Segurança a cada clique!

Compartilhe essas dicas, proteja suas informações pessoais e da Unimed do Brasil

Unimed

SEGURANÇA DA INFORMAÇÃO

Uma responsabilidade de todos!

Segurança a cada clique!

Compartilhe essas dicas, proteja suas informações pessoais e da Unimed do Brasil

O que é essa cartilha?

É um material com informações e dicas práticas para você desenvolver hábitos seguros em ambientes físicos e digitais. Hábitos que precisam ser compartilhados por todos, por isso, sinta-se à vontade para dividir nossa cartilha com seus familiares e amigos.

Alguns descuidos com nossas informações podem trazer muitos prejuízos. Nosso objetivo é garantir que você conheça os perigos, se proteja dos riscos e compartilhe os ensinamentos aprendidos. Fazendo com que mais pessoas percebam a importância da segurança da informação no cotidiano.

Se houver alguma dúvida durante a leitura, não guarde para você! Entre em contato com a equipe de Segurança da Informação:
seginfo@unimed.coop.br

Índice

1

Por que precisamos falar sobre a **segurança dos dados?**

A segurança e proteção de dados coletados está cada vez mais virando uma necessidade, devido ao avanço tecnológico. Por essa razão a Unimed do Brasil, alinhada com a Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em agosto/2018 no Brasil, compromete-se com a proteção e segurança dos dados de seus colaboradores, clientes e parceiros de negócios.

Qual seu papel na **proteção de dados** da empresa?

Essa ação faz parte da nossa estratégia de proteção e garante que todos os colaboradores tenham conhecimento em como ter práticas seguras no dia a dia. O cuidado que cada um de nós passará a ter todos os dias no trato de informações é fundamental para a manutenção dos métodos e objetivos de defesa dos dados da instituição. Quando todos os colaboradores estão conscientizados, nossa empresa está mais segura.

Defesa dos dados deve ir **além da empresa**

Assuntos de casa no trabalho

Ferramentas de trabalho, só para trabalho: seu e-mail e outros recursos corporativos devem ser usados apenas para questões de negócio. Não cadastre seu e-mail corporativo em sites de e-commerces, por exemplo.

Caso seja convidado a realizar palestras, benchmarks, escrever artigos para públicos externos ou utilizar informações corporativas em trabalhos acadêmicos, obtenha antes a autorização de seu gestor imediato e/ou das áreas responsáveis pelas informações.

Assuntos do trabalho em casa

Não envie arquivos a um e-mail externo e nem utilize outras mídias de compartilhamento. Os documentos da cooperativa devem ser acessados somente nas ferramentas e dispositivos corporativos, durante o expediente de trabalho.

Você sabe o que é **Criptografia**?

Trata-se de um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la.

Você sabia que até mesmo uma pesquisa feita no Google utiliza o protocolo de criptografia HTTPS?

Conte sempre com a **Segurança da Informação**

É muito importante que todos os colaboradores se preocupem com a Segurança da Informação da Unimed do Brasil e do Sistema Unimed. Se no dia a dia surgirem dúvidas de como proceder, seja na instalação de softwares ou no compartilhamento de arquivos, entre em contato com a equipe de Segurança da Informação.

2

Mais que importante, **agora é uma questão de legislação**

O que é **LGPD**?

A Lei Geral de Proteção de Dados Pessoais (LGPD) chega para dar aos cidadãos maior controle sobre as informações compartilhadas em plataformas online e offline.

A LGPD possui aplicabilidade extraterritorial, com isso todas as empresas que tiverem negócios no Brasil, sejam elas públicas, privadas, nacionais ou estrangeiras, precisam se adequar à lei. A partir de agosto de 2020, data que a lei entrará em vigor, as companhias deverão estar aptas a informar, de maneira clara, quais dados possuem e o que fazem com eles.

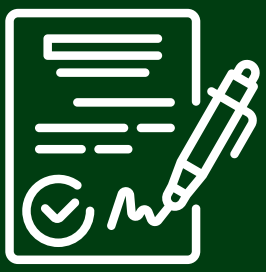
Se for comprovado um vazamento causado por negligência (como sistemas desatualizados ou senhas fracas), advertências e multas de até R$ 50 milhões (ou 2% do faturamento anual), a depender da gravidade do incidente, podem ser aplicadas.

Riscos de ter os **dados confidenciais vazados**

0 0 0 1 0 1 1 1 0 1 0 1 0 1 1 1 0 1 1 0 0 0 0 1 1 0 1 0 1 1 1 0 1 0 0 0 1 0 0 1 0 1 1 0 1 0 1
0 0 1 0 1 1 1 1 0 1 1 1 0 0 0 1 0 0 1 1 1 1 1 0 0 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 1 1 0 1 1 0
0 1 0 1 1 1 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 1 1 1 0 0 0 0 1 0 0 1 1 0 0 0 1 1 0 1 0 1 1 1 0 1 0 0
0 1 0 1 1 1 0 1 0 1 0 1 0 1 1 1 0 1 1 0 1 0 0 0 1 0 1 1 0 0 1 0 1 0 0 0 0 1 1 1 0 1 0 1 0 1 0

O vazamento de dados (data breach) ocorre quando a segurança do ambiente corporativo é comprometida e como consequência há a destruição, perda, modificação, retenção não autorizada ou acesso não autorizado aos dados pessoais de clientes, parceiros de negócios e/ou colaboradores. Você não gostaria de ter as informações por aí, sem sua autorização, certo? Por isso temos que ter o cuidado com as informações que trabalhamos.

De olho nos **termos de uso e privacidade**



Assim como em qualquer contrato, os Termos de Uso possuem muitas cláusulas e essas explicam quais são os direitos da empresa, o que elas poderão fazer com os seus dados caso aceitem os termos.

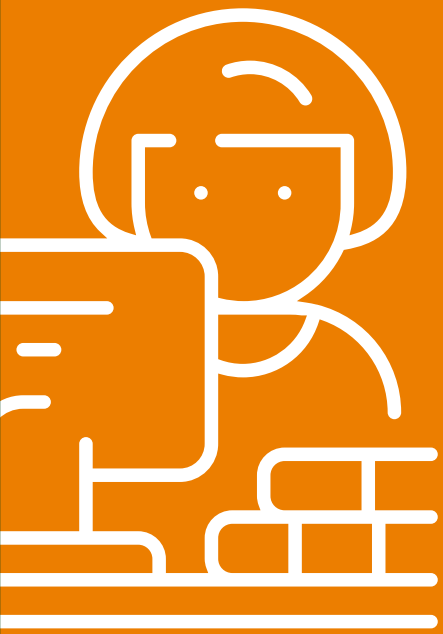
3

Protegendo a empresa no **ambiente físico**

O local de trabalho é um ambiente que possui muitas informações que vão desde aquelas que não trazem nenhum prejuízo à empresa até as mais sigilosas e que somente pessoas autorizadas podem ter conhecimento. É principalmente com as sigilosas que devemos ter uma atenção maior no dia a dia para garantir que estão devidamente seguras.

O cuidado começa **na sua mesa**

A primeira coisa a fazer na sua mesa é somente manter aquilo que é necessário para o seu trabalho. Menos é mais! Tudo o que não estiver sendo utilizado guarde em gavetas ou armários. E não deixe à mostra:



- Dados sigilosos, como papéis com senhas e logins ou aquela lista de ramais das áreas
- Documentos com informações de clientes
- Chaves de armários e gavetas
- Itens pessoais de valor, como carteira, chaves, celular e outros dispositivos

E continua em **seu computador**

Em geral, os computadores são bloqueados automaticamente após alguns minutos de inatividade, certo? Mas para ajudar ainda mais na segurança:

- Bloqueie a tela ao sair da sua mesa, mesmo que por um instante;
- Mantenha seu crachá sempre com você nas dependências da empresa e ao sair, guarde-o.

Dica para o trabalho e para vida pessoal: sempre fique atento aos curiosos, veja se há pessoas ao seu redor de olho no que você faz. Essa também é uma forma para descobrir suas informações e até para descobrir suas senhas.

Descarte seguro

Você já pensou que alguém pode vasculhar o lixo da empresa atrás de dados? Sim, isso pode acontecer. Por isso:

- Antes de jogar fora qualquer documento, veja se ele possui informações sigilosas ou se possui algum dado importante. Se possuir, use as fragmentadoras para descarte seguro.

- Em casa, não jogue no lixo faturas, cartões de crédito e outras correspondências que tenham dados sobre você. Rasgue o máximo possível antes!

Atenção aos locais de livre circulação

Salas de reuniões, corredores, hall de entrada e impressoras geralmente são locais que pessoas de fora também têm acesso. Então, é preciso ter bastante atenção com as informações que estiverem presentes nesses espaços:

- Não deixe folhas, anotações e qualquer outro dado nesses ambientes

E também com conversas...

Tudo é informação, então é preciso ter cuidado também com o que for conversado nos corredores da empresa ou em locais públicos. Dados podem ser vazados dessa maneira.

4

O futuro é online e também **seguro**

É justamente pela quantidade de dados que são gerados diariamente que o ambiente online é grande alvo de invasores. Por essa razão, precisamos nos preocupar com a proteção das informações digitais, estejam elas online ou offline, desde o seu momento de criação até seu descarte. Veja a seguir como você pode ajudar a Unimed:

Como usar com segurança minhas **contas e senhas?**

A senha é um dos meios de autenticação mais utilizados hoje em dia, com ela você assegura que realmente é o proprietário da conta e que possui o direito de acesso ao ambiente desejado. Por conta disso que é tão importante que só você saiba suas senhas, pois senão alguém pode:

Trocar/Alterar suas senhas de outras contas, impedindo que você consiga acessá-las

Acessar seu computador e utilizar sua identidade para realizar fraudes e outros ataques

Alterar a definição de privacidade de suas informações, expondo-as

Se passar por você nas redes sociais para colher informações de conhecidos

O que uma **senha segura** tem?

Os cibercriminosos são insistentes, uma das maneiras para descobrir uma senha é por meio da "tentativa e erro" e só há uma forma de se proteger disso: criando uma senha forte. Veja como nas dicas a seguir:

- Quanto maior, melhor. Assim, fica mais difícil de ser descoberta
- Misture letras maiúsculas e minúsculas, números e símbolos
- Se a senha só puder ter números, crie a ordem mais aleatória possível;
- Se possível, não utilize informações de sua vida pessoal como senha: exemplo, datas de aniversários, nomes de pessoas da família e números de documentos.

Cuidados com **e-mail**

Você já imaginou como seria trabalhar nos dias de hoje sem e-mail? Por conta da dependência que as empresas tem do e-mail, os criminosos criam vários golpes visando essa ferramenta. Afinal, ao invadir um conta de e-mail, um atacante pode:

Se passar por você e enviar golpes a outras pessoas

Pegar todo conteúdo compartilhado, salvo e recebido

Ter toda sua lista de contatos

É por isso que é importante que todos façam o **uso correto do e-mail**. Assim, jamais envie:

- Senhas e outros dados de cadastros
- Conteúdos, fotos ou vídeos que não tenham relação com seu trabalho
- Informações sensíveis sem a devida autorização
- E-mails com anexos ou links que sejam de fontes desconhecidas ou suspeitas
- Correntes

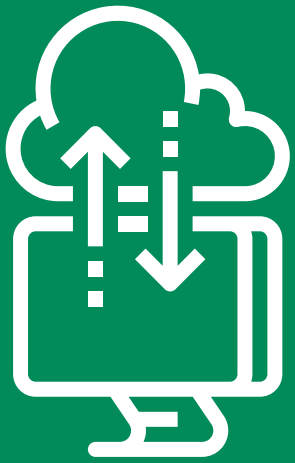
Lembre-se!

Você é responsável pelas informações enviadas pela Internet.

A Unimed do Brasil monitora todas as atividades realizadas pelos seus colaboradores!

Cuidados com **cloud**

Vai ficar nas nuvens? Fique com segurança. O Cloud computing, ou computação na nuvem, é uma forma prática de criar, armazenar e compartilhar documentos, onde tudo é feito on-line. Mas ela também exige cuidados. A UB não dispõe de cloud corporativa, mas para uso pessoal se atente:



- A privacidade dos documentos, principalmente quando forem informações sigilosas
- Ao compartilhar dados, veja qual é o acesso que está sendo liberado para outra pessoa (se pode visualizar, comentar ou editar)
- Realize sempre o backup das informações salvas na cloud para que não haja o risco de perdê-las
- Jamais compartilhe seus dados de cadastro (login e senha)

Cuidados com **backup**

Essa é uma etapa importante para a segurança. Por isso, não salve seus documentos apenas localmente em sua estação de trabalho. Utilize sempre o respectivo diretório de rede destinado ao seu departamento.

5

Você consegue **diferenciar um site falso de um seguro**?

Computadores e celulares também podem ser infectados se você acessar sites suspeitos. Geralmente, páginas seguras começam com HTTPS, um protocolo que criptografa as informações geradas na navegação.

Todo **cuidado** é necessário

Mas o HTTPS não é o único ponto a ser observado. Até porque, atacantes já utilizam esse protocolo em sites falsos para aumentar a credibilidade em seus golpes. Para garantir uma navegação segura, sempre observe se:

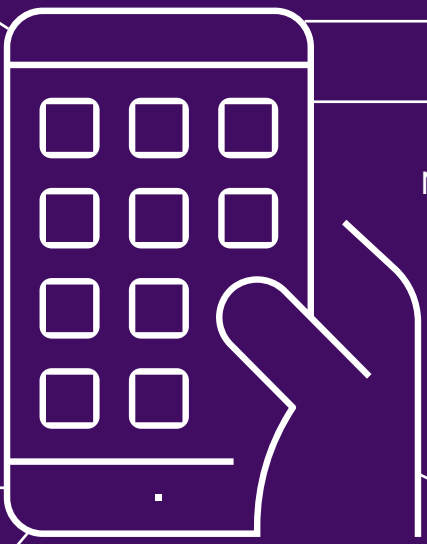
- Antes do endereço do site aparece um símbolo de cadeado
- O domínio está realmente correto, sem erros ortográficos
- Surgem pop-ups suspeitos na tela ou se downloads automáticos são realizados
- Pedem dados pessoais para liberar seu acesso

Ataques por links falsos são muito comuns, comece a prestar atenção aos caminhos que você percorre pela internet! Quando você cuida da sua proteção, também cuida da proteção da empresa.

De olho nos **aplicativos do seu celular**

Evite instalar aqueles que vêm de lojas externas e fontes desconhecidas

Somente baixe aplicativos que sejam oferecidos nas lojas oficiais, como a App Store ou a Play Store



Preste bastante atenção às permissões solicitadas de cada app para não fornecer acessos indevidos

No caso do Android, mantenha a opção de downloads de Fontes Desconhecidas desabilitada

Desconfie de aplicativos que fazem grandes promessas, como saber quem viu seu perfil no Facebook. Além de não cumprirem com o prometido, ainda podem roubar suas informações

Para limitar o acesso indevido ao seu celular e aumentar sua segurança, habilite o bloqueio de tela

De olho também nas **redes sociais**

As redes sociais são sites em que a navegação é livre e qualquer um pode ter acesso ao seu perfil, independente das coisas que podem ser vistas. Dessa forma, ter um comportamento seguro é essencial:

Não adicione pessoas que você não conheça

Evite conversar com desconhecidos e preste atenção ao que será dito

Não divulgue seus dados pessoais, seja nas publicações abertas, seja nas privadas

Evite informar sua localização

Não divugue dados de clientes, telas de computador, crachás, imagens (fotos ou vídeos) do ambiente corporativo ou qualquer coisa que ajude nos golpes direcionados

Cuidado com a superexposição em suas fotos. Dados bancários, códigos de barras, documentos pessoais, cartões de embarque, ingressos de eventos com código de barras ou QR Code devem ser evitados

Não deixe de ler a Diretriz Executiva DE.059 – Política de Segurança da Informação, disponível no sistema de documentação vigente da Unimed Brasil.

Caso queira conversar ou esclarecer dúvidas sobre qualquer assunto dessa cartilha, entre em contato com a equipe de Segurança da Informação:

seginfo@unimed.coop.br

ANOTAÇÕES

Alameda Santos, 1.827 – 10º andar
01419-909 – Cerqueira César
São Paulo, SP
Tel.: (11) 3265-4000
www.unimed.coop.br