AMCEL - AMAPÁ FLORESTAL E CELULOSE S.A.

INTRODUÇÃO

A política de segurança da informação, também conhecida como PSI, é o documento que estabelece as diretrizes, normas, procedimentos e as boas práticas dos recursos tecnológicos da empresa, sempre buscando proteger o seu ativo de maior valor estratégico a "**INFORMAÇÃO**".

A presente PSI, baseia-se nas recomendações propostas pelas normas ABNT NBR ISO/IEC 2700; 27002:2005; ISO/IEC 17799; BS 7799; RFC 2196 reconhecida mundialmente como um código de boas práticas e gestão da segurança da informação, bem como, estão de acordo com as leis vigentes em nosso país, incluindo a LGPD.

1. OBJETIVO

Estabelecer diretrizes que permitam aos funcionários, prestadores de serviços e visitantes seguirem padrões de comportamento relacionados à segurança da informação, adequando-os as necessidades de negócios da empresa e a legislação vigente do país.

Nortear as definições das normas, procedimentos, orientar seus colaboradores das boas práticas dos recursos tecnológico, bem como implementar controles e processo buscando proteger as informações e manter a continuidade dos negócios da empresa.

Preservar as informações da AMCEL - Amapá Florestal e Celulose S.A, quanto:

* **INTEGRIDADE**: Garantia de que as informações sejam mantidas em seu estado original, visando protegê-las de vazamento, utilização indevida intencionais ou acidentais dentro e fora da corporação.

* **CONFIDENCIALIDADE**: Garantir que todos os acessos à informação sejam obtidos somente por pessoas autorizadas pela empresa.

* **DISPONIBILIDADE**: Garantia de que os usuários autorizados obtenham acesso as informações e aos ativos correspondentes sempre que necessário.

2. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser cumpridas com o máximo rigor, abrangendo todos os seus funcionários, sem exceção. Estendendo também a seus prestadores e

visitante que façam uso do ambiente tecnológico da empresa (Sistemas, Hardware, Software, Celulares, Impressoras, Scanner, Copiadora, Telefone de mesa, Notebook, Tablet, Wifi, Câmera IP, DVR, ou qualquer outro ativo tecnológico aqui não mencionado).

Deverá ser do conhecimento de todos os funcionários, prestadores de serviço e visitantes que qualquer equipamento que esteja conectado no ambiente tecnológico da empresa, independente do meio utilizado (Cabo, Wifi ou Bluetooth) poderá sofre monitoramento e/ou auditoria sem aviso prévio por parte da TI ou a pedido do gerente da área através de e-mail, sempre justificando seu pedido para que o Departamento de TI possa apresentar seu Parecer Técnico.

3. PRINCÍPIOS DA PSI

Toda e qualquer informação produzida pelos funcionários ou prestadores de serviço da AMCEL com resultado de sua atividade profissional, pertencerá a referida empresa, salvo em casos explicito em contrato entre as partes.

Todos os recursos de informação e telecomunicações fornecidos pela AMCEL a seus funcionários e prestadores de serviços, deverão ser de uso exclusivo para as atividades profissionais, salvo em caráter emergencial autorizado pela TI e que não cause nenhuns danos a infraestrutura tecnológica da empresa.

4. REQUISITOS DA PSI

Para que haja a uniformidade e o fluxo da informação e as diretrizes desta PSI, deverá ser comunicado a todos os colaboradores da AMCEL, assim como a seus prestadores de serviços de todas as suas unidades, a fim de que a política seja cumprida dentro e fora da empresa quando houver o uso de seus ativos de informação.

Deverá haver um **Comitê de Proteção de Dados Pessoais** (CPDP) para levantar, analisar e julgar junto com a TI as diretrizes mais adequadas para a empresa objetivando a continuidade de seus negócios.

Tanto está PSI, quanto as boas práticas de segurança da informação deverão ser revistas e atualizadas periodicamente, sempre que algum membro do comitê gestor apresentar em seus encontros mensais algum fato ou evento relevante que motive sua revisão ou atualização.

A partir da aprovação desta PSI, deverá constar em todos os contratos dos funcionários e prestadores de serviço o anexo de acordo de confidencialidade ou clausula de confidencialidade das informações nas renovações contratuais ou em novos contratos,

deixando-os cientes que essa condição será imprescindível para que possa ser concedido o acesso aos ativos e informações disponibilizados pela empresa AMCEL.

As responsabilidades legais em relação à segurança da informação deverão ser comunicadas aos funcionários e aos prestadores de serviços durante a fase de contratação e integração na empresa. Todos os colaboradores devem serem orientados sobre os procedimentos de segurança da informação, bem como o uso correto dos ativos, afim de reduzir possíveis riscos de mau uso ou vazamentos de dados da empresa, ficando esses obrigados a assinar um termo de responsabilidade e de acordo com esta PSI.

Todo Incidente que afete a segurança da informação deverá ser comunicado inicialmente a gerência da área de TI e, se este julgar necessário, deverá encaminhar posteriormente ao Comitê de Proteção de Dados Pessoais para os devidos analises e apresentações de melhorias.

Deverá ser apresentado pela TI um plano de contingência e continuidade dos negócios dos principais sistemas e serviços, os mesmos deverão ser implantados e testados no mínimo a cada 4 meses, visando reduzir riscos de perdas de dados, o plano de contingência deverá ser todo documentado para que em uma eventualidade o profissional responsável possa utiliza-lo como base na recuperação.

O ambiente de produção (Data Center) e seus controladores devem ser segregados para que não haja a interferências ou visibilidade dos funcionários ou terceiros em suas atividades visando a confidencialidade da informação.

A AMCEL deverá atuar com o máximo rigor no cumprimento desta PSI, quando comprovado irregularidade, irresponsabilidade, negligencia ou imprudência do colaborador ou prestador de serviço no uso de suas informações. O Departamento de TI, sempre que observar qualquer suspeita de irregularidade deverá auditar, analisar, e coletar as evidencias e apresentar ao Comitê de Proteção de Dados Pessoais - CPDP para que a situação seja discutida e se necessário aplicado as sanções administrativas pertinentes.

5. ATRIBUIÇÕES, RESPONSABILIDADES E PAPÉIS

Com o objetivo de regulamentar as responsabilidades e os papéis que serão empreendidos por cada agente e cada área da AMCEL no atual Programa de Governança e Proteção de Dados, distinguem-se os papéis, responsabilidades e indicações da gestão e das respectivas definições, de acordo com o disposto abaixo.

5.1. ATRIBUIÇÕES DO COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS

São atribuições do Comitê de Proteção de Dados Pessoais, conforme determinado pelo Regimento Interno e aprovado pela Diretoria da AMCEL:

- Implementar as atividades previstas no trabalho de estruturação e Governança à Privacidade e Proteção de Dados Pessoais;
- Implementar, acompanhar, avaliar e propor alterações à Política de Segurança da Informação, Tratamento de Dados Pessoais e de suas normas internas complementares;
- Formular propostas e recomendar ferramentas e medidas de adequação atinentes à Segurança da Informação e Tratamento de Dados Pessoais, que serão submetidas à Diretoria para deliberação;
- Supervisionar e acompanhar o calendário de treinamentos das equipes sobre o tema;
- Propor a adoção de medidas corretivas e adequações normativas e procedimentais necessárias à prevenção de situações de vulnerabilidade à Segurança da Informação e violação à Lei Geral de Proteção de Dados Pessoais;
- Instituir Equipe de Tratamento e Resposta a Incidentes em casos de quebra de segurança e violação à Lei Geral de Proteção de Dados Pessoais;
- Solicitar apurações quando da suspeita de ocorrências de quebras de segurança;
- Disponibilizar o conhecimento das práticas mais modernas e adequadas afetas à segurança da informação e proteção de dados pessoais, assim como compartilhar informações sobre novas tecnologias, produtos, ameaças, vulnerabilidades, gerenciamento de risco, políticas de segurança e outras atividades relativas à segurança corporativa nessa área;
- Avaliar a classificação, reclassificação e desclassificação de informações quanto ao grau de sigilo e os prazos de restrição de acesso à informação no âmbito da Política de Tratamento de Dados Pessoais;
- Analisar o Regimento Interno e suas alterações;

- Avaliar a efetividade e a suficiência da estrutura de controles internos e dos processos da **AMCEL**, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias;
- Opinar sobre as matérias que lhe sejam submetidas pela Diretoria, bem como sobre aquelas que considerar relevantes no âmbito de sua competência;
- Monitorar constantemente o Programa de Governança em Privacidade e Proteção de Dados Pessoais.
- Propor ideias e investimentos relacionados à segurança da informação com objetivo de reduzir os risco e incidentes que possam afetar os ativos de informação da AMCEL.
- Propor alterações de versões desta PSI desde que tenha embasamento técnico e aprovado pela maioria dos membros do CPDP e Diretoria;
- Avaliar os incidentes de segurança da informação e propor ações preventivas ou corretivas;
- Definir as medidas cabíveis nos casos de descumprimento desta PSI e/ou das normais e procedimentos de segurança da informação complementares.

5.2. ATRIBUIÇÕES DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

São atribuições do Encarregado pelo Tratamento de Dados Pessoais:

- Recepcionar solicitações e enviar comunicados aos titulares de dados pessoais, prestar os devidos esclarecimentos e adotar as providências necessárias ao exercício dos direitos que a LGPD lhes confere;
- Realizar a gestão e atualização do mapeamento dos dados;
- Enviar e receber quaisquer comunicados e demandas de autoridades públicas, incluindo a Autoridade Nacional de Proteção de Dados (ANPD), referentes à proteção de dados pessoais e adotar as providências necessárias ao seu cumprimento, comunicando imediatamente ao Comitê de Proteção de Dados

Pessoais e demais áreas envolvidas;

- Realizar, sempre que necessário, as avaliações de impacto, redigindo os respectivos relatórios (RIPD's), obtendo a aprovação da Diretoria e transmitindo o documento às autoridades públicas;
- Prestar orientações aos funcionários, terceiros, fornecedores e todas as demais partes e unidades da Companhia, sobre as melhores práticas a serem adotadas em relação à proteção de dados pessoais;
- Prestar apoio consultivo ao Comitê de Proteção de Dados Pessoais em suas deliberações e funções;
- Prestar apoio na gestão de ameaças e incidentes envolvendo dados pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, as autoridades competentes e titulares afetados, sempre que esta representar risco ou dano relevante aos titulares;
- Promover ações e apoiar na fiscalização no sentido de garantir o cumprimento aos termos das Políticas de Privacidade e Proteção de Dados Pessoais.

5.3. ATRIBUIÇÕES DO DEPARTAMENTO TECNOLOGIA DA INFORMAÇÃO:

São atribuições do Departamento de Tecnologia da Informação:

- Preservar as informações com valor comprobatório para fins de auditorias, legais e judiciais, na forma e pelo prazo correto;
- Atuar para que os ativos computacionais de hardware e software estejam sempre atualizados e reflitam as melhores práticas do mercado, no sentido de garantir a segurança e privacidade da informação;
- Prestar apoio aos gestores no provisionamento, gestão, auditoria e cancelamento de acessos de pessoas a diretórios e sistemas da **AMCEL**, a fim de que informações e dados pessoais somente sejam acessados por pessoas autorizadas e para fins legítimos;

- Apoiar os departamentos na definição de controles adequados de Segurança da Informação;
- Avaliar, monitorar e tratar, vulnerabilidades, riscos e incidentes com a formalização de procedimentos para assegurar respostas rápidas, efetivas e ordenadas, acionando o departamento impactado/responsável quando necessário;
- Avaliar os aspectos de segurança da informação necessários a cada processo e, sempre que possível, empregar criptografia para proteger ativos estratégicos;
- Implementar medidas para higienização da base de dados da **AMCEL**, de modo que informações e dados pessoais sejam armazenados unicamente pelo tempo necessário ao cumprimento de sua finalidade, sendo posteriormente eliminados de forma segura;
- Apoiar a difusão e propagação da cultura de Segurança e Privacidade da Informação, apoiando demais departamentos, promovendo eventos, treinamentos e demais ações de conscientização;
- Reportar periodicamente ao Comitê de Proteção de Dados Pessoais o status e indicadores de Segurança da Informação e Proteção de Dados Pessoais;
- Instituir, gerir e divulgar canal destinado a receber comunicações de riscos ou incidentes associados à Segurança da Informação e Proteção de Dados Pessoais, divulgando amplamente sua existência e forma de utilização aos Usuários, os quais devem ter a possibilidade de apresentar comunicações anônimas ou identificadas;
- Promover ou solicitar a realização de auditorias externas em funcionários, prestadores de serviços, terceiros, parceiros e fornecedores;
- Testar a eficácia dos controles utilizados e informar ao gestor da área de TI os riscos residuais;
- Acordar com os gestores o nível de serviços que será prestado e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos funcionários com todos os controles necessários para cumprir os requerimentos de segurança

estabelecidos por esta PSI e as normas de segurança da informação complementares se houver.

- Os administradores e operadores de sistemas computacionais podem pela característica de seus acessos como usuários admin ter privilégios de acessos a arquivos de outros usuários. No entanto, isso só será permitido quando for necessário para execução de atividades operacionais, monitoramento ou auditoria sob sua responsabilidade, assim como para manutenção de computadores e/ou cópias de seguranças.
- Segregar as funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo reduzindo e eliminando a existência de pessoas que possam excluir os logs e trilhas de auditorias das suas próprias ações.
- Garantir segurança especial para sistemas com acessos público como Internet, podendo guardar evidencias que permitam a rastreabilidade para fins de auditoria ou investigação.
- Implantar controles de integridade para torna-las judicialmente válidas como evidencias.
- Administrar, proteger e testar as cópias de segurança dos programas e sistemas relacionados aos processos críticos e relevantes para a AMCEL.
- Implantar controles que gerem registros auditáveis para acesso, retirada e transporte de mídias e equipamentos da TI tanto de sua matriz como de suas filias.
- O usuário da informação deve ser previamente informado sobre o fim do prazo de retenção para que tenha a alternativa de altera-lo ou retira-los seus arquivos pessoas antes que a informação seja definitivamente descartada pela TI.
- Quando ocorrer a movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de uma forma irrecuperáveis antes de disponibilizar o ativo a outro usuário.
- Planejar, implantar, fornece e monitorar a capacidade de armazenagem, processamento e transmissão necessária para garantir a segurança requerida pelas áreas de negócios.

- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a uma responsável pessoa física, sendo que:
    - Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
    - Os Usuários (Logins) de terceiros são de responsabilidade do gestor da área contratante.
- Proteger ativamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambientes de produção corporativo, exigindo seu cumprimento dentro da empresa.
- Realizar auditorias periódicas de configurações técnicas e analises de riscos.
- Responsabiliza-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir da forma mais rápido possível, com solicitação formal, o bloqueio de acesso de colaborador ou terceiros por motivos de desligamento ou rescisão contratual da empresa, incidentes, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com horário oficial da região.
- Monitorar ambientes de TI gerando indicadores e históricos de:
    - Uso da capacidade instalada da rede e dos equipamentos;
    - Tempo de resposta no acesso à Internet e aos sistemas críticos da AMCEL;
    - Período de indisponibilidade no acesso à Internet e aos sistemas críticos da AMCEL;
    - Incidentes de segurança (vírus trojans, ransoware, sniffer, cavalo de troia, malware, keylog, fishing furtos e acessos indevidos);
    - Atividades de todos os funcionários durante os acessos às redes externas, inclusive internet (sites visitados, e-mails recebidos e enviados,

upload/downloads de arquivos);

5.4. DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Propor as metodologias e processos específicos para a segurança da informação, assim como avaliação de riscos de processos e sistemas, sempre definindo sua classificação.
- Propor, analisar e apoiar iniciativas apresentadas pelo CPDP (Comitê de Proteção de Dados Pessoais) que visem a à segurança dos ativos da informação da AMCEL.
- Publicar e promover as versões desta PSI, desde que analisadas pelo CPDP e Diretoria da AMCEL.
- Promover a conscientização de todos os funcionários, prestadores de serviços a relevância da segurança da informação para os negócios da AMCEL, mediante campanhas, palestras, treinamentos, notícias e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
- Analisar criticamente incidentes em conjunto com o CPDP e Diretoria.
- Apresentar as atas e os resumos das reuniões do CPDP, destacando os assuntos que exijam intervenção do próprio comitê ou de membros da Diretoria.
- Manter comunicação efetiva com o CPDP (Comitê de Privacidade de Dados Pessoais) sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar os ativos da AMCEL.
- Buscar alinhamento com as diretrizes corporativas da instituição.

5.5. ATRIBUIÇÕES DO DEPARTAMENTO DE RECURSOS HUMANOS:

São atribuições do Departamento de Recursos Humanos:

- Garantir que os contratos de trabalho ou similares prevejam a aplicação e cumprimento das Políticas e Normas instituídas pelo Programa de Governança em Privacidade da **AMCEL**;

- Assegurar que durante a integração de novos funcionários, sejam aplicados treinamentos em relacionados as rotinas periódicas de Segurança da Informação e Proteção de Dados;
- Asseverar que em todos os procedimentos adotados pelo Departamento de Recursos Humanos/Pessoal seja observada a Privacidade e Proteção de Dados Pessoais dos funcionários e de seus respectivos dependentes;
- Auxiliar o Encarregado de Proteção de Dados Pessoais no desempenho de suas responsabilidades;
- Apoiar na realização de treinamentos e ações de conscientização para difusão da cultura de Privacidade e Segurança da Informação;
- Assegurar que o Departamento de Tecnologia da Informação seja informado previamente acerca da suspensão ou corte de acesso de funcionários, em férias, afastados, alterações de cargos, funções, desligados.

5.6. ATRIBUIÇÃO DO CORPO DE GESTÃO:

São atribuições do corpo de Gestão da AMCEL (Diretores, Gerentes, Coordenadores Supervisores e Gestores de Processo):

- Ter postura exemplar em relação a segurança da informação, servindo de modelo de conduta, cumprir e fiscalizar o cumprimento as Políticas e Normas instituídas pela **AMCEL**;
- Garantir que seus subordinados sejam capacitados para tratar e operar Ativos de Informação e de Dados Pessoais da **AMCEL** de acordo com as Políticas e Normas;
- Assegurar que as medidas de descarte seguro de informações sejam utilizadas de forma correta de acordo com a Norma de Manuseio e Descarte de Informações adotada pela **AMCEL**;
- Indicar ao Departamento de Tecnologia da Informação a definição de perfis de acesso aos sistemas e *softwares* adotados pela **AMCEL**, incluindo-se de terceiros

que venham a ter acesso a tais sistemas, garantindo sempre o mínimo de acesso para o desempenho das funções necessárias;

- Manter controle acerca dos níveis de acesso às informações e Dados Pessoais dos membros de sua área e terceiros sob sua responsabilidade;
- Realizar ou solicitar ao Departamento de Tecnologia da Informação revisão de nível de acesso de seus subordinados em periodicidade semestral ou sempre que entender como necessário;
- Participar, sempre que for convocado, das reuniões do Comitê e, prestar todos os esclarecimentos solicitados;
- Executar e fazer executar corretamente a classificação de fornecedores e terceiros, de acordo com seus níveis de criticidade, de acordo com a Norma para Contratação de Terceiros;
- No desenvolvimento de novos processos de trabalho, produtos e serviços, respeitar e garantir que a privacidade dos afetados seja considerada desde a concepção até a execução, de acordo com a Cartilha Orientava – Privacidade na Concepção de Produtos e Serviços.
- Antes de conceder acesso às informações da AMCEL, exigir a assinatura do acordo de confidencialidade dos colaboradores e prestadores de serviço que não estejam cobertos por um contrato existente, durante a fase de levantamento para apresentação de proposta comercial.
- Adaptar as normas, os processos, os procedimentos e sistemas sob a sua responsabilidade para atender a esta PSI, bem como aos termos das normas da empresa.

5.7. ATRIBUIÇÕES DO DEPARTAMENTO JURÍDICO:

São atribuições dos Usuários:

- Acompanhar os Incidentes de Segurança da Informação e Proteção de Dados Pessoais que violem significativamente as Políticas e Normas de Segurança da Informação e Proteção de Dados;
- Apoiar e auxiliar juridicamente o Comitê de Proteção de Dados Pessoais, Departamento de Tecnologia da Informação e o Encarregado de Proteção de Dados Pessoais;
- Orientar para a melhor forma de coleta e preservação de prova eletrônica, com o objetivo de manter sua eficácia para uso em juízo, quando necessário;
- Apoiar na revisão de documentos, Políticas, Normas, contratos e consultas relacionadas à Segurança da Informação e Proteção de Dados Pessoaid, bem como na análise e interpretação da regulação de Proteção de dados aplicável à **AMCEL**;
- Assessorar procedimentos, processos e auditorias voltadas à avaliação de incidentes, uso indevido, inadequado de Ativos de Informação e de Dados Pessoais;
- Analisar e apoiar os Gestores, Diretores e afins na definição do nível de exigência junto aos Fornecedores, nos termos da Norma para Contratação de Terceiros;
- Garantir que todos os contratos firmados pela **AMCEL** contenham cláusulas voltadas à Segurança e Privacidade da Informação e Proteção de Dados Pessoais;
- Prestar apoio, em conjunto com o Encarregado, aos responsáveis pela segurança da informação e privacidade a toda e qualquer legislação aplicável, especialmente em temas relativos a:
    - *Proteção de dados e privacidade de informações pessoais;*
    - *Direito de Propriedade Intelectual;*
    - *Proteção de registros organizacionais;*
    - *Prevenção de mau uso de recursos de processamento de informação;*
    - *Atualizações legislativas.*
- Responsabilizar-se por prejuízos ou danos que vier a sofre ou causar a AMCEL e/ou a terceiros em decorrência da não obediência às diretrizes e normas aqui referidas.

5.8. ATRIBUIÇÕES DOS USUÁRIOS

São atribuições de todos os funcionários, independentemente do nível hierárquico ou competência de atuação, papel e a responsabilidade de cumprir, observar o cumprimento e respeitar as Políticas e Normas instituídas pela **AMCEL**, assim como:

São atribuições dos Usuários:

- Zelar pelos Ativos de Informação e de Dados Pessoais, assegurando que não ocorra acesso, alteração, compartilhamento, divulgação, destruição e eliminação sem a devida autorização;
- Utilizar os Ativos de Informação e ativos de tecnologia da informação e comunicação ("ATICs", ex. rede de internet, computadores, celulares, impressoras, energia elétrica, etc.) da **AMCEL** para fins únicos e exclusivos do interesse da **AMCEL**, ressalvadas exceções autorizadas;
- Assegurar que toda Informação ou Dado Pessoal esteja sendo tratado e operado de forma correta e, caso haja dúvidas buscar orientações nas Políticas, Normas ou superiores hierárquicos;
- Participar dos treinamentos disponibilizados e nos casos obrigatórios obter nota mínima de aproveitamento;
- Comunicar imediatamente o Encarregado de Proteção de Dados Pessoais e o Departamento de Segurança da Informação e/ou Tecnologia da Informação caso suspeite de qualquer ameaça, risco ou incidentes de segurança da informação ou proteção de dados.

6. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE PELA TI

Para garantir as regras mencionadas nesta PSI, bem como de suas versões, poderá:

Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexão com a internet, dispositivos moveis ou wireless e outros componentes da rede, a informação gerada por esse sistema poderá ser usada para identificar usuários

e respectivos acessos efetuados, bem como manipulação ou vazamentos de dados da empresa;

Apenas tornar público as informações obtidas pelo sistema de monitoramento e auditoria, em casos de exigência judicial, por solicitação formal pela gerência da área, ou por determinação do CPDP ou Diretoria;

Realizar a qualquer momento, inspeção física nas máquinas de propriedade da empresa AMCEL;

Instalar sistemas de proteção, preventivos e detectáveis para garantir a segurança das informações e dos acessos a qualquer ativo de informação da empresa.

7. DO USO DO CORREIO ELETRONICO

* O uso do correio eletrônico da AMCEL é para fins unicamente corporativos, podendo o usuário utilizar o seu e-mail pessoal desde que não prejudique a empresa e também não cause impacto no tráfego da rede ou no link de Internet.

* Nunca realizar o envio de e-mails de forma desnecessária, a fim de comprometer o tráfego da rede interna e link de Internet, Ex: Envio de e-mail ao grupo All@amcel.com.br, assim como responder os e-mails a este grupo.

* Nunca utilizar o e-mail corporativo ou pessoal dentro das dependências da empresa para enviar conteúdo malicioso, a fim de colocar em risco o destinatário ou colocando a AMCEL em situações vexatórias.

* Nunca divulgar informações, imagens de tela, sistemas, documentos sem autorização expressa e formal concedida pelo proprietário do ativo de informação.

* Nunca falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade do remetente e/ou destinatários, com objetivo de camuflar as normas prevista nessa PSI.

* Nunca produzir, transmitir ou divulgar e-mails que:

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

- Contenha ameaças eletrônicas como spam; e-mails bombas; vírus de computador ou qualquer código malicioso;

- Vise obter acesso não autorizado a outro computador, servidor ou qualquer equipamento da infraestrutura de TI da AMCEL;

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado (ataque DDOS, etc.);

- Vise burlar qualquer sistema de segurança;

- Vise vigiar secretamente outro usuário, salvo nos casos de solicitação expressa por uma gerência ou diretoria e/ou por auditorias feitas pela TI em casos de suspeita de algo ilícito na empresa;

- Vise acessar informações confidenciais sem explicita autorização formal do proprietário dos dados;

- Inclua imagens criptografadas ou de qualquer forma mascarada sem o consentimento do proprietário do ativo;

- Conteúdo considerado impróprio ou obsceno ou ilegal dentro das dependências da empresa;

- Informações de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros que venha a prejudicar o destinatário;

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

- Tenha fins políticos locais ou nacionais (propaganda política);

As mensagens de assinaturas de correio eletrônico sempre deverão obter os seguintes dados abaixo, diminuir possíveis ataques de engenharia social:

- Logo da Empresa

- Nome da Empresa;

- Nome do Colaborador;

- Departamento

- Telefone comercial para contato;

As informações no crachá dos colaboradores sempre deverão possuir os seguintes dados, diminuindo os possíveis ataques de engenharia social:

- Nome/Logo da Empresa;

- Departamento;

- Chapa;

- Foto 3x4

8. DA INTERNET

Todas as regras atuais da AMCEL, visam basicamente o desenvolvimento de uma conduta eminentemente ética e profissional do uso da Internet. Embora a mesma seja permanente filtrada pelo firewall da empresa, ainda assim, oferece potencialmente de risco a empresa quando mal utilizada. Desta forma, qualquer informação que é acessada, transmitida, recebida ou produzida na Internet estará sujeita a auditoria pelo departamento de TI. Por tanto, a AMCEL tem total conformidade legal para monitorar todo e qualquer acesso que seja feito dentro de sua infraestrutura de TI.

Os equipamentos tecnológicos e sistemas fornecidos pela AMCEL, por se tratarem de propriedade da mesma, poderão ser analisados e se necessário poderão ser bloqueados sites, arquivos, correio eletrônico ou qualquer aplicação armazenada na rede/internet ou intranet, visando assegurar o cumprimento de sua política de segurança da informação.

A AMCEL, ao monitorar a rede interna, pretende garantir a integridade dos seus ativos de informação, por tanto, toda tentativa de alteração dos parâmetros de segurança por qualquer funcionário sem o devido credenciamento ou autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao CPDP e Diretoria para avaliar e julgar a situação. O uso de qualquer recurso para atividades ilícitas poderá acarretar em ações administrativas e as penalidades decorrentes de processo cível e criminal, nesse caso, a AMCEL deverá cooperar ativamente com as autoridades competentes quando solicitado.

A internet disponibilizada pela AMCEL a seus funcionários e parceiros, independentemente de sua relação contratual, poderá ser utilizada para fins pessoais, desde que não prejudique o andamento de suas atividades e que não seja utilizada para fins ilícitos. Tal parágrafo é valido para todas as suas unidades.

Como é do interesse da AMCEL que seus funcionários estejam bem informados, o uso de sites de notícias ou serviços, serão aceitáveis desde que não comprometa a banda do

link e internet em horários comerciais e que não perturbe o bom andamento dos trabalhos nem implique em conflitos de interesses com os seus objetivos de negócios.

Apenas os funcionários autorizados pela instituição poderão copiar, imprimir ou enviar imagens da tela do computador para terceiros ou órgãos governamentais, devendo atender sempre as Leis de Direitos Autorais e a Lei Geral de Proteção de Dados (LGPD).

É proibido a divulgação e/ou o compartilhamento de informações da empresa a terceiros e a órgão governamentais, salvo quando autorizado por escrito pelo gestor da área justificando tal situação.

Os funcionários com acesso à internet poderão fazer download somente de programas ou software ligado diretamente a suas atividades funcionais, desde que esteja licenciado. Cabendo a TI analisar e autorizar a instalação do mesmo nas estações de trabalho.

Os funcionários em hipótese alguma poderão utilizar os recursos da AMCEL para fazer download de distribuições de software pirateado (crackeados) para uso em suas atividades, tal pratica será considerada delituosa conforme legislação em vigor no país,

O download e a utilização de programas de entretenimento, redes sociais, TV digital, jogos ou músicas (em qualquer formato) não poderão ser realizados dentro da infraestrutura da empresa, salvo com autorização por escrita e justificada pelo gestor da área.

Regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso de informação da AMCEL, ficando os envolvidos sujeitos as penalidades administrativas quando julgado procedentes pelo CPDP e pelo DPO.

Todos os funcionários sem exceção, não poderão utilizar sem as devidas analises e autorização da TI de software de acesso remoto como (Teanviwer, Anydesk, Tmbuktu, Webex, VNC, TightVNC ou qualquer outro software afim), onde possa colocar em risco a infraestrutura de Tecnologia da Informação da AMCEL.

Fica estritamente proibido o uso de qualquer software que possibilitem burlar regras do firewall da empresa.

9. IDENTIFICAÇÃO

Tal procedimento, visa estabelecer critérios e regras de segurança da informação e responsabilidade sobre o uso dos dispositivos computacionais, dando maior segurança aos ativos da empresa.

Fica estritamente proibido a utilização e acesso por login e senha de outro funcionário nos sistemas computacionais da empresa a fim de obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem. Tal pratica é caracterizada em crime de falsa identidade pelo código penal brasileiro - art. 307.

Todos os dispositivos de identificação utilizados na AMCEL. Como o número de registro do funcionário, o crachá, as identificações de acesso a certificados, assinaturas digitais, dados biométricos deverão está associado a uma pessoa física e atrelado inequivocamente a seus documentos oficiais reconhecidos pela legislação brasileira vigente.

Os usuários vinculados a tais dispositivos como token de identificação, que respondem pela empresa, serão responsáveis pelo uso correto perante as instituições e órgãos governamentais, ficando sujeitos as sanções administrativas, civil e criminal quando comprovado o seu mal-uso.

Todo e qualquer dispositivo de identificação pessoal, não poderá ser compartilhado com outro usuário em hipótese alguma.

É estritamente proibido o compartilhamento do login de administrador dos sistemas computacionais e banco de dados a qualquer outro colaborador ou terceiro que não faça parte do quadro da TI.

É de responsabilidade do Departamento de TI, a criação, alteração, exclusão de perfil e de usuários da rede, assim como das contas de e-mails e sistemas internos (Protheus, site, integra, full controll, off-line, etc.).

Todas as senhas criadas pelos usuários, deverão conter as seguintes especificações técnicas: ter no mínimo 7 (sete) caracteres alfanuméricos, utilizando caracteres especiais (@, #, $, %) e variando entre caixa alta e caixa baixa (maiúscula e minúscula) e números, obrigatoriamente.

Os usuários que possuem perfil de administrador ou acesso privilegiado, deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérico, utilizando caracteres especiais (@, #, $, %) e variações entre caixa alta e caixa baixa (maiúscula e minúscula) e números, obrigatoriamente.

O acesso a rede wifi deverá ser solicitada por e-mail, seguido da justificativa do uso, sempre colocando em cópia seu gestor para evitarmos vazamento de informações e acessos indevidos.

É de responsabilidade de cada usuário, a memorização de sua própria senha, assim como a proteção e guarda dos dispositivos de que lhes foram designados para suas atividades.

As senhas não deverão ser anotadas ou armazenadas em arquivos eletrônicos. As mesmas não devem ser criadas baseadas em informações pessoas, como nome, data de nascimento, endereços, placa de veículos, nome de empresa ou departamento. Tal prática poderá colocar em risco os ativos da empresa.

Após a 3ª tentativa errada de login do usuário na rede, a conta será bloqueada automaticamente, para que a conta seja desbloqueada o usuário deverá procurar o departamento de TI para solicitar o desbloqueio e/ou trocar a senha por medida de segurança.

As senhas de rede, deverão ser solicitados alteração automática em 3 em 3 meses, não podendo a nova senha ser igual a nenhuma outra anterior ou que não esteja dentro dos critérios estabelecidos nos parágrafos anteriores.

10. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos computacionais disponíveis aos funcionários são de propriedade da AMCEL, cabendo a cada usuário utiliza-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pela área de TI.

Fica estritamente proibido todo e qualquer procedimento de manutenção, física ou lógica, instalação de programas, desinstalação, configuração ou modificação de lugar de qualquer equipamento sem o acompanhamento técnico da área de TI, em caso de necessidade, o solicitante deverá informar a TI por e-mail, 24 horas antes da execução para que a TI possa avaliar e se planejar para a mudança.

Arquivos pessoais não pertinentes ao negócio da AMCEL (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os drivers de rede ou computador,

No uso dos computadores, equipamentos e recursos de informação, algumas regras devem ser atendidas:

- Os funcionários tem o dever de comunicar ao Departamento de TI ou a qualquer membro do CPDP (Comitê de Proteção de Dados Pessoais), sempre que observar alguma praticas em desacordo a está política da informação causada por alguma de seus colegas de trabalho, ficando sua identidade preservada pelos detentores da informação.

- Os funcionários deverão informar de imediato ao Departamento de TI quando observar qualquer situação estranha em seu dispositivo para que as medidas adequadas sejam tomadas o quanto antes.

- É vedada a abertura e o manuseio de computadores, notebook, smartphone, tablet ou qualquer outro equipamento de informática, salvo por algum técnico da TI e/ou empresa especializada quando necessário, sempre informado por escrito ao Departamento de TI para que seja atualizado em seus controles

- Fica estritamente proibido o uso de Modem, Pendriver, HD externo ou qualquer mídia de armazenamento externo (pessoal) nos computadores da empresa, salvo quando houver extrema necessidade e que seja autorizado pela equipe de TI.

- O funcionário fica proibido de alterar qualquer configuração do equipamento cedido para sua atividade, cabendo apenas a TI executar este procedimento.

- É de responsabilidade do funcionário ou terceiro, manter e preservar qualquer equipamento ou dispositivo que esteja sobre sua guarda, podendo o mesmo assumir os custos pelo mal-uso ou danos do mesmo quando detectado pela TI.

- Todas as senhas padrões deverão ser alteradas no 1º acesso do funcionário.

Acrescentamos algumas situações em que é proibido no uso dos computadores e recursos tecnológicos da AMCEL:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede, salvo pela TI em auditoria;

- Burlar qualquer sistema de segurança;

- Fazer mal-uso de informações confidencias da empresa, afim de se auto favorecer;

- Utilizar secretamente, qualquer tipo de analisador de pacote (sniffer) na rede afim de obter informações confidencias, salvo pela TI;

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado, salvo pela TI;

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cumprisse de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- Hospedar, armazenar, salvar, compartilhar ou transferir material pornográfico, racista, ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública utilizando a infraestrutura da AMCEL.

- Utilizar qualquer software pirata, com uso de cracker, desde que autorizado pelo gestor da TI.

11. DISPOSITIVOS MOVEIS

É responsabilidade do funcionário o custo com reparo de dispositivo móvel por mal-uso, quebra ou acidente com derramamento de produtos liquido no equipamento cedido pela AMCEL para suas atividades diárias;

Em caso de furto ou roubo, o funcionário deverá informar o Gestor da Área de TI e em seguida, procurar a autoridade policial para registro do boletim de ocorrência (BO) para as devidas tratativas.

Fica estritamente proibido, o uso de equipamentos portáteis, como smartphones, palmtops, pen drives HDs e players de qualquer espécie, quando não autorizados e analisados pela gerência de TI, não poderão ser utilizados nos equipamentos da empresa.

12. DATA CENTER

- O acesso as dependências da sala do Data Center ficam restrito aos profissionais de TI e/ou pessoas autorizadas pela gerência da área, sempre acompanhado por um profissional da área por medida de segurança.

- Fica proibido uso de câmeras de vídeos, celulares e maquinas fotográficas nas dependências do Data Center, com exceção a câmeras de segurança do local da sala;

- Todas as senhas MASTER de Administrador da Redes, Banco de Dados, PABX, Sistemas Internos e Clou, deverão ficar restrita ao responsável técnico da área e ao Gestor de TI;

- Nas filiais onde não existam funcionários da área de TI, a área deverá solicitar o auxílio do colaborado mais indicado para auxilia-los em eventuais situações emergencial;

- Todo e qualquer incidente de grande relevância nas dependências da Sala do Data Center, deverá ser registrado nos controles da TI e apresentado quando achar necessário nas reuniões mensais do CPDP para conhecimento e sugestões de melhorias quando for algo que coloque em risco os ativos tecnológicos da empresa.

- O departamento Administrativo deverá apresentar trimestralmente ao Departamento de TI o planejamento de manutenções preventivas nas centrais de ar da Sala do data Center, assim como informar qualquer necessidade de acesso a sala no mínimo de 24h antes para que a TI possa se programar, salvo em casos emergências.

- Deverão existir apenas 2 cópias da chave da porta do Data Center, uma deverá ficar com o responsável técnico e a outra com o gestor da área de TI;

- A Sala do Data Center deverá ser mantido sempre limpa e organizada. Sempre que necessário, a equipe de serviços gerais deverá executar a limpeza acompanhado de um profissional da TI;

- Fica estritamente proibido, a entrada de qualquer tipo de alimento, bebida ou produtos inflamáveis;

- A entrada ou retirada de qualquer equipamento do Data Center somente se dará com o procedimento de autorização formal pelo responsável técnico da área ou pelo gestor da TI para que não ocorra nenhuma paralisação em nenhum serviço ou sistema;

13. BACKUP

- Todos os backups devem serem automatizados por sistemas de agendamento automático fora do horário comercial, salvo em casos de extrema necessidade poderá ser manual;

- O responsável técnico pelos backups deverá realizar pesquisa frequente para identificar atualizações e correções de versões do produto, sempre buscando melhorias nos processos;

- As cópias de backups deverão ser armazenadas em locais seguros como NAS 1 (SALA DATA CENTER) e NAS 2 (SALA DA BALANÇA), assim como também deverá ser replicado para o GOOGLE DRIVER pelo NAS 1, sempre seguindo a redundância em mais de um lugar.

- O período máximo para a guarda dos históricos de backups das bases de dados Zenith e Divamprod serão de 30 dias, ficando o responsável técnico livre para restaura-lo a qualquer momento para teste de consistência.

- Testes de restauração de backup devem ser executados uma vez por semana

- Para formalizar o controle de execução de backup e restaure, deverá haver um formulário de controle rígido de execução dessa rotina, o qual deverá ser preenchido detalhadamente com data e hora e o resultado do mesmo, o qual será apresentado quando necessário na reunião com o CPDP para conhecimento.

- O controlador responsável pelos procedimentos, poderá delegar a outro técnico a execução deste processo por motivo de força maior, entre tanto, o mesmo deverá sempre

certificar se o procedimento foi feito corretamente, não eximindo as responsabilidades técnicas de quem o fez.

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança da informação deve ser entendida como parte fundamental da cultura interna da AMCEL. Ou seja, qualquer incidente de segurança derivado de um funcionário deverá ser investigado e aplicado as punições necessária para manter a preservação dos ativos da empresa.