

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

Para qualquer dúvida relativa a esta política, falar com:

Segurança da Informação

Gestor: Segurança da Informação

Aprovado por: Vice-Presidência

Usuários: Todos os colaboradores

Esta política aplica-se à ABC IB HOLDING LTDA., seus funcionários, filiais e subsidiárias, inclusive as controladas ABC DCM LTDA., ABC M&A e ECM LTDA. Em caso de conflito entre esta política e as legislações locais onde se encontram as representações do exterior impossibilitando seguir as disposições aqui contidas, os pedidos de exceção deverão seguir as diretrizes determinadas em políticas específicas.

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

Índice

1. Introdução	4
2. Escopo.....	4
3. Definição.....	5
4. Responsabilidades	6
5. Requerimentos da Política	7
6. Revisão da Política	10
Apêndice A – Formulário de Exceção à Política de Segurança da Informação ..	11

ABC IB HOLDING LTDA.

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

Histórico:

Versão	Data	Descrição	Gestor
01	27/09/2023	Criação da Política de Segurança da Informação.	Segurança da Informação

Nota: Esta Política deverá ser revista pelo Gestor a cada dois anos, ou em menor período, caso necessário.

Data de Aprovação:
22/01/2024

Pág. 3 de 11

Última Revisão:
22/01/2024

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

1 – Introdução

Informação e seus sistemas de suporte são bens críticos, e como tais, devem ser protegidos por controles adequados. A Política de Segurança da Informação da **ABC IB HOLDING LTDA.** é o fundamento da visão e estrutura de gestão de segurança da informação. Ela especifica os requisitos e define as linhas gerais para a organização da segurança da informação no nível mais alto de gestão sênior. A política de segurança será suportada por diretrizes e procedimentos detalhados.

A presente Política protegerá contra ameaças, incluindo o acesso não autorizado, modificação, roubo, perda, destruição, ou divulgação inadequada, de forma deliberada ou acidental, de informações, sistemas e aplicativos que processam as informações, e os recursos de informação.

Objetivos

- Proteger a reputação, integridade, ética e a imagem pública do grupo ABC;
- Manter a confiança dos clientes, órgãos regulatórios e acionistas na organização;
- Proteger a confidencialidade de informações sensíveis (pessoais, financeiras, etc.);
- Proteger dados operacionais sensíveis evitando disseminação indevida;
- Impedir ações ilegais ou maliciosas através dos sistemas da organização;
- Suportar o grupo para maximizar o valor dos recursos investidos em TI, garantindo que não sejam mal utilizados ou desperdiçados;
- Impedir fraudes;
- Impedir incidentes caros ou que causem paralisação de serviços;
- Aderir a leis e regulamentações;
- Suportar os objetivos de negócio, protegendo as informações da **ABC IB HOLDING LTDA.**;
- Reduzir o risco de confidencialidade, integridade e disponibilidade, definindo os princípios para uso da informação e dos sistemas de informação;
- Definir uma base onde políticas, diretrizes, padrões e procedimentos mais detalhados possam ser derivados.

2 – Escopo

Esta política aplica-se a:

- Todas as formas, incluindo atividades de processamento de informação, informação computadorizadas, armazenadas em servidores, computadores pessoais, bases de dados ou manualmente armazenadas em arquivos;

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

- Todos os aplicativos, sistemas operacionais e softwares;
- Todos os equipamentos, servidores, estações de trabalho, laptops, componentes de rede, dispositivos de comunicação e periféricos de propriedade da **ABC IB HOLDING LTDA.**;
- Todas as localidades que hospedam sistemas de informação da **ABC IB HOLDING LTDA.**, e todos os recursos que suportam os sistemas de informação;
- Todos os colaboradores e contratados permanentes, consultores, vendedores e fornecedores assinalados para trabalhar junto à **ABC IB HOLDING LTDA.**;
- É MANDATÓRIO que todos os indivíduos que são membros dos grupos acima acatem esta política e qualquer outro padrão derivado dela.

3 – Definição

Segurança da Informação - são esforços contínuos para a proteção dos ativos de informação, auxiliando a organização a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

- **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas, sendo acidentais ou propositais;
- **Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

Ativo de Informação - é uma entidade definida de informação, armazenada de uma maneira que é reconhecida como valiosa. Um ativo de informação possui uma ou mais das seguintes características:

- É reconhecido como tendo valor para a organização;
- Não é facilmente trocado sem custo, conhecimento, tempo recursos ou uma combinação destes itens;
- É parte da identidade da corporação, sem a qual, a organização pode estar ameaçada;
- Sua classificação normalmente indica algo proprietário, altamente confidencial ou até mesmo segredo.

É propósito da Segurança da Informação identificar ameaças contra ativos de informação, os riscos potenciais de danos e assegurar que estejam protegidos.

Comitê de Risco Operacional e Compliance (CROC) - Fórum institucional para discussão e aprovação de assuntos relativos a risco operacional, controles internos, agenda normativa, acompanhamento de planos de ação e pontos de auditoria.

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

4 – Responsabilidades

4.1 – Colaborador

Responsável por:

- Observar e seguir as normas, padrões e procedimentos estabelecidos para o cumprimento da presente Política de Segurança da Informação;
- Coletar todas as assinaturas necessárias para que a regra de exceção seja permitida.

4.2 - Área de Recursos Humanos

Responsáveis por assegurar que todos os colaboradores admitidos estejam cientes desta política de segurança da informação.

4.3 – Auditoria Interna

Responsável por executar auditorias periódicas para assegurar que as unidades de negócio da **ABC IB HOLDING LTDA.** estão aderentes às políticas, diretrizes, padrões e procedimentos de segurança da informação.

4.4 – Proprietário da Informação

Responsáveis por definir a classificação e autorização nos sistemas sob seu controle.

4.5 – Usuários de Informações ou Sistemas

Responsáveis pela proteção da informação de acordo com as regras estabelecidas por esta política.

4.6 – Gestores

Responsáveis por:

- Assegurar que todos os colaboradores de sua equipe estejam cientes desta política de segurança informação;
- Devem aplicar e executar os controles projetados para salvaguardar os ativos de informação, incluindo informações de negócio;
- Avaliar os controles que impeçam a aderência às Políticas de Segurança da Informação e aprovar a solicitação encaminhada pelo solicitante;
- Definir os níveis de controle e segurança necessários, em função da exceção solicitada, considerando os riscos do Negócio.

4.7 – Segurança da Informação

Data de Aprovação:
22/01/2024

Pág. 6 de 11

Última Revisão:
22/01/2024

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

Responsáveis por:

- Dar manutenção a esta política e todas as políticas específicas derivadas desta;
- Ter conhecimento da exceção assinando o formulário de Exceção à Política de Segurança da Informação;
- Assegurar que as exceções aprovadas sejam revisadas dentro do prazo definido, compatível com o nível de risco do processo associado e salvaguardados para controle com a auditoria;
- Submeter ao CROC possíveis riscos em função da concentração de exceções em determinadas áreas.

5 – Requerimentos da Política

É missão e responsabilidade de cada colaborador da **ABC IB HOLDING LTDA.**, prestador de serviços, parceiro e visitante, observar e seguir as normas, padrões e procedimentos estabelecidos para o cumprimento da presente Política de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança de informações em suas atividades diárias.

Todas as atividades executadas pela **ABC IB HOLDING LTDA.**, por meio de seus colaboradores, prestadores de serviços, parceiro e visitante, devem observar a legislação vigente e a normatização de entidades governamentais regulatórias, com relação à segurança da informação.

Faz parte do conjunto de responsabilidades de todos em conhecer o conjunto de políticas de segurança e suas definições mais específicas.

Para auxiliar a todos os colaboradores nessa missão a **ABC IB HOLDING LTDA.** criou uma área de Segurança da Informação que administra as disciplinas de conhecimento que dão suporte a essa ciência. A área de Segurança da Informação da **ABC IB HOLDING LTDA.** é responsável por editar as normas, padrões e procedimentos que apoiam a todos na proteção dos ativos de informação, e está preparada para auxiliar na resolução de problemas relacionados ao tema.

5.1. Proteção da Informação

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos da **ABC IB HOLDING LTDA.**, a informação deve ser adequadamente manuseada e protegida.

A informação pode estar presente em diversas formas, tais como: sistemas de informação, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes ou até mesmo por meio da comunicação verbal.

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

Toda informação gerada ou desenvolvida nas dependências da **ABC IB HOLDING LTDA.** constitui ativo da organização, essencial à condução de negócios e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da **ABC IB HOLDING LTDA.**

É diretriz da **ABC IB HOLDING LTDA.** que toda informação de propriedade da **ABC IB HOLDING LTDA.** seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

5.2 Princípios de Segurança da Informação

5.2.1 Proteção dos Sistemas de Informação

As informações e os sistemas de informação devem ser classificados segundo seu nível de confidencialidade e devem ser tratados em conformidade com sua classificação durante sua posse e comunicação a outros colaboradores, prestadores de serviço e público em geral.

Todos os sistemas de informação devem possuir um gestor, responsável pela definição da sua correta utilização e por sua segurança. O gestor de cada sistema é o responsável por autorizar o acesso à informação e ao sistema e garantir que a sua utilização está aderente à Política de Segurança da Informação da **ABC IB HOLDING LTDA.**

5.2.2 Acesso a Sistemas e Recursos de Rede

O colaborador é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

O acesso e uso de todos os sistemas de informação devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados.

Todos os acessos remotos à recursos de rede e sistemas internos devem ser realizados através de meios seguros adicionando um segundo fator de autenticação, acessos remotos para suporte pontual podem ser realizados sem autenticação, porém devem ser autorizados pelo colaborador responsável pela solicitação de suporte e acompanhar as ações 100% do tempo conforme política de acesso remoto.

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

A concessão de acesso às informações e sistemas deve ser autorizada pelo respectivo gestor responsável com base na regra de mínimo acesso necessário para o desempenho da sua função.

O acesso e uso de recursos de rede, incluindo mensagens eletrônicas e acesso à Internet, devem estar alinhados às atividades de negócio da **ABC IB HOLDING LTDA.** O uso esporádico e responsável para fins pessoais é permitido, à medida que não interfiram no trabalho do colaborador ou impliquem em conflito de interesses da **ABC IB HOLDING LTDA.**

A utilização de recursos de rede, sistemas e outras fontes de informação serão monitorados pela **ABC IB HOLDING LTDA.**, por meio de registros de auditoria em computadores, sistemas, mensagens eletrônicas e acessos à Internet, entre outros. Essas informações podem ser coletadas e utilizadas, a critério da **ABC IB HOLDING LTDA.**, para a execução de investigações internas ou para atendimento de medidas judiciais, sem aviso prévio às pessoas envolvidas, respeitando-se, porém, a privacidade dos colaboradores.

Apenas os equipamentos e software disponibilizados ou homologados pela **ABC IB HOLDING LTDA.** serão permitidos nas suas dependências. Equipamentos pessoais de colaboradores e prestadores de serviço devem ser controlados pelo gestor da área e devem ter sua conexão de rede controlada e restringida.

Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

5.2.3 Privacidade

Todos os colaboradores devem tomar conhecimento da Política de Privacidade, disponível no site <https://www.abcbrasil.com.br/abc-corporate/investment-banking>, onde estão descritos os princípios básicos adotados pela **ABC IB HOLDING LTDA.** para recepção, armazenamento e utilização das informações pessoais disponibilizadas por clientes e visitantes.

5.3 Violação da Política, Normas e Procedimentos de Segurança

Violações as regras estabelecidas pela Política de segurança da informação devem ser informadas ao seu gestor imediato, e simultaneamente, à área de Segurança da Informação. Toda violação ou desvio será investigado para a determinação das medidas necessárias visando à correção da falha ou reestruturação de processos.

Os princípios de segurança da informação estabelecidos na presente política possuem total aderência da administração da **ABC IB HOLDING LTDA.** e devem

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

ser observados por todos na execução de suas funções. A não conformidade com as diretrizes desta política e a violação de normas derivadas dela, sujeita os colaboradores da **ABC IB HOLDING LTDA.** a ações disciplinares e trabalhistas e, aos prestadores de serviços, inclui-se a rescisão de contratos e a penas de responsabilidade civil e criminal na máxima extensão que a lei permitir.

5.4 – Exceções a Política de Segurança da Informação

A política de exceção ao grupo de Políticas de Segurança da Informação é um recurso para ser usado em casos especiais onde existam:

- Incapacidade técnica;
- Limitação sistêmica;
- Carência de refinamento de controles internos que impeça a aderência plena às regras definidas na política de segurança corporativa.

O documento de dispensa padrão deve ser revisado anualmente com as devidas aprovações.

As exceções à Política de Segurança da Informação devem assegurar que a inexistência dos controles a estas regras, sejam devidamente geridas e registradas.

5.4.1 - Formulário de Exceção

O formulário anexo (**apêndice A**) deve ser preenchido e aprovado sempre que houver necessidade de justificar uma exceção ao grupo de Políticas de Segurança da Informação.

A falta de uma ou mais aprovações descaracteriza o formulário como válido.

O formulário de exceção pode ser cancelado a qualquer momento pelo requerente, pela área de Segurança da Informação mediante prévio aviso ou caso a condição solicitada seja resolvida e não mais necessária.

6 – Revisão da Política

6.1 – Esta Política deve ser revisada pelo Gestor no período máximo de dois anos, ou menor, se necessária alguma alteração.

Política:

Código.Versão:

Segurança da Informação

5052.ORG.01

Apêndice A– Formulário de Exceção à Política de Segurança da Informação

FORMULÁRIO DE EXCEÇÃO À POLÍTICA		
Solicitante: <Nome do solicitante>	Data: <Data deste formulário>	
Área: <Nome da área>	Gestor: <Nome do gestor >	
Sistema/Recurso: <Nome do sistema ou recurso envolvido>	Responsável pelo Sistema/Recurso: <Nome do responsável pelo sistema ou recurso>	
Política impactada: <Política para a qual está sendo solicitada a exceção>		
CLASSIFICAÇÃO DE SEGURANÇA DA INFORMAÇÃO		
Confidencialidade: <Nível de risco> <ALTA/MÉDIA/BAIXA>	Integridade: <Nível de risco> <ALTA/MÉDIA/BAIXA>	Disponibilidade: <Nível de risco> <ALTA/MÉDIA/BAIXA>
DESCRIÇÃO DO SISTEMA / RECURSO		
<Descrever o sistema/recurso para o qual está sendo solicitada a exceção>		
JUSTIFICATIVA		
<p><Identificar o item na política de segurança para o qual se está solicitando e justificar a necessidade de exceção. ></p> <p><declarar as limitações técnicas, de processos ou pessoas que serão envolvidas. Identificar qual o processo que está sendo alterado e quais serão as pessoas que nominalmente terão dispensa na política de segurança. Identificar os controles técnicos que serão modificados e o nível de acesso privilegiado, se for o caso. Documentar o Período de validade para esta dispensa></p> <p><declarar se esta dispensa ainda infringe alguma regra ou exigência regulatória></p>		
POTENCIAL PERDA FINANCEIRA OU IMPACTO		
<p>Integridade dos dados: <descrever se esta dispensa afeta o nível de integridade de algum dado da ABC IB HOLDING LTDA.></p> <p>Disponibilidade dos dados: <descrever se esta dispensa afeta o nível de disponibilidade de algum componente da ABC IB HOLDING LTDA.></p> <p>Confidencialidade dos dados: <descrever se esta dispensa afeta o nível de confidencialidade de algum dado da ABC IB HOLDING LTDA.></p>		
APROVAÇÕES		
<Obter a aprovação do Gestor, Solicitante e Segurança Informação>		

O FORMULÁRIO PREENCHIDO DEVE SER ENTREGUE A ÁREA DE SEGURANÇA DA INFORMAÇÃO APÓS AS DEVIDAS APROVAÇÕES PARA QUE A EXCEÇÃO SEJA LIBERADA.