POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1 – INTRODUÇÃO

Denomina-se Segurança da Informação a proteção existente sobre as informações de uma determinada empresa ou pessoa. Entende-se por informação todo e qualquer conteúdo ou dado de grande valor.

A informação representa um dos bens mais valiosos de uma organização, garantindo a continuidade dos negócios, minimizando os riscos de perdas financeiras e a imagem da empresa no mercado.

A informação precisa ser adequadamente protegida, levando em consideração as inúmeras formas nas quais a informação pode ser apresentada, como por exemplo, em papel, mídia eletrônica, e até mesmo falada.

Além disso, a informação pode ser transmitida pelos mais variados meios, como armazenamento em nuvem, e-mails, documentos, arquivos, internet, apresentações e até mesmo em conversas. Independente como é apresentada ou o meio através do qual a informação é compartilhada ou armazenada, deve-se protegê-la contra ameaças e riscos.

A segurança da informação é baseada em três pilares:

1 – Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas;

2 – Integridade: salvaguarda da exatidão e completude da informação;

3 – Disponibilidade: garantia de acesso à informação sempre que preciso.

Para assegurar esses três pilares, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

2 – OBJETIVO

O objetivo é estabelecer as diretrizes a serem seguidas pela Cooperativa no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

3 – RESPONSABILIDADE DA COOPERATIVA

A **Cooperativa de Economia e Crédito Mútuo dos Empregados da Merck Sharp & Dohme Farmacêutica - COOPERMSD** poderá obter dados cadastrais de seus associados, em situações específicas, tais como associação, atualização de dados, cadastro de endereço, e-mail, entre outros.

Os dados fornecidos pelos associados serão mantidos em absoluto sigilo e, por esta razão, a Cooperativa assegura que os mesmos não serão, sob nenhuma hipótese, vendidos, alugados, cedidos, nem de outra forma repassados a terceiros.

A coleta de dados tem por finalidade possibilitar a adesão como COOPERADO(A) e operações junto a COOPERATIVA, para fins estatísticos e gerenciais internamente, envio de mensagens e-mail/WhatsApp, obrigações legais, fornecedores, empresas de cobrança e bancos. Os dados ficarão arquivados em meios digitais e físicos, sendo utilizados ou somente guardados – Servidor/Software CooperMSD, Fácil, por tempo indeterminado.

O funcionário, ciente da política, é responsável pelas informações, normas e procedimentos executados em suas atividades.

Cabe também, aos prestadores de serviços a ciência e responsabilidade desta política.

Cabe à Diretoria:

a) Cumprir e fazer cumprir esta política, as normas e os procedimentos de segurança da informação;

b) Assegurar que a equipe possua acesso e conhecimento desta política, das normas e dos procedimentos de segurança da informação;

c) Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas em relação à segurança tecnológica, a fim de resguardar os interesses e a imagem da Cooperativa;

d) Revisar as normas e os procedimentos de segurança da informação, quando necessário;

e) Informar, à área de TI, os desligamentos, afastamentos e eventuais modificações no quadro funcional da Cooperativa;

f) Aprovar a política de segurança da informação e suas revisões em reunião da Diretoria;
g) Tomar as decisões administrativas referentes aos casos de descumprimento da política e/ou de suas normas.

4 – ESTRUTURA E SEGURANÇA FÍSICA

Os equipamentos de informática, comunicação, sistemas e informações utilizados pelos funcionários são destinados à realização de atividades profissionais.

Atualmente a Cooperativa possui 3 (três) computadores – desktop e 4 (quatro) notebooks cedidos pela empresa participante. Para o seu acesso, cada funcionário da Cooperativa possui uma senha individual.

O acesso ao Sistema Fácil (Sistema operacional utilizado pela Cooperativa), possui senha exclusiva de acordo com cada perfil, sendo o acesso permitido, ao Coordenador Administrativo e os funcionários.

As instalações da Cooperativa que abriga as informações, documentos, equipamentos de processamento de informação confidencial serão classificadas como perímetros de segurança e considerados, no mínimo, os seguintes requisitos de segurança de instalações:
I. manutenção de controles de entrada nos perímetros de segurança, para assegurar o acesso somente a pessoas formalmente autorizadas;
II. armazenamento de materiais perigosos, a distância apropriada dos perímetros de segurança;
III. posicionamento correto de equipamentos de detecção e de combate a incêndios;
IV. monitoramento das áreas destinadas ao acesso público e/ou de pessoas não autorizadas.

O processo de segurança física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

5 – DIRETRIZES

É fundamental que os funcionários e dirigentes da Cooperativa adotem comportamento seguro e consistente quanto as informações confidenciais:

a) Os colaboradores devem compreender as ameaças externas que podem afetar a segurança das informações da Cooperativa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação;

Nota: Cuidado com os vírus de computador:

- Eles são instalados e funcionam sem que o usuário perceba;
- Estão por todos os lados na internet;
- Podem roubar senhas e apagar informações preciosas de seu computador;
- Ao perceber que foi infectado por um vírus, desligue seu computador e acione a equipe de informática ou procure ajuda de um profissional da sua confiança;
- Vírus e outros malwares (programas maliciosos) se disseminam de diversas formas, tais como:

- Acessando páginas Web maliciosas, utilizando navegadores vulneráveis;
- Embutidos em arquivos ou programas baixados pela Internet, anexados a e-mails ou recebidos por meio de sites de relacionamento e redes sociais;
- Acessando links patrocinados fraudulentos (Malvertising) obtidos através de ferramentas de busca como Google/Yahoo;
- Através da exploração de vulnerabilidades existentes em programas instalados.

b) Todo tipo de acesso à informação da Cooperativa que não for explicitamente autorizado é proibido;

c) Assuntos confidenciais não devem ser discutidos em locais públicos;

d) Sem a devida autorização documentada e proteção, os colaboradores não podem transportar informações sigilosas em CD, Pen Drive, DVD ou Papéis;

e) As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros, anotadas em papel e visível;

f) Somente softwares autorizados pela Cooperativa podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de serviços de informática contratada da COOPERMSD;

g) O uso de internet deve seguir as regras de acesso e bloqueio a páginas eletrônicas para que não seja comprometida a segurança da informação, e as regras de negócio não sejam afetadas, e que não causem danos à imagem, sendo feito diretamente pelo suporte de tecnologia. O uso da internet para assuntos pessoais (home banking, lojas virtuais e afins) é permitido desde que com bom senso e respeitando as demais diretivas de segurança estabelecidas.

Os acessos externos à rede interna, para fins de manutenção de infraestrutura ou sistemas, somente poderão ser realizados através de empresas formalmente contratadas pela COOPERMSD.

Os acessos à internet serão monitorados através de identificação do usuário, podendo ser bloqueados a qualquer momento pela equipe de tecnologia quando for identificado risco ao funcionamento do ambiente.

h) Os arquivos de origem desconhecida nunca devem ser abertos;

i) Os documentos impressos e os arquivos devem ser armazenados e protegidos em local adequado.

O acesso às informações e aos ambientes lógicos da Cooperativa deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação.

A gestão de controle de acesso deve ser documentada e formalizada por meio de normas e procedimentos que contemplem, pelo menos, os seguintes itens:

✓ Procedimento formal de concessão e comprovação de autorização de acesso a um usuário aos sistemas de informação;

✓ Utilização de identificadores de usuários (ID dos usuários individualizados) para assegurar a responsabilidade de cada usuário por suas ações;

✓ Remoção imediata quando ocorrer o desligamento ou alteração de função;

✓ Revisão no processo na política e suas normas quanto as autorizações concedidas, manutenção e uso de senhas.

6 – NORMAS DE SEGURANÇA – GERAIS

A Segurança da Informação da Cooperativa estabelece os principais controles, denominados diretrizes:

a) Os funcionários e prestadores de serviço da Cooperativa (usuários) só poderão acessar os sistemas, programas e informações as quais tem permissão/ autorização;

b) As senhas do usuário de acesso a programas e sistemas são de uso pessoal e intransferível e devem ser trocadas periodicamente;

Na Cooperativa, as senhas conterão os seguintes padrões mínimos de segurança:

b1) terão, pelo menos, oito caracteres, entre os quais, três dos seguintes grupos:

- Letras minúsculas;
- Letras maiúsculas;
- Números; e letras e;
- Símbolos (por exemplo, @, =, -, etc.);

b2) estarão de acordo com as seguintes recomendações de segurança:

- Não será anotada em papel ou arquivada em quaisquer dispositivos de armazenamentos, tais como: celulares, pendrives e arquivos gravados no computador.

b3) A troca da senha será realizada, preferencialmente, de 3 (três) em 3 (três) meses.

c) A internet e o e-mail fornecidos pela Cooperativa deverão ser utilizados apenas para uso profissional, sendo que o mesmo se aplica ao uso dos computadores e a ferramenta de comunicação eletrônica interna:

c1) A Cooperativa através do pessoal designado (empresa de suporte contratada), podem monitorar, investigar, ler toda a atividade executada pelos funcionários (as informações, dados, conteúdo e mensagens ou arquivos enviadas, recebidas ou armazenadas), com o objetivo de verificar a conformidade com os termos de utilização dos sistemas.

c2) Os sites de internet vistos pelos funcionários, também, serão verificadas, devendo ser utilizadas com bom senso e respeitando as regras de segurança definidas.

d) Na ausência do funcionário, em sala de trabalho, deverá bloquear o computador;

e) Os papéis para uso “rascunho” só devem ser utilizados quando não possuir informações confidenciais e de uso interno da Cooperativa;

f) Os documentos jogados no lixo deverão ser rasgados;

g) Os documentos deverão ser guardados em gavetas e armários fechados após o expediente de trabalho;

h) Outros aspectos importantes relacionados à segurança da informação estão mencionados no Código de Ética da Cooperativa que devem ser cumpridos rigorosamente por todos os envolvidos;

i) Somente softwares homologados poderão ser utilizados no ambiente da Cooperativa;

j) Todos os equipamentos da COOPERMSD, sejam eles servidores ou estações, devem possuir antivírus instalados;

k) Somente será dado acesso à informação para a pessoa que tiver a necessidade de conhecer tal informação;

l) Manter registro de todas as chaves de criptografia e certificados digitais existentes, informando o dono e o mantenedor;

m) As rotinas deverão ser executadas por empresa especializada para testar a defesa contra possíveis ataques aos seus sistemas de informação;

n) A Cooperativa implementa redes sem fios (wi-fi), 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.

7 – NORMAS DE SEGURANÇA – BACKUP (CÓPIA DE SEGURANÇA)

As diretrizes gerais relacionadas com a segurança do Backup:

a) As pastas (Documentos e Área de Trabalho) dos 4 (quatro) notebooks cedidos pela empresa mantenedora para o trabalho em home office, se baseia na sincronização dos arquivos no serviço “OneDrive” e o backup é feito pela empresa participante conforme os procedimentos mencionados abaixo:

Serviço: Backup e recuperação
Publicado em 6 de fevereiro de 2019 I Verificado em 19 de setembro de 2020 I GLOBAL.
Esta página é sobre proteção pontual e recuperação de dados residentes em servidores qualificados no ambiente da Merck contra vírus, roubo, desastres naturais, sistema falhas ou mesmo erro humano.

Descrição
Os serviços de backup e recuperação fornecem proteção automática de ponto no tempo dos sistemas empresariais, bancos de dados e dados de aplicativos da Merck.
Ele fornece backup e recuperação de dados para todos os sistemas pertencentes ou gerenciados pela Global Technology Operations (GTO).
O serviço também permite recursos abrangentes de recuperação de desastres e é confiável para OR para todos os sistemas não Classe A (de missão crítica).
Benefícios:
Gerenciamento centralizado, configuração, suporte e relatórios de sistemas e clientes gerenciados de backup e recuperação empresarial. Usando as melhores práticas e soluções padrão da indústria que são projetadas, testadas e mantidas de acordo com os padrões SDLC \ IML da Merck.
Todos os sistemas (servidores, bancos de dados) que solicitaram que os backups sejam gerenciados pela equipe da B&R, serão protegidos em uma abordagem automatizada onde os administradores de plataforma / banco de dados não são obrigados a iniciar o trabalho de backup. O sistema requer conectividade de rede e os trabalhos são executados com base em uma programação predeterminada. A janela de backup pode variar de site para site, dependendo das necessidades locais.
Conectividade de armazenamento direto para backup e recuperação rápidos e eficientes

Fornece restaurações imediatas de dados de versões ativas ou mais antigas de arquivos, com base na retenção para:
o Arquivos e / ou pastas individuais / múltiplos
o Drives de disco completos, sistemas de arquivos / diretórios
o Estado do sistema completo
o Bancos de dados (SQL, Oracle, SAP, etc.)
o Metal puro e recuperação total de VM
Ofertas padrão:
Soluções corporativas de backup e recuperação (Commvault Simpana, TSM, DDBoost)
Todos os sistemas qualificados (físicos, virtuais, em nuvem) têm backup programado todas as noites com base em uma janela de backup de 12 horas. Todos os bancos de dados qualificados têm um backup diferencial diário e um backup completo semanal.

Os backups de log são realizados a cada 4 horas com base na solicitação e qualificação do Banco de Dados usando (DDBoost, TSM ou Commvault Simpana).
24 x 7 x 365 dias Administração de infraestrutura de backup e recuperação, suporte, monitoramento e gerenciamento de serviço usando as melhores práticas, padrões, diretrizes, SOP e ITSM.
Administração proativa da infraestrutura da solução de backup e recuperação, monitoramento, alertas, relatórios, capacidade e gerenciamento de desempenho.
Escopo de oferta:
Os serviços e soluções de backup e recuperação cobrirão os data centers globais e regionais da Merck, sites remotos, filiais e provedor de nuvem (AWS).
Recursos:
Recuperação rápida de aplicativos e dados de ambientes tão diversos como máquinas virtuais, sistemas de arquivos, drives, bancos de dados e nível de arquivo.
Eficiência de armazenamento e aumento de dados usando centralizar desduplicação em linha, armazenamento corporativo altamente disponível e proteção baseada em instantâneos. Centralize e operações eficientes com relatórios integrados centralize os painéis que fornecem informações sobre o ambiente. Proteção automática de VM's implantadas em POD's protegidos.

Dispositivos de armazenamento altamente disponíveis (usando redundância de hardware interna) para replicar dois (2) conjuntos de cópias dos dados de backup em locais de data center centralizados.
Proteja os dados legados por mais tempo, mediante solicitação, para retenções legais usando o processo de 'Arquivo'.
Restaure uma cópia de um ou mais arquivos / diretórios de um backup para fins de revisão, reprocessamento e / ou reconstrução. Teste de recuperabilidade e planejamento de aplicação mediante solicitação.
Conjunto abrangente e integrado de cronogramas, que fornecem a base para um gerenciamento de dados eficiente com pouca necessidade de intervenção durante as operações normais.
Serviços:
Backup e recuperação para plataformas empresariais - ambientes físicos e virtuais (Windows, Linux, UNIX) Servidores:
o Configurações do sistema / proteção e recuperação do estado do sistema
o Sistemas de arquivos
o Proteção e recuperação de granularidade de nível de arquivo

Backup e recuperação para backup de aplicativos corporativos e suporte a serviços de recuperação (SAP, HANA) Backup e recuperação para bancos de dados (Oracle, SQL, DB2)
Serviços de backup para solução Converge Appliance (Teradata, Exadata)
Soluções de backup e recuperação para escritórios remotos, DMZ e filiais
Retenção de dados padrão:
30 dias para servidores de produção
O 7 dias para não produção (servidores Dev / Test)
Monitoramento diário e serviços de relatórios para todos os backups
Planos de remediação imediata e procedimentos para backups perdidos / com falha Processo de auditoria para verificações regulamentares e conformidade
Exercício de recuperação operacional
Notas:
BACKUP do arquivo de dados pessoais do Microsoft PST Outlook (TSM / COMMVAULT): BACKUP DE ARQUIVOS PST (EXCLUSÃO TSM / COMMVAULTI:
É um padrão da equipe GIO Backup and Recovery excluir arquivos PST (arquivo de dados do Outlook) em qualquer um de seus backups globais de cliente de servidor Windows / Linux / Unix. Os arquivos PST são adicionados à lista de exclusão padrão dos servidores de backup e recuperação (TSM, Commvault). Isso significa que os arquivos PST serão ignorados automaticamente durante os backups agendados.
Não haverá recuperação disponível de qualquer arquivo PST localizado em qualquer um dos servidores que a equipe de backup e recuperação GIO está gerenciando atualmente, com exceção dos servidores de Retenção Legal.

b) A Cooperativa também, realizou a licença para o armazenamento em nuvem até 02/11/2021 com a **Microsoft 365 Business Basic,** incluso o armazenamento e compartilhamento de arquivos com 1 TB de armazenamento no OneDrive (Informações técnicas: https://www.microsoft.com/pt-br/microsoft-365/onedrive/compare-onedrive -lans?activetab=tab:primaryr2). Será salvo os arquivos neste local também, além do OneDrive da MSD.

c) A COOPERMSD conta também, com os serviços de hospedagem do site, manutenção e suporte técnico de informática da empresa contratada (SAVEMAIS TECNOLOGIA);

d**)** A Cooperativa utiliza o sistema operacional da empresa Rezek Ferreira Informática Ltda. O backup externo fica armazenado em nuvem pela empresa contratada – Fácil Informática (Sistema Operacional). O backup alternativo fica localizado na cidade e estado de Belo Horizonte – MG onde disponibiliza a cópia de segurança do sistema operacional da Cooperativa, relativo aos processos críticos de negócios (financeiro, crédito, cadastro e contábil).

A COOPERMSD tem acesso com senhas e logins individuais para todos os funcionários, caso seja necessário abrir uma ocorrência/chamado, se ocorrer um determinado problema no sistema contratado da Empresa Fácil Informática.

Caso ocorra um evento, o funcionário deverá comunicar imediatamente o Coordenador da Cooperativa, a necessidade de uma solicitação de restauração de backup e os motivos. Após a comunicação, o coordenador ou na sua ausência a Diretoria fará os seguintes procedimentos:

- Acessar através da internet, pelo endereço eletrônico: facilinformatica.com.br, área restrita;
- Registrar um chamado técnico, solicitando a restauração de backup;
- O coordenador, comunicará a Diretoria o ocorrido;
- A Diretoria terá que registrar a ocorrência na ata da reunião;
- Dar ciência ao Conselho Fiscal;
- A ata e os documentos ficarão à disposição das auditorias.

A Cooperativa em caso de impossibilidade de acessar a página de internet da Empresa Fácil informática, conforme mencionado acima, por diversos motivos, tem a opção de acessar remotamente a este serviço, ligando para o telefone 31-3319-1900, opção 1, e quando estiver conversando com o atendente de suporte e comunicando a ocorrência, fazer este acesso remoto através do link conexão.facilinformatica.net.br, e assim obter os procedimentos necessários para a restauração de backup.

Conforme nosso Contrato, o sistema FacCred e os dados por ele operacionalizados estão hospedados utilizando a estrutura da Amazon AWS, empresa multinacional e líder mundial na prestação dos serviços de armazenamento em nuvem, com garantia de alta disponibilidade, sigilo, segurança e acessibilidade ao sistema e dados hospedados.

Além disso, o Contrato define claramente o escopo dos serviços de hospedagem.

As políticas da Amazon de segurança compliance e SLA podem ser acessadas nos links:

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

https://aws.amazon.com/pt/compliance/programs/

https://d1.awsstatic.com/legal/amazon-ec2-sla/Amazon_EC2_Service_Level_Agreement_-_Portuguese_Translation__2018-02-12_.pdf

O Contrato particular de licença de uso de software de prestação de serviços de suporte, manutenção e atualização e de armazenamento em nuvem de número CT-NUV-22014-2019 com a Empresa Fácil Informática, contendo em seu item 6, como, quando e onde estão sendo armazenados todas as informações. Segue abaixo, a cláusula do contrato:

6. DO ARMAZENAMENTO (HOSPEDAGEM) EM NUVEM

6.1. O SISTEMA completo – e os dados operacionalizados por ele – ficarão hospedados em DataCenter com disponibilidade de tempo (99,97%), em nuvem, utilizando a estrutura da empresa AMAZON, em região geográfica que não é divulgada por razões de segurança, sabendo-se, extraoficialmente, que um deles está localizado no Estado da Virginia, EUA.

6.2. A CONTRATANTE declara que conhece os termos – e com eles concorda – a que se encontra rigidamente submetida a CONTRATADA perante a AMAZON, termos estes que restringem e delimitam as responsabilidades contratuais da CONTRATADA perante a CONTRATANTE na prestação do serviço de armazenamento. Os termos aqui referidos estão divulgados, da forma integral, nos seguintes endereços eletrônicos:

6.2.1 quanto ao SLA: http://aws.amazon.com/pt/ec2-sla/;

6.2.2 quanto ao Contrato do Cliente (a CONTRATADA, no caso): http://aws.amazon.com/pt/agreement/;

6.2.3 quanto aos Termos de Serviço: http://aws.amazon.com/pt/serviceterms/; e,

6.2.4 quanto ao Uso Aceitável: http://aws.amazon.com/pt/aup/.

6.3. Concomitantemente ao armazenamento, a CONTRATADA prestará os serviços de:

6.3.1. disponibilização para uso de todos os módulos licenciados do SISTEMA, sem a necessidade de instalação de softwares nas estações-clientes da CONTRATANTE e com a dispensa de aquisição de licenças dos softwares de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem;

6.3.2. realização de backup em nuvem, totalmente automatizado, em ambiente de alta disponibilidade e durabilidade, com garantia da integridade dos dados por meio de restaurações periódicas em ambiente de homologação e confidencialidade das informações;

6.3.3. acompanhamento do banco de dados, contemplando desde o dimensionamento, instalação e configuração até tuning, backup/recover, monitoramento e aplicação de patches; e,

6.3.4. monitoramento de servidores e serviços, com notificações em caso de falhas, com características Proativas (ações para antecipação de falhas), Reativas (ações de resposta a eventuais falhas) e Preventivas (ações para minimizar probabilidade de falhas);

6.4. A CONTRATADA deverá efetuar o backup a que alude o subitem 6.3.2., acima, de acordo com a periodicidade abaixo detalhada e manter cada um dos backups efetuados sob a política cíclica de armazenamento, que garante a disponibilidade de restauração de backup dos 7 (sete) últimos dias, com as seguintes características:

6.4.1 backup diário de todo o Banco de Dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,9999999% de durabilidade e de 99,97% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais; e,

6.4.2 os backups serão testados semanalmente (restauração em ambiente de homologação) para garantir sua integridade;

6.5. Além dos procedimentos de segurança dos dados a que alude o subitem anterior, a CONTRATADA disponibilizará, diariamente, um arquivo contendo o backup lógico do banco de dados da CONTRATANTE. Por questões de segurança, este arquivo estará disponível dentro do ambiente da AMAZON e caberá à CONTRATANTE realizar a transferência (download) para sua máquina local utilizando-se do recurso de copiar e colar (Ctrl+C e Ctrl+V). Cabe à CONTRATANTE, ainda, especificar quais usuários deverão ter acesso ao arquivo. O arquivo será disponibilizado no formato EXPDP do Oracle 11g R2 e compactado através de ZIP.

6.6. A interrupção justificada dos serviços de acesso ao ambiente de nuvem com conseqüente exclusão de responsabilidade da CONTRATADA, ficará caracterizada pela ocorrência de:

6.6.1. casos fortuitos, assim entendidos os fatos humanos perniciosos aos serviços, alheios à vontade da CONTRATADA e sobre os quais ela não tem controle;

6.6.2. casos de força maior, assim entendidos os fenômenos naturais que interfiram de modo nefasto ou desastroso na prestação de serviços a que se obriga a CONTRATADA;

6.6.3. remanejamento interno do serviço de hospedagem, com aviso prévio à CONTRATANTE;

6.6.4. falha de conectividade decorrente de falhas em operadoras de telecomunicações e rotas de comunicação com o DataCenter onde está hospedado o SISTEMA em nuvem;

6.6.5. falha na conexão de Internet, sem culpa da CONTRATADA, mediante laudo técnico oferecido pela CONTRATADA;

6.6.6. as interrupções necessárias para ajustes técnicos ou manutenção, serão informadas, quando possível, com antecedência e se realizarão, preferencialmente, em horários noturnos, de baixo movimento;

6.6.7. as intervenções emergenciais decorrentes da necessidade de preservar a segurança dos dados, destinadas a evitar ou fazer cessar a atuação de hackers ou destinadas a implementar correções de segurança; e,

6.6.8. suspensão da prestação dos serviços contratados por determinação de autoridades competentes.

d) Os prestadores de serviço devem ser responsáveis pela manutenção dos backups relativos as suas atividades.

8 – CONSIDERAÇÕES FINAIS

O sistema, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Cooperativa, não podendo ser interpretados como de uso pessoal.

O descumprimento das diretrizes desta política, 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.

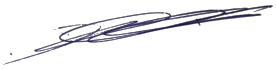
É dever de todo funcionário comunicar ao coordenador a ocorrência de incidente que afete a segurança da informação, que por sua vez comunicará a Diretoria para análise quando assim for necessário.

Declaramos que a respectiva Política foi aprovada e registra em Ata na reunião da Diretoria.

São Paulo/SP, 01 de dezembro de 2020.

Electronically signed by: Carlos Kanji Cesar Kamijo
Reason: Approved
Date: Nov 30, 2020 20:18 GMT-3

Carlos Kanji César Kamijo
Diretor Presidente



Electronically signed by: Jose Angelo Francolin
Reason: Approved
Date: Dec 1, 2020 14:17 GMT-3

José Angelo Françolin
Diretor Administrativo

Electronically signed by: Rubio Vinicius de Marcantonio
Reason: Approved
Date: Dec 1, 2020 09:11 GMT-3

Rúbio Vinicius de Marcantonio
Diretor Operacional

POLITICA SEGURANCA DA INFORMACAO v01122020

Final Audit Report 2020-12-01

Created:	2020-11-30
By:	Janete Aparecida Rogante (janete_rogante@merck.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAXINwW6NrStsfMcamUfku5ih_cQmftXhA

"POLITICA SEGURANCA DA INFORMACAO v01122020" History

Document created by Janete Aparecida Rogante (janete_rogante@merck.com)
2020-11-30 - 9:10:58 PM GMT- IP address: 155.91.45.238

Document emailed to Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com) for signature
2020-11-30 - 9:11:44 PM GMT

Email viewed by Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com)
2020-11-30 - 9:12:14 PM GMT- IP address: 155.91.45.235

Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com) verified identity with Adobe Sign authentication
2020-11-30 - 11:18:25 PM GMT

Document e-signed by Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com)
Signature Date: 2020-11-30 - 11:18:25 PM GMT - Time Source: server- IP address: 155.91.45.235

Document emailed to Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com) for signature
2020-11-30 - 11:18:27 PM GMT

Email viewed by Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com)
2020-12-01 - 12:10:01 PM GMT- IP address: 155.91.45.236

Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com) verified identity with Adobe Sign authentication
2020-12-01 - 12:11:18 PM GMT

Document e-signed by Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com)
Signature Date: 2020-12-01 - 12:11:18 PM GMT - Time Source: server- IP address: 155.91.45.236

Document emailed to Jose Angelo Francolin (joseangelo_francolin@merck.com) for signature
2020-12-01 - 12:11:20 PM GMT

Email viewed by Jose Angelo Francolin (joseangelo_francolin@merck.com)

2020-12-01 - 5:16:06 PM GMT- IP address: 155.91.45.236

Jose Angelo Francolin (joseangelo_francolin@merck.com) verified identity with Adobe Sign authentication

2020-12-01 - 5:17:44 PM GMT

Document e-signed by Jose Angelo Francolin (joseangelo_francolin@merck.com)

Signature Date: 2020-12-01 - 5:17:44 PM GMT - Time Source: server- IP address: 155.91.45.236

Agreement completed.

2020-12-01 - 5:17:44 PM GMT