HOSSEGOR GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CYBERSEGURANÇA E LGPD

Versão Atualizada: 5.0 – AGO/2025

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CYBERSEGURANÇA E LGPD

Contexto Operacional e de Negócios

A Política de Segurança da Informação, Cybersegurança e LGPD foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da HOSSEGOR:

- A HOSSEGOR executa suas atividades utilizando sistemas proprietários e de terceiros, todos apenas acessíveis via *web ou nuvem*, não possuindo nenhum sistema que necessite de instalações locais para ser executado;
- 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 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 diários, 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 e criptografia;
- 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.

Responsabilidades

Todos os Colaboradores devem atender aos procedimentos estabelecidos nesta Política de Segurança da Informação, Cybersegurança e LGPD, informando quaisquer irregularidades ao Diretor de Risco, *Compliance* e PLD, que deverá avaliá-las e submetê-las ao Comitê de Risco e *Compliance*, quando e conforme for o caso.

O Diretor de Risco, *Compliance* e PLD deve garantir o atendimento a esta Política de Segurança da Informação, Cybersegurança e LGPD, sendo o responsável na HOSSEGOR por temas de segurança da informação/cibernética.

Informações Confidenciais

São consideradas Informações Confidenciais aquelas não disponíveis ao público, que:

- Identifiquem dados pessoais ou patrimoniais da HOSSEGOR ou de clientes;
- Sejam objeto de NDA celebrado com terceiros;
- Identifiquem ações estratégicas dos negócios da HOSSEGOR, seus clientes ou dos portfólios sob gestão[5];
- Sejam informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da HOSSEGOR, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral; e
- Sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória.

Não caracteriza descumprimento desta Política de Segurança da Informação, Cybersegurança e LGPD a divulgação de Informações Confidenciais: (i) mediante prévia autorização do Diretor de Risco, *Compliance* e PLD; (ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente; e (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de Risco, *Compliance* e PLD acerca da possibilidade de compartilhamento da Informação Confidencial.

Identificação e Controle da Informação Confidencial

O Colaborador que recebe ou prepara uma informação pode classificá-la como Informação Confidencial considerando: (i) as questões de natureza legal e regulatória; (ii) estratégia negocial; (iii) os riscos do compartilhamento; (iv) as necessidades de restrição de acesso; e (v) os impactos no caso de utilização indevida da informação.

O acesso à Informação Confidencial deve ser restrito, controlado e as alçadas de acesso definidas em conjunto com a Área de Risco e/ou seu diretor. Seu arquivamento deve receber proteção adequada e seu descarte em meio físico deve ser efetuado utilizando preferencialmente máquina fragmentadora/trituradora de papéis ou incineradora.

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores, mesmo quando trabalhando remotamente. Ao usar uma impressora coletiva, o documento impresso contendo Informação Confidencial deve ser imediatamente recolhido.

Caso uma Informação Confidencial necessite ser divulgada a terceiros, deve ser precedida de assinatura de NDA, sob supervisão do Diretor de Risco, *Compliance* e PLD e eventualmente da assessoria jurídica da HOSSEGOR.

Princípios e Diretrizes – Segurança da Informação

Os seguintes princípios norteiam a segurança da informação na HOSSEGOR:

- Confidencialidade: o acesso à informação deve ser obtido somente por pessoas

[5] Cuja divulgação possa prejudicar a gestão dos negócios, clientes e portfólios a cargo da HOSSEGOR, ou reduzir sua vantagem competitiva.

autorizadas e quando for de fato necessário;
- Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário; e
- Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da HOSSEGOR para garantir a segurança da informação:

- As Informações Confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- A informação deve ser utilizada apenas para os fins sob os quais foi coletada; e
- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

Gestão de Acessos às Informações (dependências, rede, *internet, e-mail*)

Os Colaboradores terão acesso[6] somente às dependências, sistemas, arquivos, diretórios, pastas na rede e *e-mail* individual pertinentes a seu cargo e escopo de trabalho e deverão providenciar senha de proteção de acesso. Serão providenciadas, pela HOSSEGOR, as segregações, física e lógica, necessárias para cumprir com as diretrizes das políticas internas.

As senhas de proteção de acesso e os crachás utilizados para identificar o Colaborador e preservar a confidencialidade de informações são de uso pessoal e intrasferível, e qualificam o Colaborador como responsável por qualquer ação realizada por ele. As estações de trabalho devem ser acessadas via senha de proteção de acesso, tendo seu acesso bloqueado após minutos de inatividade.

A HOSSEGOR poderá, a qualquer momento, mediante prévia aprovação do Diretor de Risco, *Compliance* e PLD, e sem obrigação de cientificação prévia:

- inspecionar conteúdo e registrar o tipo de uso dos *e-mails* feitos pelos Colaboradores;
- disponibilizar esses recursos a terceiros, caso entenda necessário;
- solicitar aos Colaboradores justificativas pelo uso efetuado;
- monitorar acesso a *sites,* aplicativos etc.; e
- bloquear acesso a *sites*.

No caso de mudança de área ou desligamento do Colaborador, a senha de proteção de acesso será cancelada, impedindo acesso não autorizado pelo ex-Colaborador.

Os serviços de rede, *internet* e *e-mail* disponíveis na HOSSEGOR são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares.

[6] Quaisquer exceções deverão ser previamente solicitadas ao Diretor de Risco, *Compliance* e PLD.

Gestão de Riscos e Tratamento de Incidentes de Segurança da Informação

Os riscos e incidentes de segurança da informação, o vazamento de informação ou acesso indevido à informação devem ser reportados ao Diretor de Risco, *Compliance* e PLD, que adotará as medidas cabíveis[7].

Testes de Controles

A efetividade da Política de Segurança da Informação, Cybersegurança e LGPD é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de Risco, *Compliance* e PLD e reportados ao Comitê de Risco e *Compliance*.

Os testes[8] devem verificar se:

- Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;
- Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- Há segregação física e lógica;
- Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos; e
- A manutenção de registros permite a realização de auditorias e inspeções.

Os principais sistemas e serviços fornecidos por terceiros também devem ser objeto de testes, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. O Diretor de Risco, *Compliance* e PLD deve solicitar o resultado de tais testes aos fornecedores de tais sistemas, bem como acompanhar a solução de eventuais deficiências apontadas nos testes.

Riscos de Cybersegurança

As principais ameaças e riscos aos ativos cibernéticos da HOSSEGOR são:

- Malwares – softwares desenvolvidos para corromper os computadores e redes (vírus, cavalos de Tróia, *spywares* e *ransomware*);
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito *(pharming, phishing, vishing, smishin);*
- ataques de DDoS (*distributed denial of services*) e *botnets* – ataques visando a negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
- invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

[7] Podendo variar de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada (para que apague em definitivo o seu conteúdo), até o estudo e implementação efetiva de providências judiciais, quando e se for o caso, sem prejuízo da investigação e eventual punição dos Colaboradores envolvidos.

[8] Que podem ser realizados por terceiros, ou objeto de obrigação contratual, passível de reporte por prestadores de serviço, provedores de dados, aplicativos e ferramentas/*softwares*. Tais conteúdos podem ser passíveis de compor o relatório anual de *Compliance* exigido pela regulação aplicável da CVM.

Obrigações de Cybersegurança

Na prestação de seus serviços, a HOSSEGOR obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos[9].

São itens obrigatórios de cybersegurança (HOSSEGOR):

- A adequada proteção dos ativos cibernéticos, incluídos sua rede, sistemas, *softwares*, *websites*, equipamentos e arquivos eletrônicos.
- Restrição e controle do acesso e privilégios de usuários não pertencentes ao quadro de colaboradores;
- Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;
- Quando necessário, bloquear chaves de acesso de usuários, e, quando necessário, realizar auditoria para verificação de acessos indevidos;
- Excluir ou desabilitar contas inativas;
- Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;
- Garantir o cumprimento do procedimento de *backup* para os servidores e ativos cibernéticos, eletrônicos e computacionais;
- Detectar, identificar, registrar e comunicar ao Diretor de Risco, *Compliance* e PLD as violações ou tentativas de acesso não autorizadas;
- Organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário;
- Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;
- Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;
- Dispor de segurança nos servidores para acesso à sua rede, visando a manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado; e
- É realizado *backup* de arquivos de forma sistemática. Os dados de *backup* atualizados são armazenados em local seguro, com monitoramento.

São itens obrigatórios de cybersegurança (Colaboradores):

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Somente imprimir as mensagens quando realmente necessário;
- Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abrí-la, para vírus ou códigos maliciosos;
- No caso de recebimento de mensagens que contrariem as regras estabelecidas pela HOSSEGOR, nunca as repassar, alertando o responsável da sua área e o Diretor de Risco, *Compliance* e PLD, se for o caso;

[9] Os riscos potenciais relativos a tais dados envolvem invasões, disseminação errônea ou dolosa, acesso indevido e/ou seu roubo/desvio.

- Ao se ausentar do seu local de trabalho, mesmo quando estiver trabalhando remotamente e mesmo que temporariamente, bloquear a estação de trabalho;
- Quando sair de férias ou se ausentar por períodos prolongados, utilizar o recurso de ausência temporária de *e-mail*;
- Utilizar equipamentos, aplicativos, impressoras, acesso a *sites*, e *e-mail* (e demais ferramentas tecnológicas) com a finalidade primordial de atender aos interesses da HOSSEGOR;
- Não utilizar para fins particulares, nem repassar para outrem, tecnologias, marcas, metodologias e quaisquer informações que pertençam à HOSSEGOR, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho; e
- Ter acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

São itens vedados de cybersegurança (Colaboradores):

- Enviar *e-mail* ou acessar *sites* que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais[10];
- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico[11];
- Prejudicar intencionalmente usuários da *internet,* mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da HOSSEGOR;
- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo *e-mail* da HOSSEGOR;
- Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo Diretor de Risco, *Compliance* e PLD;
- Contratar provedores de acesso sem autorização prévia ou ciência do Diretor de Risco, *Compliance* e PLD; e
- Usar compartilhadores de informações, tais como redes *Peer-to-Peer* (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da HOSSEGOR.

Exceções a esta Política de Cybersegurança (Colaboradores):

- Caso haja uso de equipamentos ou dispositivos eletrônicos de propriedade dos colaboradores para desempenhar suas atividades na HOSSEGOR, estes se comprometem a adotar as medidas de segurança anteriormente citadas a fim de preservar seus equipamentos e minimizar o risco de comprometimento de segurança às informações sensíveis da HOSSEGOR, seus clientes e parceiros de negócio, podendo utilizar tais equipamentos para os diversos fins que considerar pertinentes;
- É facultado ao Diretor de Risco, *Compliance* e PLD autorizar exceções à esta política, devendo estar formalizadas por *e-mail*.

[10] Sendo proibido, sobretudo, conteúdo pornográfico, racista ou ofensivo à moral e aos princípios éticos.

[11] Exceção, é claro, a fluxos de informações necessários para a gestão de fundos e carteiras com instituições envolvidas nas operações dos clientes.

Proteção de Dados Pessoais (LGPD)

A HOSSEGOR, no exercício de suas atividades, tem e/ou pode vir a ter acesso a dados pessoais, conforme definidos na Lei n.º 13.709, de 14 de agosto de 2018 ("LGPD").

O tratamento de tais dados é feito nos estritos limites e finalidades da lei e da regulação aplicável (especialmente, sem limitação, as normas da CVM relativas a cadastro e identificação de clientes e operações), dado que o acesso de que aqui se trata é condição obrigatória para o desempenho das atividades da HOSSEGOR junto ao público investidor: assim, seu acesso e tratamento se dá em conformidade com estrutura, escala e ao volume de operações da HOSSEGOR, bem como à sensibilidade dos dados tratados.

Os dados pessoais, desta forma, são coletados e armazenados apenas e tão somente para estrito cumprimento da legislação e regulação aplicável às atividades da HOSSEGOR, sendo absolutamente vedada a sua destinação diversa pela HOSSEGOR e/ou quaisquer de seus Colaboradores: o seu eventual uso compartilhado com reguladores e autoridades poderá ser realizado somente nos estritos termos e limites das normas vigentes aplicáveis à HOSSEGOR, e para estrito cumprimento destas.

O tratamento e armazenamento dos dados pessoais recebidos durará pelo tempo em que perdurar o relacionamento entre a HOSSEGOR e o(s) titular(es) dos dados pessoais, sempre respeitando simultaneamente o prazo determinado pelas normas vigentes a elas aplicáveis.

As informações de contato e responsáveis da HOSSEGOR a esse respeito encontram-se em seu *website*, cabendo ao Diretor de Risco, *Compliance* e PLD supervisionar Colaboradores e zelar pelo tratamento de tais dados, sempre resguardados os direitos do titular contemplados no art. 18 da LGPD, quais sejam:

- confirmação, para o titular dos dados pessoais, da existência do tratamento destes;
- acesso aos seus dados em poder da HOSSEGOR;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- eliminação dos dados pessoais tratados com o consentimento do titular (exceto, nos termos do art. 16 da LGPD, nas hipóteses de (a) cumprimento de obrigação legal ou regulatória pela HOSSEGOR, (b) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD, ou (c) uso exclusivo da HOSSEGOR, vedado seu acesso por terceiro, e desde que anonimizados os dados);
- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
- revogação do consentimento.

Nas hipóteses em que o consentimento para o tratamento de dados pessoais for necessário, se houver mudanças da finalidade para o tratamento de dados pessoais não

compatíveis com o consentimento original, a HOSSEGOR deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- fim do período de tratamento;
- comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento; ou
- determinação da autoridade nacional, quando houver violação ao disposto na LGPD.