POLÍTICA DE SEGURANÇA CIBERNÉTICA
CONGLOMERADO VR

Em consonância com a Resolução 4658/18, o Conglomerado VR formalizou sua Política de Segurança Cibernética. Apresentamos, a seguir a versão resumida da referida Política.

Legislação aplicável

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018 - Política de Segurança Cibernética e Requisitos para a Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem.

Resolução BACEN 4.557/2017 – Estrutura de Gerenciamento Integrado de Riscos.

NBR e ISO/IEC 27001:2005 – Normas brasileiras e internacionais para sistemas de gestão da segurança da informação.

COBIT - *Control Objectives For Information and Related Technology* – "Framework" de boas práticas para Governança e Gestão de TI.

Objetivo:

Estabelecer princípios de segurança da informação, com a definição de diretrizes e normas mínimas necessárias à implementação e manutenção da segurança da informação e privacidade de dados, bem como, orientar a conduta dos colaboradores e todos os envolvidos com os negócios do Banco VR, visando a continuidade dos negócios, a confidencialidade, integridade, disponibilidade e privacidade das informações.

Os princípios de Segurança da Informação e Segurança Cibernética estabelecidos na política está em plena consonância com as diretrizes da alta administração da organização.

POLÍTICA DE SEGURANÇA CIBERNÉTICA
CONGLOMERADO VR

A Política de Segurança Cibernética é compatível com:

O porte, o perfil de risco e o modelo de negócio do Banco VR, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos do Banco VR e a sensibilidade dos dados e das informações sob responsabilidade do Instituição.

Aplicação

A Política de Segurança da Informação é aplicável a todas as áreas e colaboradores (funcionários, estagiários e terceiros) do Banco VR. Terceiros em uso das informações e de ativos do Banco VR também devem estar em conformidade para com as diretrizes desta Política. Como “Terceiros” estão incluídos, entre outros:

Prestadores de serviços de apoio e manutenção, Prestadores de serviços de operações relacionadas a sistemas de TI, serviços de coleta de dados, operações de atendimento, Clientes, Consultores, Auditores, Desenvolvedores (terceirizados), fornecedores externos de serviços de TI e para outras áreas, pessoal temporário, estagiários e outros contratados de curta duração, pessoal de limpeza e outros serviços de apoio terceirizados.

Princípios da Política

a. Segurança da Informação cobre todos os aspectos da Organização e é uma parte inseparável das operações rotineiras, da segurança corporativa, da gestão de riscos e dos controles internos do Banco VR.

b. Um aspecto importante e atual da Segurança da Informação é a privacidade de dados, tema este abordado na Lei 13.709 de 2018, que dispõe sobre a proteção e dados pessoais. Tão logo a referida lei esteja em vigor, essa Política poderá sofrer alterações.

c. A informação produzida ou recebida como resultado da atividade profissional dos colaboradores pertence à **Banco VR** e/ou a seus clientes e parceiros.

d. Divulgar informações confidenciais, restritas e estratégicas é crime previsto nas leis de propriedade intelectual e industrial (Lei nº 9279 de 1996) e de direitos autorais (Lei nº 9610 de 1998).

e. A segurança da informação depende de processos gerenciais de controle e sistemas de segurança da informação. No entanto, todas as pessoas são diretamente responsáveis pela segurança das informações que acessam e manipulam. Sem o total comprometimento das pessoas com a segurança da informação, mesmo sistemas e processos gerenciais bem estruturados não podem prover um nível adequado de segurança.

Escopo

A política contempla os objetivos de segurança cibernética do Banco VR, os procedimentos e os controles adotados para reduzir a vulnerabilidade do Banco VR a incidentes e atender aos demais objetivos de segurança cibernética;

I. Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
II. O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Banco VR;
III. As diretrizes para:

a. A elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;
b. A definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais do Banco VR;
c. A definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes; e
d. A classificação dos dados e das informações quanto à confidencialidade;

IV. Os mecanismos para disseminação da cultura de segurança no Banco VR, incluindo:
a. a implementação de programas de capacitação e de avaliação periódica de pessoal;
b. a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços; e
c. o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e
V. As iniciativas para compartilhamento de informações sobre os incidentes relevantes.

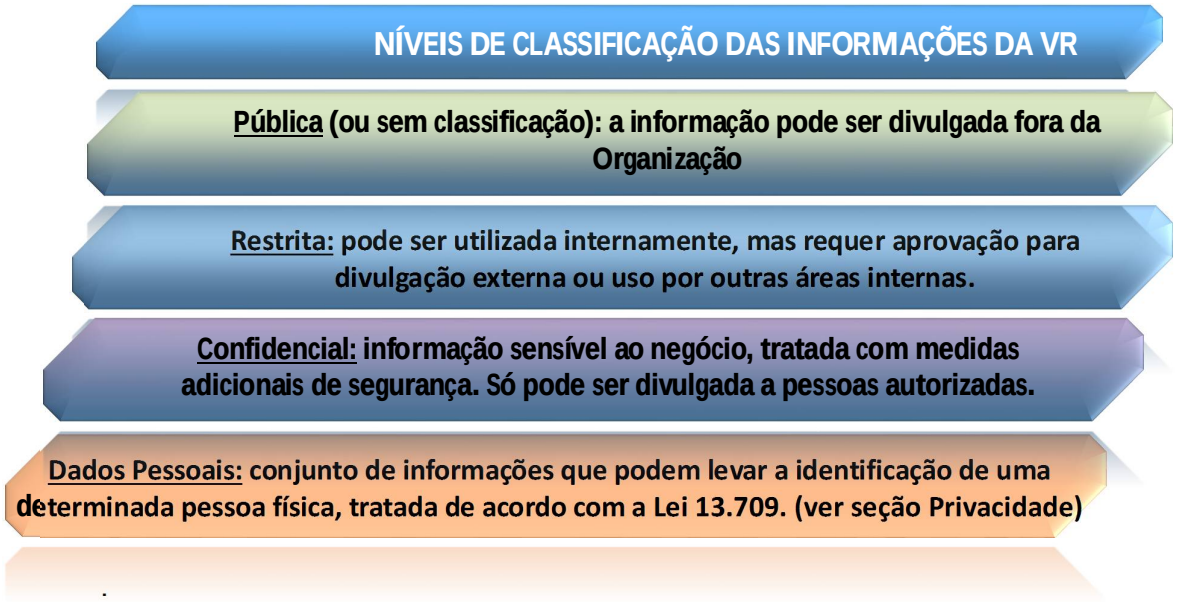
CLASSIFICAÇÃO DA INFORMAÇÃO

Pelo fato de o Banco VR armazenar informações de seus clientes, fornecedores e parceiros de negócios, a responsabilidade da companhia em proteger estas informações é maior pois qualquer divulgação não autorizada pode expor a Empresa à riscos financeiros, legais, de imagem ou operacionais.

Para que um processo de segurança das informações funcione corretamente, é necessário que as informações sejam devidamente classificadas e de acordo

com essa classificação sejam implementados o nível de segurança e os investimentos adequados.

A informação é classificada de forma a se indicar a confidencialidade e o nível esperado de proteção, conforme esta classificação. A informação possui diferentes níveis de sensibilidade e criticidade. No Banco VR adotamos os seguintes níveis de classificação das informações:



Comunicação de contratações ao Banco Central do Brasil, vide disposições do art. 15 da Resolução 4.658/18.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada formalmente ao Banco Central do Brasil.

POLÍTICA DE SEGURANÇA CIBERNÉTICA
CONGLOMERADO VR

Gestão de Incidentes de Segurança da Informação.

São consideradas como incidentes de segurança da informação as situações e ocorrências que caracterizem a violação de qualquer diretriz e norma listadas na Política. O Banco VR mantém procedimentos de reporte de incidentes de segurança da Informação, bem como, possui mecanismos de acionamento dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional.

Caso um incidente de origem cibernética seja identificado pelo público geral, o mesmo deverá ser reportado pelo e-mail securityoffice4@vr.com.br.

Aderência à Política

Caso seja identificada uma conduta não aderente à política ou o seu descumprimento, o Banco VR tomará as medidas legais, tecnológicas ou disciplinares necessárias de forma a manter a aderência a mesma.