Controle de alterações

Versão	Início de vigência	Principais alterações
3.0	21.09.2018	CONAD – 254ª RO – 21/09/2018
4.0	28.01.2019	Alteração de periodicidade de atualização - CONAD – 258ª RO, de 28.01.2019
5.0	29.01.2021	Revisão anual.

1. Objetivo

Esta Política define os princípios para a segurança da informação, visando preservar a integridade, confidencialidade e disponibilidade das informações (incluindo dados pessoais que sejam tratados pela Companhia nos termos da Lei nº 13.709/18 – Lei Geral de Proteção de Dados ou LGPD).

2. Abrangência

Esta Política aplica-se a qualquer fato, evento ou atividade que afete a segurança das informações corporativas, seja por colaborador (diretor, funcionário, estagiário, jovem aprendiz e membros de órgãos estatutários) ou relacionado (terceiro, fornecedor, parceiro comercial e parte relacionada) que tenha algum tipo de relação de negócio ou contratual com o IRB Brasil RE, suas filiais e suas controladas, diretas e indiretas, no Brasil e no exterior, definida doravante como “Companhia”.

3. Referências

3.1. As normas, internas e externas, abaixo relacionadas, foram consideradas na elaboração desta política:

a) Norma – 5.01.08 – Gestão de Incidentes de Segurança da Informação
- Define a estrutura formal, sua operacionalização e as responsabilidades necessárias para analisar, responder e registrar os incidentes de segurança da informação, bem como propor medidas preventivas e corretivas relativas aos mesmos.

b) Norma – 5.03.01 – Classificação e Tratamento da Informação
- Descreve os principais controles para assegurar que as informações do IRB Brasil RE possuam um nível adequado de proteção, considerando sua sensibilidade e criticidade.

c) Norma – 5.01.12 – Norma de Uso Aceitável de Ativos de TI
- Descreve as regras de uso aceitável dos ativos de TI do IRB Brasil RE e as atividades consideradas proibidas.

d) Norma – 8.01 – Uso e Tratamento de Dados
- Orienta os colaboradores no tratamento de dados pessoais de clientes, potenciais clientes, outros colaboradores, fornecedores, prestadores de serviço, dentre outros, no âmbito do desenvolvimento de suas funções na Companhia, respeitando às legislações de proteção de dados pessoais, em especial à LGPD.

e) Norma – 8.04 – Uso e Privacidade do Site
- Regula a relação com o IRB BRASIL RESSEGUROS S.A. (“IRB Brasil RE” ou “Companhia”) quando um indivíduo utiliza o website irbre.com, detalhar em que hipóteses e para quais finalidades utilizamos suas informações quando o mesmo interage com o site.

f) Norma – 5.01.04 – Glossário de Segurança da Informação
- Esclarece os conceitos utilizados dentro do corpo normativo da Política de Segurança da Informação do IRB Brasil RE.

g) Norma – 5.02.01 – Controle de Acesso
- Estabelece diretrizes de controle para o acesso físico às dependências que hospedam ativos críticos de TI da Companhia e estabelecer diretrizes de controle para o acesso lógico às informações.

h) Norma – 5.01.14 – Desenvolvimento Seguro
- Regulamenta o processo de desenvolvimento e manutenção de sistemas do IRB Brasil RE.

i) ABNT NBR ISO/IEC 27000, 27001, 27002, 27003, 27004 – SGSI (Conjunto de diretrizes estabelecidas pela Associação Brasileira de Normas Técnicas a respeito do Sistema de Gestão de Segurança da Informação)

j) Circular SUSEP nº 605/2020 (Estipula prazo para guarda de documentos e dispõe sobre armazenamento de documentos).

3.2. Além dessas referências, esta Política é instrumentalizada por normas de natureza operacional, procedimentos e outros documentos afins que orientam a sua aplicação prática.

4. Definições

a) Os termos utilizados nesta Política encontram-se definidos na norma 5.01.04 – Glossário de Segurança da Informação.

5. Princípios

5.1. Todas as informações devem ser classificadas quanto ao acesso e uso, de maneira que possam ser adequadamente gerenciadas, protegidas e manipuladas durante o seu ciclo de vida. A classificação das informações deverá ser realizada de acordo com a norma 5.03.01 – Classificação e Tratamento da Informação.

5.2. O princípio da segregação de função deve ser aplicado para as atividades que envolvam riscos para a organização. No caso de impossibilidade, controles adicionais devem ser estabelecidos, no sentido de mitigar riscos.

5.3. As informações da Companhia devem ser utilizadas de modo ético e seguro.

5.4. Os recursos e as informações geradas internamente – salvo aquelas protegidas por lei e os dados pessoais – são de propriedade do IRB Brasil RE e seu uso deve servir exclusivamente ao atendimento dos interesses da Companhia.

5.5. Mesmo após se desligarem de suas atribuições, colaboradores e demais agentes não poderão revelar ou divulgar informações sigilosas com as quais tenham lidado no exercício da função. As relações laborais e de serviços (contratos), devem prever este compromisso formalmente.

5.6. Testes nos sistemas em ambiente de produção podem ser realizados somente com autorização formal do Diretor de Tecnologia da Informação, uma vez que tenham informações sobre início e fim das atividades bem como escopo do que será testado e avaliação dos possíveis impactos e planos de recuperação estabelecidos. A realização de qualquer teste, ainda que autorizada deve ser monitorada e registrada em trilhas de auditoria.

Nota:
É proibida a realização de qualquer outra atividade fora do escopo e/ou horário autorizados.

5.7. O acesso ao ambiente de produção por consultor terceirizado é permitido somente com a autorização expressa e formal do Diretor de Tecnologia da Informação. Os contratos devem estabelecer claramente as responsabilidades e obrigações dos mesmos.

5.8. Os recursos tecnológicos disponibilizados pelo IRB Brasil RE, incluindo o acesso à internet, são ferramentas de trabalho e devem ser usados para atividades de interesse da Companhia, de acordo com a norma 5.01.12 – Norma de Uso Aceitável de Ativos de TI.

5.9. O uso dos recursos tecnológicos para fins particulares pode ser tolerado, em conformidade com os normativos internos complementares e desde que:

a) não viole a legislação e a regulamentação aplicável;
b) não comprometa a imagem da Companhia;
c) não comprometa a imagem de seus colaboradores;
d) não comprometa a imagem de terceiros;
e) não prejudique as atividades de trabalho;
f) não prejudique os processos da gerência;
g) não prejudique a segurança das informações e dos recursos corporativos; e
h) não seja usado para nenhuma manifestação política e religiosa.

5.9.1. No caso do exercício desta opção por partes dos usuários, a Companhia se isenta de qualquer responsabilidade quanto aos dados particulares instalados nos referidos recursos.

5.10. O acesso ao recurso disponibilizado para o usuário deve ser o estritamente necessário e indispensável ao exercício de suas atividades.

5.11. A troca de informações internas da organização com parceiros de negócios e entidades externas deve seguir requisitos mínimos de segurança da informação a ser definido em normas complementares à esta política.

5.12. Todos os recursos computacionais corporativos (Laptops, Desktops, Smartphones e outros) capazes de armazenar dados devem ser examinados antes do descarte pela área de Tecnologia da Informação, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança, de acordo com norma 5.03.01 – Classificação e Tratamento da Informação.

5.13. Toda a documentação dos sistemas deve ser protegida contra acessos não autorizados.

5.14. Em computadores corporativos devem ser utilizados somente softwares fornecidos pela Tecnologia da Informação da Companhia.

5.15. As informações devem ter a sua disponibilidade garantida pelo período requerido pelo negócio, pelo período de guarda legal e regulamentar e durante os processos judiciais nos quais componham evidências objetivas.

5.16. Os recursos computacionais são corporativos e o IRB Brasil RE se reserva ao direito de monitorar o uso e a custódia de suas informações bem como o uso dos seus recursos de informação independente de tais recursos computacionais, por opção dos usuários, conterem dados pessoais.

5.17. A credencial concedida para o acesso aos recursos de informação (senha), é pessoal, intransferível e deve ser mantida de modo seguro, de acordo com a norma 5.02.01 – Controle de Acesso.

5.18. A aquisição, desenvolvimento e manutenção de sistemas deve obedecer às regras de segurança estabelecidas pelo IRB Brasil RE.

5.19. A arquitetura de tecnologia e segurança, ativos tecnológicos, bem como modelos de acesso a aplicações e informações deve obedecer às regras de segurança estabelecidas em normas complementares de segurança da informação, assim como qualquer proposta de alteração destes ambientes deve ser submetida de maneira prévia a área de segurança da informação para emissão de parecer consultivo, de acordo com a norma 5.01.14 – Desenvolvimento Seguro.

5.20. Os incidentes de segurança da informação devem ser registrados, evidenciados, tratados e monitorados, nos termos da Norma 5.01.08 – Gestão de Incidentes da Segurança da Informação.

5.21. Todos os colaboradores são responsáveis por reportar incidentes de segurança da informação, uma vez que sejam detectados, através dos meios oficiais de reporte de incidentes.

5.22. Os processos críticos de negócios devem ser assegurados por um Plano de Continuidade de Negócios.

5.23. 5.23. Sempre que possível, caberá a Administração buscar proteções aos riscos, inclusive seguros especializados.

6. Comprometimento

6.1. Conforme previsto no Estatuto é responsabilidade-do Conselho de Administração:

a) aprovar objetivos e diretrizes de Segurança da Informação refletidos na Política de Segurança da Informação;

6.2. São responsabilidades da Diretoria em relação à Segurança da Informação:

a) estabelecer e comunicar objetivos corporativos de segurança da informação;
b) estabelecer papéis e responsabilidades pela Segurança da Informação;
c) manter a organização comprometida com os objetivos da Segurança da Informação e com a importância de manter a conformidade com os requisitos de segurança emanados de instâncias internas e externas;
d) prover os recursos para a operação do SGSI;
e) estabelecer e comunicar diretrizes de aceitação de riscos relativos à segurança da informação;
f) garantir a realização de auditorias periódicas do SGSI; e
g) estabelecer penalidades para quem descumprir esta política e normas relacionadas, considerando dosimetrias em razão do nível de gravidade de cada ato.

6.3. São responsabilidades dos gestores:

a) analisar os procedimentos de suas respectivas áreas à luz das normas de Segurança da Informação e identificar pontos de melhoria em processos, nos controles, na proteção dos ativos utilizados e na capacidade do pessoal agir em conformidade com os ditames da Segurança da Informação;
b) adotar medidas destinadas a reduzir os riscos identificados, sempre em consonância com as normas da Companhia e com as orientações emitidas pelo Comitê Executivo de Segurança da Informação;
c) atuar cotidianamente no aumento do grau de conscientização de seus subordinados quanto à importância de considerar as medidas de segurança da informação no desempenho de suas atividades; e
d) assegurar que os fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis de modo a reduzir o risco de roubo, vazamento ou mau uso da informação.

6.4. São responsabilidades do Comitê Executivo de Segurança da Informação:

a) estabelecer as diretrizes e práticas de Segurança da Informação, que irão atender os objetivos corporativos, bem como, liderar sua implementação e o contínuo aprimoramento de um Sistema de Gerenciamento da Segurança da Informação na Companhia;
b) supervisionar o manuseio dos ativos de informação da organização; e
c) aprovar o Plano Diretor de Segurança de Informação e prover o suporte necessário para sua execução em todos os seus aspectos.

6.5. Cabe à Diretoria de Pessoas adotar as medidas necessárias para que os colaboradores sejam capazes de atuar eficientemente e utilizar os recursos adequados no desempenho das atividades inerentes à salvaguarda de informações. Para tal, ela deverá:

a) determinar as competências necessárias para o pessoal que executa atividades relacionadas ao SGSI;
b) fornecer treinamento para que o pessoal desenvolva estas competências;
c) avaliar a eficácia das ações de capacitação realizadas; e
d) manter registros detalhados deste processo contínuo de capacitação.

6.6. É dever de cada um dos colaboradores, prestadores de serviço, membros da Diretoria e Conselho de administração zelar pela segurança da informação da Companhia, observar a Política de Segurança da Informação, atuar em linha com normas, padrões e procedimentos vigentes, sugerindo aperfeiçoamentos e agindo proativamente na salvaguarda da segurança de informações pertinentes aos negócios da Companhia.

7. Disposições finais

7.1. O desconhecimento da Política de Segurança da Informação da Companhia não exime os colaboradores e demais agentes de suas responsabilidades perante a Companhia.

7.2. A inobservância das regras da Política de Segurança da Informação pode implicar em sanções previstas no Regime Disciplinar, conforme o caso e julgamento da Diretoria da Companhia.

7.3. O cumprimento das normas de Segurança da Informação deve ser auditado periodicamente pela Auditoria Interna da Companhia.

7.4. Os casos omissos serão analisados pelo Comitê Executivo de Segurança da Informação e encaminhados para deliberação da Diretoria Estatutária e Conselho de Administração.

7.5. Na eventualidade da dissolução do comitê de segurança, suas responsabilidades ficarão a cargo do novo órgão de governança superior.

7.6. Esta política deve ser revisada e atualizada, em caráter ordinário, anualmente, e extraordinariamente por demanda, pela Gerência de Governança, Segurança da Informação e Controle, e submetida à deliberação da Diretoria Estatutária e do Conselho de Administração, sempre que houver mudanças na legislação, de cenários ou operacionais.