Política de Segurança da Informação/PSI

2023

Versão 2.2

São João da Boa Vista, 30 de junho de 2023

Sumário

APRESENTAÇÃO

Em uma economia baseada em dados e cada vez mais digital, o modo como as empresas gerenciam suas informações e seu conhecimento revela-se um fator muito importante para o sucesso dos negócios. Da mesma forma, a proteção à privacidade dos dados de cooperados, colaboradores e parceiros é fundamental para a criação de um ambiente de negócios seguro, confiável e próspero. A Cooperativa de Crédito Mútuo dos Servidores Municipais de São João da Boa Vista, doravante neste documento entitulada CREDIVISTA, entende que a informação, os dados e o conhecimento são ativos de grande valor e essenciais a qualquer processo de negócio, devendo, portanto, ser gerenciados, controlados e protegidos de forma eficaza fim de assegurar a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Logo, faz-se necessária a implementação de medidas e soluções de Segurança da Informação que se baseiem nos princípios da confidencialidade, integridade, disponibilidade e autenticidade que busquem prevenir a empresa de acessos indesejados, fraudes ou perda de informações. A Política de Segurança da Informação (PSI) é um documento que define o conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os seus colaboradores e prestadores de serviços. Por ser um "documento vivo", a Política de Segurança da Informação (PSI) é analisada, testada e revisada periodicamente para que reflita as práticas de gestão de Segurança da Informação necessárias à organização em seu contexto de tempo e espaço.

Esta política tem como guias principais os conceitos e orientações das normas ABNT ISO/IEC da família 27000, com suas alterações posteriores e as normativas do Banco Central.

1. INTRODUÇÃO

Segurança da Informação é o termo que descreve o conjunto de controles utilizados para a proteção das informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

São características básicas da Segurança da Informação os atributos de:

Integridade – Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas;

Confidencialidade – Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade – Garantia de que os usuários autorizados obtenham acesso às informações e aos ativos correspondentes sempre que necessário;

Não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

Este documento estabelece um conjunto de diretrizes que possibilitam as partes interessadas adotarem padrões de comportamento adequados com relação à utilização e preservação das informações. Foi elaborado pela Area de Tecnologia da Informação com base nas melhores práticas do mercado de TI.

1.1. Objetivo

Disseminar aos usuários a regras para utilização dos recursos de Tecnologia da Informação e orientá-los a utilizar esses recursos de maneira adequada.

1.2. Abrangência

A Política de Segurança da Informação da CREDIVISTA aplica-se a todos os usuários, sejam eles colaboradores, prestadores de serviços, consultores, temporários e estagiários que estejam a serviço da instituição, incluindo toda a mão de obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas.

Para este documento, consideram-se recursos de Tecnologia da Informação equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pela CREDIVISTA.

1.3. Validade

Esta versão da Política de Segurança da Informação entra em vigor em 01/10/2021 e possui validade indefinida, podendo ser substituída a cada 2 anos por uma versão atualizada.

1.4. Divulgação

A divulgação da política deve ser clara e ampla para que todos os usuários tenham acesso e possam compreendê-la.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 *Classificação da informação*

A Política de Segurança da Informação é aplicável a todas as informações sob gestão da CREDIVISTA, incluindo aquelas que são:

- Armazenadas e transmitidas por meios eletrônicos (correio eletrônico, mensagem de texto, fax e afins);
- Armazenadas em qualquer tipo de mídia (pendrive, câmeras digitais, DVD, CD e afins);
- Transmitidas em conversas formais e informais;
- Impressas ou escrita em papel.

A gestão da Informação na CREDIVISTA prima pela transparência, tanto em âmbito interno como em âmbito externo. Entretanto, algumas informações, seja no ato de sua geração, guarda, uso, transparência ou destruição – por seu imediatismo, cunho técnico relacionado a projetos específicos e/ou provenientes dos sistemas de informação, diretórios de rede e banco de dados aos quais o usuário em geral tenha conhecimento por força das atividades profissionais – deverão ser tratadas, manuseadas, preservadas e gerenciadas adequadamente. As informações confidenciais e sigilosas só devem ser acessadas mediante solicitação de acesso do responsavel imediato junto a Area da Tecnologia da Informação.

Todos os colaboradores têm a obrigação de cumprir, na íntegra, a Política de Segurança da Informação, servindo como exemplo de conduta em todas as situações vividas na cooperativa, observando as regras estabelecidas.

2.2 *Regras / Responsabilidades Gerais*

É de responsabilidade de todos o controle sobre a segurança das informações armazenadas nos equipamentos que estão sob seu poder, dentro da estrutura física e lógica da CREDIVISTA.

Os acessos realizados no ambiente informatizado através da utilização dos seus usuários e senhas de acesso, devendo sempre manter o sigilo sobre as informações e dados da CREDIVISTA. Usuário e senha são de uso pessoal e intransferível.

O usuário deverá solicitar permissão sempre que houver a necessidade de instalação de aplicativos ou alteração das configurações dos equipamentos da CREDIVISTA.

São expressamente proibidas as seguintes atividades:

- Criação, modificação, execução ou retransmissão de quaisquer instruções ou programas de computador com o intuito de obter acesso não autorizado a um recurso, equivalendo, neste caso, à tentativa de "quebra" da segurança de sistemas;
- A cópia, para utilização externa, de softwares adquiridos e/ou desenvolvidos pela instituição, a menos que formalmente autorizada e justificada pela Area da Tecnologia da Informação;
- A utilização de softwares não homologados pela Area da Tecnologia da Informação;
- A utilização dos recursos de informática dentro da estrutura física e lógica CREDIVISTA para fins que não sejam relacionados à sua atividade profissional.

Qualquer incidente que possa afetar a segurança da informação deverá ser comunicado imediatamente a Area da Tecnologia da Informação, mesmo que haja dúvida quanto às consequências.

2.2.1 *Area da Tecnologia da Informação*

Cabe Area da Tecnologia da Informação:

- Propor melhorias da Pormas de Segurança da Informação;
- Avaliar orçamentos adequados para investimentos em Segurança de informação;
- Disseminar e verificar o cumprimento das diretrizes e políticas de Segurança da Informação;
- Ter conhecimento sobre incidentes de Segurança da informação;
- Efetuar reuniões periódicas.

A Area da Tecnologia da Informação definira Plano Diretor de Tecnologia da Informação.

A coordenação dos trabalhos da Area da Tecnologia da Informação quanto a Segurança da Informação está sob sua responsabilidade, cujas atribuições abrangem a convocação e a realização de outros atos de suporte às atividades desenvolvidas, as demais atribuições realizadas para segurança da informação também vinculado a Area da Tecnologia da Informação.

2.2.2 Area da Tecnologia da Informção

Cabe a Area da Tecnologia da Informação:

- Manter e aplicar a política em todos os dispositivos de rede;

- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores da CREDIVISTA;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso à rede, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar os riscos referentes à segurança da informação e apresentar relatórios relacionados a tais riscos, acompanhado de proposta de aperfeiçoamento quando for o caso;
- Estabelecer o mecanismo e Registro de não conformidade no Relatório de Ocorrências;
- Realizar trabalhos de análise de vulnerabilidade, com o intuito de melhorar o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da cooperativa.

2.2.3 Proprietário da Informação:

O proprietário da informação ou dados decorrentes de suas atividades diárias são da CREDIVISTA conforme contrato de trabalho firmado entre colaborador e cooperativa.

A confidencialidade da informação está sob responsabilidade de um gerente ou diretor, responsável por solicitar concessão, revisão, manutenção e cancelamento de autorizações de acesso a determinado conjunto de informações que sejam de sua responsabilidade.

Cabe ao proprietário da informação:

- Para toda a informação sobre sua custodia elaborar uma matriz que relacione cargo e função às autorizações de acesso concedidas (perfil x função);
- Autorizar à liberação de acesso a informação sob sua responsabilidade, observando a Política e as Normas de Seguraça da Informação;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, solicitando o cancelamento daquelas que não são mais necessárias;
- Participar da investigação de incidentes relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões da Area da Tecnologia da Informação, prestando os esclarecimentos necessários.

2.2.4 Gerentes e Diretores

- Cumprir e fazer cumprir a Política de Segurança da Informação e suas Normas e Procedimentos;
- Assegurar que seu colaboradores possuem acesso e conhecimento desta Política, das Normas e Procedimentos da Segurança da Informação;
- Comunicar imediatamente eventuais casos de violação de segurança da informação à Area da Tecnologia da Informação.

2.2.5 Recursos humanos

Cabe à área de Recursos humanos:

- Colher a assinatura do Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- Informar, prontamente, todos os desligamentos, afastamentos e modificação no quadro de funcionários Area da Tecnologia da Informação.

3. POLÍTICA DE GESTÃO DE ATIVOS

3.1 Utilização da estação de trabalho

Cada estação de trabalho possui códigos internos que permitem sua identificação na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário do equipamento.

Esse tópico visa definir as regras de utilização da estação de trabalho que abrangem o login, a manutenção de arquivos no servidor e as tentativas não autorizadas de acesso.

- É recomendado encerrar ou bloquear a sessão do sistema ao se ausentar da estação de trabalho, de modo a prevenir o acesso indevido;
- O usuário deverá desligar sua estação de trabalho no final do expediente;
- A senha de acesso à estação de trabalho é de uso pessoal e intransferível, sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio usuário a cada 60 dias ou quando da suspeita de perda do sigilo;
- A senha deve ser composta com letras, números e caractere especial, além de ter no mínimo 8 caracteres e não pode ser usada na troca as 10 últimas senhas já utilizadas.
- É recomendado fazer a manutenção do diretório pessoal, evitando acúmulo de arquivos desnecessários;
- Não será permitida a instalação de programas e qualquer alteração não prevista e autorizada pela Area da Tecnologia da Informação;
- Não será permitida a abertura de recursos tecnológicos para qualquer tipo de reparo. Caso seja necessário, o reparo deverá ser solicitado a Area da Tecnologia da Informação.

3.2 Utilização da rede

O descarte de informações consideradas críticas e confidenciais deve ser feito de modo a impossibilitar a recuperação das mesmas.

Não são permitidas as seguintes atividades:

- Transmissão ou posse de informação que contenha material obsceno, indecente, lascivo ou outro material que explícita ou implicitamente se refira à conduta sexual;
- Transmissão ou posse de Informação, que contenha linguagem profana ou constitua apologia ao fanatismo, à prática sexual ou a quaisquer formas de discriminação;
- Transmissão ou posse de Informação que ameace a integridade física, que intimide outra pessoa ou organização;
- Transmissão de Informação que implique violação de quaisquer leis ou constitua incitamento de qualquer crime;
- Violação de direitos autorais, particularmente sobre software, dados e publicações;
- Divulgação de qualquer informação restrita ou confidencial sem a permissão de seu proprietário ou do gestor do recurso ao qual a informação pertence;
- Jogos direcionados ao entretenimento não poderão ser acessados, gravados ou instalados no diretório pessoal do usuário, na estação de trabalho ou em qualquer outro diretório de rede;

- Alterações das configurações de rede e inicialização das máquinas, bem como modificações que possam trazer problemas.

3.3 Utilização do correio eletrônico

O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fim pessoal não é permitida, pois podem prejudicar a CREDIVISTA de forma administrativa, jurídica, causar impacto no tráfego da rede e pôr em ricos a segurança das informações.

É proibido a utilização de correios eletrônicos de uso particular para assuntos da CREDIVISTA, pois prejudicam a cooperativa de forma administrativa, jurídica, causam impacto no tráfego da rede e põem em ricos a segurança das informações. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da CREDIVISTA:

-. enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

-. enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

-. enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a CREDIVISTA vulnerável a ações civis ou criminais;

-. divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

-. falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

-. produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da CREDIVISTA;

- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf e outros) ou qualquer outra extensão que represente um risco à segurança;

- Vise obter acesso não autorizado a outro computador, servidor ou rede;

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer

método ilícito ou não autorizado;

- Vise burlar qualquer sistema de segurança;

- Vise vigiar secretamente ou assediar outro usuário;

- Vise acessar informações confidenciais sem explícita autorização do proprietário;

- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

- Inclua imagens criptografadas ou de qualquer forma mascaradas;

- Tenha conteúdo considerado impróprio, obsceno ou ilegal;

- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

- Tenha fins políticos locais ou do país (propaganda política);

- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da empresa
- Telefone(s)
- Correio eletrônico

3.4 Utilização de dispositivos móveis

Para estabelecer as regras de dispositivos móveis, serão considerados quanto a seu proprietário:

3.4.1 Pertencentes a CREDIVISTA

- Será de responsabilidade da Area da Tecnologia da Informação a configuração desses equipamentos para que estejam aptos a interagir com os demais dispositivos fixos pertencentes à rede da CREDIVISTA. Deverão ser seguidos os mesmos critérios relativos à segurança da informação adotados para os equipamentos fixos (desktop);

- Cabe ao colaborador, usuário do dispositivo móvel, seguir os mesmos padrões de segurança adotados para os usuários de dispositivos fixos;
- Além dos procedimentos de segurança usuais para todos os equipamentos, o usuário de equipamento móvel deverá utilizar todos os meios disponíveis no equipamento destinados à proteção dos dados nele contidos, como senhas de acesso, travamentos de hardware ou outros recursos;
- No caso de conexão a uma rede externa por motivo de viagem, compete ao colaborador, além da manutenção da configuração original por meio de backup e/ou de ponto de restauração, o cuidado especial com as redes externas eventualmente utilizadas, de forma a não expor conteúdo corporativo que viole a confidencialidade;
- A Area da Tecnologia da Informação poderão realizar, a qualquer tempo, inspeção para verificar os aspectos relativos à configuração e à segurança dos equipamentos.

3.4.2 Pertencentes a usuários e visitantes

Os usuários e visitantes não poderão utilizar seus equipamentos portáteis nas dependências da CREDIVISTA, com as seguintes ressalvas:

- O equipamento poderá se conectar à rede WiFi (WiFi-Credista), exclusivamente para navegação da internet, onde serão considerados todos os itens de segurança e restrições de acesso à internet contidos neste documento;
- A conexão de equipamento particular do colaborador poderá se conectar à rede WiFi (WiFi-Credista), para conexão na rede coorporativa só será possível após análise e autorização da Area da Tecnologia da Informação, ressalvados todos os itens de segurança estabelecidos neste documento.

3.5 Acesso à internet

Todas as regras atuais da CREDIVISTA visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da cooperativa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a CREDIVISTA, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privados da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A CREDIVISTA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo responsável da sua área. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela cooperativa aos seus colaboradores, independentemente de sua relação contratual, não pode ser utilizada para fins pessoais.

Somente os colaboradores que estão devidamente autorizados a falar em nome da CREDIVISTA para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela cooperativa poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na CREDIVISTA e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Area da Tecnologia da Informação.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Area da Tecnologia da Informação.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da CREDIVISTA para

fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos responsáveis.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a CREDIVISTA ou de dados de sua propriedade aos seus parceiros e cooperados, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da CREDIVISTA para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos.

Os serviços de streaming (rádios on-line, canais de broadcast e afins) não serão permitidos.

Porém, os serviços de comunicação instantânea serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o responsavel entenda que seja necessário por estar causando impacto negativo ao andamento das atividades do departamento, troca de mensagens de assédio, perturbação, ofensivas e outras, e que requisite formalmente à Area da Tecnologia da Informação.

Não é permitido acesso a sites de proxy anônimos.

3.6 Antivirus

A CREDIVISTA deve possuir software antivírus apropriado, para proteção contra vírus e software malicioso. O software antivírus deve estar instalado e mantido devidamente atualizado em todas as estações de trabalho dos usuários, servidores, notebooks e netbooks. Todo e-mail recebido ou enviado deve ser verificado pelo software antivírus, assim como todo o acesso à Internet.

3.7 Midias Removiveis

O uso de mídias removíveis (mídias regraváveis, gravadores ópticos, discos rígidos externos, pen drives, cartões de memória ou similares) não são permitidos, somente por necessidade de

serviço ou por determinação expressa de superior hierárquico, e com a analise da integralidade do dispositivo pela da Area daTecnologia da Informação

3.8 Acesso aos sistemas informatizados

Este tópico visa definir as regras de utilização dos sistemas informatizados que abrangem seu acesso e uso.

- Os sistemas informatizados devem ser acessados somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, às normas e disposições contidas na legislação;
- As senhas de acesso aos sistemas informatizados deverão ser mantidas em caráter confidencial e intransferível;
- Os usuários serão responsáveis pelos acessos realizados com o login que lhes forem atribuídos. No caso de empresas terceiras, essa responsabilidade será do responsavel contratante, isto é, que utiliza os serviços contratados. É de responsabilidade do usuário cuidar da integridade, confidencialidade e disponibilidade dos dados, informações e sistemas aos quais tem acesso, devendo comunicar por escrito, ao responsavel, quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas, sendo proibida a exploração de falhas ou vulnerabilidade porventura existentes nos sistemas;
- Não é permitido o acesso aos sistemas com fins escusos ou imotivados.

3.9 Acesso Remoto

Quando o acesso remoto à rede corporativa se faz necessário para manter os serviços da CREDIVISTA. Contudo, este acesso pode ter origem em redes comprometidas ou nível de segurança significativamente menor que nossa rede corporativa. Embora essas redes remotas estejam fora do controle da CREDIVISTA, deve-se evitar os riscos externos para garantir a segurança da rede corporativa da CREDIVISTA.

Definir os padrões e requisitos para acesso remoto às estações de trabalho e servidores que compõem o ambiente tecnológico interno da CREDIVISTA; minimizar o potencial de exposição da CREDIVISTA às perdas e prejuízos resultante de uso não autorizado, pela exposição de

informações que comprometam imagem pública, reputação econômica social e disponibilidade, confidencialidade e integridade dos sistemas críticos da CREDIVISTA.

- O acesso remoto de uma rede externa às estações de trabalho e servidores da CREDIVISTA deverá ser rigorosamente controlado, autorizado, utilizando criptografia por uma VPN e autenticação com senha forte;
- As solicitações de acesso remoto aos usuários devem ser solicitadas a Area da Tecnologia da Informação através do formulário específico, com justificativa e período de trabalho. Estas solicitações devem ser autorizadas pelo Gerente Geral e arquivado para fins de auditoria;
- A disponibilização do acesso remoto deve ser autorizada pelo responsável em conformidade com o perfil funcional, priorizando o acesso em expediente regulamentar de trabalho, salvo casos de exceção devidamente justificado;
- O usuário com acesso remoto autorizado, acessará os mesmos ambientes que visualiza internamente, ou seja, terá o mesmo perfil de acesso;
- Os usuários autorizados ao acesso remoto, devem proteger suas credenciais e em nenhum momento devem disponibilizar seu login e senha de rede, e-mail, VPN, ou qualquer informação de acesso, para outra pessoa;
- Os usuários com acesso remoto autorizado devem garantir a não utilização do seu perfil de acesso remoto por outras pessoas.

Boas práticas:

- Recomenda-se que o usuário com autorização de acesso remoto utilize redes externas seguras, para acessar o ambiente tecnológico da CREDIVISTA;
- Os usuários que acessam a rede remotamente devem estar atentos para que sua estação de trabalho, notebook etc., não esteja também acessando outra rede ao mesmo tempo;
- O usuário, quando da utilização do acesso remoto, deverá permanecer conectado apenas a rede da CREDIVISTA, enquanto estiver efetivamente usando os serviços disponibilizados, devendo desconectar-se nas interrupções e no término do trabalho;
- Os usuários com acesso remoto devem cuidar para que informações sigilosas não sejam capturadas por terceiros que estejam próximos ao equipamento.

3.10 Acesso ao Data Center

O acesso ao Data Center Site A localizado na Rua Rua Senador Saraiva nº 59, bairro Centro, a Area da Tecnologia da Informação ou depessoas acompanhadas por estes.

A CREDIVISTA possue um rack central, o acesso à sala é restrito e o acesso é feito atraves de senha e leitura biometrica, com monitoramento e controle dos acessos.

3.11 Backup

Conforme estabelecido na Política de Backups:
Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

A Area da Tecnologia da Informação responsáveis pela gestão dos sistemas de backup deverão 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, entre outros.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios CREDIVISTA, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com os Níveis de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 15 ou 30 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo responsável da Area da Tecnologia da Informação. Maiores detalhes podem ser obtidos na Política de Backup da cooperativa

4. PENALIDADES

O não atendimento aos requisitos previstos nesta Política de Segurança da Informação será considerado violação às regras internas da CREDIVISTA.

Toda violação ou desvio caracteriza infração funcional. O infrator ou facilitador, seja por ação ou omissão, estará sujeito a medidas administrativas e legais cabíveis.

5. MONITORIA E AUDITORIA DO AMBIENTE

A Area da Tecnologia da Informação dispõe de recursos que poderão registrar e controlar a utilização dos sistemas e serviços disponibilizados, incluindo acesso à internet, visando garantir a disponibilidade e segurança das informações institucionais.

6. CONSIDERAÇÕES FINAIS

Este documento deverá ser amplamente divulgado a todos os colaboradores e prestadores de serviço.

É importante que todos estejam cientes de que os ambientes, sistemas, computadores e rede da instituição poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

Em caso de dúvida quanto ao uso e/ou descarte de informações, deverá ser obtida a orientação necessária com a Area da Tecnologia da Informação.