GRUPO RENDIMENTO

Política Regulatória

RESUMO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

	Título: RESUMO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		
GRUPO RENDIMENTO	Data Inicial: Abril 2020	Data Atualização: Abril 2021	POL SEG 01

Índice

1. Objetivo 3
2. Público Alvo 3
5. Referências 3
6. Definições e Siglas 3
7. Descrição 5
7.1 Domínios da Segurança da Informação e Cibernética 5
7.1.1 Gestão de Ativos 5
7.1.2 Avaliação de Riscos Cibernéticos de Produtos ou Serviços 5
7.1.3 Classificação da Informação 5
7.1.4 Proteção de Dados e Privacidade 5
7.1.5 Segurança Física e do Ambiente 5
7.1.6 Gestão de Identidades e Acessos 6
7.1.7 Controles dos Recursos de Tecnologia 6
7.1.8 Proteção da Rede, Informações e Sistemas 6
7.1.9 Governança de servidores e sistemas 6
7.1.9.1 Gestão de patches de segurança 6
7.1.9.2 Gestão de vulnerabilidades 6
7.1.9.3 Gestão de mudança 6
7.1.9.4 Gestão de configuração de segurança 7
7.1.9.5 Cópias de Segurança e Recuperação 7
7.1.10 Procedimentos de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação 7
7.1.10.1 Contratação 7
7.1.10.2 Segurança no Armazenamento 7
7.1.10.3 Serviços de Processamento e Armazenamento de Dados Relevantes e em Nuvem 7
7.1.11 Gestão de Prestadores de Serviços de TI 7
7.1.12 Gestão da Continuidade dos Negócios (GCN) 7
7.1.13 Monitoramento e Inspeção 8
7.1.14 Conscientização e Treinamento em Segurança da Informação 8
7.1.15 Relatório anual 8

7.2 Exceções 8
7.3 Dúvidas 8
8. Controle de Versão 8
9. Anexo 8

1. Objetivo

A **Política de Segurança da Informação e Cibernética** tem por objetivo estabelecer as diretrizes adotadas pelo **GRUPOBRSA** para assegurar a confidencialidade, integridade e disponibilidade das informações e dos sistemas de informação utilizados em nossas operações.

2. Público Alvo

Esta Política se aplica a todos os colaboradores, sejam eles diretores, executivos, gestores, funcionários, aprendizes, estagiários, prestadores de serviços e parceiros que possuam acesso às informações do **GRUPOBRSA**.

5. Referências

Resolução 4.893/21 do Banco Central do Brasil que dispõe sobre a Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições.

6. Definições e Siglas

Para melhor compreensão deste resumo ou da **Política de Segurança da Informação e Cibernética** em seu texto integral, é essencial a compreensão dos termos e abreviaturas utilizadas, a seguir:

Sigla/Definição	Descrição
Ameaça	Risco ou potencial perigo de incidente que pode resultar em dano ao **GRUPOBRSA**.
Ativo	Qualquer coisa com valor para o **GRUPOBRSA**, demandando a devida proteção.
Autenticidade	Garantia de que a informação é procedente e fidedigna, capaz de gerar evidências aceitáveis da identificação de quem a criou, editou ou emitiu.
Backup	Cópia de segurança realizada por meio de reprodução e/ou espelhamento de uma base de arquivos, com capacidade de recuperação plena em caso de incidente, necessidade de restauração ou qualquer outra justificada pelo **GRUPOBRSA**.
Colaboradores	Conselheiros, diretores executivos, gestores, funcionários e estagiários do **GRUPOBRSA**.
Confidencialidade	Garantia de que as informações sejam acessadas somente por pessoas expressamente autorizadas, protegendo-a do acesso de terceiros não-autorizados.

Data Center	Centro de processamento de dados. Local onde estão concentrados os sistemas computacionais do **GRUPOBRSA**.
Disponibilidade	Garantia de acesso à informação por pessoas autorizadas sempre que necessário.
Homologação	Processo de avaliação e aprovação técnica de recursos de TI para serem utilizados dentro do ambiente do **GRUPOBRSA**.
Identidade Digital	Identificação do colaborador em ambientes lógicos, composta por login e senha ou outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.
Incidente de segurança da informação	Evento adverso que indica possível violação à política de segurança da informação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação.
Informação	Conjunto de dados que podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
Integridade	Garantia de que a informação seja mantida em seu estado original, visando protegê-la, no armazenamento ou transmissão, contra alterações indevidas, intencionais ou acidentais.
Legalidade	Garantia de que todas as informações sejam instituídas e gerenciadas de acordo com as disposições da legislação vigente.
PCN	Plano de Continuidade dos Negócios.
PSIC	Política de Segurança da Informação e Cibernética
Risco	Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.
Segurança cibernética	Preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação contra diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação no espaço cibernético.
TI	Tecnologia da Informação

7. Descrição

Em cumprimento ao Art. 5º da Resolução Bacen n. 4.893 de 26 de fevereiro de 2021, e como forma de manter a clareza na prestação de informações ao nosso público, este documento, que apresenta um resumo da nossa **Política de Segurança da Informação e Cibernética**, detalha de forma objetiva os principais pontos sobre o tema e assim reitera a robustez de nossas operações.

7.1 Domínios da Segurança da Informação e Cibernética

A segurança da informação e do ambiente cibernético está relacionada aos domínios da ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27032:2015 assegurando os controles na organização:

7.1.1 Gestão de Ativos

Aplicamos na gestão de ativos as melhores práticas recomendadas. O responsável pela custódia do ativo realiza o inventário e garante um descarte seguro, enquanto o gestor da área é responsável por manter e instruir sobre a sua utilização. Os ativos do **GRUPOBRSA** não podem ser retirados sem autorização do gestor responsável e são transportados em condições adequadas que assegurem sua integridade física e lógica.

7.1.2 Avaliação de Riscos Cibernéticos de Produtos ou Serviços

Os riscos identificados são avaliados e administrados em conformidade com os requisitos especificados na política de Gestão Integrada de Riscos, bem como nos controles de proteção e as respostas, proporcionais aos riscos identificados. A área de Segurança da Informação é envolvida nas recomendações sobre controles e proteções de segurança da informação e cibernética no desenvolvimento de novos produtos ou serviços do **GRUPOBRSA** bem como na avaliação de riscos dos mesmos, buscando identificar ameaças e impactos sobre os ativos de informação.

7.1.3 Classificação da Informação

A informação é um importante ativo do **GRUPOBRSA** e deve ser preservada e salvaguardada, em conformidade com suas políticas, normas, procedimentos e controles internos, bem como, com as leis e regulamentos dos órgãos reguladores e autorreguladores sobre o tema, sempre de acordo com os requisitos especificados na **Política de Classificação da Informação**.

7.1.4 Proteção de Dados e Privacidade

A proteção de dados e da privacidade das pessoas naturais deve ser administrada de acordo com os requisitos especificados na **PSIC** e na **Política de Classificação da Informação**, bem como nas leis e regulamentos sobre o tema.

7.1.5 Segurança Física e do Ambiente

Com objetivo de prevenir o acesso físico não autorizado, danos às instalações, fraude ou sabotagem, entre outras ameaças, controles foram implementados nos data centers e os acessos podem ocorrer somente, após autorização e agendamento prévio do Departamento de Tecnologia da Informação.

7.1.6 Gestão de Identidades e Acessos

O **GRUPOBRSA** possui procedimento de concessão, exclusão e revisão dos direitos de acesso, que identifica e registra todos os privilégios de acesso aos servidores e sistemas destinados às informações, conforme regras da **política de Controle de Acesso a Sistemas e Informações**.

7.1.7 Controles dos Recursos de Tecnologia

Os recursos de tecnologia utilizados pelos colaboradores e com possibilidade de envio de informações são protegidos por controles de prevenção ao vazamento de dados. Também são configurados de acordo com a última atualização de segurança fornecida pelo fabricante, homologados e aplicados pelo Departamento de Tecnologia da Informação.

7.1.8 Proteção da Rede, Informações e Sistemas

Visando a proteção das informações e a confiabilidade e qualidade dos serviços e sistemas do **GRUPOBRSA**, é adotado sistemas de rede virtual; monitoramento do volume de dados trafegados; gestão e resposta na identificação de picos de tráfego e uso de portas “incomuns” na rede; isolamento de redes ou sistemas na identificação de uma atividade “incomum”; permissão apenas para protocolos de comunicações aprovados; e restrição de horário de login.

O Departamento de Tecnologia da Informação estabelece controles na rede corporativa contra acessos não autorizados, além de implementar controles contra o uso de ferramentas que permitam a captura ou interceptação de informações na rede ou realizem a varredura no ambiente lógico do **GRUPOBRSA**.

7.1.9 Governança de servidores e sistemas

O **GRUPOBRSA** possui procedimento de monitoramento de seu ambiente para controlar a infraestrutura de TI, bem como a performance e a capacidade de processamento atual da mesma.

7.1.9.1 Gestão de patches de segurança

Visando a proteção dos servidores e estações de trabalho utilizados, o **GRUPOBRSA** estabeleceu e segue as recomendações da **norma especifica de Gestão de Patches**.

7.1.9.2 Gestão de vulnerabilidades

O Departamento de Segurança da Informação realiza Análise, Avaliação e Documentação das Vulnerabilidades em seus sistemas relevantes de acordo com a **norma de Gestão de Vulnerabilidades**.

7.1.9.3 Gestão de mudança

O andamento e o resultado de uma mudança em sistema ou infraestrutura tecnológica relevante, zela pela preservação dos controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade dos dados, que são geridos pelo Departamento de Tecnologia da Informação de forma planejada, aprovada, testada e obedecendo ao processo de gerenciamento de mudanças.

7.1.9.4 Gestão de configuração de segurança

Considerando a **política de Hardening**, o Departamento de Segurança da Informação estabelece e monitora as configurações básicas de segurança e controles que foram aplicadas de modo adequado pelo Departamento de Tecnologia da Informação.

7.1.9.5 Cópias de Segurança e Recuperação

O **GRUPOBRSA** possui **políticas de Cópias de Segurança e Recuperação** e mantém o processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes, a fim de atender aos requisitos operacionais e legais, assegurar a continuidade do negócio em caso de falhas ou incidentes, além de auxiliar em sua ágil recuperação.

7.1.10 Procedimentos de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação

A aquisição, desenvolvimento e manutenção de sistemas relevantes e a garantia de qualidade e segurança são administrados em conformidade com as políticas e as recomendações do Departamento de Segurança da Informação.

7.1.10.1 Contratação

O Departamento Jurídico e de Compliance e PLD/CFT são envolvidos previamente à contratação para avaliar condições contratuais indicadas por fornecedores e parceiros.

7.1.10.2 Segurança no Armazenamento

O armazenamento de dados confidenciais prevê a proteção adequada conforme a **política de Classificação da Informação**.

7.1.10.3 Serviços de Processamento e Armazenamento de Dados Relevantes e em Nuvem

No licenciamento de serviços relevantes de processamento e armazenamento de dados e computação em nuvem, são adotados os procedimentos de segurança estabelecidos na **política de Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem**.

7.1.11 Gestão de Prestadores de Serviços de TI

O **GRUPOBRSA** estabelece controles apropriados para assegurar que as informações tratadas por seus prestadores de serviços de TI relevantes estejam devidamente protegidas de acordo com os requisitos da sua **política de Gestão de Fornecedores de TI**.

7.1.12 Gestão da Continuidade dos Negócios (GCN)

As informações confidenciais e sistemas relevantes são assegurados de erros ou perdas por meio de um PCN, cópias de segurança e planos de contingência que incluem cenários de incidentes relevantes a serem considerados nos testes de continuidade de negócios pelo **GRUPOBRSA**

7.1.13 Monitoramento e Inspeção

O Departamento de Segurança da Informação pode monitorar ou inspecionar os recursos de tecnologia que estiverem em suas dependências ou que interajam com os ambientes lógicos do **GRUPOBRSA** sempre que considerar necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

7.1.14 Conscientização e Treinamento em Segurança da Informação

O **GRUPOBRSA** promove a disseminação das diretrizes e os princípios de segurança da informação e Cibernética por meio de programas de conscientização e treinamentos periódicos com objetivo de fortalecer a cultura de segurança.

7.1.15 Relatório anual

O Departamento de Segurança da Informação elabora o relatório anual sobre a implementação do plano de ação e de resposta a incidentes com data-base de 31 de dezembro. O relatório é submetido primeiramente para a aprovação do Comitê de Segurança até 31 de março do ano seguinte ao da data-base.

7.2 Exceções

As solicitações de exceção devem ser encaminhadas formalmente pelo Gestor do colaborador ao Departamento de Segurança da Informação para análise de viabilidade e aprovação do Diretor responsável pela segurança cibernética.

7.3 Dúvidas

Qualquer dúvida relativa a **PSIC** deve ser encaminhada ao Departamento de Segurança da Informação por meio do endereço eletrônico: < seguranca.informacao@rendimento.com.br >

8. Controle de Versão

Versão	Data de Atualização	Conteúdo Revisado
1	03/2021	Sem alteração.

9. Anexo

Não se aplica.