Versão	Vigência/Aprovação	Principais alterações	Área gestora
003	21.09.2018	CONAD – 254ª RO, de 21.09.2018	Gerência de Governança, Seg. da Informação e Controle
004	28.01.2019	Alteração de periodicidade de atualização - CONAD – 258ª RO, de 28.01.2019	Gerência de Governança, Seg. da Informação e Controle
005	29.01.2021	Revisão anual	Gerência de Governança, Seg. da Informação e Controle
006	27.04.2023	Revisão anual, de adequações solicitadas pelo Conselho de Administração e adequações relativas à Circular SUSEP 638/2021 – Aprovada na 309ª RO do CA.	Gerência de Governança, Seg. da Informação e Controle
007	25.07.2023	Alteração de layout, obedecendo o novo modelo proposto no projeto de revisão de normativos	Gerência de Governança, Seg. da Informação e Controle
008	20.12.2024	Revisão das responsabilidades das 3 linhas quanto ao tema segurança da informação; inclusão de diretrizes sobre uso de inteligência artificial e incidentes de segurança da Informação.	Gerência de Governança, Seg. da Informação e Controle

Sumário

1. Objetivo e Abrangência

Esta Política define os princípios para a segurança da informação e cibersegurança, 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) e em cumprimento ao disposto na Circular SUSEP 638/2021 e demais regulamentações aplicáveis.

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(Re), suas filiais e suas controladas, diretas e indiretas, no Brasil e no exterior, definida doravante como “Companhia”.

2. Definições

- **Ativo:** Tudo aquilo que possui valor para a companhia.
- **Colaborador:** Funcionários com vínculo empregatício de qualquer área do IRB(Re) ou terceiros alocados na prestação de serviços, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do IRB(Re) para o desempenho de suas atividades profissionais.
- **Confidencialidade:** Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Controle:** Medida de segurança que mantém ou modifica um risco. Os controles incluem, mas não se limitam a qualquer processo, política, dispositivo, prática ou outras condições e/ou ações que mantenham e/ou modifiquem o risco.
- **Controle de Acesso:** Garantia que o acesso físico e lógico aos ativos seja autorizado e restrito com base nos requisitos de segurança da informação.
- **Disponibilidade:** Garantia de que as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da Companhia.
- **Integridade:** Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Segurança da Informação**: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da Companhia de forma global, incluindo a Segurança Cibernética que se concentra na segurança de redes, dispositivos e sistemas contra ameaças.
- **Sistema de Gestão de Segurança da Informação - SGSI**: Conjunto de políticas, processos, procedimentos, manuais e recursos que visam proteger as

informações de uma empresa, garantindo a confidencialidade, integridade e disponibilidade das mesmas.

- **Plano Diretor de Segurança da Informação - PDSI**: Instrumento que ajuda a alinhar a segurança com os objetivos da empresa, estabelecendo a estratégia, e controles para garantir a segurança da informação de uma organização.

3. Desenvolvimento

3.1. Princípios

A proteção da segurança da informação pode ser definida como: garantir a confidencialidade, integridade e disponibilidade.

A Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários, o que significa que sua aplicação, ou a falta dela, afeta todas as áreas de uma Companhia, organização ou empresa. Deve, portanto, ser cumprida e aplicada em todas as áreas do IRB(Re).

Dessa forma, o IRB(Re) estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção às informações da Companhia ou sob sua responsabilidade.

3.2. Diretrizes

Todas as informações devem ser classificadas pelo proprietário quanto ao acesso e uso, de maneira que possam ser adequadamente gerenciadas, protegidas e manipuladas durante o seu ciclo de vida, de acordo com os seguintes níveis de classificação: Pública, Reservada, Confidencial ou Sigilosa e seguindo as demais regras estabelecidas na Norma de Classificação e Tratamento da Informação.

Funções conflitantes e áreas conflitantes de responsabilidade devem ser segregadas, conforme o princípio de segregação de função. Sempre que a segregação de funções não seja tecnicamente viável, devem ser implementados outros controles compensatórios para minimizar os riscos, tais como o acompanhamento das atividades.

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

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

Mesmo após se desligarem de suas atribuições, colaboradores e partes interessadas (relacionados) 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.

Testes nos sistemas em ambiente de produção podem ser realizados somente com autorização formal do Diretor de Tecnologia da Informação uma vez que tenha 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.

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

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

Nota: Na ausência do Diretor de Tecnologia da Informação, as autorizações citadas acima devem ser concedidas de maneira formal por todos os gerentes de tecnologia existentes na estrutura organizacional da TI ou pelo substituto descrito na Norma de Alçadas e Substituições.

Os recursos tecnológicos disponibilizados pelo IRB(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 de Uso Aceitável de Ativos de TI.

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

A troca de informações internas da organização com parceiros de negócios e entidades externas deve seguir requisitos mínimos de segurança da informação a serem definidos em normas complementares à esta Política.

Conforme Norma de Uso Aceitável de Ativos de TI é recomendável que os colaboradores utilizem o diretório de rede respectivo ao seu drive pessoal para backup de suas informações corporativas, ou canal equivalente designado pela TI, para evitar a perda de informações.

Para as informações corporativas presentes nos recursos computacionais do IRB(Re) devolvidos à TI, por ocasião do desligamento do colaborador, é obrigatória a preservação destas informações por até 7 dias corridos após a devolução, caso não seja solicitada a retenção. Caso o gestor da informação solicite, essas informações poderão ser cedidas a ele, por meio de diretório de rede ou canal equivalente designado pela TI.

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

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

Em computadores corporativos devem ser utilizados somente softwares fornecidos pela Gerência de Governança, Segurança da Informação e Controle.

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.

Os recursos computacionais são corporativos e o IRB(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.

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 de Controle de Acesso.

Instalação ou desinstalação de programas, exclusão de dados e formatação em recursos computacionais corporativos (Laptops, Desktops, Smartphones e outros) devem ser realizados por profissionais técnicos da área de TI (HelpDesk) responsáveis por prestar suporte aos colaboradores, e devem possuir acesso de “administrador” a estes recursos para a execução destas atividades.

O acesso a dados da companhia só deve ser efetuado por meio de dispositivos e aparelhos de propriedade do IRB(Re). Entretanto, o acesso a dados por meio de dispositivos não corporativos pode ser efetuado, de forma segura, somente através de soluções ou ferramentas corporativas disponibilizadas pela Gerência de Governança, Segurança da Informação e Controle, que asseguram a proteção do ambiente (por exemplo, Citrix, App Stream ou similar etc.).

A aquisição, desenvolvimento e manutenção de sistemas deve obedecer às regras de segurança estabelecidas pelo IRB(Re).

Não é aceitável ou permitido o uso de dispositivos externos de comunicação durante o exercício da atividade funcional (como exemplo, pen drive), acesso a e-mail pessoal, chats de comunicação pessoais, evitando expor indevidamente dados, documentos e informações do IRB(Re). Dispositivos externos podem ser utilizados por profissionais técnicos da área de TI (HelpDesk) responsáveis por prestar suporte aos colaboradores. Exceções devem ser aprovadas pela Gerência de Governança, Segurança da

Informação e Controle, superior hierárquico na estrutura organizacional ou lavrado em ata de reunião de Diretoria Estatutária do IRB(Re).

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 deve ser submetida de maneira prévia a Gerência de Governança, Segurança da Informação e Controle para emissão de parecer consultivo, de acordo com a Norma de Desenvolvimento Seguro.

Os incidentes de segurança da informação devem ser registrados no canal corporativo disponibilizado pela TI, considerando alguns elementos como: data e hora do incidente, a origem da ocorrência, classificação do incidente e os impactos para a organização; analisados, contidos, tratados, corrigidos e, posteriormente, utilizados para refletir sobre as lições aprendidas, conforme definido na Norma de Gestão de Incidentes de Segurança da Informação.

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.

Os processos críticos de negócios devem ser assegurados pelo Plano de Continuidade de Negócios.

A terceirização de serviços de processamento e armazenamento de dados, em especial os relevantes, requer uma análise e avaliação de segurança da informação pela Gerência de Governança, Segurança da Informação e Controle, através de diligência técnica para avaliar se o prestador de serviços possui certificações de segurança ou documentos comprobatórios que garantam a aderência com as recomendações dos principais frameworks de cibersegurança do mercado, conforme preconiza a Circular SUSEP 638 e a Norma de Serviços Relevantes de Processamento e Armazenamento de Dados. As alçadas relativas à aprovação e alteração de contratos devem seguir o Norma de Compras e Contratações e Norma de Alçadas e Substituições.

O IRB(Re) deverá exigir que os prestadores de serviço de processamento e armazenamento de dados observem as disposições legais e regulamentações em vigor relacionadas à segurança cibernética.

A utilização de sistemas de inteligência artificial (IA) é permitido desde que implementados de forma segura e confiável, preservando a ética, segurança da informação, a confidencialidade dos dados e cumprindo as legislações vigentes, seguindo as regras estabelecidas na Norma de Uso Responsável de Inteligência Artificial.

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

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

3.3. Responsabilidade

- **Conselho de Administração:** aprovar objetivos e diretrizes de segurança da informação refletidos na Política de Segurança da Informação.

- **Gerência de Governança, Segurança da Informação e Controle** a unidade responsável por segurança)**:** estabelecer e garantir a estratégia de Segurança da Informação, por meio do PDSI ou qualquer outro instrumento formal; estabelecer e comunicar objetivos corporativos de segurança da informação; garantir que a Política de Segurança da Informação e os objetivos de segurança da informação sejam estabelecidos e compatíveis com a direção estratégica da Companhia; estabelecer papéis e responsabilidades das coordenações de TI relacionadas ao tema de segurança da informação; gerenciar riscos cibernéticos no âmbito da primeira linha; estabelecer e comunicar diretrizes de aceitação de riscos relativos à segurança da informação; liderar respostas à incidentes de segurança; desenvolver normas e políticas de segurança da informação; liderar o Plano de Recuperação de Desastres, componente do Plano de Continuidade de Negócios; e estabelecer agendas regulares e tempestivas com a Diretoria Estatutária e os Comitê de Riscos e Solvência, Comitê de Auditoria Estatutário (mínimo a cada 3 meses) e Conselho de Administração (mínimo a cada 6 meses) para tratar de temas relacionados à segurança da informação, acompanhamento da execução da estratégia estabelecida, demonstração de indicadores de desempenho etc.

- **Coordenação de Segurança e Controle:** garantir que a Política de Segurança da Informação e os objetivos de segurança da informação sejam executados e cumpridos; 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; prover os recursos para a operação do Sistema de Gestão de Segurança da Informação - SGSI; assegurar a disponibilidade dos recursos necessários para o SGSI; assegurar que o SGSI atinja os resultados pretendidos; promover reforços da segurança da informação, para assegurar que procedimentos padrões, com base em melhores práticas de mercado sejam implementados e observados, visando à segurança e à preservação dos dados; orientar e apoiar as pessoas a contribuírem para a eficácia do sistema de gestão da segurança da informação; assegurar a execução dos serviços gerenciados de segurança: Monitoramento 24x7 e Inteligência de Ameaças; atuar sobre eventos de segurança identificados; atuar na resposta à incidentes; realizar a gestão de vulnerabilidades; executar a gestão de segurança da cadeia de suprimentos; executar o programa hacker ético; executar a gestão de acessos; executar as diretrizes de desenvolvimento Seguro (DevSecOps); conduzir o programa de privacidade de dados (LGPD); executar as atividades previstas no Plano de Recuperação de Desastres, componente do Plano de Continuidade de

Negócios; realizar programa de treinamento e conscientização quanto à segurança da informação, seguindo as diretrizes desta Política; e promover a melhoria contínua.

- **Coordenação de Data Center:** examinar antes do descarte todos os recursos computacionais corporativos; fornecer os softwares necessários para os computadores corporativos; usar os ativos de informação em conformidade com todas as normas complementares de segurança da informação da companhia; fornecer ferramentas para acesso a dados de forma segura em equipamentos não corporativos; implementar diretrizes técnicas de segurança da informação; configurar e operar as Ferramentas de Segurança da Informação; corrigir as vulnerabilidades identificadas; atuar sobre eventos de segurança identificados; atuar na resposta à incidentes; e executar as atividades previstas no Plano de Recuperação de Desastres, componente do Plano de Continuidade de Negócios.

- **Gerência de Controles Internos:** apoiar a primeira linha no mapeamento de processos, riscos e controles relacionados à segurança da informação do IRB(Re); avaliar os controles de segurança da informação por meio de testes de desenho; apoiar na elaboração de possíveis planos de ação para os apontamentos oriundos da Auditoria Externa, Interna e Órgãos Reguladores; apoiar a unidade responsável por segurança no desenvolvimento de instrumentos normativos de segurança da informação desenvolvidas pelo CISO; e acompanhar e avaliar as melhorias decorrentes dos programas de segurança e avaliações internas.

- **Gerência de Riscos Corporativos:** monitorar as ações acerca dos riscos de segurança cibernética através do relatório anual sobre prevenção e tratamento de incidentes; e considerar os riscos de segurança cibernética como componentes da categoria “riscos operacionais” no que se refere ao desenvolvimento e à aplicação de modelagem de riscos e capital.

- **Gerência de Auditoria Interna:** realizar auditoria anual; e realizar follow-up sobre a finalização dos planos de ação oriundos de apontamentos da Auditoria Interna e da Susep.

- **Gestores:** compreender as suas responsabilidades pelo cumprimento da Política de Segurança da Informação, bem como as demais normas de segurança complementares; 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 as políticas e normas da segurança da informação; adotar medidas destinadas a reduzir os riscos identificados, sempre em consonância com as normas da Companhia; 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 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.

- **Colaboradores:** compreender as suas responsabilidades pelo cumprimento da Política de Segurança da Informação, bem como as demais normas de segurança complementares; tornar-se ciente e concordar em cumprir todas as políticas, padrões e diretrizes aplicáveis que foram estabelecidas; usar os ativos de informação em conformidade com todas as normas complementares de segurança da informação da companhia; procurar orientação da Gerência de Governança, Segurança da Informação e Controle para dúvidas ou questões relacionadas à segurança da informação; participar na identificação de potenciais riscos às informações da Companhia, contribuindo para a implementação de controles apropriados; acessar apenas as informações das quais necessita para desenvolver suas funções; não passar ou compartilhar as informações sob sua gestão para outras pessoas, sejam elas colaboradores ou partes interessadas (relacionados), sem verificar se estas pessoas possuem o direito de acesso a esta informação; manter o devido cuidado para preservação da integridade física e/ou lógica da informação sob a sua responsabilidade; manipular a informação respeitando sua classificação e as implicações decorrentes dela, independentemente dos meios; e reportar à Gerência de Governança, Segurança da Informação e Controle eventuais situações não previstas ou violações desta Política que possa a colocar em risco a segurança das informações ou dos recursos computacionais da companhia.

- **Nota:** É dever de cada um dos colaboradores, prestadores de serviço, membros da Diretoria Estatutária 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.

4. Disposições gerais

A Política de Segurança da Informação, além de definir os princípios para a segurança da informação, preserva a integridade, a confidencialidade e a disponibilidade das informações, tem como objetivo complementar a Política de Gestão de Riscos.

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

A inobservância das regras da Política de Segurança da Informação pode implicar em sanções previstas na Política de Consequência e Medidas Disciplinares.

O cumprimento dos instrumentos normativos de Segurança da Informação deve ser auditado periodicamente pela Auditoria Interna da Companhia.

Esta política deve ser revisada e atualizada, em caráter ordinário, a cada 2 anos, 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.

Política aprovada na 329ª RCA de 20/12/2024.

5. Documentos de Referência

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

- Circular SUSEP 638/2021;
- ABNT NBR ISO/IEC 27001: Sistemas de Gestão da Segurança da Informação;
- ABNT NBR ISO/IEC 27002: Técnicas de segurança – Código de Prática para Controles de Segurança da Informação;
- Política de Gestão de Riscos;
- Política de Consequência e Medidas Disciplinares;
- Norma de Gestão de Incidentes de Segurança da Informação;
- Norma de Classificação e Tratamento da Informação;
- Norma de Uso Aceitável de Ativos de TI;
- Norma de Controle de Acesso;
- Norma de Desenvolvimento Seguro;
- Norma de Plano de Continuidade de Negócios (PCN);
- Norma de Uso Responsável de Inteligência Artificial;
- Norma de Serviços Relevantes de Processamento e Armazenamento de Dados;
- Norma de Compras e Contratações; e
- Norma de Alçadas e Substituições.

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