação e deve ser revisado, no mínimo, anualmente, ou sempre que houver:

- Alteração regulatória relevante;
- Incidente que resulte na ativação do PCN ou do DRP;
- Resultado de teste que evidencie necessidade de atualização;
- Mudança material nos processos de negócio, na infraestrutura tecnológica ou na estrutura organizacional;
- Determinação da governança competente, de órgão regulador ou de auditoria.

Informação para uso interno

17. Aprovação

Data	Aprovadores	
14/10/2026	Head de Tecnologia	Head de Compliance

Informação para uso interno