POL ASTI 001 - POLITICA INSTITUCIONAL

ELABORAÇÃO: 02/2016
RESPONSÁVEL: TODOS OS COLABORADORES
ATIVIDADE: POLÍTICA INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO

CONTROLE HISTÓRICO				
REVISÃO	**DATA**	**ELABORAÇÃO**	**VERIFICAÇÃO**	**APROVAÇÃO**
00	01/02/2016	Marcus Jimenez	Cely Gomes	Euracy Bonner
01	25/11/2016	Marcus Jimenez	Cely Gomes	Marcus Jimenez

SIGLAS E DEFINIÇÕES
TI – Sigla de "Tecnologia da Informação".
TIC – Sigla de "Tecnologia da Informação e Comunicação".
ASTI – Sigla de "Assessoria de Tecnologia da Informação".
Informação – é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe.
Recursos de TI – consistem nos recursos físicos e lógicos, periféricos e sistemas de software relacionados com a Tecnologia da Informação.
Segurança da Informação – consiste no conjunto de ações que tem como objetivo viabilizar e assegurar a disponibilidade, integridade, confidencialidade e a autenticidade das informações, não se restringindo somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento, pois o conceito se aplica a todos os aspectos de proteção de dados e informações.
Disponibilidade – é a propriedade que tem por objetivo assegurar que a informação esteja acessível e utilizável em tempo oportuno sempre que demandada por uma pessoa, setor, unidade organizacional ou sistema de informação.
Integridade – é a propriedade que tem por objetivo assegurar que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Confidencialidade – é a proprieade que tem por objetivo assegurar que a informação não esteja acessível às pessoas, setores, unidades organizacionais ou sistemas de informação que não estejam devidamente credenciados e autorizados para tal.
Autenticidade – é a propriedade que tem por objetivo assegurar que a informação foi realmente produzida, modificada ou descartada por uma determinada pessoa, setor, unidade organizacional ou sistema de informação.
Usuário – todas as pessoas, quais sejam: cooperados; colaboradores; gestores; terceiros; fornecedores; setores; e processos que utilizem direta ou indiretamente os recursos tecnológicos disponibilizados pela Unimed Rio Branco.
Usuário Interno – todas as pessoas diretamente ligadas à Unimed Rio Branco, quais sejam: diretores, assessores, gerentes, supervisores, demais colaboradores e terceiros que estejam atuando em nome da cooperativa.
CGTI – Comitê Gestor de Tecnologia da Informação.

OBJETIVOS

O conhecimento não existe se não houver uma fonte, uma origem de informação que forneça subsídios para sua construção. No ambiente corporativo a informação é um recurso essencial e de fundamental importância para qualquer tipo de empresa, independente do seu mercado de atuação ou do seu porte econômico. No ramo da Saúde Suplementar não é diferente. Por este motivo, devem ser considerados todos os riscos associados aos sistemas de informação utilizados no âmbito das operadoras de planos de saúde, bem como a necessidade de preservar a confidencialidade, integridade e disponibilidade dos mesmos, atentando sempre para o atendimento às disposições da legislação vigente, além das demais normas e diretrizes dos conselhos Federal e Regional de Medicina, da Agência Nacional de Saúde Suplementar e dos demais órgãos reguladores, além da Unimed do Brasil.

O objetivo da Unimed Rio Branco, por meio deste documento, é definir as diretrizes que irão nortear as práticas que deverão ser adotadas no âmbito da cooperativa a fim de assegurar a proteção dos dados e informações integrantes de seu patrimônio ou que estejam sob sua guarda, bem como das ferramentas utilizadas para obtenção, geração, armazenamento e disponibilização das mesmas, garantindo que estejam de acordo com todas as obrigações legais, independentemente do meio em que se encontrem.

ABRANGÊNCIA

A Política de Segurança da Informação se aplica a todos os usuários, processos de negócio e sistemas de informação que a utilizam direta ou indiretamente, independentemente do local e da forma como estejam armazenadas, contidas ou distribuídas na cooperativa.

Todos devem ter ciência do conteúdo desta política, atestando, por meio da assinatura do Termo de Sigilo e Responsabilidade, que conhecem todas as suas disposições, não sendo admitida a alegação do desconhecimento de seu conteúdo para justificar violações ou descumprimento da mesma.

DIRETRIZES GERAIS

Iniciaremos nossas diretrizes com a seguinte colocação: “Boas regras de segurança da informação não são definidas para satisfazer a própria segurança, elas são implantadas para proteger recursos de informação utilizados no funcionamento da organização e consequentemente protegem os objetivos da organização (PELTIER, 2005, p. XV)”.

Desse modo, as diretrizes desta política institucional serão classificadas segundo dimensões da Segurança da Informação, quais sejam: acesso à informação; classificação da informação; recursos tecnológicos; ambiente físico; modelo operativo da segurança da informação; conscientização e treinamento de usuários; e continuidade de negócio.

1. **Dimensão de Acesso a Informação**: A dimensão de acesso à informação dispõe sobre as regras e os controles necessários para o acesso seguro à informação, tanto no ambiente de tecnologia como no ambiente convencional, segundo as seguintes perspectivas:

    a. Gestão da Identidade – a identificação tem como propósito informar para o ambiente da informação quem é a pessoa que deseja acessá-lo. Esta identificação deverá ser individual, não poderá ser reutilizada por outra pessoa e deve ter uma ligação com o usuário, podendo ser o seu CPF, matrícula, nome e sobrenome ou outra característica, conforme o recurso tecnológico a ser utilizado;

    b. Gestão da Autenticidade – para determinar se o usuário que está se apresentando ao ambiente da informação é realmente quem alega ser, deverão ser utilizadas credenciais de acesso com adoção de senhas, as quais precisarão conter no mínimo seis caracteres, entre letras e números, e sua alteração deve ser realizada com periodicidade máxima de sessenta dias. O usuário poderá requerer a troca de senha sempre que julgar necessário e cabe ao mesmo ter consciência do uso da senha e seus controles, não podendo em hipótese alguma ceder suas credenciais de acesso a outra pessoa;

c. Gestor da Informação – para que a informação seja utilizada pelo usuário é necessário que haja uma autorização para tal. Sendo assim, cada informação deverá ter o seu gestor, o qual terá autoridade para negar ou liberar o acesso. O acesso à informação deve ser única e exclusivamente para o cumprimento de suas funções. O acesso deve ser revisado periodicamente pelo gestor e deve haver pelo menos uma pessoa alternativa ao gestor principal da informação;

2. **Dimensão Classificação da Informação** – A informação deverá ser classificada, quanto à confidencialidade, de acordo com o seu nível de importância para a cooperativa em termos de valor, requisitos legais, sensibilidade e criticidade.

Desse modo, o controle de acesso à informação tem por objetivo garantir que o acesso à informação seja disponibilizado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

O acesso às informações que não sejam classificadas como públicas deve ser restrito às pessoas que tenham necessidade de conhecê-las, e se submete a controles compatíveis com a sua classificação quanto à confidencialidade.

Para fins desta política as informações são classificadas em:

a. Públicas – informações de livre acesso, que podem ser divulgadas para o público em geral, a exemplo de usuários, clientes, organizações e prestadores de serviço;

b. Internas – informações que não possuem segredo de negócio e podem ser acessadas pelos usuários internos da Unimed Rio Branco;

c. Restritas – informações que possuem um nível de confidencialidade maior do que as informações internas e podem ser acessadas somente pelos usuários internos explicitamente indicados, em razão do cargo que ocupam ou área a qual pertencem;

d. Confidenciais – informações que possuem forte restrição de uso tendo, portanto, um nível de confidencialidade maior do que o das informações restritas, e somente podem ser acessadas por determinados usuários internos da cooperativa;

Caberá à Diretoria Executiva, por meio de ato normativo específico, definir a classificação de confidencialidade das informações e dos tipos de documentos existentes na cooperativa.
Os dados cadastrais e clínicos dos beneficiários não deverão divulgados por nenhum colaborador a não ser para o próprio beneficiário ou seu representante legal, para a Agência Nacional de

Saúde Suplementar (ANS) e demais órgãos de regulação, por força de decisão judicial, ou para setores internos da Operadora, a depender do contexto e da necessidade da informação, sabendo que, todas essas informações devem permanecer no contexto da operadora para garantir a segurança e a proteção da confidencialidade da informação clínica de seus beneficiários e de todos os dados pessoais que possam causar riscos ou danos, inclusive morais aos mesmos.

3. **Dimensão Recursos Tecnológicos** – Esta dimensão tem como objetivo apresentar as disposições acerca do uso dos recursos tecnológicos de maneira protegida e alinhada com o negócio. Para tanto, serão considerados aspectos relacionados ao controle de sistemas de informação, gestão de vulnerabilidades, auditoria de sistemas de informação e controles de rede, de acordo com as normas da ABNT (2013), e detalhados a seguir.

    a. Controle de sistemas de informação – as operações de instalação e atualização de sistemas de informação, bem como demais aplicativos e bibliotecas, só poderão ser realizadas por pessoas capacitadas e autorizadas pela Assessoria de Tecnologia da Informação (ASTI). Os sistemas utilizados pelos usuários devem conter somente os executáveis necessários para seu funcionamento, de modo que jamais devem estar disponíveis ao usuário seus instaladores ou códigos fonte. Os sistemas a serem implantados deverão ser testados com relação ao uso, segurança e efeitos sobre os demais sistemas existentes. Todos os sistemas e demais recursos tecnológicos a serem adquiridos deverão, obrigatoriamente, ser avaliados pela ASTI a fim de garantir a sua compatibilidade com a infraestrutura tecnológica disponível na cooperativa;

    b. Gestão de vulnerabilidade – os sistemas e demais aplicativos deverão ser frequentemente atualizados para a versão estável mais recente, de modo a evitar que vulnerabilidades já corrigidas pelo fornecedor venham a comprometer a segurança;

    c. Auditoria de sistemas de informação – os sistemas de informação utilizados na cooperativa deverão oferecer funcionalidades que permitam realizar a auditoria completa das ações realizadas nos mesmos, a fim de que possa ser possível determinar usuário, data, hora e ação realizada;

    d. Controle de rede – o controle do uso da rede corporativa, bem como de todos os recursos disponibilizados por meio dela, tem como objetivo assegurar a proteção e disponibilidade das informações. Para tal, deverão ser adotados mecanismos de auditoria que permitam monitorar efetivamente as atividades realizadas no

ambiente de rede. Não é permitido ao usuário obter, armazenar ou distribuir, por meio dos recursos de rede, arquivos, dados e informações que não estejam relacionadas às atividades desenvolvidas no âmbito da cooperativa. Uma vez detectados, os itens identificados serão imediatamente excluídos, não cabendo à cooperativa nenhuma responsabilidade sobre dados pessoais de seus funcionários, sem prejuízo de notificação ao superior imediato em relação à falta cometida;

4. **Dimensão Ambiente Físico -** O ambiente físico da informação precisa ser adequadamente protegido. Desse modo, é necessário que existam os seguintes controles:

    a. Acesso Físico – o acesso físico ao ambiente que possui recursos de informação deve ser restrito às pessoas que trabalham e utilizam esse ambiente ou, ainda, que tenham autorização expressa da Assessoria de Tecnologia da Informação para acessá-los. Devem ser utilizados crachás de identificação individual, vigilância presencial ou outros controles equivalentes. No caso específico das salas de equipamentos das unidades administrativas, deverá ser mantido um registro dos acessos realizados contendo: data, horário, pessoa e o motivo pelo qual o acesso foi realizado;

    b. Combate a incêndio – a cooperativa deverá possuir mecanismos de detecção e combate a incêndio;

    c. Instalações elétricas – as instalações elétricas devem ser mantidas em excelente padrão de qualidade de maneira a evitar situações que possam impedir o funcionamento da energia elétrica ou de funcionamento do ambiente;

    d. Treinamento de pessoas - as pessoas que utilizam o ambiente físico precisam ser treinadas para saber o que devem fazer diante de uma situação de incêndio para abandono do local, ou mesmo diante de um problema elétrico;

5. **Dimensão Modelo Operativo da Segurança da Informação -** o objetivo desta dimensão é estabelecer uma estrutura de gerenciamento para iniciar e controlar a implantação e operação da Segurança da Informação dentro da organização. Na Unimed Rio Branco essas atividades serão de responsabilidade do Comitê Gestor de Tecnologia da Informação (CGTI), o qual será responsável por:

    a. Definir os recursos humanos, papéis e responsabilidades: a cooperativa deverá definir o conjunto de pessoas que formarão o comitê e as áreas de atuação. O papel e a responsabilidade do comitê e das pessoas que o compõem precisam estar explicitados e formalizados para toda a organização;

b. Definição da forma de atuação: o CGTI pode atuar de maneira centralizada, descentralizada, mista ou de qualquer outra forma que a organização entenda. O fundamental é que esta definição de atuação esteja alinhada com o que a organização necessita e esteja formalizada para toda a organização. Na Unimed Rio Branco a área de atuação será mista, ou seja, atuará sempre com o auxilio da Diretoria Executiva;

c. Definição da estrutura organizacional: o CGTI precisa estar inserido formalmente na estrutura hierárquica da organização, devendo estar ligado à presidência;

d. Promover a gestão participativa: o modelo operativo da segurança da informação deve considerar o público que será diretamente impactado pelas ações da operacionalização dos controles, ou seja, qualquer controle a ser aplicado deverá ser analisado juntamente com quem será afetado por ele.

6. **Dimensão Conscientização e Treinamento de Usuários -** O objetivo principal desta dimensão é estabelecer critérios que devem ser satisfeitos a fim de garantir, por meio de iniciativas de conscientização e treinamento, que os usuários compreendam a importância de seguir os controles de Segurança da Informação. É responsabilidade da cooperativa orientar todos os funcionários e partes externas para que atendam as disposições desta política, assegurando a eles que:

a. Estejam adequadamente instruídos sobre as suas responsabilidades e papéis pela Segurança a Informação, antes de terem acesso às informações sensíveis ou aos sistemas de informação;
b. Recebam diretrizes que definam quais as expectativas sobre a Segurança da Informação de suas atividades dentro da cooperativa;
c. Sejam motivados para cumprir com as disposições da Política de Segurança da Informação;
d. Atinjam um nível de conscientização sobre Segurança da Informação que seja relevante para os seus papéis e responsabilidades dentro da organização;
e. Cumpram com os termos e condições de trabalho, incluindo as relacionadas à Política de Segurança da Informação da cooperativa;
f. Tenham as habilidades e qualificações apropriadas e sejam treinadas regularmente; e

g. Tenham disponível um canal de notificação de forma anônima para reportar violações às disposições desta política.

Para garantir que os itens acima especificados ocorram adequadamente, é necessário, ainda:

a. Considerar todos os tipos de usuários nas iniciativas de conscientização e treinamento, de modo a abranger funcionários, prestadores de serviço, estagiários, menor aprendiz, membros do conselho, diretores etc;
b. Planejar as ações de conscientização e treinamento de maneira estruturada, considerando usuários antigos e novos, considerando, ainda, a maneira de comunicação para com os diversos tipos de usuários, bem como o melhor aproveitamento possível das diversas mídias e meios de comunicação possíveis de serem utilizados pela organização;
c. Envolver a alta direção da cooperativa a fim de que seja evidenciado, explicitamente, o apoio às ações de treinamento e conscientização de usuários. O treinamento de novos funcionários deve ter sua abertura realizada por um gestor executivo da organização. Os treinamentos periódicos devem também de maneira criativa, mas contundente, deixar evidente que a direção da organização apoia estas iniciativas de treinamento porque quer que todos saibam o que deve fazer com a informação da organização e o que não pode ser feito.
d. Criar uma cultura de segurança para que a conscientização e a internalização dos controles de Segurança da Informação aconteçam de maneira efetiva. Vale lembrar que para criar essa cultura, é preciso a existência de um forte processo de Segurança da Informação, e do apoio da direção da organização e de profissionalismo com os controles de segurança.

7. **Dimensão Continuidade de Negócio** - O objetivo desta dimensão está em garantir que a cooperativa esteja preparada para enfrentar situações emergenciais de contingência que venham a comprometer a disponibilidade dos recursos de informação. Caberá à Assessoria de Tecnologia da Informação levar ao CGTI e, posteriormente à Diretoria Executiva, propostas que visem assegurar a manutenção da infraestrutura tecnológica mínima necessária para mitigar o risco de perda de informações e indisponibilidade de recursos, atentando ainda para os itens abaixo:

a. A cooperativa deve garantir que continuará operando mesmo que em condições de contingência ou desastre, criando para isto um plano de continuidade mantendo seus dados replicados em outra unidade administrativa;

b. A diretoria deve ter conhecimento do plano de continuidade, qual o escopo, ameaças contempladas, impacto aceito, soluções e tempo de recuperação;

c. O plano de continuidade deverá ser atualizado sempre que modificado;

d. O plano de continuidade deve ser testado e validado com periodicidade de pelo menos 180 dias;

É de responsabilidade da Diretoria Executiva manter a continuidade do negócio ao longo do tempo e para isto deve garantir a continuidade da informação.

Os prazos máximos de atendimento seguem a Resolução Normativa 323, art.3°:

VI – fixação de prazo máximo não superior a 7 (sete) dias úteis para resposta conclusiva às demandas dos beneficiários, sendo admitida a pactuação junto ao beneficiário de prazo maior, não superior a 30 (trinta) dias úteis, nos casos excepcionais ou de maior complexidade, devidamente justificados.

Este prazo será contato a partir da data de abertura da demanda, que será informado ao cliente juntamente com o número de protocolo.

Em caso de justificada impossibilidade de atendimento à demanda no prazo inicial, a Ouvidoria comunicará ao cliente as providências já adotadas, as razões de tal impossibilidade e o prazo adicional para resposta final.

OBRIGAÇÕES DO OUVIDOR

- Encaminhar às áreas responsáveis as notificações e, caso necessário, propor melhorias nos procedimentos, rotinas e normas, em decorrência da análise das reclamações recebidas.
- Mapear e acompanhar todas as notificações.
- Responder as notificações recebidas.

Elaborar relatórios para a Direção acerca da atuação da ouvidoria.

CANAIS DE OUVIDORIA

- Os clientes poderão contatar a Ouvidoria por:
- Correspondência para o endereço: Rua José de Melo, 418- Bosque.
- Ligação gratuita para o telefone 0800.0072.0045
- Site: http://www.unimed.coop.br – Fale Conosco

Presencialmente na sede da Unimed Rio Branco

CONSIDERAÇÕES FINAIS

Esta política foi aprovada pela Diretoria Executiva e amplamente divulgada entre os funcionários da cooperativa, através de treinamentos e divulgada no Sigquali.

CONTROLE HISTÓRICO
RN 323, ANS de 03 de abril de 2013.

INDICADORES - EFETIVIDADE	
INDICADOR	DESCRIÇÃO
81915	Cumprimento dos prazos de resposta da Ouvidoria para o cliente.
72376	Cumprimento do prazo de resposta das áreas para a Ouvidoria.

ITEM OBSOLETO	ATUALIZAÇÃO
Cabeçalho da política.	Revisão: 01 - 17/11/2016 • Atualizamos o modelo da política (cabeçalho)
Siglas e definições alteradas.	Inserimos mais siglas e as definimos: • **POL** – Política • **GPOU** – Gerência de processos de Ouvidoria • **RN** – Resolução Normativa • **ANS** – Agência Nacional de Saúde Suplementar
Não havia dados de indicadores.	• Indicador 81915 – Cumprimento dos prazos de resposta da Ouvidoria para o cliente. • Indicador 72376 – Cumprimento do prazo de resposta das áreas para a Ouvidoria. Informamos quais os instrumentos apropriados: • Formulário de registro presencial; • Planilha de demandas.