POLÍTICA DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

AGORACRED S.A SOCIEDADE DE CRÉDITO, FINANCIAMENTO E INVESTIMENTOS

VITÓRIA (ES)

2020

CONSIDERAÇÕES INICIAIS

A informação é um dos principais geradores de valor para uma instituição e a qualidade do fluxo de dados é o principal subsídio para tomada de decisão e interpretação dos movimentos de negócio. Como consequência é importante um acompanhamento constante no intuito de combater riscos e ameaças, ao mesmo tempo em que se atue de maneira a manter a integridade e segurança dos dados (sejam eles *online* ou *offline).*

1. OBJETIVO

Esta Política busca garantir que os recursos computacionais e a manipulação de dados estejam de acordo com o nível de segurança exigido pela organização e pelos órgãos reguladores bem como nortear a definição de normas e procedimentos específicos de segurança da informação, tal qual a implementação de controles e processos para seu atendimento.

2. ABRANGÊNCIA E ÁREAS AFETADAS

Esta Política se aplica a todos os colaboradores, gestores, representantes, fornecedores, parceiros, terceiros e acionistas da Agoracred S/A.

3. DOCUMENTOS RELACIONADOS

Esta Política está relacionada a:

- Política de Atividades em Banco de Dados;
- Política de Relacionamento com Fornecedores e Terceiros;
- Política de Gerenciamento de Cadastros;
- Política de Gestão de Incidentes;
- Política de Gerenciamento de Riscos, Capital e Divulgação de Informações;

4. DOCUMENTAÇÃO SUBORDINADA

São documentos desdobrados a partir desta Política:

- Plano de Ação e Resposta a Incidentes Cibernéticos.

5. ASPECTOS REGULATÓRIOS

A criação desta Política teve como base os seguintes regulatórios:

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados)
- Lei nº 9.609/1998 (Lei de Software)
- Resolução nº 4.557/17 do Banco Central do Brasil;
- Resolução nº 4.658/18 do Banco Central do Brasil;
- ISO 27.000

6. DEFINIÇÕES

6.1 SOFTWARE

É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

6.2 BACKUP

É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

6.3 MÍDIAS REMOVÍVEIS

Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

6.4 VIRTUAL PRIVATE NETWORK (VPN)

Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

6.4 FIREWALL

É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

6.6 INFORMAÇÃO DE PROPRIEDADE DA AGORACRED S/A

Toda informação sobre a Agoracred S/A, seus colaboradores, fornecedores, terceiros, clientes, diretores e acionistas.

7. DA POLÍTICA DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Dentro da cibersegurança e proteção de dados, considera-se:

7.1 DOS FUNDAMENTOS

Esta Política está construída sob diretrizes orientativas que instruem a construção dos processos e atividades executadas, a saber:

i. Toda informação – *online* ou *offline* - que seja propriedade da Agoracred S/A deve ser protegida de qualquer ameaça que possa comprometer sua confidencialidade, integridade ou disponibilidade;

ii. No que tange à Cibersegurança e proteção de dados, a Agoracred S/A, deve empregar esforços compatíveis com a natureza das operações e complexidade de seus produtos;

iii. A Agoracred S/A deve disseminar cultura de Cibersegurança e proteção de dados a todos seus stakeholders;

iv. A Agoracred S/A deve adotar postura prospectiva no gerenciamento de Cibersegurança e proteção de dados, atuando com procedimentos e controles que reduzam sua vulnerabilidade a falhas e incidentes;

v. Independentemente da forma como é gerada, tratada ou compartilhada, toda informação sob propriedade da Agoracred S/A deve ser utilizada unicamente para finalidade com a qual foi autorizada;

vi. A contratação de serviços relevantes, fornecedores e terceiros que atuem no processamento e armazenamento de dados deve obedecer, além do estipulado na POLÍTICA DE RELACIONAMENTO COM FORNECEDORES E TERCEIROS, às disposições específicas do item 7.6 desta política;

vii. O tratamento de incidentes relativos ao sistema cibernético e de dados deve obedecer, além da POLÍTICA DE INCIDENTES, às disposições específicas no item 7.7 desta política;

viii. A Gestão de Continuidade de Negócios (GCN) deve considerar o tratamento de incidentes cibernéticos e definir protocolos de ação para cenários de interrupção dos serviços de processamento e armazenamento de dados e de computação em nuvem;

ix. É de propriedade da Agoracred S/A, todos os *designs*, criações ou procedimentos desenvolvidos por qualquer funcionário ou terceiro durante o curso de seu vínculo com a Agoracred S/A;

x. A Agoracred S/A deve indicar Diretor Responsável pela Cibersegurança e Proteção de Dados e este pode acumular funções, desde que não configure conflito de interesse.

7.2 DOS OBJETIVOS DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Para assegurar que as informações e dados sob propriedade da Agoracred S/A estejam gerenciadas e protegidas contra roubo, fraude, espionagem, perda e quaisquer outras ameaças, tornam-se objetivos da cibersegurança:

i. **Confidencialidade:** é a garantia que as informações e dados sejam acessíveis somente ao pessoal especificamente autorizado;

ii. **Integridade:** é a garantia de exatidão e inteireza das informações e dados, sem modificações indevidas (sejam intencional ou não);

iii. **Disponibilidade:** é a garantia que as pessoas autorizadas a tratar as informações e dados tenham acesso ao seu conteúdo e possam consultá-las a qualquer momento;

7.3 DA UNIDADE RESPONSÁVEL PELA CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Fica eleito a unidade organizacional de TI INFRAESTRUTURA como a responsável pela gestão de cibersegurança e proteção de dados, tendo como atuação a proposição de ajustes, melhorias,

aprimoramentos, validações e modificações desta Política; executar todas as atividades para gestão de segurança da informação; realizar a gestão de controle, distribuição e instalação de softwares utilizados. A TI INFRAESTRUTURA também é responsável por colaborar juntamente à unidade organizacional responsável pela gestão de riscos e de capital para melhoria contínua da operação de gestão de risco e evolução de sua governança corporativa.

7.4 DA CLASSIFICAÇÃO DA INFORMAÇÃO

Em conformidade com a POLÍTICA DE GERENCIAMENTO DE CADASTROS, as informações e dados são classificados em:

i. **Pública:** é toda informação de propriedade da Agoracred S/A oriunda de base pública e/ou com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional, sendo destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma;

ii. **Pessoal:** é toda informação de propriedade da Agoracred S/A relacionada a pessoa natural identificada ou identificável;

iii. **Pessoal Sensível:** é toda informação de propriedade da Agoracred S/A sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

iv. **Interna:** é toda informação de propriedade da Agoracred S/A que esta não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos mínimos ou irrelavantes à imagem da Organização o que permite seu acesso sem restrições por todos os empregados e prestadores de serviços da Agoracred S/A.

v. **Confidencial:** é toda informação de propriedade da Agoracred S/A considerada crítica para os negócios da instituição e cuja divulgação não autorizada pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

vi. **Restrita:** é toda informação de propriedade da Agoracred S/A que pode ser acessada somente por usuários desta Instituição explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

7.5 DOS PROCEDIMENTOS DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Dentro dos procedimentos adotados para gerenciamento da Cibersegurança e proteção de dados, deve-se observar:

7.5.1 REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

Os servidores que armazenam os sistemas críticos à operação da Agoracred S/A devem ser hospedados em *Data Centers* que possua acessos controlados e monitorados, bem como garantam disponibilidade dos ativos informacionais a esta Instituição com perenidade, inclusive quando acionados os protocolos de continuidade de negócio.

Os *Data Centers* devem aderir às Políticas pertinentes da Agoracred S/A bem como atender às quaisquer solicitações desta instituição, inclusive de visitação, além de garantir sua capacidade de resposta a incidentes e continuidade de negócio.

Já as máquinas e estações de trabalhos dos colaboradores e terceiros que atuem na Agoracred S/A devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos. Observa-se que estes ativos físicos devem utilizar apenas softwares licenciados ou autorizados pela unidade responsável, bem como é obrigatório o uso de software de Endpoint para fins de controle de ameaças eletrônicas, vírus, zero-day, ransonware.

7.5.2 REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente, com papéis de responsabilidade claramente definidos e registrados. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir os objetivos desta política.

7.5.3 DA AUTENTICAÇÃO E SENHA

O usuário (seja colaborador ou terceiro) é responsável por todos os atos executados com seu login e senha, sendo papel do usuário manter a confidencialidade de seus dados e alterar a senha periodicamente, utilizando combinações de qualidade e difícil adivinhação. Também é papel do usuário bloquear seu equipamento sempre que se ausentar.

7.5.4 DA MESA LIMPA E TELA LIMPA

O usuário deve adotar postura aderente as práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.)

não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo.

7.5.5 DO BACKUP

Os backups devem ser automatizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial. As mídias de backup (como DAT, DLT, LTO) devem ser acondicionadas em local seco, climatizado, seguro (e sempre que possível em salas cofres e/ou cofres corta-fogo segundo as normas de segurança) e fora do site de produção. Já as fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome com etiquetas não manuscritas.

O tempo de vida, qualidade e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante, o parque de fitas deverá ser substituído no máximo após 2 anos de uso. É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

A unidade responsável pela gestão dos sistemas de backup deverá realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias e testes periódicos de restauração (restore) com prazo máximo de 120 dias, de acordo com a criticidade do backup.

7.5.6 DA VPN

O uso do acesso via VPN deve ser restrito e utilizado para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades, sendo vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários. Todo acesso por meio de VPN deverá ser antecedido pela formalização do pedido de acesso, seguido da finalidade e período necessário para a realização da tarefa, após o período de liberação o mesmo deverá ser bloqueado.

7.5.7 DA VIOLAÇÃO DESTA POLÍTICA

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis. O infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato e a Diretoria.

7.6 DA CONTRATAÇÃO DE SERVIÇOS RELEVANTES, DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A contratação de serviços relevantes para processamento e armazenamento de dados e de computação em nuvem são solicitadas através da unidade responsável pela Cibersegurança, que deve:

i. Observar a contratação com aderência à estratégia, apetite e gestão de riscos e capital da Agoracred S/A;

ii. Assegurar que o potencial prestador de serviço tenha capacidade de fornecer o produto/serviço dentro das especificações técnicas bem como garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e informações processados ou armazenados;

iii. Assegurar que o potencial prestador de serviço esteja em condições de cumprir a legislação vigente e fornecer à Agoracred S/A, a qualquer tempo, o acesso aos dados e informações a serem processados ou armazenados;

iv. Assegurar que o potencial prestador de serviço seja devidamente certificado para a prestação do serviço e disponibilize para Agoracred S/A relatórios de auditoria independente – contratada pelo prestador – a respeito dos procedimentos e controles adotados na prestação do serviço;

v. Assegurar que o potencial prestador de serviço demonstre a identificação e segregação dos dados dos clientes da Agoracred S/A por meio de controles físicos ou lógicos, bem como a qualidade dos controles de acessos voltados à proteção de dados e informações dos clientes da instituição;

vi. Documentar a diligência realizada para contratação do prestador de serviço e disponibilizar tais relatórios à unidade responsável pela gestão de riscos e de capital;

vii. Quando pertinente, comunicar ao Banco Central do Brasil a respeito das contratações de serviços relevantes de processamento e armazenamento de dados, bem como quaisquer alterações contratuais relevantes;

viii. Garantir que o contrato firmado entre as partes apresente de maneira clara a adoção de medidas de segurança para transmissão e armazenamento de dados, além da manutenção da segregação de dados e controle de acesso para proteção de informações dos clientes da Agoracred S/A;

ix. Garantir que o contrato firmado entre as partes apresente de maneira clara as cláusulas, em caso de extinção, que versam sobre a transferência de dados e informações ao novo prestador de serviço bem como a exclusão dos mesmos após a transferência.

7.7 DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES CIBERNÉTICOS

Fica autorizado a gestão específica e direcionada do Plano de Ação e de Resposta a Incidentes Cibernéticos, que deve abranger:

i. Mapeamento dos principais incidentes, tanto observado em base histórica quanto incidentes de probabilidade significativa;

ii. As rotinas, os procedimentos, os controles e a tecnologia empregada na prevenção e na resposta aos incidentes mapeados;

iii. Produção de relatório anual onde conste os incidentes registrados e a efetividade das ações adotadas, os resultados obtidos e quaisquer mudanças necessárias para evolução da Cibersegurança.

7.8 DA DIVULGAÇÃO DA POLÍTICA DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Esta política deve ser divulgada aos colaboradres, fornecedores e terceiros que atuem na Agoracred S/A com linguagem clara, acessível e compatível as funções desempenhadas.

7.9 DAS EXCEÇÕES

Configuram exceções à esta Política:

i. Fica permitido, sem configurar quebra de sigilo ou confidencialidade, o trânsito de informações com o Banco Central do Brasil, Receita Federal, Poder Judiciário, Agência Nacional de Proteção de Dados, PROCON, representantes da Agoracred S/A devidamente qualificados (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros) e qualquer informação divulgadas após o consentimento escrito de ao menos dois Diretores Estatutários da Agoracred S/A.

ii. Fica dispensado de pedido formalizado à VPN as situações de crise descritos no Plano de Continuidade de Negócio (PCN).

8. RESPONSABILIDADES E ATRIBUIÇÕES

Competem as seguintes responsabilidades.

8.1 DIRETORIA

Aprovar esta Política;

Empreender esforços para aprimoramento e disseminação da cultura de cibersegurança e proteção de dados;

8.2 DEPARTAMENTO RESPONSÁVEL PELA CIBERSEGURANÇA

A gestão da cibersegurança e proteção de dados e as atividades descritas no item 7.3 desta Política.

8.3 GESTORES DA AGORACRED

Observar e cumprir esta Política na contratação de Fornecedores e Terceiros;

8.4 UNIDADE RESPONSÁVEL PELA GESTÃO DE RISCO E DE CAPITAL

Observar esta política na elaboração e gereciamento de riscos e de capital.

9. VIGÊNCIA

Esta política entra em vigência na data de sua aprovação e são concedidos 20 dias utéis para adaptação de processos pertinentes.

10. INFORMAÇÕES DE VERSÃO

DATA DA 1ª VERSÃO	27/07/2020
VERSÃO ATUAL	01
PERIODICIDADE DE REVISÃO	01 ano a partir de sua aprovação

Registro de Informações

Versão	Item Modificado	Modificação	Motivo
1ª	-	-	-

APROVAÇÃO

Política aprovada pelos Diretores da Agoracred S/A SCFI na data de sua assinatura. *ASSINATURA DIGITAL*

LEONARDO LIMA BORTOLINI:85011959791

Assinado de forma digital por LEONARDO LIMA BORTOLINI:85011959791
Dados: 2020.09.03 13:30:54 -03'00'

IVONE MATOS DE OLIVEIRA SABATINI:05542929710

Assinado de forma digital por IVONE MATOS DE OLIVEIRA SABATINI:05542929710
Dados: 2020.09.08 18:05:56 -03'00'