HOSSEGOR GESTÃO DE RECURSOS LTDA.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Versão Atualizada: 5.0 – AGO/2025

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Objetivo

Definir as bases, princípios e regras para contingências e continuidade de negócios da HOSSEGOR GESTÃO DE RECURSOS LTDA ("HOSSEGOR").

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a HOSSEGOR (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos neste Plano de Contingência e Continuidade de Negócios, informando imediatamente qualquer irregularidade ao Diretor de Risco, *Compliance* e PLD.

Responsabilidades

Caberá ao Diretor de Risco, *Compliance* e PLD a avaliação das ocorrências, podendo fazer uso do Comitê de Risco e *Compliance* para registro de ocorrências e tomadas de decisão.

Revisão, Atualização e Testes

Este Plano de Contingência e Continuidade de Negócios deverá ser revisado e atualizado a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

Sem prejuízo do parágrafo anterior, este Plano de Contingência e Continuidade de Negócios será igualmente objeto de validação e testes a cada 12 (doze) meses.

Contexto Operacional e de Negócios

Este Plano de Contingência e Continuidade de Negócios foi elaborado considerando as seguintes premissas e particularidades do modelo operacional e de negócio da HOSSEGOR:

- A HOSSEGOR não possui sistemas desenvolvidos internamente e desempenha suas atividades utilizando sistemas de terceiros, todos apenas acessíveis via *web*, não possuindo nenhum sistema que necessite de instalações locais para ser executado;
- Os arquivos eletrônicos de trabalho da HOSSEGOR são armazenados em nuvem e localmente, com *backups* feitos diariamente com redundância;
- Os fornecedores dos sistemas utilizados pela HOSSEGOR se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da HOSSEGOR;

- Os Colaboradores da HOSSEGOR estabelecem tratativas e formalizam seus entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou *e-mail* corporativo;
- A HOSSEGOR aloca recursos sob gestão e tem seus produtos distribuídos, mediante a utilização de corretoras/plataformas de investimento acessíveis pela *web* e disponíveis para qualquer dispositivo eletrônico (*laptops, smartphones, tablets* ou computadores de mesa);
- O sistema de consolidação de carteiras utilizado pela HOSSEGOR identifica os clientes por meio de siglas, dispensando a identificação mediante o preenchimento de cadastro com informações pessoais;
- Os arquivos contendo informações pessoais e financeiras dos clientes da HOSSEGOR são armazenados em nuvem, com *backups* periódicos não superiores a 7 (sete) dias corridos, podendo ser recompostos solicitando tais informações aos próprios clientes;
- Os dispositivos eletrônicos (*laptops, smartphones, tablets*) utilizados no exercício das atividades da HOSSEGOR possuem senha de acesso;
- A HOSSEGOR utiliza redes sem fio para fornecer acesso à *web* para seus Colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas. Em caso de indisponibilidade temporária para acesso à *web*, os Colaboradores utilizam redes/roteadores de redundância. Neste caso, e em caso de trabalho remoto, os Colaboradores da HOSSEGOR comprometem-se a utilizar redes sem fio seguras para desempenhar suas atividades; e
- O espaço físico/escritório da HOSSEGOR deve ser o local preferencialmente utilizado para as atividades da HOSSEGOR, reuniões com clientes, comitês e reuniões comerciais com Colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas da HOSSEGOR estão parametrizados para serem passíveis de serem executadas de forma remota.

Princípios e Obrigações

O Plano de Contingência e Continuidade de Negócios é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los no prazo previamente estabelecido.

Para identificação dos ativos críticos[1], devem ser considerados os riscos a seguir, no caso de interrupção do processo:

- impacto financeiro – situações em que a descontinuidade de negócios possa atingir fundos sob gestão ou a situação financeira e patrimonial da HOSSEGOR;

[1] Todo e qualquer sistema, equipamento, arquivo etc., em suma, todo ativo essencial para o mínimo funcionamento da HOSSEGOR, atendendo a suas obrigações legais críticas.

- impacto legal – descontinuidade de negócios passível de gerar consequências legais aos fundos sob gestão, seus cotistas, ou mesmo à própria HOSSEGOR;
- impacto de imagem – risco de a descontinuidade de negócios impactar a reputação e confiabilidade da HOSSEGOR perante seus clientes e/ou o público investidor; e
- acidentes, casos fortuitos e força maior – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle da HOSSEGOR, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

As posições, áreas e sistemas considerados críticos constam no Anexo I – Atividades e Sistemas Críticos - a este Plano de Contingência e Continuidade de Negócios.

Classificação de Riscos e Providências

A HOSSEGOR adota a seguinte classificação de riscos, com as respectivas providências a serem tomadas:

- Nível 1: baixa probabilidade de ocorrência e/ou de impacto nas atividades da HOSSEGOR, com monitoramento cotidiano para a sua prevenção. Exemplos:
    - situações não diretamente relacionadas à HOSSEGOR e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle.

- Nível 2: riscos demandantes de atenção constante, com impacto potencial médio nas atividades da HOSSEGOR e necessidade de maior nível de controles preventivos. Exemplos:
    - falha de segurança/manutenção das instalações da HOSSEGOR, que têm como medidas preventivas a verificação da manutenção de extintores, *sprinklers* e detectores de fumaça instalados nas suas dependências, além da operação/instalação de controles de acesso às suas dependências.

- Nível 3: riscos que devem ser incondicionalmente evitados, com impacto relevante nas atividades da HOSSEGOR, com adoção de rigorosos controles preventivos. Exemplos:
    - indisponibilidade e inacessibilidade total de pessoas a seus meios. Nestes casos, medidas preventivas incluem a definição de substitutos para as posições chave devidamente treinados, habilitados e capacitados para atuar no desempenho das funções requeridas;
    - Falha de segurança/manutenção/atualização dos *softwares* e serviços críticos utilizados pela HOSSEGOR no exercício de suas operações e monitoramentos periódicos[2];

[2] Que têm como medidas preventivas a obtenção dos respectivos planos de contingência dos provedores de tais *softwares* ou serviços, bem como o acompanhamento dos resultados periódicos dos testes de

- Interrupção do funcionamento de equipamentos utilizados pelos Colaboradores da HOSSEGOR que inviabilizem sua utilização nas atividades de operação e monitoramentos periódicos[3]; e
- Situações de indisponibilidade dos serviços e sistemas das instituições administradoras e custodiantes dos fundos geridos pela HOSSEGOR, bem como das plataformas por ela utilizadas para distribuição de tais fundos[4].

Controles Preventivos da HOSSEGOR

- Identificação, treinamento e capacitação profissional de substitutos para exercer as atividades chave da operação da HOSSEGOR;
- Controle de acesso às dependências da HOSSEGOR;
- Respeito às normas de acesso estipuladas pelo condomínio no qual a HOSSEGOR está sediada;
- Manutenção de provedores para acesso a arquivos eletrônicos, planilhas e demais documentos de forma segura e transparente ao usuário, bem como dos respectivos *back-ups* desses materiais;
- Manutenção de sistema antivírus e *firewall* para salvaguardar os arquivos eletrônicos utilizados pela HOSSEGOR; e
- Servidores/provedores de serviços tecnológicos, de dados, ferramentas contratadas etc. – controles e redundâncias dos serviços de servidores e prestadores de serviço em ambiente em nuvem, com as devidas proteções antivírus, *firewall*, *backup* etc.

A HOSSEGOR trabalha com níveis consistentes de redundância. Os arquivos são armazenados localmente e em nuvem, e o *backup* é armazenado diariamente em ambiente em nuvem com redundância de provedores de *internet* e telefonia.

Os serviços de *e-mail* e servidores também são armazenados em nuvem e a interface operacional do administrador pode ser acessada de qualquer lugar via *internet*.

Localmente, a HOSSEGOR conta com uma estrutura de contingência preparada para atender a quaisquer situações críticas que impossibilitem as áreas de negócio de exercerem suas atividades diárias, com recursos necessários e suficientes à continuidade das suas rotinas.

contingência aplicados e dos planos de ação estabelecidos para mitigar eventuais falhas identificadas em tais testes (quer sejam nas dependências da HOSSEGOR ou nas dos fornecedores).

[3] Cuja medida preventiva inclui a manutenção *backup* dos arquivos necessários para o desempenho das atividades cotidianas de modo a sempre possibilitar a continuidade normal de suas atividades, mesmo em eventos de crise, quer seja nas dependências da HOSSEGOR ou fora delas.

[4] Que tem como medidas preventivas a obtenção dos respectivos Plano de Contingência e Continuidade de Negócios de tais parceiros de negócio.

Os procedimentos definidos a seguir compõem este Plano de Contingência e Continuidade de Negócios:

Procedimentos	Periodicidade	Responsável
Identificar as pessoas críticas para a operação da HOSSEGOR e suas respectivas atividades e garantir que estejam capacitadas para exercer tais atividades	Sempre que necessário, no caso de novas atividades e pessoas, no mínimo anualmente.	Anualmente, o Diretor de Risco, *Compliance* e PLD solicita a revisão do Anexo I.
Identificar e reavaliar os sistemas críticos, e atualizar o Anexo I, bem como os telefones do plano de comunicação.	Sempre que necessário, no caso de novas atividades, pessoas e sistemas, no mínimo anualmente.	Anualmente, o Diretor de Risco, *Compliance* e PLD solicita a revisão do Anexo I.
Decidir pelo início da contingência. A comunicação deve ser efetuada conforme o Anexo II.	Na efetiva ocorrência de incidentes.	Dois sócios e/ou dois Diretores, ou um sócio e um Diretor em conjunto.
Acionar o plano de contingência.	Na aprovação do início da contingência.	O plano de continuidade poderá ser acionado pelas pessoas autorizadas pela HOSSEGOR, conforme Anexo II.
Informação à equipe.	Após decisão pelo início da contingência na estrutura alternativa.	O plano de comunicação consta do Anexo III.
Após a contingência, verificar o que motivou o incidente/crise, e se o motivo é passível de ações de aprimoramentos, bem como aprimoramento do Plano de Contingência e Continuidade de Negócios.	Após contingência.	Gestores das áreas, com reporte e registro no Comitê de Risco e *Compliance*.
Realizar testes do Plano de Contingência e Continuidade de Negócios	Anualmente.	Diretor de Risco, *Compliance* e PLD coordena com os gestores das respectivas áreas na HOSSEGOR.

Controles Preventivos Fora da HOSSEGOR

A HOSSEGOR conta, ainda, com a estrutura operacional, computacional e processos de contingência de: (i) administradores dos seus fundos de investimento e seus custodiantes e das plataformas nas quais tais fundos são distribuídos; e (ii) plataformas nas quais os investimentos de seus clientes estão custodiados.

ANEXO I

Atividades e Sistemas Críticos

Quadro mínimo de profissionais com acesso aos sistemas, redes etc. em situação de contingência
Diretor de Investimentos
Diretor de Risco, *Compliance* e PLD
Outros Diretores Estatutários

Sistemas críticos com acesso em situação de contingência
Sistemas de gestão
Sistemas do administrador, plataformas, corretoras etc. (ordens de compra e venda, aplicação e resgate e demais movimentações, saldos etc.)
Sistema de gerenciamento de risco
Sistema de análise de ativos, carteiras etc.
Conexão de *internet*
Pacote Office e demais ferramentas de apoio
E-mail e Microsoft Teams
Dados e arquivos da HOSSEGOR

No caso de impossibilidade temporária ou definitiva de atuação do responsável junto à CVM pela administração de carteira de valores mobiliários, a HOSSEGOR nomeará um responsável (temporário ou definitivo), devendo a CVM ser comunicada por escrito, no prazo de 1 (um) dia útil a contar da sua ocorrência, no caso de total ausência e necessidade de substituição do titular.

ANEXO II

Pessoas Autorizadas a Iniciar Plano de Contingência e Continuidade de Negócios na Estrutura Alternativa

- Diretor de Investimentos ou profissional delegado da equipe
- Diretor de Risco, *Compliance* e PLD ou profissional delegado da equipe
- Outros Diretores Estatutários
- Sócios Majoritários

As pessoas acima estão autorizadas a ativar o Plano de Contingência e Continuidade de Negócios na eventual ausência, por qualquer razão, das demais, de forma a sempre possibilitar a preservação ininterrupta das atividades da HOSSEGOR.

ANEXO III

Plano de Comunicação

Modelo – "*Call Tree*"

A HOSSEGOR utiliza primordialmente *e-mail* de acesso remoto (via celular ou computadores pessoais) e listas em aplicativos de mensagens via telefone celular (Microsoft Teams) como forma de comunicação de contingência, visando principalmente à efetividade e agilidade proporcionada por tais ferramentas em contextos dessa natureza.

A comunicação é iniciada pelos indivíduos mencionados no Anexo II e enviada a todos os membros das respectivas equipes, os quais participam dos grupos pertinentes, de maneira a assegurar a pronta e eficiente comunicação da contingência em questão, em tempo hábil e oportuno.

Não obstante, está disponível no diretório público a lista com ramais e telefones celulares e pessoais atualizados, inclusive com telefones alternativos e endereços de contingência de seus membros.