

Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

SUMÁRIO

1. DEFINIÇÕES	3
2. NORMAS APLICÁVEIS	4
3. APRESENTAÇÃO E OBJETIVOS	4
4. ABRANGÊNCIA	5
5. ATRIBUIÇÕES E RESPONSABILIDADES	5
6. PRINCÍPIOS	6
7. DIRETRIZES GERAIS	7
7.1. Aprovação e Revisão	9
8. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	9
8.1. Gestão de Ativos	9
8.2. Autenticação	10
8.3. Segmentação de rede	10
8.4. Classificação da Informação	10
8.5. Controle de acesso	11
8.6. Gestão de riscos	11
8.7. Gestão de fornecedores	13
8.8. Segurança física do ambiente	14
8.9. Backup e gravação de LOG	14
8.10. Proteção contra vírus, arquivos e softwares maliciosos	14
8.11. Testes de varredura para detecção de vulnerabilidade	14
8.12. Criptografia	15
8.13. Plano de continuidade	15
8.14. Incidentes de segurança	16
8.14.1. Classificação de relevância dos incidentes	16
8.14.2. Gestão de incidentes	16
8.14.3. Plano de compartilhamento de incidentes	17
8.14.4. Plano de ação e resposta a incidentes	17



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

8.14.5.	Relatório anual de incidentes	17
8.15.	Mecanismos de rastreabilidade	18
8.16.	Registro de impacto	18
8.17.	Treinamentos e conscientização	18
8.18.	Contratação de serviços de processamento e armazenamento de dados e computação em nuvem	19
8.18.1.	Seleção de terceiros.....	19
8.18.2.	Execução de aplicativos pela internet.....	20
8.18.3.	Serviços de computação em nuvem.....	21
8.18.4.	Contratação de serviços de computação em nuvem no exterior	21
8.18.5.	Contrato de prestação de serviços	22
8.19.	Comunicação ao Bacen.....	24
8.20.	Continuidade de negócios.....	25
8.21.	Arquivamento de informações	26
8.22.	DECLARAÇÃO DE RESPONSABILIDADE	26
8.23.	DISPOSIÇÕES GERAIS.....	27
ANEXO I.....		28



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

1. DEFINIÇÕES

- **Ativos:** todas as formas de tratamento de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.
- **Alta Administração:** diretores responsáveis pela **SER FINANCE SOCIEDADE DE CRÉDITO DIRETO S.A. (SER FINANCE SCD)**.
- **Bacen:** Banco Central do Brasil
- **Colaboradores:** funcionários, trainees e estagiários da SER FINANCE SCD.
- **Gestão de Ativos:** são as boas práticas utilizadas pela SER FINANCE SCD em seu processo de controle de ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas e materiais, *know-how*), que buscam alcançar um resultado desejado e sustentável para a operação.
- **Informações Sensíveis:** que tem valor estratégico para o desenvolvimento dos negócios e das operações da SER FINANCE SCD, ganhando tangibilidade por meio de transações, processamentos, bancos de dados, entre outras formas, e que serão tratados com base no legítimo interesse da SER FINANCE SCD, estritamente necessários para a finalidade pretendida nos termos desta Política e da legislação em vigor.
- **Log:** registro de eventos de um sistema.
- **Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da SER FINANCE SCD.
- **Segurança Cibernética:** conjunto de práticas, tecnologias e processos desenvolvidos para proteger as informações e os sistemas internos, computadores, redes, softwares e dados da SER FINANCE SCD contra ataques cibernéticos, danos, ameaças ou acesso não autorizado.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

2. NORMAS APLICÁVEIS

Resolução CMN nº 4.893/2021 – 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 autorizadas a funcionar pelo Banco Central do Brasil.

3. APRESENTAÇÃO E OBJETIVOS

A SER FINANCE SCD, é uma Sociedade de Crédito Direto, pertencente ao grupo Ser Educacional S.A. e Uninassau Participações S.A., que irá realizar operações de empréstimo, de financiamento e de aquisição de direitos creditórios por meio de plataforma eletrônica, com atuação predominante nas operações de empréstimos e emissão de moeda eletrônica aos clientes do Grupo Ser Educacional, um dos melhores grupos educacionais do Brasil.

Esta Política de Segurança da Informação e Segurança Cibernética (“Política”) tem o objetivo de estabelecer diretrizes que permitem a SER FINANCE SCD preservar e proteger as informações de seus clientes, Colaboradores e partes interessadas e da própria SER FINANCE SCD contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da SER FINANCE SCD a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A SER FINANCE SCD deve implementar e manter esta Política formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Esta Política está compatível com:



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

CODIGO DOC

POL.01.05

Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

- O porte, o perfil de risco e o modelo de negócio da SER FINANCE SCD;
- A natureza das atividades da SER FINANCE SCD e a complexidade dos produtos, serviços oferecidos, atividades e processos, enquanto uma SCD e emissão de moeda eletrônica, nos termos da regulamentação em vigor; e
- A sensibilidade dos dados e das informações sob responsabilidade da SER FINANCE SCD.

4. ABRANGÊNCIA

A Política se aplica a todos os Colaboradores, Alta Administração e empresas prestadoras de serviço¹ da SER FINANCE SCD cujas atividades sejam desempenhadas visando ao desenvolvimento das operações atinentes a esta Política.

5. ATRIBUIÇÕES E RESPONSABILIDADES

São deveres e responsabilidades de implementação, execução e manutenção desta Política:

- **Diretor responsável pela execução e manutenção desta Política:** responsável pela implementação, execução e manutenção da política, assim como, pela convocação das reuniões periódicas do comitê de segurança da informação e segurança cibernética;
- **Comitê de Segurança da Informação e Segurança Cibernética:** comitê conduzido pelo Diretor responsável por esta



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Política, e formado por Colaboradores indicados pelas áreas de SER FINANCE SCD, e aprovadas pela Alta Administração, com o objetivo de deliberar a respeito de assuntos relacionados à Segurança da Informação e Segurança Cibernética;

- **Usuários:** Alta Administração e Colaboradores da SER FINANCE SCD, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da SER FINANCE SCD, e que devem, no que couber: (i) cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta Política; (ii) informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivos, serviços ou processos relacionados à Segurança da Informação e Segurança Cibernética, para que sejam tomadas ações de forma tempestiva; (iii) utilizar as informações relacionadas à esta Política, como patrimônio da SER FINANCE SCD, e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade.

6. PRINCÍPIOS

A SER FINANCE SCD tem o compromisso garantir a segurança e o tratamento adequado das informações, sistemas internos, computadores, redes, softwares e dados. Para tanto, adota as atividades que se baseiam nos seguintes princípios:

- **Autenticidade:** garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação;
- **Confidencialidade:** garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;



Elaboração 27/10/21	Revisão 16/11/23	Versão 02	Área Responsável: Segurança da Informação
------------------------	---------------------	--------------	--

- **Disponibilidade:** garantia de que a informação estará disponível somente às pessoas autorizadas e sempre que for necessário;
- **Integridade:** garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

7. DIRETRIZES GERAIS

Para garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na SER FINANCE SCD.
- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A SER FINANCE SCD adotará mecanismos que visam a assegurar a utilização segura de senhas.
- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela SER FINANCE SCD.
- Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar ou, ao menos, registrar acessos indevidos, modificações, destruições ou divulgações não autorizadas.
- Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.
- Assegurar o cumprimento dos procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, a autenticação, a criptografia, a prevenção e a detecção de intrusão,



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração 27/10/21	Revisão 16/11/23	Versão 02	Área Responsável: Segurança da Informação
------------------------	---------------------	--------------	--

a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis.
- Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da SER FINANCE SCD.
- Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos negócios;
- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da SER FINANCE SCD;
- Classificar os dados e as informações quanto à relevância;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:
 - A implementação de programas de capacitação e de avaliação periódica de pessoal;
 - A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços financeiros oferecidos.
- Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com as demais instituições autorizadas a funcionar pelo Bacen.
- Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da SER FINANCE SCD, inclusive de informações recebidas de



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

CODIGO DOC

POL.01.05

Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis.

- Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela SER FINANCE SCD e por esta Política.

7.1. APROVAÇÃO E REVISÃO

Esta Política foi elaborada pela área de segurança da informação e cibernética, e aprovada pela Alta Administração, e será revisada com a periodicidade mínima anual.

A Política também poderá ser alterada, a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.

8. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a SER FINANCE SCD adotará políticas e procedimentos para os processos elencados a seguir.

8.1. GESTÃO DE ATIVOS

Os ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com armazenagem de documentos físicos deve ser restrito e limitado, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A SER FINANCE SCD deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da autenticidade, confidencialidade, disponibilidade e integridade sejam cumpridos integralmente.

8.2. AUTENTICAÇÃO

A SER FINANCE SCD adota mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, bem como deverá prever processos de autorização levando em consideração o princípio do menor privilégio, a segmentação de funções e a classificação da informação.

8.3. SEGMENTAÇÃO DE REDE

A SER FINANCE SCD adota mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

Caso o Colaborador queira criar, alterar ou excluir regras nos *firewalls* e Ativos de rede deverá enviar uma requisição ao departamento de tecnologia da informação, que fará análise e aprovação.

8.4. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações são classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a SER FINANCE SCD deve adotar a seguinte classificação:



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração 27/10/21	Revisão 16/11/23	Versão 02	Área Responsável: Segurança da Informação
------------------------	---------------------	--------------	--

- **Informação Pública:** aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e dados promocionais;
- **Informação Interna:** aquela que pode ser acessada somente por Colaboradores da SER FINANCE SCD. São exemplos de Informação Interna: normas, procedimentos e formulários da SER FINANCE SCD;
- **Informação Restrita:** aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos, sistemas e documentos estratégicos da SER FINANCE SCD.
- **Informação Confidencial:** aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.

8.5. CONTROLE DE ACESSO

A SER FINANCE SCD adota controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados, aos sistemas internos e as informações que não sejam de livre acesso e sem permissão prévia. Desta forma, a SER FINANCE SCD tem mecanismos para a autenticação de usuários, manutenção de segregação de funções, rastreabilidade de acesso e aprovação de acesso, quando aplicável, de forma a garantir procedimentos internos adequados e consistentes.

8.6. GESTÃO DE RISCOS

A SER FINANCE SCD possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

Os processos de gestão de riscos englobam os controles de mudanças no ambiente de tecnologia da SER FINANCE SCD, que são estruturados e aplicados através de um conjunto de processos que vão atuar em todas as áreas potencialmente impactadas, bem como a capacitação e o engajamento dos Colaboradores diretamente envolvidos nas ações mitigatórias dentro da SER FINANCE SCD, com o objetivo da preparação para essas situações.

Neste processo, será levado em conta: (i) o levantamento dos impactos organizacionais; (ii) a priorização das ações de mudanças no ambiente de tecnologia da SER FINANCE SCD; (iii) o planejamento; (iv) os testes; (v) a mobilização; (vi) a comunicação; e (vii) os treinamentos contínuos para a devida capacitação das pessoas diretamente envolvidas no processo de gestão de riscos e controle dos respectivos ambientes de tecnologia da SER FINANCE SCD, da seguinte forma:

- i. O levantamento dos impactos organizacionais irá detalhar quais áreas da SER FINANCE SCD podem vir a ser impactadas direta e/ou indiretamente;
- ii. A priorização das ações de mudanças no ambiente de tecnologia irá avaliar e elencar todas as mudanças que precisam ser implementadas, definindo quais demandas serão tratadas com prioridade e quais poderão ser mitigadas;
- iii. O planejamento irá definir os planos de implementação, impactos e correções, visando maximizar a segurança e integridade dos ambientes de tecnologia, e minimizar ao máximo riscos de ações ineficientes e ineficazes;
- iv. Os testes irão monitorar todo o processo e se certificar que tudo está acontecendo conforme o planejamento realizado. Através dos testes serão elaborados relatórios, os quais serão revisados pelo Diretor responsável pela execução e manutenção desta Política, que descreverão os resultados, funcionalidades e correções;



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração 27/10/21	Revisão 16/11/23	Versão 02	Área Responsável: Segurança da Informação
------------------------	---------------------	--------------	--

- v. A mobilização irá, através do Diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes, direcionar a SER FINANCE SCD e todos os Colaboradores ao encontro do objetivo deste processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da SER FINANCE SCD;
- vi. A comunicação irá informar e detalhar os objetivos da mudança através dos canais de comunicação e do desenvolvimento do plano de comunicação, para que todos os Colaboradores da SER FINANCE SCD tenham conhecimento da relevância e da necessidade do engajamento para o alcance de todas as medidas adequadas e mitigatórias, para neutralizar ou minimizar os eventuais ou potenciais danos;
- vii. O treinamento contínuo irá garantir a transferência e o nivelamento de conhecimentos relacionados ao trabalho desenvolvido no processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da SER FINANCE SCD.

8.7. GESTÃO DE FORNECEDORES

A SER FINANCE SCD verifica o grau de comprometimento com relação a controles de Segurança da Informação e Segurança Cibernética de todos os seus prestadores de serviços, fornecedores e provedores que processam e armazenam dados da SER FINANCE SCD, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A SER FINANCE SCD deve disponibilizar um canal para que seus prestadores de serviços, fornecedores e provedores comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da SER FINANCE SCD.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

8.8. SEGURANÇA FÍSICA DO AMBIENTE

A SER FINANCE SCD deve implementar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores e provedores aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível devem ser mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

8.9. BACKUP E GRAVAÇÃO DE LOG

A SER FINANCE SCD deve adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

A SER FINANCE SCD também deve realizar gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acessos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

8.10. PROTEÇÃO CONTRA VÍRUS, ARQUIVOS E SOFTWARES MALICIOSOS

A SER FINANCE SCD adotará mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (*phishing*, *spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a SER FINANCE SCD a vulnerabilidades.

8.11. TESTES DE VARREDURA PARA DETECÇÃO DE VULNERABILIDADE



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



A SER FINANCE SCD se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

A SER FINANCE SCD adota processo de atualização periódica de segurança no parque tecnológico, de forma a prevenir vulnerabilidades que possam ocasionar brechas de segurança para ataque de vírus e outros tipos de software, que se propaguem nos computadores, sistemas e servidores da SER FINANCE SCD.

8.12. CRIPTOGRAFIA

Os Ativos de informação da SER FINANCE SCD devem possuir criptografia adequada, conforme a classificação da informação, em todo tráfego que ocorrer em rede pública, a fim de se garantir proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

8.13. PLANO DE CONTINUIDADE

A SER FINANCE SCD realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da SER FINANCE SCD sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, a SER FINANCE SCD realizará o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança.



Elaboração 27/10/21	Revisão 16/11/23	Versão 02	Área Responsável: Segurança da Informação
------------------------	---------------------	--------------	--

Devem ser aplicados testes de continuidade de negócios e realização testes periódicos para garantir a eficácia e segurança dos processos. O teste deve ser conduzido em um ambiente controlado que permita que a SER FINANCE SCD certifique a conformidade dos planos desenvolvidos com os objetivos da SER FINANCE SCD e requisitos legais.

8.14. INCIDENTES DE SEGURANÇA

8.14.1. CLASSIFICAÇÃO DE RELEVÂNCIA DOS INCIDENTES

A SER FINANCE SCD classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade de negócios da SER FINANCE SCD.

8.14.2. GESTÃO DE INCIDENTES

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador ou cliente devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio dos canais indicados pela SER FINANCE SCD através do e-mail segurancadainformacao@buni.digital.

Os incidentes reportados serão classificados segundo o risco que representam para a SER FINANCE SCD e o impacto na continuidade de negócios da SER FINANCE SCD. Além disso, devem ser devidamente registrados, tratados e comunicados.

A SER FINANCE SCD adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



8.14.3. PLANO DE COMPARTILHAMENTO DE INCIDENTES

Sem prejuízo do dever de sigilo e da livre concorrência, a SER FINANCE SCD deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com as demais instituições autorizadas a funcionar pelo Bacen, por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a SER FINANCE SCD comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas, informando o prazo para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, estabelecendo e documentando os critérios que configuraram a situação de crise.

8.14.4. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

A SER FINANCE SCD deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

8.14.5. RELATÓRIO ANUAL DE INCIDENTES

A SER FINANCE SCD deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

- A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;



Elaboração 27/10/21	Revisão 16/11/23	Versão 02	Área Responsável: Segurança da Informação
------------------------	---------------------	--------------	--

- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes deve ser apresentado à Alta Administração da SER FINANCE SCD até 31 de março do ano seguinte ao da data-base.

8.15. MECANISMOS DE RASTREABILIDADE

A SER FINANCE SCD deve adotar controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

8.16. REGISTRO DE IMPACTO

A SER FINANCE SCD deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da SER FINANCE SCD, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

8.17. TREINAMENTOS E CONSCIENTIZAÇÃO

A SER FINANCE SCD preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



integrantes desta Política, garantindo-se a capacitação e conscientização para toda a Alta Administração e todos os seus Colaboradores.

A SER FINANCE SCD promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, no que couber, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

Além disto, a Alta Administração da SER FINANCE SCD deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética.

8.18. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

8.18.1. SELEÇÃO DE TERCEIROS

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a SER FINANCE SCD deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da SER FINANCE SCD aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;



Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A aderência do prestador de serviço a certificações exigidas pela SER FINANCE SCD para a prestação do serviço a ser contratado;
- O acesso da SER FINANCE SCD aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da SER FINANCE SCD por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da SER FINANCE SCD.

Na avaliação da relevância do serviço a ser contratado, a SER FINANCE SCD também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos devem ser documentados.

Ademais, a SER FINANCE SCD deve adotar recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

8.18.2. EXECUÇÃO DE APLICATIVOS PELA INTERNET

No caso da execução de aplicativos por meio da internet, a SER FINANCE SCD deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



8.18.3. SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Os serviços de computação em nuvem disponibilizados à SER FINANCE SCD, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à SER FINANCE SCD implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela SER FINANCE SCD ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela SER FINANCE SCD, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A SER FINANCE SCD é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pela SER FINANCE SCD ao Bacen.

8.18.4. CONTRATAÇÃO DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM NO EXTERIOR

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, a SER FINANCE SCD deverá observar os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;



Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

- Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
- Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços;
- Previsão de alternativas para a continuidade de negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a SER FINANCE SCD solicitará autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, a SER FINANCE SCD deverá solicitar autorização 60 dias antes da alteração contratual.

A SER FINANCE SCD deve assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso da SER FINANCE SCD e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deverão ser documentados.

8.18.5. CONTRATO DE PRESTAÇÃO DE SERVIÇOS

A SER FINANCE SCD deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;
- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à SER FINANCE SCD, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.
- O acesso da SER FINANCE SCD às informações fornecidas pela empresa contratada; bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação da empresa contratada notificar a SER FINANCE SCD sobre a subcontratação de serviços relevantes para a SER FINANCE SCD;
- A permissão de acesso do Bacen aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;
- A adoção de medidas pela SER FINANCE SCD, em decorrência de determinação do Bacen;
- A obrigação de a empresa contratada manter a SER FINANCE SCD permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Em caso de decretação de regime de resolução da SER FINANCE SCD pelo Bacen, o contrato de prestação de serviços deve prever:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;

- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços. A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:
 - A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
 - A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da SER FINANCE SCD.

8.19. COMUNICAÇÃO AO BACEN

A comunicação ao Bacen, referente a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, deve conter as seguintes informações:

- O nome da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual, salvo na hipótese prevista no item 8.18.04.



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



8.20. CONTINUIDADE DE NEGÓCIOS

No tocante à continuidade de negócios, a SER FINANCE SCD deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
- Os procedimentos a serem seguidos no caso de interrupção de serviços de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da SER FINANCE SCD;
- Os cenários de incidentes considerados nos testes de continuidade de negócios.
- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela SER FINANCE SCD, bem como das providências para o reinício das suas atividades;
- Estabelecer e documentar os critérios que configurem a situação de crise.

A SER FINANCE SCD deve instituir mecanismos de acompanhamento e de controle visando a assegurar a implementação e a efetividade desta Política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Os mecanismos de acompanhamento e controle devem incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.



8.21. ARQUIVAMENTO DE INFORMAÇÕES

A SER FINANCE SCD deve armazenar em meio físico ou digital, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;
- O documento relativo ao plano de ação e de resposta a incidentes;
- A ata da reunião com a aprovação da Alta Administração referentes a esta Política e ao plano de ação e de resposta a incidentes;
- O relatório anual sobre a implementação do plano de ação e de resposta a incidentes;
- A documentação sobre os procedimentos desta Política;
- A documentação com os critérios que configurem uma situação de crise;
- A documentação no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados.

8.22. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores da SER FINANCE SCD, a ela devem aderir formalmente por meio de um termo em que se comprometem a agir de acordo com esta Política.

Os contratos celebrados com terceiros pela SER FINANCE SCD e que tratem de Ativos de informação referentes a esta Política devem possuir cláusula que assegure a segurança das informações.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

CODIGO DOC

POL.01.05

Elaboração	Revisão	Versão	Área Responsável: Segurança da Informação
27/10/21	16/11/23	02	

8.23. DISPOSIÇÕES GERAIS

Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética, que deverá ser assinado pela Alta Administração e pelos Colaboradores, e no que couber, os prestadores de serviços, fornecedores e provedores.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site www.buni.digital



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

CODIGO DOC

POL.01.05

Elaboração
27/10/21

Revisão
16/11/23

Versão
02

Área Responsável: Segurança da
Informação

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento desta Política Segurança da Informação e Segurança Cibernética, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da SER FINANCE SCD.

Declaro ainda ter conhecimento de que, diante de um incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do e-mail contido nesta Política.

_____/_____/_____
Data

Assinatura



Rua Bandeira Paulista,
702, 10º andar,
conj. 102,
Bairro Itaim Bibi,
São Paulo-SP
CEP 04532-002

www.buni.digital
0800 969 6000

