Política	Data da última atualização
Política de Segurança da Informação e Cibernética	26.03.2021
Área Responsável	**Versão**
Segurança da Informação	29

1. Objetivo

Estabelecer as diretrizes para execução das atividades relacionadas à manutenção da confidencialidade, integridade e disponibilidade da informação no Conglomerado Voiter, considerando as regulamentações vigentes e melhores práticas de mercado e observando os seguintes princípios:

- Confidencialidade: Assegurar que a informação é acessível somente por pessoas autorizadas;
- Integridade: Proteger a exatidão e a Completeza da informação e dos métodos de processamento; e
- Disponibilidade: Assegurar que todos os usuários autorizados tenham acesso à informação e ativos associados, quando necessário.

Também tem como objetivo a proteção dos ativos de informação e formar a base para o estabelecimento de procedimentos de Segurança da Informação e cibernética do Conglomerado.

2. Abrangência

Esta Política aplica-se a todo o Conglomerado, inclusive às empresas subsidiárias e unidades estabelecidas no exterior, as quais deverão, no que couber, adequá-la às exigências da legislação e regulamentação locais.

3. Conceitos

Segurança da Informação: é a proteção da informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (Definição ISO 27.002)

Risco Cibernético: refere-se aos potenciais resultados negativos associados aos ataques cibernéticos. Por sua vez, os ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas tecnológicos.”. (Definição adotada pela IOSCO)

Usuário: todos os funcionários, prestadores de serviços, terceiros ou estagiários aos quais possuem acesso a algum recurso sistêmico ou de infraestrutura do Conglomerado.

Acesso Lógico: são qualquer tipo de aplicação ou equipamento que usa da tecnologia para impedir que pessoas acessem documentos, dados ou qualquer tipo de informação sem a

autorização adequada. Uma tela de login de um e-mail qualquer, em que se pede um nome de usuário e senha, é uma forma de controle de acesso lógico, por exemplo.

Acesso Físico: são aqueles que administram o acesso de pessoas, veículos e materiais a uma área restrita e protegida. Uma simples cerca ou muro já podem ser considerados controles de acesso físicos, por exemplo.

4. Diretrizes

As informações devem ser protegidas contra acesso, modificação, destruição ou divulgação não autorizada, independentemente do meio em que se encontrem.

As informações são de propriedade da instituição as quais são monitoradas rotineiramente, não havendo privacidade ou sigilo para seus conteúdos entre funcionários e o Voiter.

É proibido enviar materiais de uso exclusivo da instituição para pessoas de fora dela, sem as devidas autorizações.

As informações confidenciais deverão ser tratadas com o sigilo necessário.

Os recursos disponibilizados devem ser utilizados somente para os propósitos e finalidades aprovados pela Instituição, sendo vedada a utilização para fins pessoais.

As senhas de acesso corporativo são de uso pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto a sua guarda.

É proibido o compartilhamento de senhas de acesso, sendo passíveis de sanções os descumprimentos.

Para os acessos core do Conglomerado foram desenvolvidas as matrizes de segregação de acessos, nelas estão detalhados os sistemas, módulos, perfis e departamentos autorizados a utilizarem os acessos à determinados perfis dos sistemas.

O acesso ao Webmail Corporativo é liberado somente para Coordenadores, Gerentes, Superintendentes, Diretores, Vice-Presidentes e Presidentes, e as exceções deverão ser aprovadas pontualmente.

É proibido o uso de câmeras fotográficas ou de filmagem, sem autorização prévia, a ser concedida pela área de Segurança da Informação, dentro das instalações do Conglomerado.

Todas as instalações de processamento e guarda de informações, deverão ser mantidas em áreas seguras e protegidas.

O acesso remoto para fins relacionados às atividades da instituição será liberado para Supervisores, Coordenadores, equipes de apoio de processos críticos, Gerentes, Superintendentes, Diretores, Vice-Presidentes e Presidentes, sendo ele realizado através de meios de conexões seguras utilizando-se de técnicas criptográficas, e as exceções deverão ser aprovadas pontualmente.

O Voiter disponibilizará acesso à Internet via rede Wireless, segregado da rede corporativa, sendo este acesso exclusivo para os colaboradores da instituição ou visitantes em caráter de uso corporativo.

As atividades de processamento da informação serão monitoradas, detectadas e registradas através de trilha de auditoria. O monitoramento e o registro devem estar de acordo com a legislação vigente.

O Conglomerado realizará backups rotineiros e testes periódicos de restauração de dados, visando salvaguardar os ativos de informação da instituição.

Todo hardware desktop, hardware móvel, mobile, deverão ser utilizados para fins corporativos de acordo com as regras estipuladas pela instituição, sendo responsabilidade do funcionário a guarda e zelo do equipamento.

Não será permitida sem autorização previa do gestor imediato e da área de Segurança da Informação a utilização de hardware externos do tipo: unidade de armazenamento de dados, dispositivos de comunicação externas, dispositivos de transmissão de dados e unidade de leitura de dados internos e externos.

A violação ou não aderência às políticas e procedimentos de segurança de informações podem ocasionar sanções disciplinares e, em alguns casos, levar ao desligamento do funcionário, inclusive por justa causa, se aplicável, ou ao cancelamento do contrato de serviço.

4.1. Contratação de Serviços de Processamento e Armazenamento de Dados de Computação em Nuvem

4.1.1. Diretrizes para contratação de serviços para processamento e armazenamento de dados e de computação na Nuvem

- Verificar a capacidade do potencial do prestador de serviço, assegurando o acesso aos dados e às informações a serem processadas ou armazenados pelo prestador do serviço visando a mitigação de eventuais vulnerabilidades;
- Considerar os três princípios da Segurança da Informação;
- Verificar a aderência a certificações exigidas;
- Acesso à 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;
- Identificar, proteger e segregar os dados de clientes por meio de controles físicos ou lógicos.

4.1.2. Os serviços de computação em nuvem abrangem a disponibilidade sob demanda e de maneira virtual, de ao menos um dos seguintes serviços

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a implantação ou execução de softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- Implantar e executar aplicativos desenvolvidos pelo Voiter ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;

- Executar por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

Observação: A contratação de serviços de processamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil em no máximo 10 dias após a contratação do serviço, bem como alterações contratuais.

4.1.3. Da prestação de serviço por terceiros no exterior

- Verificar a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados, em caso de inexistência de convênio, deverá ser solicitada a autorização do Banco Central do Brasil para a contratação;
- Assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;
- Definir previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

4.1.4. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever

- A indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A Manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- A obrigatoriedade, em caso de extinção do contrato, de transferência dos dados ao novo prestador de serviços ou à instituição contratante e a exclusão dos dados citados no pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;
- O Voiter deverá ser notificado sobre a subcontratação de serviços e a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.

4.1.5. Para a decretação de regime de resolução do Voiter pelo Banco Central do Brasil

- O prestador de serviço deve obrigar-se a conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações e aos códigos de acesso, que estejam em poder da mesma.
- Realizar a notificação prévia sobre a intenção de a empresa contratada interromper a prestação de serviços (pelo menos trinta dias de antecedência) da data prevista para a interrupção;
- O prestador de serviço deve aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução e a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

4.1.6. Gestão de Vulnerabilidades

- A finalidade desde processo é descrever todas as atividades relacionadas à iniciação, implementação e manutenção dos registros de correções, ações corretivas e preventivas.
- Este procedimento aplica-se a todas as atividades implementadas no Sistema de gestão da segurança da informação (SGSI).

4.1.7. Não Conformidades e correções

- Uma não conformidade é qualquer falha decorrente do não atendimento dos requisitos especificados nas documentações internas, regulamentações, contratos e outras obrigações dentro do SGSI.
- Não conformidades podem ser identificadas durante uma auditoria interna ou externa, com base na revisão de gestão, após incidentes, durante operações de negócio normais ou em qualquer outra ocasião.

5. Papeis e Responsabilidades

5.1. Conselho de Administração

- Aprovar a política de Segurança da Informação e Cibernética anualmente;
- Emitir ciência sobre o relatório anual sobre a implementação do plano de ação e de resposta a incidentes;
- Promover a divulgação desta política a todos os administradores, funcionários, prestadores de serviços, consultores e fornecedores, doravante denominados Usuários;

- Divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética;
- Prover recursos de gestão para monitorar os serviços a serem prestados.

5.2. Usuários

- Cumprir as Políticas e Diretrizes estabelecidas neste documento e nos controles internos disponíveis na Intranet, conforme termo firmado na contratação;
- Bloquear o desktop/notebook ao ausentar-se do posto de trabalho;
- Salvaguardar os ativos de informação do Conglomerado;
- Utilizar os sistemas de computação ou acesso a informações, em qualquer meio, somente para exercer suas funções no Conglomerado e quando autorizado pelos seus superiores;
- Seguir os procedimentos de forma a garantir que papéis e mídias removíveis, bem como as informações manipuladas por sistemas aplicativos, planilhas Excel, documentos Word, etc., não fiquem expostos ao acesso de pessoas não autorizadas;
- Observar e atender a todas as normas que regulamentam as atividades da Instituição;
- Utilizar o correio eletrônico e quaisquer outras ferramentas apenas para fins corporativos;
- Zelar pelo token utilizado para uso de senha forte. Em caso de perda o usuário devera contatar a área de Segurança da Informação para a obtenção de um novo.
- Agir imediatamente para controlar, conter e corrigir, não conformidades e lidar com suas consequências;
- Propor ações corretivas em casos de incidentes;
- Enviar informações da não conformidade para a Segurança da Informação através dos canais de comunicação conforme procedimento de referência (Procedimento Gerenciamento de Incidentes)
- Adotar a Política de Mesa Limpa, evitando a manutenção de informações confidenciais sobre clientes e fornecedores em cima das mesas.

5.3. Gestores

- Garantir que os seus subordinados sigam e apliquem diariamente as políticas e os procedimentos referentes à Segurança das Informações;
- Autorizar o acesso às informações e recursos necessários para que as pessoas que estão sob sua gestão, mesmo terceiros exerçam suas atividades;
- Solicitar a revogação dos acessos, para as pessoas que tenham sido desligadas e estavam sob sua gestão;

- Garantir que todas as solicitações de concessões e revogações de acesso aos Sistemas sejam solicitadas através de abertura de chamado com devida anuência do Proprietário da Informação;
- Gerir os acessos daqueles que estão sob sua gestão;
- Gerir os acessos dos sistemas sob sua responsabilidade.

5.4. Área de Segurança da Informação

- Gerenciar os controles de acesso lógico, considerando os seguintes itens:
  - Registro e gestão de novos usuários;
  - Gestão das senhas de usuários;
  - Liberação de acesso inerente à função (Perfil) necessário;
  - Reavaliação ou revogação de acessos não autorizados;
  - Controle de acesso lógico a aplicações e sistemas.
- Manter bloqueados sites das seguintes categorias:
  - Pornografia;
  - Conteúdo racista, discriminatório ou apologias semelhantes (apologia ao crime, nazismo e etc);
  - Jogos (ex: jogos online, miniclip, jogos em flash e etc);
  - Webmail (ex: uol, yahoo, terra e etc).
- Gerir a Matriz de Segregação de Funções;
- Realizar periodicamente a revisão de acessos;
- Garantir a manutenção de antivírus em todas as estações de trabalho, servidores e demais equipamentos;
- Executar monitoramentos diários com relação a acessos, usos e conteúdo, visando identificar ações indevidas com as funções desempenhadas na instituição, bem como, aquelas que deponham contra os princípios éticos do Conglomerado.

5.5. Área de Infraestrutura

- Os procedimentos operacionais de administração de redes e sistemas devem estar claramente definidos e documentados, de forma a garantir uma operação correta e segura. Isso inclui os seguintes procedimentos, sem limitar-se a eles:
  - Ativação e desativação de equipamentos;
  - Backup de dados;
  - Manutenção de equipamentos;
  - Configuração e administração de ambiente de tecnologia;
  - Procedimentos de reinicialização e recuperação de Servidores.

- Devem ser controladas todas as alterações e ou mudanças realizadas nas redes e sistemas, como:
  - Aquisição de novos equipamentos;
  - Devolução e remanejamento de equipamentos;
  - Alterações de ambiente;
  - Controle de software e aplicativos: instalação, configuração, atualização de versões etc.
- As atividades e o estado da rede devem ser monitorados, com ação pró-ativa para prever possíveis problemas e ao planejamento da capacidade dos equipamentos.
- Manter Backup para arquivos localizados nos diretórios de rede que não foram acessados no período de "02" anos;
- Armazenar em fitas de Backup os arquivos removidos da Rede;
- Recuperar arquivos, caso necessário.

5.6. Área de Compliance

- Avaliar as solicitações de acesso em exceção, em conjunto com o gestor imediato avaliando se o acesso será permitido ou não, podendo este ser submetido à aprovação de um diretor caso necessário.
- Elaborar o relatório anual de resposta a incidentes.

5.7. Área de Recursos Humanos

- Comunica a admissão de novos funcionários, via ferramenta workflow, às diversas áreas da instituição que atuam nas concessões de acesso, quer sejam físicos ou lógicos, para que os respectivos acessos básicos inerentes à função desempenhada sejam adequadamente concedidos;
- Informar o desligamento dos usuários via ferramenta de Workflow, para que a área de Segurança da Informação possa remover os acessos físicos e lógicos dos colaboradores;
- Reter o dispositivo OTP Token e crachá de identificação encaminhar à área de Segurança da Informação.
- Bloquear Funcionário em férias, podendo inserir as datas de início e fim do bloqueio e automaticamente a ação será executada no Active Directory;
- Informar transferência de colaboradores entre áreas aos envolvidos, para a concessão de acessos necessários e revogação de acessos da área anterior.

6. Regulamentação Associada

Norma ISO/IEC 27001

Resolução CMN nº 4.658, de 26 de abril de 2018

Resolução CMN nº 4.557, 23 de fevereiro de 2017

Edital de Consulta Pública 57/2017 do BACEN

Guia ANBIMA de Cibersegurança

Procedimento de Gerenciamento de Incidentes

Procedimento de Gerenciamento de Incidentes Cibersegurança

Política de Continuidade de Negócio

Procedimento de Continuidade de Negócio

Política de Contratação de Fornecedores e Prestadores de Serviços

7. Validade

26.03.2022

8. Responsáveis

Elaboração	Revisão	Aprovação
Segurança da Informação	Segurança da Informação	Conselho de Administração (26.03.2021)

9. Histórico

Publicação/Revisão		Itens Alterados	Razões da Alteração
Nº	Data		
29	26.03.2021	-	Revisão Periódica
28	01.10.2019	7.3 11 16.2	- Complemento sobre o item 7.3 sobre Revisão de Acessos - Removido item sobre "11. Agentes Autônomos de Investimentos Externos" relacionado à Guide Investimentos - Atualização dos ramais "16.2. Não Conformidades e correções"
27	11.06.2019	Diversos	Revisão e melhorias.
26	26.10.2018	-	Inclusão SmartBank
25	31.07.2018	15	Inclusão sobre Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem
24	16.07.2018	7.3	Inclusão sobre Tópico de Revisão de Acessos

23	05.12.2017	5.1	Atualizado item sobre usuários locais
22	20.11.2017	7.3	Atualizado Título do sub tópico e incluído informações referentes as planilhas de apoio no preenchimento de novas demandas.
21	20.11.2017	12.4	Atualizado texto: previa do gestor imediato e da área de Segurança da Informação.
20	20.11.2017	17 / 17.1 e 17.2	Adicionado Tópico Gestão de Vulnerabilidade (“de acordo com Requisito de Edital do Banco Central sobre Ciberseguranca)
19	20.11.2017	Diversos	Adicionado Tópico Referências.
18	20.11.2017	16	Adição do tópico Risco Cibernético.
17	20.11.2017	Diversos	Alterado nome da Política de acordo com Requisito de Edital do Banco Central sobre Ciberseguranca.
16	24.07.2017	5.9.4	Removida a matriz acessos físicos aos CPDs.
15	05.07.2017	Diversos	Unificação do procedimento de Acesso Lógico com a Política de Segurança da Informação.
14	21.11.2016	1 e 7.1	Adicionado Conglomerado e perfil padrão sistema Intranet.
13	29.09.2016	5.9, 5.9.1, 7.1	Inclusão do uso em celulares particulares, inclusão de gerentes gerais, inclusão do sistema CIM e exceções da matriz de segregação.
12	27.04.2016	8	Inclusão do sistema Risk Broker
11	05.04.2016	7.1 e 8.	Alteração do item 7.1 e inclusão do item 8
10	11.11.2015	4.Diretrizes: Acesso Lógico e Físico/Webmail Corporativo/Controle de Entrada Física do Ambiente	- Adicionados os Coordenadores para terem acesso liberado ao Webmail Corporativo - Adicionada periodicidade para revisão de acessos lógicos e físicos.
09	19.02.2015	Definição de liberação do recurso restrito Webmail Corporativo	Alinhado com o RH o fluxo de aprovação desse recurso
08	18.08.2014	Diversos	- Alterado os processos de solicitação de acesso aos recursos: (Webmail corporativo e Webmail Pessoal). - Alterado a informação sobre a abrangência das áreas que utilizam o Token (hardware e dispositivo mobile). - Alteradas as informações referente à atuação do RH nos processos de admissão, demissão, férias, licença e alteração de departamento dos funcionários, estagiários e terceiros.
07	04.11.2013	-	Reestruturação e Logotipo

06	23.09.2013	Webmail Corporativo/ Utilização Dispositivo Mobile Pessoal	Adicionado tópico relacionado à restrição da utilização de Webmail Coorporativo e Dispositivo Móvel Pessoal.
05	28.08.2013	Webmail pessoal	Adicionado tópico relacionado a restrição da utilização de Webmails particulares.
04	18.02.2013	Diversos	Adição de condutas de preservação de informação
03	10.05.2012	Sistemas de Banco de Dados	Revisão Anual / Inclusão de Informações Base de Dados
02	12.04.2011	Diversos	Reestruturação Geral