POLITICA DE SEGURANÇA DA INFORMAÇÃO

COOPERATIVA DE CREDITO MUTUO DOS EMPREGADOS EM EMPRESAS ADMINISTRADORAS DE AEROPORTOS - AEROCRED

Art. 27. Ficam revogadas:

I - a Resolução nº 4.658, de 26 de abril de 2018; e

II - a Resolução nº 4.752, de 26 de setembro de 2019.

Rua Dr. Ramos de Azevedo, nº 159 – Conj. 1708 – 17º andar – Edif.Central Office - Cento - Guarulhos – SP CEP 07012-020
Fone: 2408-8870 – www.aerocred.org.br - e-mail: aerocred@aerocred.org.br

INTRODUÇÃO

A PSI tem por objetivo preservar a integridade dos dados, garantir sua disponibilidade e a utilização correta dos sistemas, além de estabelecer a confidencialidade das informações, e o gerenciamento e tratamento das mais críticas para a gestão do negócio.

PRECEITOS LEGAIS

A PSI tem como base a legislação específica para o tema e leva em consideração as orientações da Resolução 4658/2018 – do BCB , Res CMN 2554/98 e Norma ABNT ISO/IEC Família 27000 e as alterações introduzidas pela Lei 13.853/2019 LGPD (Lei Geral de Proteção de Dados Pessoais)

CONCEITOS BÁSICOS

Para efeitos de entendimento e fácil compreensão da política de proteção de dados é necessário apresentar algumas definições e conceitos importantes ao entendimento do instrumento;

a. Dados: Parte elementar da estrutura do conhecimento incapaz de, por si só, gerar conclusões inteligíveis ao destinatário, mas computáveis. Representa uma ação não descrita, uma quantidade sem especificar o objeto, por exemplo, dentro da LGPD temos os seguintes tipos de categorização de dados:

b. Dados pessoais: São todos os tipos de dados que pod Dados pessoais: em levar a identificação de uma pessoa, de forma direta ou indireta. Alguns tipos de dados pessoais incluem (nome completo, RG e CPF, passaporte e carteira de habilitação, endereço, telefone, e-mail, endereço de IP, data de nascimento, localização via GPS, entre outros).

c. Dados sensíveis: Qualquer informação que relacione Dados sensíveis: com a origem racial, étnica, credo, opinião política, filiação a sindicato; que se referem à saúde ou vida sexual, dados genéticos e biométricos

d. Dados anonimizados: Operação que seja realizada com Dados anonimizados: os dados pessoais de forma anônima, sem que haja identificação do indivíduo

e. Dados públicos: São dados que ainda públicos podem Dados públicos: ser restringidos pelo indivíduo.

f. ANPD – Autoridade nacional de proteção de dados Autoridade nacional de proteção de dados Autoridade nacional de proteção de dados: Órgão da administração pública direta federal com atribuições relacionadas a regulamentação e fiscalização do cumprimento da LGPD

g. Titular: Pessoa natural a quem se referem os dados Titular: pessoais que são objeto de tratamento.

h. Controlador: Pessoa natural ou jurídica, a quem competem as decisões referentes ao tratamento de dados pessoais

i. Operador: Operador: Pessoa natural ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador

j. Encarregado de dados: Encarregado de dados: Responsável frente à ANPD e aos titulares indicados pelo controlador.

k. Tratamento de dados: Qualquer operação que seja real Tratamento de dados realizada com os dados pessoais (incluindo: acesso, armazenamento, arquivamento, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização.

l. Cliente (cooperado) : Pessoa natural ou jurídica que contrate os serviços da AEROCRED, ou que estejam em vias de contratar serviços.

m. Colaborador: Pessoa natural que faz parte do quadro Colaborador: de contratados e societário da AEROCRED,
n. Parceiro/Prestador Parceiro/Prestador Prestador: Pessoa natural ou jurídica que prestas serviços a AEROCRED no âmbito das atividades
o. Recursos tecnológicos: Recursos tecnológicos: São todos os recursos físicos e digitais utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar informações. Entre os tipos de recursos podemos destacar: computares de mesa ou portáteis, smartphones, tablets, pen drive, discos externos, mídias, impressoras, scanner, entre outros
p. Dispositivo móvel Dispositivo móvel dispositivo móvel: Entende-se qualquer equipamento eletrônico com atribuições de mobilidade, como: notebooks, smartphones e tablets.
q. Incidentes de segurança da informação: Incidentes de segurança da informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à esta política, a LGPD, falha de controles, ou situação previamente desconhecida, que possa ser relevante à segurança da informação. São exemplos de Incidentes de Segurança da Informação:
i. Perda de serviços ou recurso;
ii. Mau funcionamento ou sobrecarga de sistema;
iii. Erros humanos;
iv. Não conformidade com a Política e a Norma;
v. Observações ou suspeitas de fragilidade em sistemas ou serviços;
vi. Vazamento de informação de clientes ou pessoas físicas que estejam armazenadas e tratadas em nosso ambiente digital;
vii. Violações de procedimentos de segurança e violações de acesso
r.LGPD – Lei geral de proteção de dados pessoais: Lei geral de proteção de dados pessoais: Lei geral de proteção de dados pessoais: Lei de nº 13.709/2018 que “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.
s. Criptografia: Criptografia: é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

PRINCIPAIS AMEAÇÃS

Com os procedimentos adotados busca-se eliminar e proteger os dados das principais ameaças à segurança da informação, a seguir:

- ransomware (malware que realiza criptografia para sequestro de dados das organizações);
- infecção por malware;
- exploração de vulnerabilidades ocasionadas por falhas de segurança ou negligência das organizações em atualizar seus sistemas e softwares;
- tentativa de phishing (quando ocorre uma tentativa de fraude eletrônica por hackers, tentando obter dados pessoais, fingindo ser uma comunicação eletrônica oficial);
- fraude interna, ou seja, quando seus próprios funcionários cometem o ato ilícito;
- ações indevidas de funcionários, como acesso a sites indevidos durante o trabalho, o que abre portas de vulnerabilidade para ações de hackers;

- indisponibilidade do serviço, causada por ações, como ataques DDoS, com o objetivo de provocar instabilidade ou queda do sistema;
- acesso facilitado indevido aos dados, seja de forma interna ou externa, ou seja, quando a confidencialidade de determinados dados é quebrada.

OBJETIVO

A PSI busca orientar e hierarquizar o acesso aos dados, garantindo a efetividade de ações na hora de proteger as informações, baseando-se nos

três pilares, primordiais para a segurança dos dados: confidencialidade, integridade e disponibilidade.

REGRAS DE SEGURANÇA DA INFORMAÇÃO

Todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas pelos colaboradores e parceiros, são de propriedade e direito de uso exclusivo da AEROCRED.

Os colaboradores e parceiros devem zelar para que as informações inseridas nos sistemas coopcred, ou quando enviadas ao cliente, sejam livres de erro, transparentes e verídicas.

O acesso e uso das informações da AEROCRED, incluindo o e-mail, devem estar limitados à jornada de trabalho ou período contratual do colaborador.

O envio da documentação deverá ser feio via os meios de comunicação oficial
correio eletrônico (e-mail), whatsapp corporativo, sendo vedado outro meio de transmissão.

INSTALAÇÃO DE APLICATIVOS E SISTEMAS

O colaborador deve utilizar apenas softwares e hardwares previamente homologados ou autorizados pelo responsável do TI , o qual tem o poder de acesso à instalação de programas e ou aplicativos, ficando proibido o usuário colaborador efetivar qualquer instalação sem a devida ciência do Depto de TI.
O usuário tem seu login restrito a utilizar somente seu ambiente homologado para trabalho.
Não havendo autorização para acesso a outras instancias de usuários.

ACESSO À INTERNET

O acesso à internet fica sujeito a proteção de Firewall, e programa de anti vírus, instalados em servidor próprio, sendo armazenado logs de acessos e consumo.
Tendo acesso somente a sites liberados pelo corpo direcional da cooperativa.

BACKUP E RESTAURAÇÃO DE DADOS.

O acesso à internet fica sujeito a proteção de Firewall, e programa de anti vírus, instalados em servidor próprio, sendo armazenado logs de acessos e consumo.

Os Backups são efetuados diariamente pelo servidor e armazenado em espaço próprio direcionado a recepção dos dados, internamente, por volta das 17:00 h.

Os Backups do Banco de Dados do sistema operacional Coopcred, é de responsabilidade da empresa contratada Cashway Tecnologia da Informação Ltda, q qual possui política, procedimentos próprios para execução dos *backups* de seus arquivos e documentos, deixando claras as definições técnicas, normas e quadro de responsabilidades, além de toda a metodologia de recuperação dos dados e ativos. Anexo III.

EQUIPE DE TI

A equipe de T.I, é divida de forma a se adequar as necessidades apresentadas pela cooperativa, sempre tomando como base a estrutura operacional da cooperativa e é dividida da seguinte forma>

Suporte – T.I
- Máquinas, estrutura de rede de dados e internet
Composta pela equipe da empresa G.D.S.A. Sanchini Informatica ME - CNPJ 23.362.139/0001-80-, que trabalha sob demanda e com base nos procedimentos técnicos de segurança e atualização dos dados, envolvidos no controle das atividades internas de suporte e manutenção.

Suporte Externo - T.I
Para os casos de suporte do sistema operacional da cooperativa a responsabilidade técnica de manutenção, backup e administração do banco de dados, fica a cargo da empresa contratada para esta finalidade, que é incumbida do suporte ao site da cooperativa bem como estrutura do Banco de dados da Cooperativa de Crédito e suporte ao sistema Coopecred.- Empresa Redzone Informática Ltda - ME - CNPJ: 94.119.330/0001-46

SISTEMAS UTILIZADOS

Com base nos protocolos de segurança da informação utilizados pela AEROCRED, somente os sistemas abaixo descritos estão autorizados e fazem parte da PSI.
- WINDOWS SERVER 2019
-WINDOWS 10 PROFISSIONAL
-OFFICE 365
- ANTIVURUS
- LINKS DE INTERNET
- SISTEMA COOPCRED - Licenciado pela empresa Cashway Teconologia da Informação.

DESCRITIVO DE ACESSO

Os acessos ao sistema de dados COOPCRED (Cashway), são controlados através da hierarquia de acesso e divisões de acordo com a responsabilidade e o grau hierárquico das funções, para melhor visualização, dados completos nos **Anexo I** e **Anexo II**.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Colaboradores em Geral Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da cooperativa de crédito. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a AEROCRED e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

2 - Dos Gestores ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da AEROCRED.

HOME OFFICE

É expressamente proibido o uso de equipamentos particulares não autorizados pelo responsável de TI em conexões remotas ao ambiente da AEROCRED. No caso de dispositivos habilitados e autorizados para acesso remoto, devem estar configurados pelo responsável de TI, obrigatoriamente, com mecanismos de segurança.

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Cooperativa de Crédito Mutuo dos Empregados em Empresas Administradoras de Aeroportos - Aerocred. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela cooperativa.

Esta política deve ser revista e atualizada em intervalos não superiores a 2 (dois) anos, visando garantir que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente no Brasil.

AEROCRED
Cooperativa de Créd Mútuo dos Empreg em empresas Adm Aeroportos

ANEXOS A POLITICA DE SEGURANÇA DA INFORMAÇÃO.

- ANEXO I - USUÁRIOS POR GRUPO

- ANEXO II - PERMISSÕES POR GRUPO

- ANEXO III - POLITICA DE BACKUP E ARMAZENAMENTO BANCO DE DADOS

Política de Segurança da Informação - PSI – AEROCRED - Versão - 04 - aprovada AGO março/2022