Política Operacional
Operating Policy

Título / Title	Política de Segurança Cibernética Cybersecurity Policy

Responsável / Responsibility	Gerência da Tecnologia da Informação Management of Information Technology

A quem se destina / Applicable for	Deutsche Sparkassen Leasing do Brasil Banco Múltiplo S.A e/ou Locadora DL do Brasil Ltda. (ou simplesmente DLBR) Deutsche Sparkassen Leasing do Brasil Banco Múltiplo S.A. and/or Locadora DL do Brasil Ltda. (or simply DLBR)	Versão / Version	2.0

Vigente desde / Valid from	19.04.2021	Substitui Política / Replaces policy	10.01.2020

	Português	**English**
Propósito da Política / Purpose of the policy	A Política de Segurança Cibernética da Deutsche Sparkassen Leasing do Brasil Banco Múltiplo S.A. e/ou Locadora DL do Brasil Ltda. (ou simplesmente DLBR) constitui um documento no qual estão definidos os princípios, as responsabilidades e as estratégias adotadas para reduzir a vulnerabilidade da instituição a incidentes relacionados ao ambiente cibernético.	The Cybersecurity Policy of Deutsche Sparkassen Leasing do Brasil Banco Múltiplo S.A. and/or Locadora DL do Brasil Ltda. (or simply DLBR) is a document that defines the principles, responsibilities and strategies adopted to reduce the vulnerability of the institution to incidents related to the cyber environment.
	A presente Política será revisada sempre que necessário ou, no mínimo, anualmente, sendo aprovada pela Diretoria Colegiada e pelo Conselho de Admnistração.	This Policy will be reviewed whenever required or, at minimum, annually and approved by the Management and the Board of Directors.
Conteúdo / Content		
Definições / Definitions	**Segurança cibernética** = coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e	**Cybersecurity** = collection of tools, policies, security concepts, security safeguards, guidance, risk management approaches, actions, training, best practices, insurance, and technologies that may be used to protect the cyber environment, organization, and users' properties. "Cybersecurity is looking to

	propriedades de usuários(as). “A segurança cibernética tem por objetivo garantir a obtenção e a manutenção das propriedades de segurança da organização e das propriedades do(as) usuários(as) contra riscos de segurança relevantes no ambiente cibernético” - ITU (União Internacional das Comunicações, um órgão da ONU).	ensure that the organization's security properties and users' properties are secured and maintained against relevant security risks in the cyber environment” - ITU (International Union of Communications, a UN body).
	Organização e as propriedades de usuários(as) = incluem dispositivos de computação conectados, funcionários(as) e colaboradores(as), infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade de informação transmitida e/ou armazenada no ambiente cibernético.	**Organization and users' properties** = include connected computing devices, employees and employees, infrastructure, applications, services, telecommunications systems and all information transmitted and/or stored in the cyber environment.

Descrição	**Description**
1 Responsabilidades e competências	**1 Responsibilities and duties**
Através da Política de Segurança Cibernética, a DLBR ratifica o comprometimento de todos os administradores e colaboradores, no que concerne a adoção da devida diligência para garantir a manutenção das propriedades de segurança da organização e de usuários(as), contra riscos de segurança relevantes, bem como prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.	Through the Cybersecurity Policy, DLBR confirms the commitment of all administrators and employees regarding the adoption of due diligence to ensure the maintenance of the organization's security and users' properties against any relevant security risks, as well as to prevent, detect and reduce vulnerability to cyber-related incidents.
Conselho de Administração e Diretoria Colegiada	**Board of Directors and Management Board**
Promover a melhoria contínua dos procedimentos relacionados à segurança cibernética, a capacitação dos colaboradores e a disseminação da cultura, bem como incentivar o compartilhamento de informações com outras instituições, na forma estabelecida pelo Banco Central do Brasil.	Promote continuous improvement of cyber security procedures, employee training and culture dissemination, as well as encourage the sharing of information with other institutions, as established by the Brazilian Central Bank.
Gerência de Tecnologia da Informação	**Information Technology Management**
Adotar medidas, procedimentos, controles, sistemas e tecnologias necessárias para reduzir a vulnerabilidade da instituição a incidentes relacionados à segurança cibernética e de modo a garantir a continuidade de negócios.	Implement the necessary measures, procedures, controls, systems and technologies to reduce the institution's vulnerability to cyber security incidents and to ensure business continuity.

Gerência de Controles Internos e Compliance conjuntamente com a Gerência de Tecnologia da Informação	**Internal Controls and Compliance Management jointly with Information Technology Management**
Assegurar a implementação de procedimentos e controles internos que garantam a redução das vulnerabilidades da instituição a incidentes relacionados à segurança cibernética e de modo a garantir a continuidade de negócios.	Ensure the implementation of internal procedures and controls to ensure the reduction of the institution's vulnerability to cyber security incidents and to ensure business continuity.
Consultoria Jurídica	**Legal Consultant**
Dar suporte e assessoria a todas as áreas, de modo a garantir que condutas praticadas ou contratos celebrados atendam às normas e regulamentos vigentes, no que concerne à segurança cibernética.	Provide support and advice to all areas to ensure that practices or contracts entered into comply with current cyber security rules and regulations concerning cyber security.
Todos os Colaboradores	**All Employees**
Inteirar-se dos materiais educativos para perfeita compreensão de temas relativos a Segurança Cibernética, bem como prestar informações, a clientes e usuários, através de canais de atendimento, acerca das precauções na utilização de produtos e serviços disponibilizados pela instituição.	Be updated about educational materials for a perfect understanding of topics related to Cyber Security, as well as provide information to customers and users, through service centers about precautions in the use of products and services provided by the institution.
2 Procedimentos e controles para redução de vulnerabilidades e registro e análise de incidentes relevantes	**2. Procedures and controls for reducing vulnerability and relevant incident record and analysis**
A Gerência de TI é responsável pela adoção dos procedimentos e controles necessários para reduzir a vulnerabilidade da instituição a incidentes relacionados à segurança cibernética, inclusive relativo a rastreabilidade da informação e medidas de contorno, no caso de ocorrências, bem como aplicadas quando do desenvolvimento de sistemas e novas tecnologias.	IT Management is responsible for adopting the necessary procedures and controls to reduce the institution's vulnerability to cyber security related incidents, including information traceability and contour measures in the event of occurrences, as well as applied at the time of development of systems and new technologies.
A DLBR deve estabelecer controle sobre a base de conhecimento de possíveis incidentes abrangendo inclusive os fatos relacionados com prestadores de serviço, os quais devem ser monitorados e controlados.	DLBR must establish control over the knowledge base of possible incidents including facts related to service providers which must be monitored and controlled.
Anualmente será elaborado o relatório de Análise de Impacto no Negócio (AIN) ou *Business Impact Analysis* (BIA) que tem por finalidade apresentar todos os prováveis impactos de forma Quantitativa e Qualitativa relativos a incidentes relevantes, bem como derivados de empresas prestadoras de serviço que manuseiam dados ou informações sensíveis consideradas relevantes para a condução das atividades da companhia.	The Business Impact Analysis (BIA) report will be prepared annually to present all probable Quantitative and Qualitative impacts relating to relevant incidents, as well as derivatives of service providers that handle sensitive data or information deemed relevant to the conduct of the company's activities.

Os procedimentos e controles utilizados para prevenção e tratamento de incidentes adotados por empresas prestadoras de serviço que manuseiam dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais devem ser compatíveis aos utilizados pela DLBR.	Procedures and controls used for incident prevention and treatment adopted by service providers that handle sensitive data or information or deemed relevant to the conduct of operating activities shall be consistent with those used by DLBR.
A elaboração de Plano de Ação e de resposta a incidentes com a identificação de ações necessárias a serem desenvolvidas e implementadas para adequação da estrutura organizacional e operacional a fim de assegurar a prevenção e o tratamento de eventos relevantes relacionados ao ambiente cibernético deverá ser submetida e aprovada pelo Conselho de Administração.	The preparation of an Action Plan and incident response with the identification of necessary actions to be developed and implemented to adapt the organizational and operational structure to ensure the prevention and treatment of relevant events related to the cyber environment should be submitted and approved by the Board of Directors.
3 Comitê para Deliberação dos Riscos relacionados à Segurança Cibernética	**3. Committee for the Resolution of Cyber Security Risks**
É de responsabilidade do Comitê de Gestão de Continuidade de Negócios e/ou Segurança da Informação, conforme o caso, deliberar acerca de fatos ou incidentes ocorridos relacionados à Segurança Cibernética e considerados relevantes para a condução das atividades operacionais da instituição.	The Business Continuity Management and/or Information Security Committee, as the case may be, is responsible for resolving on facts or incidents related to Cyber Security and deemed relevant to the conduct of the institution's operational activities.