POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ÍNDICE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

O presente documento constitui uma declaração formal da Cooperativa de Economia e Crédito Mútuo dos Servidores Municipais de São João da Boa Vista, doravante neste documento intitulada CREDIVISTA, acerca de seu compromisso com a proteção das informações de sua propriedade, estabelecendo diretrizes corporativas que permitam aos colaboradores, cooperados e prestadores de serviços seguirem padrões de comportamento relacionados à segurança, adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

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.

2. RESPONSABILIDADE

É responsabilidade de cada colaborador da cooperativa manter-se atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de Tecnologia sempre que não estiver absolutamente seguro quanto a aquisição, uso e/ou descarte de informações. As diretrizes aqui definidas são extensíveis a prestadores de serviços da empresa, sendo responsabilidade da área contratante o repasse e respeito à política.

O Comitê Gestor da Segurança Cibernética e de Ética e Conduta, representado pelos membros da Diretoria Executiva e um colaborador de cada setor, é responsável pela criação e atualização desta política, assim como normas e procedimentos derivados. A atualização ocorrerá anualmente ou sempre que algum fato relevante motive sua revisão antecipada.

Os colaboradores da CREDIVISTA devem assinar um documento de responsabilidade pelo cuidado físico e integridade dos equipamentos ou componentes de tecnologia designados pela CREDIVISTA, incluindo aqueles designados aos fornecedores ou terceiros sob sua responsabilidade. Este documento deve incluir a assinatura do responsável pelo gestor responsável ao que foram designados os equipamentos. É obrigação dos referidos usuários informar ao gestor qualquer situação anormal ao respeito.

3. ÁREA GESTORA DA POLÍTICA DE SEGURANÇA

Responsável: Comitê Gestor da Segurança Cibernética e de Ética e Conduta

Atribuições:

– Responsável pela Política de Segurança

4. ESCOPO

As diretivas desta política visam proteger a informação de diversos tipos de ameaças, garantindo a continuidade dos negócios, minimizando os danos e maximizando as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

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;

Quaisquer informações geradas ou recebidas por colaboradores como resultado da atividade profissional pertence a referida instituição, sendo que as exceções devem ser explicitamente formalizadas em contrato entre as partes. Os equipamentos de informática, comunicação, sistemas e informações utilizados pelos colaboradores são destinados à realização de atividades profissionais, sendo o uso pessoal não permitido pois podem prejudicar o desempenho e pôr em ricos os sistemas e serviços.

A CREDIVISTA poderá monitorar e registrar o uso dos sistemas, internet e serviços visando garantir a disponibilidade e segurança das informações utilizadas.

Esta política se aplica a todas as áreas da CREDIVISTA suas dependências e outras unidades que possam vir a ser constituídas.

5. DIRETRIZES

A seguir são listadas as diretrizes gerais dos assuntos relacionados com a segurança da informação:

Os colaboradores e prestadores de serviços, usando a infraestrutura de tecnologia, concedem sua conformidade absoluta com as políticas corporativas de tecnologia.

Incluindo, ilimitado, seu consentimento para investigações, leitura e / ou revisões que as áreas designadas fazem relativas às informações, dados, arquivos, conteúdo e mensagens que enviam, recebem, armazenam ou acesso, utilizando a infraestrutura de Tecnologia da CREDIVISTA, incluindo informações, dados e documentos pessoais, sujeito a restrições provenientes de legislação aplicável e com conformidade com as diretrizes de gestão de dados pessoais de acordo à legislação do país.

Os colaboradores devem consultar com o gestor, quaisquer perguntas sobre o uso de qualquer componente da infraestrutura de tecnologia para fins pessoais.

Na CREDIVISTA é considerado "PROIBIDO" os serviços de e-mail, mensagem instantânea e internet, aplicações e infraestrutura como segue:

a) Qualquer atividade que interfira com as funções ou demanda de produtividade dos colaboradores da CREDIVISTA.

b) Busca, acesso, consulta, publicação ou transferência de conteúdo que não cumpre o código de ética do negócio da CREDIVISTA

c) Uso do software ou acesso a sites da internet ou quaisquer atividades realizadas e / ou na transferência de informação da internet de forma anônima.

d) Enviar mensagens, documentos ou bens da informação da CREDIVISTA, dos colaboradores, dos seus cooperados ou dos seus fornecedores, a sites ou contas pessoais ou públicos sem haver a devida autorização do gestor da Cooperativa;

e) uso de e-mail, mensagem instantânea e internet como mídia de comunicação oficial a CREDIVISTA por quem não está autorizado a fazer;

Em casos de violação desta política, a CREDIVISTA reserva o direito de restringir ou cancelar o acesso a qualquer serviço mensagens instantâneas, e-mail, mídia social ou página de internet, total ou parcialmente, como determinado pela área de segurança.

Todas as conexões de rede de internet da CREDIVISTA dever ser feito por meio de mecanismos de segurança (por exemplo firewall), filtro de conteúdo e registro de atividade, de acordo com as normas de tecnologia, todo tráfego de mensagens, dados ou informações, de

ou para qualquer equipe que está conectada às redes CREDIVISTA deve seguir por tais mecanismos, ou o equipamento informático que este conecte à rede CREDIVISTA em nenhum evento deve ser simultaneamente conectada às redes de terceiros.

5.1 - Correio Eletrônico

O objetivo desta norma é informar aos colaboradores da CREDIVISTA quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

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 instituição 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 ou suas unidades vulneráveis 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 Cooperativa de Economia e Crédito Mútuo dos Servidores Municipais de São João da Boa Vista;

- 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;

- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)

- 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

5.2 - 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 instituição 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 gestor. 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 instituição 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 CRDEIVISTA 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 instituição 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 Gerência de Sistemas.

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 Gerência 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 gestores.

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 clientes, 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 gestor entenda que seja necessários 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 Gerencia da Tecnologia da Informação.

Não é permitido acesso a sites de proxy anônimos.

5.3 - Controle de Acesso Físico

Manter restrito, por controles físicos apropriados e proporcional à criticidade dos equipamentos, o acesso a todas as áreas onde serão processadas ou armazenadas informações pertinentes à operação da cooperativa, mantendo lista de acesso a estes ambientes.

5.4 - Controle de Acesso (Lógico)

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a CREDIVISTA anônimos e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na CREDIVISTA, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a CREDIVISTA e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos da CREDIVISTA é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência da Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência da Tecnologia da Informação da Cooperativa de Economia e Crédito Mútuo dos Servidores Municipais de São João da Boa Vista. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 60 (sessenta) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato a Gerencia da Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

5.5 - Backup

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 Gerência 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 a Norma 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 30 ou 60 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 Coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

Maiores detalhes podem ser obtidos na Política de Backup.

5.6 - Softwares

Programas de computador ou software são propriedade intelectual, protegida pela Lei 9.609/1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei 9.610/1998 que trata dos direitos autorais. Deve-se considerar que o uso de softwares não licenciados pode prejudicar a segurança dos dados, deve ser considerado que o uso de software não licenciado é crime. E a penalidade pode chegar à multa proporcional ao valor comercial do software, segundo interpretações baseadas no Art. 56 da Lei 9.610/98. Conforme legislação federal, principalmente a Lei de Direitos Autorais e na Lei de Software, nenhum colaborador da CREDIVISTA deve se envolver em qualquer atividade que viole os direitos de propriedade intelectual referentes a licenças de software ou qualquer outra política relacionada a softwares de computador ou conteúdo em formato digital. Obter, usar, copiar ou distribuir software para outros usuários ou computadores, caso tal hipótese não seja contemplada na sua licença, é ilegal e viola as leis de software e de direitos autorais, implicando nas sanções legais. Fica estabelecido que para utilizar qualquer software ou hardware de propriedade ou licenciado pela CREDIVISTA, os usuários:

- Devem concordar com todos os termos do acordo de licença de software;

- Devem estar cientes que todos os softwares são protegidos por direitos autorais, a menos que explicitamente rotulados como software livre ou de domínio público;

- Não podem copiar software para qualquer propósito com exceção daqueles permitidos no acordo de licença de utilização;

- Não podem tornar o software disponível para outras pessoas usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de software e/ou procedimentos adotados pela CREDIVISTA;

- Não podem aceitar software não licenciado de terceiros;

- Não podem instalar, nem permitir ou induzir outros a instalarem, cópias ilegais de software, ou software sem as devidas licenças, em qualquer recurso computacional de propriedade da CREDIVISTA.

Toda aquisição de equipamento computacional deve incluir necessariamente a aquisição de licenças do software básico mínimo apropriado para o seu uso/funcionamento. Toda licença de software, de qualquer natureza, adquirida pela CREDIVISTA deve ser obrigatoriamente registrada, assim como também as licenças de software incluídas na aquisição do equipamento.

A instalação de software nos equipamentos computacionais da CREDIVISTA somente é autorizada mediante as formalizações de registro e arquivamento da licença de uso, em sistema centralizado no Órgão responsável pelo equipamento, excluídos os softwares abertos ou de uso gratuito. Todas estas disposições se aplicam também aos equipamentos e licenças de softwares doados ou adquiridos por convênios.

Em caso de detecção de alguma violação dos direitos de uso de algum software, este deve ser removido imediatamente e o responsável deve ser notificado. Em todo processo de contratação de software, deve haver um documento específico explicitando para cada exemplar, a autorização de uso e as suas condições. Sempre que possível, deve-se buscar a contratação de softwares sem restrições que possam impedir sua migração para outro equipamento

Anualmente será realizado um inventário de software em todas as estações, sendo facultado a Gerência da Tecnologia da Informação a desinstalação de qualquer software não homologado sem aviso prévio ao colaborador. A presença de softwares não homologados será comunicada ao gestor da área, que tomará as medidas cabíveis.

5.7 - Antivírus

Todos os equipamentos da empresa, sejam eles servidores ou estações, devem possuir antivírus instalados.

5.8 - Classificação dos Dados

Conceder acesso aos dados com base no que somente será dado acesso à informação para a pessoa que tiver a necessidade de conhecer aquela informação;

Classificar os dados de forma a identificar seu nível de confidencialidade;

A classificação poderá ser:

Público: quando o conteúdo puder ser distribuído a qualquer pessoa interna ou externa e for de conhecimento geral;

Somente Interno: conteúdo produzido pela Credivista para conhecimento exclusivo de seus colaboradores, terceiros e fornecedores;

Confidencial: conteúdo sensível e de acesso apenas as pessoas que devam conhecer seu conteúdo.

5.9 - Chaves de Criptografia e Certificados Digitais

Manter de forma segura, a guarda das chaves de criptografia para acesso aos recursos computacionais;

Manter registro de todas as chaves de criptografia e Certificados Digitais existentes, informando o dono e o mantenedor;

Documentar processo de guarda, renovação, revogação e inutilização de certificados digitais.

5.10 - Testes de Invasão periódicos

Periodicamente executar rotinas para testar a defesa contra possíveis ataques aos seus sistemas de informação, rotinas estas denominadas de Penetration Test;

As rotinas deverão ser executadas por empresa especializada;

Estas rotinas serão realizadas em sistemas e ambientes que sejam acessíveis via internet.

5.11 - Conscientização e Comunicação

Todos os colaboradores deverão receber periodicamente informações sobre potenciais ameaças à integridade dos sistemas de informação.

5.12 Rede Wi-fi

A empresa implementa redes sem fios segregadas, sendo a rede "Visitantes" usada basicamente para acesso à internet, sem acesso à rede corporativa e com menor rigidez e robustez. A rede "Corporativa", entretanto, tem acesso normal aos recursos da rede, exigindo liberação prévia do equipamento com a equipe de tecnologia.

5.13 Descarte ou Armazenamento de Informação

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer outros dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, o colaborador deve recolher o documento impresso imediatamente.

6. DIVULGAÇÃO

Para uniformidade da informação, a PSI – Política de Segurança da Informação deve ser divulgada tão logo aprovada pela Diretoria Executiva, seja na sua constituição ou em quaisquer atualizações que se façam necessárias. Adicionalmente deve ser disponibilizada na empresa permitindo fácil acesso ou consulta a qualquer colaborador. A política também deve ser divulgada para novos colaboradores, no processo de integração.

7. VIOLAÇÕES DA POLÍTICA E SANÇÕES

O descumprimento das diretrizes desta política, mesmo que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

É dever de todo colaborador comunicar ao Gestor a ocorrência de incidente que afete a segurança da informação, que por sua vez escalará a Diretoria Executiva para análise quando assim for necessário.

8. CONTROLE DE REVISÕES

Item	Data	Alteração	Revisado Por
V.1.0	25/11/2019	Primeira Versão do Documento	

Aprovado por: