POLÍTICA DE SEGURANÇA CIBERNÉTICA

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS EMPREGADOS DAS INDÚSTRIAS UNILEVER DO BRASIL

(19) 3869-4696 (19) 3869-6884
(19) 98886-6250 (19) 99624-2530 (19) 98911-9230 (19) 98267-6535
Das 9h30 às 15h30 faleconosco@coopercredunilever.com.br
Rua Antonio Carlos, 196 - Sala 44 - 4º Andar
Centro Valinhos - SP Cep: 13270-005

INTRODUÇÃO

O Manual de Segurança Cibernética tem por finalidade detalhar a política de segurança cibernética informando os procedimentos mantidos pôr esta instituição bem como os planos de efetivo controle para manter a segurança das informações, backups e antivírus e manter a continuidade operacional com o objetivo de fortalecer a segurança cibernética, para a Cooperativa de Economia e Crédito Mútuo dos Empregados das Indústrias Unilever do Brasil, denominada estatutariamente e nesta política pelo nome fantasia de COOPERCRED UNILEVER, CNPJ: 53.272.365/0001-31, constituída nos termos da Lei 5.764/71, atendidas as disposições da Lei 4.595/64, esse normativo serve para atender a Resolução nº 4.968/21 publicada pelo Conselho Monetário Nacional (CMN), instituída pela autorização de funcionamento do Banco Central do Brasil, sob nº 0773, a partir de 15/07/1977, com registro na Junta comercial sob o nº 35400001747, regendo-se pelas Normas e Resoluções baixadas pelo Banco Central do Brasil que disciplina o funcionamento de instituições financeiras, aplicáveis às Cooperativas de Créditos, pelo seu Estatuto Social e suas atividades disciplinares, com patrimônio próprio, autonomia administrativa e financeira, e prazo de duração indeterminado.

As instruções contidas neste manual estão baseadas legislação e na regulamentação aplicáveis ao tema.

1 – INFRAESTRUTURA DE REDE

1.1 – CONSIDERAÇÕES GERAIS

A COOPERCRED UNILEVER, possui atualmente a seguinte Infraestrutura de TI:

Rede:

- 01 Link Internet de 150 Mega
- Cabeamento UTP de aproximadamente 20 metros
- 5 Pontos de rede
- 01 Roteador
- 01 Nobreak

Microinformática:

- 03 Estações de trabalho
- 02 Impressoras Laser
- 01 Impressora jato de tinta
- 01 PABX com 4 linhas de telefone

1.2 – TOPOLOGIA DA REDE

A topologia da rede da cooperativa, por não possuir um servidor central, é constituída por um ponto de acesso central, sendo este localizado junto ao Modem. As estações de trabalho e impressoras estão ligadas a este Modem que distribuem o acesso nas dependências da cooperativa.

Cada estação de trabalho é registrada com um nome de usuário. Cada empregado ou membro estatutário da cooperativa detém o uso, durante o expediente de trabalho, de um desses usuários, sendo responsável pela conservação e correta utilização do equipamento.

Os usuários “COOPERCRED”, atualmente, estão assim distribuídos:

RESPONSÁVEL	CARGO
NILZA	GERENTE
PRISCILA	AUX. ADM. SENIOR
PATRICIA	AUX. DE ESCRITORIO

1.3 – SERVIÇOS CRÍTICOS

Os serviços listados a seguir, por serem críticos ao bom andamento e perfeito funcionamento das atividades da cooperativa, devem receber atenção especial, sendo:

a) Acesso à Internet (incluindo roteador)
b) Antivírus e Firewalls
c) Servidor DNS
d) ERP Syscoop 32 (Sistema terceirizado através de contratação dos serviços prestados pela Prodaf Informática, registrado em cartório protocolado sob o nº263.255)
e) Impressoras
f) Servidor de E-mails

Em virtude do tamanho reduzido da rede interna da cooperativa, consegue-se manter efetivo controle e supervisão, verificando periodicamente a situação de cada item citado, com relação ao funcionamento, segurança dos acessos e backup dos dados.

2 – SEGURANÇA DA INFORMAÇÃO

2.1 – CONSIDERAÇÕES GERAIS

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos da cooperativa, a informação deve ser adequadamente manuseada e protegida.

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Toda informação relacionada às operações da cooperativa, gerada ou desenvolvida em suas dependências, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

Toda informação de propriedade da cooperativa deve ser protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

2.2 – RESPONSABILIDADES

É missão e responsabilidade de todos empregados e membros estatutários, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da Política de Segurança Cibernética. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

2.3 – INFORMAÇÕES CONFIDENCIAIS

São consideradas informações confidenciais, quaisquer informações não disponíveis ao público ou reservadas, tais como, dados, especificações técnicas, desenhos,

manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma definidas pela cooperativa.

As informações confidenciais deverão ser mantidas e guardadas em caráter sigiloso, bem como de acesso limitado, controlando quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais pode ser repassada para terceiros sem consentimento por escrito da Diretoria. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições aqui estabelecidas.

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

São exemplos de informações confidenciais:

a) Informações de associados que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;
b) Informações sobre produtos e serviços que revelem vantagens competitivas da cooperativa frente ao mercado;
c) Todo o material estratégico da cooperativa (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
d) Quaisquer informações que não devem ser divulgadas ao meio externo antes da publicação pela Diretoria;
e) Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

Excetuam-se da obrigação de manutenção de confidencialidade:

a) o atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, tribunal arbitrais e de órgãos públicos administrativos;
b) a divulgação das informações confidenciais aos agentes, representantes (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros) e empregados das partes; e,
c) as informações confidenciais que forem divulgadas após o consentimento, por escrito, da Diretoria.

As cláusulas de ciência, responsabilidade e confidencialidade visam alertar e responsabilizar os empregados e membros estatutários de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

2.4 – VIOLAÇÕES

As violações de segurança devem ser informadas à Diretoria. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

a) uso de software para fins ilegais;
b) introdução (intencional ou não) de vírus de informática;
c) tentativas de acesso não autorizado a dados e sistemas;
d) compartilhamento de informações sensíveis do negócio;
e) divulgação de informações de associados e das operações contratadas.

Os princípios de segurança aqui estabelecidos possuem total aderência da Diretoria e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes e a violação de normas sujeita os empregados e membros estatutários às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

2.5 – ACESSO A SISTEMAS E RECURSOS DE REDE

Cada empregado é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Cada empregado acessará o sistema operacional apenas o imprescindível para o devido cumprimento de sua função, sendo que, caso necessário, deverá ser solicitado à Diretoria autorização para acesso à informação a qual não esteja autorizado.

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio da cooperativa.

2.5.1 – AUTENTICAÇÃO E SENHA

Cada empregado é responsável por atos executados com seu identificador (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso ao sistema da cooperativa.

Os empregados devem:

a) Manter a confidencialidade, memorizar e não registrar a senha em lugar algum;
b) Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
c) Selecionar senhas de qualidade, que sejam de difícil adivinhação;
d) Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação.

2.5.2 – CORREIO ELETRÔNICO

O uso do correio eletrônico é para fins corporativos e relacionados às atividades do empregado usuário dentro da cooperativa. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a instituição e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos empregados e membros estatutários o uso do correio eletrônico para:

a. enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da cooperativa;
b. enviar mensagem por correio eletrônico de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
c. enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a cooperativa vulneráveis a ações civis ou criminais;
d. divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
e. falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
f. produzir, transmitir ou divulgar mensagem que:

1. contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da cooperativa;
2. contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
3. contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente risco à segurança;
4. vise obter acesso não autorizado a outro computador, servidor ou rede;
5. vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
6. vise burlar qualquer sistema de segurança;
7. vise acessar informações confidenciais sem explícita autorização do proprietário;
8. vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
9. inclua imagens criptografadas ou de qualquer forma mascaradas;
10. tenha conteúdo considerado impróprio, obsceno ou ilegal;
11. seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
12. contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
13. tenha fins políticos locais ou do país (propaganda política);
14. inclua material protegido por direitos autorais sem a devida permissão.

2.5.3 – INTERNET

Embora a conexão direta e permanente da rede corporativa da cooperativa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos

para os ativos de informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a cooperativa, em total conformidade legal, reserva-se ao direito de monitorar e registrar todos os acessos à internet. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da cooperativa, 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 privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação e garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer empregado, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao empregado. 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 cooperativa cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela cooperativa aos seus empregados, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades. Como é do interesse da cooperativa que seus empregados estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

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. Empregados com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ou de dados a parceiros e associados, sem expressa autorização da Diretoria. Os empregados não poderão utilizar os recursos da cooperativa para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

2.5.4 – COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos empregados são de propriedade da cooperativa, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio da Diretoria ou, de quem ela determinar. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário. Arquivos pessoais e/ou não pertinentes ao negócio da cooperativa (fotos, músicas, vídeos, etc..), não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

2.5.5 – MANUTENÇÃO DE EQUIPAMENTOS E REDE

A manutenção dos equipamentos e rede interna da cooperativa será realizada por empresa devidamente confiável ou empregado capacitado, sendo estes responsáveis pela segurança das informações contidas nos equipamentos da cooperativa.

2.5.6 – BACKUPS E ANTIVIRUS

Os arquivos salvos em usuários/computadores locais e Outlooks (e-mails) deverão ser salvos em backup. Fica a cargo de cada empregado realizar o backup, dos dados armazenados localmente em dispositivo removível, a fim de prevenir quanto a perca de dados.

O banco de dados do sistema operacional da cooperativa, em virtude de estar em "nuvem", onde ocorre a realização de backup diário, ficando guardados com a empresa responsável pelo ambiente, não possui certa carência em se realizar backups locais diários, visto que isso já é feito pela empresa contratada para fornecimento de sistema (PRODAF).

2.5.7 – SOFTWARE - SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A parte de software para atendimento aos associados, cadastro, emissão de contratos, contabilidade e relatórios em geral é fornecida pela Prodaf Informática através do ERP Syscoop 32, o sistema é utilizado e acompanhado pelos colaboradores da entidade, quaisquer eventos onde forem apontados riscos, a entidade comunica a Prodaf e apontam as devidas providências para retomar a normalidade das atividades.

A PRODAF informática conta com um serviço de nuvem no Brasil pela empresa Dedalus e no exterior pela empresa Amazon Web Services, onde o nível de serviço prestado é o Enterprise, conforme descrição abaixo:

Nível de Serviço Enterprise

Destina-se a projetos críticos para o cliente, tais como sistema ERP, e-commerce ou ambiente web de alto impacto no negócio. Neste caso a responsabilidade da Dedalus passa a ser por toda a sustentação do ambiente, seu crescimento, contingência da infraestrutura IaaS, análise integrada de mudança, atendimento personalizado etc. Tarefas como administração, backup, monitoramento, entre outros, passam a ter uma dimensão típica de ambientes de missão crítica.

Definições Níveis de Serviço

SLA de Suporte Dedalus

O SLA de Suporte Dedalus define a forma de atendimento dos chamados abertos com a Dedalus, ou seja, tempos de atendimento, respostas e soluções dos problemas ou incidentes, conforme detalhado abaixo:

SLA de Suporte	Atendimento (abertura de chamado)	Exemplo de Tempo de Resposta

Enterprise - 24x7	24x7	até 1 hora corrida para início da análise do chamado.

Definições de Prioridade:

- **Prioridade Crítica (P1)** - Interrompe o processo produtivo ou comercial da organização;
- **Prioridade Alta (P2)** - Interrompe parcialmente o processo produtivo ou comercial da organização;
- **Prioridade Média (P3)** - Interrompe alguns passos do processo produtivo, administrativo ou comercial da organização, porém com a possibilidade de operação em contingência;
- **Prioridade Baixa (P4)** - Interrompe ou prejudica a operação de postos de trabalho individuais, dúvidas técnicas.

Definições de Complexidade:

- **Complexidade Baixa** - Soluções sem necessidade de conhecimentos técnicos, relativas a autorizações, senhas, funcionalidades de telas e conceitos básicos da ferramenta, atendimentos providos por profissionais de Suporte de Nível Junior (N1);
- **Complexidade Alta** - Soluções que envolvem questões técnicas de nível complexo, provido por profissionais de Suporte de Nível Sênior Especialista ou pelo fabricante da ferramenta (N2 e N3).

Resumo dos Tempo de Atendimento e Suporte	Atendimento	Cobertura Suporte	Prioridade	Tempo de Resposta	Tempo de Solução Complexidade Baixa	Tempo de Solução Complexidade Alta
Enterprise	24x7	24x7	P1 - Impacto Crítico	01 hora corrida	04 horas	a definir
Enterprise			P2 - Impacto Alto	02 horas corridas	06 horas	a definir
Enterprise			P3 -	04 horas	08 horas	a definir

			Impacto Médio	corridas		
Enterprise			P4 - Impacto Baixo	08 horas corridas	12 horas	a definir

Compreendidas as situações de não prestação de serviços contratado considerado crítico / essencial aos processos da Cooperativa.
Todos os serviços estão descritos e amparados por contratos, em caso de falha a Cooperativa deverá acionar a empresa prestadora de serviços para tomar as devidas providências e restabelecer a normalidade das atividades, através de chamado técnico e contato telefônico.

Título 1 - FINALIDADE DOS RECURSOS COMPUTACIONAIS:

Os recursos da tecnologia de informação disponibilizados pela **COOPERCRED UNILEVER** são destinados exclusivamente às atividades da instituição.

Seção 1 - Responsabilidades:

A Diretoria da **COOPERCRED UNILEVER** entende que o sistema de segurança adotado somente atingirá sua eficácia com o comprometimento e a cooperação de TODOS os profissionais e usuários.

Seção 2 - Direito à Propriedade:

Os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva da **COOPERCRED UNILEVER**, sendo vetada sua cópia parcial ou integral.

Seção 3 - Usuários:

São reconhecidos como usuários:

- Funcionários da **COOPERCRED UNILEVER, DIRETORIA E CONSELHO FISCAL**

Seção 4 - Atribuições do Usuário:

- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;

- Responder pelo uso exclusivo e intransferível de suas senhas de acesso.
- Adquirir conhecimento técnico necessário para a correta utilização dos recursos;
- Relatar prontamente a Diretoria qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas / diretórios de rede, acesso indevido à Internet, programas instalados sem conhecimento da Diretoria, etc;
- Não tentar obter acesso não autorizado a sistemas ou recursos de redes de computadores internas ou externas;
- Assegurar que as informações e dados de propriedade da **COOPERCRED UNILEVER** não sejam disponibilizados a terceiros, a não ser com autorização por escrito de um Diretor;
- Relatar a Diretoria a possibilidade de instalação de um novo software ou aquisição de novo Hardware para a melhoria dos serviços prestados.

Seção 5 - Atribuições dos Diretores e Gerentes:

- Zelar pelo cumprimento destas normas e procedimentos;
- Educar os funcionários sobre os princípios / procedimentos de Segurança da Informação, bem como lhes assegurar treinamento para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas;
- Advertir formalmente o usuário e aplicar as sanções cabíveis quando este violar os princípios ou procedimentos de segurança.
- Antes de aprovar a solicitação de compra ou alteração de hardware e software, assegurar que um profissional foi consultado e efetuou a autorização técnica;
- Divulgar e/ou compartilhar materiais ou informações sobre a boa pratica em segurança da informação no site, acessível pelo publico geral ou qualquer outro meio de comunicação utilizado.

Título 2 - IMPORTÂNCIA DO BACKUP

O Backup é a única forma de recuperar informações em caso de pane, seja por falha física, ou por falha humana. Ele garante a integridade dos dados, de configurações, bancos de dados e de arquivos de usuários.
Computadores e programas podem parar de uma hora para outra, impedindo acesso às informações. Não se pode prever quando isso irá acontecer, portanto é importante manter o backup sempre atualizado.

Título 3 - FREQUÊNCIA DE REALIZAÇÃO DAS CÓPIAS DE SEGURANÇA (*BACKUP*)

A freqüência com que é realizada uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o usuário cria ou modifica arquivos. A cópia de segurança será realizada mensalmente para documentos dos desktops e

será arquivado em local fora das dependências da Cooperativa e diariamente para o sistema operacional que fica na nuvem.

Título 4 - CUIDADOS COM AS CÓPIAS DE SEGURANÇA

Os usuários devem manter certos cuidados com as cópias de segurança, conforme segue:

Seção 1 - Armazenamento – deve ser realizado em mídia específica;

Seção 2 - Duplicidade de cópias – no mínimo duas cópias. Uma armazenada nas dependências da cooperativa e outra em ambiente externo;

Seção 3 - Tipos de mídias de gravação:

A escolha da mídia para a realização da cópia de segurança é essencial e depende da importância e da vida útil que a cópia deve ter. Um grande volume de dados, de maior importância, que deve perdurar por longos períodos, deve ser armazenado em mídias mais confiáveis, como, por exemplo, os Pen Drives ou HDs externos.

Seção 4 - Local de armazenamento:

As cópias de segurança serão guardadas em um local condicionado (longe de muito frio ou muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a este local (segurança física).
Além da cópia guardada na dependência da cooperativa é importantíssimo o armazenamento em locais diferentes, manteremos uma cópia em casa.

Título 5 - RESPONSABILIDADE

A realização, manutenção e integridade das cópias de segurança são de responsabilidade exclusiva das funcionárias da cooperativa de crédito.

Título 6 - REGRAS DE UTILIZAÇÃO DE CONTAS E SENHAS DA COOPERCRED UNILEVER.

Todos os usuários da Rede de Dados **COOPERCRED UNILEVER** receberão login e senha exclusivos para sua utilização e é obrigatório que todos os usuários tenham senhas individuais. É importante que os usuários não utilizem senhas de fácil identificação, tais como: data de nascimento próprio ou de parentes próximos, nomes próprios, datas comemorativas nacionais ou pessoais, iniciais de nomes próprios, números de telefones e etc;
As contas e senhas são pessoais, os usuários deverão responder pelo uso exclusivo e intransferível de suas senhas de acesso;

As senhas deverão ser trocadas pelo usuário, através de procedimento eletrônico e automático, utilizando o sistema de alteração de senhas disponível;
Os usuários desligados terão suas contas bloqueadas imediatamente, assim como o acesso a qualquer recurso da rede.
Reserva-se a **COOPERCRED UNILEVER** o direito de auditar a utilização de contas de rede fornecidas aos usuários de sua rede coorporativa, sem se caracterizar invasão de privacidade.

Título 7 - REGRAS PARA UTILIZAÇÃO DA REDE COOPERCRED UNILEVER.

Todos os recursos de rede de computadores deverão ser utilizados exclusivamente para fins profissionais, que envolvam atividades relacionadas ao bom andamento dos serviços e processos da **COOPERCRED UNILEVER**.
Todos os computadores da **COOPERCRED UNILEVER** devem ter antivírus instalado e atualizado periodicamente, é proibido desinstalar e utilizar computadores sem antivírus instalado.
É expressamente vedado aos usuários a instalação ou remoção de programas de computador, componente e periféricos;
É proibido aos usuários conectar computadores pessoais ou de terceiros à rede coorporativa da **COOPERCRED UNILEVER.**

Seção 1 - Penalidades:

A Diretoria alerta todos os usuários que a instalação ou utilização de software não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

Todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas de propriedade da COOPERCRED UNILEVER.
Todas as práticas que representam ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

Portanto, na ocorrência de infrações a este Manual, ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades:
Advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis.

2.6 – DIREITOS DE PROPRIEDADE

Todo produto resultante do trabalho dos empregados (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade da cooperativa. Em caso de

extinção ou rescisão do contrato, por qualquer motivo, deverá o empregado devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços à cooperativa, ou emitir declaração de que as destruiu.

3 – CONSIDERAÇÕES GERAIS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Para assegurar a efetividade das ações relativas a Segurança Cibernética, a cooperativa monitora, avalia e mantem estrutura compatível a seu porte, capaz de mitigar os riscos e manter a segurança em suas operações, observando-se os seguintes itens:

a) **Confidencialidade:** garantia de que a informação é acessível somente as pessoas autorizadas.
b) **Integridade:** salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
c) **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
d) **Riscos Cibernéticos:** Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, os quais podem desproteger os dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

I. Malwares:

- *Vírus*: software que causa danos a máquina, rede, softwares e banco de dados;

- *Cavalo de Troia*: aparece dentro de outro software e cria uma porta para a invasão do computador;
- *Spyware*: software malicioso para coletar e monitorar o uso de informações;
- *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

II. **Engenharia Social:**

- *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- *Acesso pessoal*: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

e. **Fraudes Externas e invasões:** Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

f. **Ataques DDoS e Botnets:** Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da cooperativa; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam

ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

Sendo os acessos à internet, o servidor de e-mails e o servidor do sistema operacional, o qual encontra-se em nuvem, as principais ferramentas de acesso à informação e consequentemente de grande vulnerabilidade a ataques cibernéticos, a cooperativa busca manter em seus computadores sistema completo de segurança (antivírus, antispyware, firewall), de ponta e totalmente atualizado, enquanto os servidores de e-mail e do sistema operacional, possuem recursos de segurança que atendem aos requisitos dispostos na legislação vigente acerca da segurança da informação e segurança cibernética.

4- INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

4.1 - Todas as ocorrências que possam acontecer com impacto negativo sobre a disponibilidade, integridade e confidencialidade dos serviços de informação ou recursos computacionais na COOPERCRED UNILEVER devem ser classificados como incidente de segurança da informação, devendo ser tratado de maneira a minimizar o impacto e recuperar os itens afetados.

4.2 – Todos os incidentes com relação a segurança da informação devem ser priorizados com base no critério dos recursos computacionais afetados e com a estimativa de impacto prevista. Para classificação da gravidade do incidente da informação, deve-se usar as seguintes categorias:

4.2.1 – **GRAVIDADE ALTA** – Todos os incidentes que possam gerar um impacto altíssimo nos negócios ou nas atividades da Cooperativa e que possam causar prejuízo.

4.2.2 – **GRAVIDADE MÉDIA** – Todos os incidentes que possam gerar um impacto médio ou que possam evoluir e vir a ter um impacto altíssimo na Cooperativa, porém não possam causar prejuízo.

4.2.3 – **GRAVIDADE BAIXA** – Todos os incidentes pequenos e que não causam prejuízo, mas que possa evoluir e vir a ter um impacto médio nos negócios ou serviços da Cooperativa.

Todos os incidentes de segurança da informação ou até mesmo suspeitas devem ser comunicados a gerencia da Cooperativa através de relatório ou outro que venha a substituir, sempre imediatamente após ser detectado, assim poderá ser adequadamente registrado, classificado, investigado, corrigido e documentado.

Fica a critério da gerência da Cooperativa a devida classificação, a comunicação das partes envolvidas/interessadas no assunto, bem como a informação à Diretoria.

Na ocorrência de incidente e na interrupção de serviços relacionados a segurança da informação, a gerencia deverá tomar as providências cabíveis à tratativa do incidente.

5- PLANO DE RESPOSTA A INCIDENTES

Este plano de resposta a incidentes é documentado para fornecer uma abordagem bem definida e organizada para lidar com qualquer ameaça potencial a computadores e dados, bem como tomar as medidas apropriadas quando a origem da intrusão ou incidente no ambiente de terceiros é rastreada até a rede privada da Cooperativa de Economia e Crédito Mútuo dos Empregados das Indústrias Unilever do Brasil. O plano de resposta a incidentes identifica e descreve as funções e responsabilidades da equipe de resposta a incidentes. A equipe de resposta a incidentes é responsável por colocar o plano em ação.

Resposta a Incidentes

A equipe de resposta a incidentes foi criada para fornecer uma resposta rápida, eficaz e ordenada a incidentes relacionados a computadores, como infecções por vírus e invasão de hackers, divulgação indevida de informações confidenciais a outros, interrupções no serviço do sistema, violação de informações pessoais e outros eventos com sérias implicações de segurança da informação.

A missão da equipe de resposta a incidentes é evitar uma perda de lucros, confiança do cliente ou ativos de informações, fornecendo uma resposta imediata, eficaz e hábil a qualquer evento inesperado que envolva sistemas de informações, redes ou bancos de dados.

A equipe de resposta a incidentes está autorizada a tomar as medidas apropriadas consideradas necessárias para conter, mitigar ou resolver um incidente de segurança de computadores. A equipe de resposta a incidentes é responsável por investigar tentativas suspeitas de invasão ou outros incidentes de segurança de maneira oportuna e econômica, além de informar as descobertas à gerência e às autoridades competentes, conforme necessário. O Diretor de Segurança Cibernética é responsável por coordenar estas investigações.

Membros do Time de Resposta a Incidentes

Nome	Cargo	Contato principal
Priscila N.C. Bittencourt	**Aux. Administrativo Sênior**	**(19) 99147-6673**
Patrícia da Silva Cavalcante	**Auxiliar de escritório**	**(19) 99268-4631**

Notificação ao Time de Resposta a Incidentes

Para facilitar a geração de relatórios e garantir uma resposta pontual 24 horas por dia, sete dias por semana, o cargo/departamento de auxiliar administrativo sênior atuará como ponto central de contato para relatar qualquer incidente.

Tipos de Incidentes

O termo “incidente” se refere a um evento adverso que afeta um ou mais ativos de informações da Cooperativa ou à iminência de tal evento. Os exemplos incluem, mas não estão limitados ao seguinte:

☑ Uso não autorizado;
☑ Negação de serviço;
☑ Código malicioso;
☑ Falhas do sistema de rede (generalizadas);
☑ Falhas do sistema de aplicação (generalizadas);
☑ Divulgação não autorizada ou perda de informação;
☑ Violação de Segurança da Informação;
☑ Outros.

Os incidentes podem resultar de qualquer um dos seguintes itens:

☑ Atos intencionais e não intencionais;
☑ Ações de funcionários;
☑ Ações de fornecedores ou constituintes;
☑ Ações de terceiros;
☑ Atos externos ou internos;
☑ Fraude de cartão de crédito;
☑ Violações potenciais das políticas da Cooperativa;
☑ Desastres naturais e falhas de energia;
☑ Atos relacionados a violência, guerra ou terrorismo;
☑ Transgressão grave;
☑ Outros.

Responsabilidades dos Usuários da Informação

Todos os funcionários da empresa devem relatar qualquer violação suspeita ou confirmada de informações pessoais de indivíduos com o cargo de auxiliar administrativo sênior imediatamente após a descoberta. Isso inclui a notificações recebidas de quaisquer provedores de serviços terceiros ou outros parceiros de negócios com os quais a organização compartilha informações pessoais de indivíduos.

O funcionário que relata a violação suspeita ajudará na obtenção de informações, preservando as evidências e prestando assistência adicional, durante a investigação.

Classificação de um Potencial Incidente

Todos os relatos de um incidente em potencial devem ser classificados como gravidade alta, média ou baixa para facilitar as ações a serem tomadas. Tais níveis são apresentados a seguir.

Gravidade: Alta

Definição: Todos os incidentes que possam gerar um impacto altíssimo nos negócios ou nas atividades da Cooperativa e que possam causar prejuízo.

Exemplo: Divulgação de informações confidenciais.

Gravidade: Média

Definição: Todos os incidentes que possam gerar um impacto médio ou que possam evoluir e vir a ter um impacto altíssimo na Cooperativa, porém não possam causar prejuízo.

Exemplo: Indisponibilidade de um servidor que possui redundância.

Gravidade: Baixa

Definições: Todos os incidentes pequenos e que não causam prejuízo, mas que possa evoluir e vir a ter um impacto médio nos negócios ou serviços da Cooperativa.

Exemplo: Tentativa de login inválida em um sistema.

Resposta a Incidentes

1. Qualquer pessoa que descubra o incidente entrará em contato com a auxiliar administrativo sênior da Cooperativa.

O suporte técnico registrará:

a) O nome do indivíduo que alertou o incidente;

b) A hora da chamada;

c) Informações de contato sobre o indivíduo;

d) A natureza do incidente;

e) Quais equipamentos ou pessoas estavam envolvidos;

f) Localização do equipamento ou pessoas envolvidas;

g) Como o incidente foi detectado;

h) Quando o evento foi notado pela primeira vez.

2. O membro da equipe de resposta a incidentes que recebe a chamada (ou que descobriu o incidente) consultará sua lista de contatos para que o pessoal da administração seja notificado

e os outros membros do time de resposta a incidentes sejam contatados. O funcionário convocará os designados na lista. O membro da equipe entrará em contato com o gerente de resposta a incidentes usando e-mail e telefone, garantindo que outras equipes apropriadas e designadas para a resposta sejam contatadas. O funcionário registrará as informações recebidas. O membro da equipe deverá adicionar o seguinte ao contexto do chamado:

a) Se o equipamento afetado é crítico ao negócio;
b) Qual é a potencial gravidade do impacto;
c) Nome do sistema que está sendo atacada, o sistema operacional, o endereço IP e a localização física;
d) Endereço IP e qualquer informação sobre a origem do ataque.

3. Os membros contatados da equipe de resposta se encontrarão ou discutirão a situação por telefone e determinarão uma estratégia de resposta:

a) O incidente é real?
b) O incidente ainda está em andamento?
c) Quais dados ou propriedades estão ameaçados e quão críticos são?
d) Qual é o impacto no negócio, caso o ataque seja bem-sucedido? Mínimo, sério ou crítico?
e) Quais sistemas ou subsistemas são afetados, onde eles estão localizados fisicamente e na rede?
f) O incidente está dentro da rede confiável?
g) A resposta é urgente?
h) O incidente pode ser rapidamente contido?
i) A resposta alertará o atacante e nós nos importamos?
j) Que tipo de incidente é esse?

4. Um ticket de incidente será criado. O incidente será categorizado no nível mais alto aplicável de uma das seguintes categorias:

a) Gravidade Alta;

b) Gravidade Média;

c) Gravidade Baixa.

5. Os membros da equipe definirão os procedimentos emergenciais necessários para a resposta do incidente, baseando suas respostas na avaliação do incidente, devendo realizar uma ou mais atividades descritas abaixo:

a) Encerrar um sistema ou vários sistemas - arriscar perder dados e tempo de inatividade significativo para operações de negócios;

b) Encerrar um segmento de rede completo - risco de perda de dados e tempo de inatividade significativo para operações de negócios;

c) Reinicializar o sistema ou sistemas - arrisque a perda de dados forenses;

d) Desconectar os sistemas de uma rede com ou sem fio;

e) Desativar certas funções;

f) Mudar o firewall para isolar a área afetada;

Observação: A equipe poderá criar procedimentos adicionais que não estão previstos neste documento. Se não houver nenhum procedimento aplicável em vigor, a equipe deverá documentar o que foi feito e depois estabelecer um procedimento para o incidente.

6. Os membros da equipe usarão todos os caminhos possíveis, incluindo a revisão dos registros do sistema, a procura de falhas nos registros, a revisão dos registros de detecção de invasões e a entrevista com testemunhas e a vítima do incidente para determinar como o incidente foi causado.

7. Os membros da equipe recomendarão alterações para evitar que o incidente aconteça novamente ou infecte outros sistemas.

8. Após a aprovação da gerência ou diretoria, as mudanças serão implementadas.

9. Os membros da equipe restaurarão o(s) sistema(s) afetado(s) para o estado não afetado, pré-incidente. Eles podem fazer um ou mais dos seguintes procedimentos:

a) Reinstale o(s) sistema(s) afetado(s) a partir do zero e restaure os dados dos backups, se necessário. Preserve as evidências antes de fazer isso;

b) Faça com que os usuários mudem as senhas, caso as senhas tenham sido detectadas;

c) Certifique-se de que o sistema foi validado, desligando ou desinstalando serviços não utilizados;

d) Certifique-se de que o sistema esteja atualizado;

e) Certifique-se de que a proteção contra vírus em tempo real e a detecção de invasão estejam em execução;

f) Certifique-se de que o sistema esteja registrando os eventos corretos e no nível adequado.

10. Documentação e preenchimento do RISI — o seguinte deve ser documentado:

a) Como o incidente foi descoberto;

b) A categoria do incidente;

c) Como o incidente ocorreu, seja por email, firewall, etc;

d) De onde veio o ataque, como endereços IP e outras informações relacionadas sobre o invasor;

e) Qual foi o plano de resposta;

f) O que foi feito em resposta;

g) Se a resposta foi eficaz.

11. Preservação de evidências - faça cópias de registros, e-mails e outras comunicações. Mantenha listas de testemunhas. Guarde evidências o quanto for necessário para concluir o processo e depois em caso de recurso.

12. Notifique as empresas externas competentes - notifique empresas apropriadas se a acusação do intruso for possível ou conforme determinado em resolução.

13. Avalie os danos e os custos - avalie os danos à organização e calcule o custo dos danos e o custo dos esforços de contenção.

14. Revise a resposta ao incidente e atualize as políticas - planeje e tome medidas preventivas para que a intrusão não aconteça novamente.

a) Considere se uma política adicional poderia ter impedido a invasão;

b) Considere se um procedimento ou política não foi seguida, o que permitiu a intrusão e, em seguida, considere o que poderia ser alterado para garantir que o procedimento ou política seja seguido no futuro;

c) A resposta ao incidente foi apropriada? Como poderia ser melhorada?

d) Toda a parte apropriada foi informada em tempo hábil?

e) Os procedimentos de resposta a incidentes foram detalhados e cobriram toda a situação? Como eles podem ser melhorados?

f) Mudanças foram feitas para evitar uma reinfecção? Todos os sistemas foram corrigidos, os sistemas foram bloqueados, as senhas foram alteradas, o antivírus foi atualizado, as políticas de e-mail foram definidas, etc.?

g) Foram feitas alterações para evitar uma infecção nova e semelhante?

h) Todas as políticas de segurança devem ser atualizadas?

i) Que lições foram aprendidas com essa experiência?

Incidente 1: Infecção por Malware

Conteúdo: Esta seção descreve os passos a serem seguidos para responder a uma infecção por *malware*.

Palavras-chaves: *malware*, infecção, vírus, *ransomware*, infectado, contaminado, contaminação, *worm*.

Sequência de resposta:

1. Qualquer colaborador que suspeitar de uma infecção por *malware* deve entrar em contato imediatamente com a Gerência ou responsável, fornecendo a estes:

1. O alerta ou a alteração de comportamento de software que levou à suspeita;

2. Localização dos equipamentos e pessoas envolvidas;

3. Quando o incidente foi detectado. O analista de suporte deve registrar data e hora deste contato inicial.

2. O analista de suporte que recebeu o chamado deve contactar o time de resposta a incidentes específico para a situação descrita no chamado e, ainda, o diretor de segurança da organização, fornecendo as informações coletadas quando da abertura do chamado pelo colaborador. Tais contatos devem ocorrer via e-mail, telefone e plataforma de atendimento de

chamados e toda a comunicação deve ser registrada pelo analista de suporte na plataforma de atendimento de chamados.

3. Um membro do time de resposta a incidentes contactado deve se deslocar imediatamente ao local onde o incidente foi reportado, de forma a diagnosticá-lo junto ao colaborador responsável pela abertura do chamado. Este deve verificar:

1. Se o evento reportado se trata de um incidente real ou se de um falso positivo;

2. Preliminarmente, o tipo e a variante do malware em questão;

3. Quais dados estão sob ameaça e o quão críticos estes são;

4. Se os equipamentos afetados estão na rede da organização;

5. Se a resposta ao incidente é urgente;

6. Se a infecção pode ser contida imediatamente.

Se as respostas aos itens “d”, “e” e “f” da listagem anterior forem afirmativas, com a anuência do diretor de segurança da informação, a infecção deve ser contida imediatamente.
Em seguida, logs de tráfego de rede e de firewall para as horas que antecederam esta fase da resposta ao incidente devem ser solicitados imediatamente ao time de infraestrutura.
O equipamento ou conjunto de equipamentos afetado deve ser isolado para análise.

Quando cabível, uma imagem dos sistemas afetados deve ser extraída.
Todas as ações e decisões tomadas nesta etapa devem ser registradas pelo membro do time de resposta a incidentes destacado para executá-la. Referências aos materiais gerados e coletados devem ser feitas no contexto do chamado em questão.

4. Após a contenção do incidente e a reunião de material acerca deste, cabe ao time de resposta a incidentes identificar, com base nos logs reunidos e eventuais imagens extraídas:

1. O tipo e, se possível, a variante do malware em questão;

2. O instante em que se deu a infecção;

3. Os danos causados pela infecção tratada, incluindo os dados eventualmente afetados e sua criticidade;
4. A causa da infecção em questão;

5. Ações a serem tomadas para evitar a propagação e a reincidência do problema. Caso julgue cabível, cabe ao time de resposta a incidentes conduzir entrevistas com os envolvidos no contexto do incidente de segurança de forma a elucidar eventos, situações e ações que levaram à infecção e obter respostas aos itens listados anteriormente.

O time de resposta a incidentes deve remeter à diretoria a respeito das conclusões extraídas desta etapa da resposta, detalhando a análise desenvolvida.

O chamado em questão deve ser atualizado com este novo conjunto de informações.

5. As ações a serem tomadas, delineadas na etapa anterior, devem ser postas em prática. Caso a infecção ainda não tenha sido contida no contexto do passo "3", isto deve ser feito.

Após devidamente sanados e restaurados ao estado pré-incidente, os sistemas afetados devem ser postos em operação novamente, com as devidas medidas preventivas a reincidências e propagações, sugeridas pelo time de resposta a incidentes na etapa anterior da resposta, implementadas.

6. Finalmente, o time de resposta a incidentes deve revisitar todas as etapas do processo de resposta, de forma a verificar a eficácia do procedimento e extrair lições a propagar a toda a equipe.

Possíveis melhorias em processos e políticas da organização devem ser sugeridas formalmente pelo time de resposta a incidentes à diretoria. Sugere-se que o time procure responder, ao menos, as perguntas abaixo:

1. Políticas adicionais teriam prevenido a infecção?

2. A causa da infecção foi o não-cumprimento de algum procedimento ou política? O que poderia ser feito para que o item em questão fosse cumprido no futuro?

3. A resposta à infecção foi apropriada? O que poderia melhorar no futuro?

4. Os recursos de comunicação do time foram adequados? Todas as partes envolvidas no processo foram informadas assertivamente ao longo do procedimento?

5. Como o procedimento aqui descrito poderia ser melhorado?

6. As mudanças implementadas são suficientes para evitar a reincidência do problema?

Incidente 2: Indisponibilidade de Serviços

Conteúdo: Esta seção descreve os passos a serem seguidos para responder a uma indisponibilidade de serviços.

Palavras-chaves: sistema, serviço, indisponível, indisponibilidade, queda, parada, offline, desconectado, desligado.

Sequência de resposta:

1. Qualquer colaborador que identificar uma indisponibilidade de serviço deve entrar em contato imediatamente com o suporte de TI, fornecendo ao analista de suporte:

1. O comportamento de software que levou à identificação da indisponibilidade;

2. O serviço cuja indisponibilidade foi identificada;

3. Quando o incidente foi detectado. O analista de suporte deve registrar data e hora deste contato inicial.

2. O analista de suporte que recebeu o chamado deve contactar o time de resposta a incidentes específico para a situação descrita no chamado e, ainda, o diretor de segurança da organização, fornecendo as informações coletadas quando da abertura do chamado pelo colaborador.

3. Um membro do time de resposta a incidentes contactado deve acessar imediatamente o serviço para o qual o incidente foi reportado, de forma a diagnosticá-lo. Este deve verificar:

1. Se o serviço em questão é provido por empresa prestadora externa;

2. Se o evento reportado se trata de um incidente real ou se de um falso positivo;

3. Preliminarmente, se o serviço em questão está operante;

4. Preliminarmente, se o serviço em questão está acessível;

5. Preliminarmente, se outras anormalidades foram identificadas na rede, segmento de rede ou rota ao serviço afetado;

6. Os prejuízos potenciais da indisponibilidade;

7. Quais dados estão sob ameaça e o quão críticos estes são;

8. Se o serviço afetado está na rede da organização;

9. Se a resposta ao incidente é urgente;

10.Se o restabelecimento da operação pode acontecer imediatamente.

Se a resposta ao item “a” da listagem anterior for afirmativa, o fluxo de resposta deve ser continuado a partir do passo “A”, abaixo, em “Sequência de resposta alternativa (serviço provido
por empresa externa)”.

Se as respostas aos itens “g”, “h” e “i” da listagem anterior forem afirmativas, com a anuência do diretor de segurança da informação, o restabelecimento do serviço deve ser feito imediatamente. Em seguida, logs de tráfego de rede e de firewall para as horas que antecederam esta fase da resposta ao incidente devem ser solicitados imediatamente ao time de infraestrutura.

O equipamento ou conjunto de equipamentos afetado deve ser isolado para análise.

Quando cabível, uma imagem dos sistemas afetados deve ser extraída.

Todas as ações e decisões tomadas nesta etapa devem ser registradas pelo membro do time de resposta a incidentes destacado para executá-la. Referências aos materiais gerados e coletados devem ser feitas no contexto do chamado em questão.

4. Após a reunião de material acerca do incidente, cabe ao time de resposta a incidentes identificar, com base nos logs reunidos e eventuais imagens extraídas:

1. O instante em que se deu a queda do serviço;

2. Os danos causados pela infecção tratada, incluindo os dados eventualmente afetados e sua criticidade;

3. A causa da indisponibilidade em questão;

4. Se a indisponibilidade do serviço afetado foi percebida por colaboradores em outros segmentos de rede da organização;

5. Se a indisponibilidade do serviço afetado foi percebida por clientes da organização, para o caso de serviços com saída para a Internet;

6. Ações a serem tomadas para evitar a propagação e a reincidência do problema. Caso julgue cabível, cabe ao time de resposta a incidentes conduzir entrevistas com os envolvidos no contexto do incidente de segurança de forma a elucidar eventos, situações e ações que levaram à indisponibilidade e obter respostas aos itens listados anteriormente.

O time de resposta a incidentes deve remeter à diretoria a respeito das conclusões extraídas desta etapa da resposta, detalhando a análise desenvolvida.

O chamado em questão deve ser atualizado com este novo conjunto de informações.

5. As ações a serem tomadas, delineadas na etapa anterior, devem ser postas em prática. Caso a indisponibilidade ainda não tenha sido tratada no contexto do passo "3", isto deve ser feito. Após devidamente verificados e restaurados ao estado pré-incidente, os serviços afetados devem ser postos em operação novamente, com as devidas medidas preventivas a reincidências e propagações, sugeridas pelo time de resposta a incidentes na etapa anterior da resposta, implementadas.

6. Finalmente, o time de resposta a incidentes deve revisitar todas as etapas do processo de resposta, de forma a verificar a eficácia do procedimento e extrair lições a propagar a toda a equipe.

Possíveis melhorias em processos e políticas da organização devem ser sugeridas formalmente pelo time de resposta a incidentes à diretoria. Sugere-se que o time procure responder, ao menos, as perguntas abaixo:

1. Políticas adicionais teriam prevenido a indisponibilidade?

2. Soluções de proteção adicionais teriam prevenido a indisponibilidade?

3. A causa da infecção foi o não-cumprimento de algum procedimento ou política? O que poderia ser feito para que o item em questão fosse cumprido no futuro?

4. A resposta à indisponibilidade foi apropriada? O que poderia melhorar no futuro?

5. Os recursos de comunicação do time foram adequados? Todas as partes envolvidas no processo foram informadas assertivamente ao longo do procedimento?

6. Como o procedimento aqui descrito poderia ser melhorado?

7. As mudanças implementadas são suficientes para evitar a reincidência do problema?

1. Um membro do time de resposta deve ser destacado como responsável primário para a tratativa do problema. Este deve contactar a empresa prestadora de serviços responsável pelo sistema indisponível, solicitando o seu restabelecimento, através do canal apropriado.

Toda a comunicação deve ser registrada no contexto do chamado em questão.

2. O responsável primário pela tratativa deve comunicar a diretoria sobre a indisponibilidade ser de responsabilidade de um prestador de serviços externo, especificando-o.

Toda a comunicação deve ser registrada no contexto do chamado em questão.

3. O responsável primário pela tratativa deve comunicar o Banco Central do Brasil sobre a indisponibilidade do serviço prestado por terceiros, bem como sobre as providências em curso para o seu restabelecimento.

Toda a comunicação deve ser registrada no contexto do chamado em questão.

4. Espera-se que a empresa prestadora de serviços restabeleça o serviço indisponível.

No caso de falta por parte da empresa prestadora de serviços, deve-se acionar fornecimento de backup para o serviço indisponível.

5. Finalmente, o time de resposta a incidentes deve revisitar todas as etapas do processo de resposta, de forma a verificar a eficácia do procedimento e extrair lições a propagar a toda a equipe.

Possíveis melhorias em processos e políticas da organização devem ser sugeridas formalmente pelo time de resposta a incidentes e a diretoria. Sugere-se que procure responder, ao menos, as perguntas abaixo:

1. Termos contratuais adicionais teriam prevenido a indisponibilidade?

2. A causa da indisponibilidade foi o não-cumprimento de algum procedimento ou política por parte da empresa prestadora de serviço? O que poderia ser feito para que o item em questão fosse cumprido no futuro?

3. A resposta da empresa prestadora de serviços foi satisfatória? O que poderia melhorar no futuro?

4. Cabe a revisão/rescisão do contrato com a empresa prestadora de serviços?

5. Os recursos de comunicação foram adequados? Todas as partes envolvidas no processo foram informadas assertivamente ao longo do procedimento?

6. Como o procedimento aqui descrito poderia ser melhorado?

Incidente 3: Substituição da empresa fornecedora de software

Conteúdo: Esta seção descreve os passos a serem seguidos para responder a uma substituição da empresa fornecedora de software.

Palavras-chaves: sistema, serviço, indisponível, indisponibilidade, queda, parada, offline, desconectado, desligado, substituição.

Sequência de resposta:

1. Indisponibilidade identificada pela Cooperativa onde o sistema esteja por pelo menos 1 dia útil sem funcionamento e sem retorno de possível normalização por parte da empresa contratada será repassado à Diretoria para registro das ocorrências.

2. Abriremos uma análise das causas da inoperabilidade bem como do impacto na Cooperativa, tentando minimizar os impactos o mais rápido possível;

2. Repassaremos a indisponibilidade ao Banco Central do Brasil bem como os procedimentos a serem adotados para normalização do funcionamento, que consistem em:

3. Cotação de empresas fornecedoras de sistemas bem como avaliação prévia dos serviços a serem prestados;

4. Análise e definição da Diretoria quanto ao melhor sistema para substituição e efetiva contratação;

5. Solicitação de backup atualizado e envio para migração;

6. Conferência de todos os itens migrados, bem como conferência de relatórios para confrontar os saldos em ambos os sistemas;

7. Reestabelecimento do atendimento aos cooperados.

8. O prazo estipulado pela cooperativa para retorno as atividades normais não poderão ser maiores que 15 (quinze) dias úteis.

Todas as ações e decisões tomadas nesta etapa devem ser registradas pelo membro do time de resposta a incidentes destacado para executá-la. Referências aos materiais gerados e coletados devem ser feitas no contexto do chamado em questão.

8. Após a reunião de material acerca do incidente, cabe ao time de resposta a incidentes identificar, com base nos logs reunidos e eventuais imagens extraídas:

a. O instante em que se deu a queda do serviço;

b. Os danos causados pela indisponibilidade do sistema, incluindo os dados eventualmente afetados e sua criticidade;

c. A causa da indisponibilidade em questão;

d. Se a indisponibilidade do serviço afetado foi percebida por colaboradores em outros segmentos de rede da organização;

e. Se a indisponibilidade do serviço afetado foi percebida por clientes da organização, para o caso de serviços com saída para a Internet;

f. Ações a serem tomadas para evitar a propagação e a reincidência do problema. Caso julgue cabível, cabe ao time de resposta a incidentes conduzir entrevistas com os envolvidos no contexto do incidente de segurança de forma a elucidar eventos, situações e ações que levaram à indisponibilidade e obter respostas aos itens listados anteriormente.

O time de resposta a incidentes deve remeter à diretoria a respeito das conclusões extraídas desta etapa da resposta, detalhando a análise desenvolvida.

O chamado em questão deve ser atualizado com este novo conjunto de informações.

5. As ações a serem tomadas, delineadas na etapa anterior, devem ser postas em prática. Caso a indisponibilidade ainda não tenha sido tratada, a substituição do sistema deve ser feita. Após devidamente verificados e restaurados ao estado pré-incidente, os serviços afetados devem ser postos em operação novamente, com as devidas medidas preventivas a reincidências e propagações, sugeridas pelo time de resposta a incidentes na etapa anterior da resposta, implementadas.

6. Finalmente, o time de resposta a incidentes deve revisitar todas as etapas do processo de resposta, de forma a verificar a eficácia do procedimento e extrair lições a propagar a toda a equipe.

Possíveis melhorias em processos e políticas da organização devem ser sugeridas formalmente pelo time de resposta a incidentes à diretoria. Sugere-se que o time procure responder, ao menos, as perguntas abaixo:

1. Políticas adicionais teriam prevenido a indisponibilidade?

2. Soluções de proteção adicionais teriam prevenido a indisponibilidade?

3. A causa da infecção foi o não-cumprimento de algum procedimento ou política? O que poderia ser feito para que o item em questão fosse cumprido no futuro?

4. A resposta à indisponibilidade foi apropriada? O que poderia melhorar no futuro?

5. Os recursos de comunicação do time foram adequados? Todas as partes envolvidas no processo foram informadas assertivamente ao longo do procedimento?

6. Como o procedimento aqui descrito poderia ser melhorado?

7. As mudanças implementadas são suficientes para evitar a reincidência do problema?

1. Um membro do time de resposta deve ser destacado como responsável primário para a tratativa do problema. Este deve contactar a empresa prestadora de serviços responsável pelo sistema indisponível, solicitando o seu restabelecimento, através do canal apropriado.

Toda a comunicação deve ser registrada no contexto do chamado em questão.

2. O responsável primário pela tratativa deve comunicar a diretoria sobre a indisponibilidade ser de responsabilidade de um prestador de serviços externo, especificando-o.

Toda a comunicação deve ser registrada no contexto do chamado em questão.

3. O responsável primário pela tratativa deve comunicar o Banco Central do Brasil sobre a indisponibilidade do serviço prestado por terceiros, bem como sobre as providências em curso para o seu restabelecimento.

Toda a comunicação deve ser registrada no contexto do chamado em questão.

4. Espera-se que a empresa prestadora de serviços restabeleça o serviço indisponível.

No caso de falta por parte da empresa prestadora de serviços, deve-se acionar fornecimento de backup para o serviço indisponível.

5. Finalmente, o time de resposta a incidentes deve revisitar todas as etapas do processo de resposta, de forma a verificar a eficácia do procedimento e extrair lições a propagar a toda a equipe.

Possíveis melhorias em processos e políticas da organização devem ser sugeridas formalmente pelo time de resposta a incidentes e a diretoria. Sugere-se que procure responder, ao menos, as perguntas abaixo:

1. Termos contratuais adicionais teriam prevenido a indisponibilidade?

2. A causa da indisponibilidade foi o não-cumprimento de algum procedimento ou política por parte da empresa prestadora de serviço? O que poderia ser feito para que o item em questão fosse cumprido no futuro?

3. A resposta da empresa prestadora de serviços foi satisfatória? O que poderia melhorar no futuro?

4. Cabe a revisão/rescisão do contrato com a empresa prestadora de serviços?

5. Os recursos de comunicação foram adequados? Todas as partes envolvidas no processo foram informadas assertivamente ao longo do procedimento?

6. Como o procedimento aqui descrito poderia ser melhorado?

6 - Política de Continuidade de Negócios

Estabelecem diretrizes e responsabilidades a serem observadas na continuidade de negócios da Cooperativa de Economia e Crédito Mútuo dos Empregados das Indústrias Unilever do Brasil, de forma a minimizar os impactos financeiros, operacionais, legais e regulatórios decorrentes de indisponibilidades de recursos – humanos, materiais e tecnológicos – essenciais para o funcionamento de suas operações.

Definição

O plano de continuidade de negócios é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual ela faz parte.

Abaixo alguns conceitos relacionados à continuidade dos negócios:

a) Sistemas críticos são sistemas cuja inoperabilidade implica em perdas irreversíveis financeiro, jurídico ou de imagem da Cooperativa e sua atividade produtiva deve acontecer em até 24 horas após ocorrência do desastre.

b) Desastre é a ocorrência de qualquer tipo de anormalidade que impeça ou impacte a atividade de produção dos sistemas críticos;

c) Recuperação é o restabelecimento da atividade produtiva dos sistemas críticos, mesmo que paliativa ou parcialmente, no caso do desastre se efetivar;

d) Pontos básicos para a elaboração do plano de contingência são necessários levantar alguns itens básicos, quais sejam:

I – Quais são os sistemas críticos que garantem a continuidade do negócio na Cooperativa;

II – Análise de impacto nos negócios;

III – Análise de riscos para os principais negócios;

IV – Homologação dos sistemas críticos por parte da Diretoria;

V – Recursos de Hardware, software e infraestrutura;

VI – Backup;

VII – Decisões pós-desastre para a recuperação.

Diretrizes

A continuidade de negócios da Cooperativa deve prever mecanismos que permitam:

a) Identificar ameaças internas e externas que possam comprometer a continuidade das operações;

b) Identificar os possíveis impactos à operação decorrentes da concretização de tais ameaças;

c) Identificar os requisitos para a continuidade dos negócios, incluindo os legais e os regulatórios;

d) Estabelecer papéis e responsabilidades das partes internas e externas à Cooperativa;

e) Desenvolver estrutura de gerenciamento e resposta às crises, suportadas por níveis adequados de autoridade e competência, que assegurem a comunicação efetiva às partes interessadas;

f) Desenvolver processos e mecanismos que viabilizem a recuperação das atividades em caso de interrupção;

g) Realizar analises que garantam a manutenção e o bom funcionamento dos planos de continuidade;

h) Aderir e cumprir diretrizes contidas nesta política;

i) Comunicação tempestiva ao Banco Central do Brasil de ocorrência de incidentes relevantes e de interrupções dos serviços relevantes que configurem uma situação de crise pela Cooperativa bem como as providencias para o reinício das atividades;

j) Para os recursos essenciais, são formalmente estabelecidos os planos com procedimentos alternativos para a recuperação das atividades exigidas, no tempo desejado. Observada a relação custo/benefício e o impacto potencial;

K) Devem ser encaminhados relatórios para os conselheiros, diretores, gestores e demais empregados com objetivo de conscientizá-los a respeito de:

I – Ameaças de geração de interrupção das atividades e seus desdobramentos;

II – Da importância do estabelecimento de estratégias de funcionamento dos planos de gerenciamento de incidentes e de continuidade de negócios;

III – De como implementar os planos de continuidade em resposta a interrupção dos processos ou atividades críticas;

l) Todos os envolvidos no processo de continuidade de negócios, ainda que não participem das deliberações, são responsáveis pela qualidade das operações que realizarem;

Plano de Continuidade de Negócios

Missão: Garantir que a restauração do processamento ocorra dentro do prazo estipulado no plano de contingência conforme criticidade de cada sistema. Exercer a coordenação geral do plano.

Tarefas pré-desastre

As tarefas pré-desastre do plano de continuidade dos negócios são:

a) Avaliar e aprovar gastos financeiros necessários ao desenvolvimento e manutenção do plano;

b) Definir local do centro de operações e de comando alternativo em caso de desastre;

c) Organizar e coordenar a execução de testes do plano;

d) Definir e montar a estrutura de retorno à normalidade;

e) Dar apoio, a todos envolvidos.

Tarefas durante o desastre

As tarefas durante o desastre do plano de continuidade dos negócios são:

a) Avaliar a situação posicionando aos diretores para decisão sobre ativação do plano;

b) Coordenar a ativação e as atividades do plano;

c) Ativar local do centro de operações alternativo;

d) Estabelecer diretrizes para situações não previstas;

e) Acionar pessoas chaves para recuperação do ambiente operacional;

f) Acionar as providências para recuperação do ambiente operacional.

Tarefa pós-desastre

Após o desastre, o gestor deve coordenar as atividades de retorno à normalidade.

Considerações Finais

O plano de continuidade de negócios é de responsabilidade da Diretoria e todas as observações e ocorrências, assim como ações a serem aprimoradas para atualização deste plano, serão inseridas na ata da Diretoria, realizada mensalmente.

7- Plano de Contingência

O plano de Contingência pode ser entendido como o conjunto de medidas preventivas e procedimentos de recuperação, no caso de qualquer interrupção de negócios. Estas medidas, vão muito além da simples adoção de um plano de seguro e, devem garantir a capacidade da Cooperativa em operar em bases contínuas. Para tanto, esse plano deve assegurar que todos os processos críticos têm seus riscos identificados, avaliados, monitorados e controlados.
A Diretoria da Cooperativa de Economia e Crédito Mútuo dos Empregados das Indústrias Unilever do Brasil é responsável pelas informações contidas neste Manual em cumprimento às exigências da Resolução 4.557/17.

Contingência de Infraestrutura Física

Assim compreendidas as situações de catástrofes naturais ou não, tais como inundação, incêndios, desabamento etc. que impeçam o acesso e/ou utilização das instalações da Cooperativa, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não e ainda falhas no fornecimento de energia elétrica.
As instalações da Cooperativa encontram-se no prédio do Edifício Elba, Centro, 4º andar, Sala:44, dentro do prédio possui equipe de brigada de incêndio preparadas em escape de incêndio, defesa civil e etc.

Acesso a Cooperativa

O prédio também conta com equipe de segurança (portaria com entrada restrita e portão com grade). O acesso de visitantes é dado parcialmente com identificação e autorização.

Serviços críticos para as atividades

A Cooperativa considera o fornecimento de energia elétrica como serviço crítico para suas atividades, tal fornecimento é disponibilizado pela CPFL, quando necessário à manutenção na rede, a CPFL informa a Cooperativa e solicita o desligamento preventivo dos equipamentos,

quando retornado à normalidade a CPFL informa a Cooperativa para religar os equipamentos, em caso de falhas no fornecimento de energia elétrica a Cooperativa deverá aguardar sua normalidade assim como as demais empresas situadas no prédio.

Contingência de Pessoal

São aquelas onde as pessoas chave não estão presentes por motivos de greves, doença, licença e etc.
Havendo necessidade de ausência em curto prazo do Gerente Administrativo, o Auxiliar Administrativo Sênior possui acesso aos sistemas e e-mails da Cooperativa, o que possibilita a continuidade de execução das rotinas da Cooperativa.
No caso de ausência por Licença, a Cooperativa poderá manter um Diretor/Conselheiro com conhecimento do manual de procedimentos internos para acompanhamento das atividades executadas e se caso o Auxiliar Administrativo Sênior também estiver ausente, ou ainda ter um colaborador devidamente treinado/capacitado para operar os mesmos sistemas, para substituição em situações de contingências.
A Cooperativa dispõe do manual de procedimentos internos com as principais rotinas executadas pelo Gerente Administrativo, onde a Diretoria deverá tomar providências para o restabelecimento da normalidade das atividades.

Contingência de infraestrutura tecnológica

Compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, rede e segurança, etc.
A Cooperativa contratará/acionará uma empresa prestadora de serviços eventuais onde um técnico de informática fara as verificações e ajustes necessários. A parte de Software é fornecida pela Prodaf Informática, e acompanhada pelos colaboradores da entidade, quaisquer eventos onde forem apontados riscos, a entidade comunica a Cooperativa e apontam as devidas providências para retomar a normalidade das atividades.

Contingência de serviços externos

Compreendidas as situações de não prestação de serviços contratado considerado crítico / essencial aos processos da Cooperativa.
Todos os serviços estão descritos e amparados por contratos, em caso de falha a Cooperativa deverá acionar a empresa prestadora de serviços para tomar às devidas providências e restabelecer a normalidade das atividades.

Considerações Finais

O presente plano de Contingência é de uso da Cooperativa, sendo sua manutenção e atualização de responsabilidade da Diretoria, a fim de mantê-lo consistente com as operações e estratégias correntes.

8- DO CONHECIMENTO

Todos os funcionários receberão uma cópia deste manual para tomarem conhecimento de todos os procedimentos pertinentes a segurança, inclusive backups necessários.

A **DIRETORIA DA COOPERCRED UNILEVER** se reserva o direito de atualizar, alterar, anular toda ou em parte as normas aqui contidas, a qualquer momento, desde que constatada a necessidade e aprovada em reunião da Diretoria.

9- RELATÓRIO ANUAL DE SEGURANÇA CIBERNÉTICA

A **COOPERCRED UNILEVER** deve avaliar a efetividade da política, dos procedimentos e dos controles cuja avaliação deverá ser documentada em relatório específico (Relatório Anual de Segurança Cibernética), conforme segue:

i. elaborado anualmente, com data-base de 31 de dezembro; e
ii. encaminhado, para ciência, até 30 de abril do ano seguinte ao da data-base à diretoria da instituição.

Valinhos, 24 de julho de 2023.

DIRETORIA:

LUIS DONIZETTI DIAS
Diretor Presidente

JULIANA ANDRETTA LOTIERSO
Diretora Operacional

MANUAL DE SEGURANÇA CIBERNÉTICA 24072023.pdf

Documento número #29f2e6e7-ec36-4ede-8949-4803dc5cb4bc

Hash do documento original (SHA256): a5d9ec5122f24f50e8c1149880ea29c33ec9a118c24947e39130b6b2ef199472

Assinaturas

LUIS DONIZETTI DIAS

CPF: 137.395.368-37

Assinou como representante legal em 04 ago 2023 às 16:22:32

JULIANA ANDRETTA LOTIERSO

CPF: 382.361.528-98

Assinou como representante legal em 07 ago 2023 às 08:40:00

Log

04 ago 2023, 15:04:30	Operador com email nilza@coopercredunilever.com.br na Conta 793dc1f9-f694-4c60-a4d5-25a6615b6099 criou este documento número 29f2e6e7-ec36-4ede-8949-4803dc5cb4bc. Data limite para assinatura do documento: 03 de setembro de 2023 (15:03). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
04 ago 2023, 15:04:49	Operador com email nilza@coopercredunilever.com.br na Conta 793dc1f9-f694-4c60-a4d5-25a6615b6099 adicionou à Lista de Assinatura: luis.d.dias77@gmail.com para assinar como representante legal, via E-mail, com os pontos de autenticação: Token via Sms; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo LUIS DONIZETTI DIAS e Telefone celular *******7040, com hash prefixo f72787(...).
04 ago 2023, 15:04:49	Operador com email nilza@coopercredunilever.com.br na Conta 793dc1f9-f694-4c60-a4d5-25a6615b6099 adicionou à Lista de Assinatura: julianalotierso@gmail.com para assinar como representante legal, via E-mail, com os pontos de autenticação: Token via Sms; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo JULIANA ANDRETTA LOTIERSO e Telefone celular *******5225, com hash prefixo fffdc6(...).
04 ago 2023, 16:22:32	LUIS DONIZETTI DIAS assinou como representante legal. Pontos de autenticação: Token via SMS *******7040, com hash prefixo f72787(...). CPF informado: 137.395.368-37. IP: 177.79.99.87. Localização compartilhada pelo dispositivo eletrônico: latitude -22.9770847 e longitude -46.9834414. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.559.0 disponibilizado em https://app.clicksign.com.

07 ago 2023, 08:40:00	JULIANA ANDRETTA LOTIERSO assinou como representante legal. Pontos de autenticação: Token via SMS *******5225, com hash prefixo fffdc6(...). CPF informado: 382.361.528-98. IP: 200.182.77.210, 136.226.62.249. Localização compartilhada pelo dispositivo eletrônico: latitude -23.6750786 e longitude -46.670534. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.559.0 disponibilizado em https://app.clicksign.com.
07 ago 2023, 08:40:01	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 29f2e6e7-ec36-4ede-8949-4803dc5cb4bc.