CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO (SI)

Conhecimentos simples
e úteis no combate
a uma ameaça complexa

Unimed

Diretoria Executiva
Gestão 2021 – 2025

Omar Abujamra Junior – Presidente
Emilson Ferreira Lorca – Vice-presidente
Dilson Lamaita Miranda – Diretor de Administração e Finanças
Rubens Carlos de Oliveira Júnior – Diretor de Desenvolvimento de Mercado
Marcos de Almeida Cunha – Diretor de Gestão de Saúde
Silvio Porto de Oliveira – Diretor de Intercâmbio
Claudio Laudares Moreira – Diretor de Regulação, Monitoramento e Serviços

Coordenação
Odilon de Oliveira
Hanna Julia Silvério Queiroz
Celso de Almeida Polvora

Texto
Hanna Julia Silvério Queiroz
Celso de Almeida Polvora

Revisão
Área de Comunicação da Unimed do Brasil

Projeto gráfico e Diagramação
Área de Marketing da Unimed do Brasil

Realização

Alameda Santos, 1.827 – 10º andar – São Paulo/SP – Brasil – CEP 01419-909
Telefone: 55 11 3265 4000 – www.unimed.coop.br

Sumário

1. SEGURANÇA DA INFORMAÇÃO (SI): O QUE É?

Segurança da Informação é uma área do conhecimento cada vez mais relevante para as atividades de pessoas e empresas no mundo contemporâneo.

Com a crescente quantidade de informações disponíveis no mundo digital, a Segurança da Informação enfrenta hoje o desafio de manter a integridade, a segurança e o sigilo desses dados.

Assim, a Segurança da Informação é um corpo de conhecimentos e técnicas que se atualiza todos os dias, tornando necessária também a nossa atualização para acompanhar o ritmo das transformações.

Com ela, a proteção dos dados de clientes, colaboradores e parceiros passa a ser uma exigência legal, ocupando lugar central na estratégia de empresas privadas e órgãos públicos em torno da manutenção da privacidade dos dados das pessoas naturais.

Isso significa que, simplesmente por ter nascido e existir, toda pessoa tem o direito de ter a sua privacidade respeitada — das camadas mais superficiais às mais íntimas.

2. LGPD:UMA BREVE APRESENTAÇÃO

LGPD (Lei 13.709/2018 ou Lei Geral de Proteção de Dados Pessoais) é o resultado da iniciativa conjunta da sociedade civil e das Instituições do Estado Brasileiro, com o objetivo de se antecipar às ameaças dos novos meios digitais de comunicação, comércio e relacionamento.

Por isso, é importante que a Unimed crie uma Política de Segurança da Informação e uma Política de Privacidade e Proteção de Dados, focadas em atender às exigências estabelecidas na LGPD.

Na Política de Segurança da Informação, você tem acesso a direcionamentos mais técnicos — que devem ser seguidos à risca para garantir a segurança dos dados tratados.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação tem como objetivo estabelecer diretrizes e práticas para a proteção dos ativos de informação da empresa contra ameaças internas e externas. É nela que você encontrará os procedimentos corretos a adotar em cada caso.

Os esforços para a proteção dos dados tratados pelas Unimeds devem contar, sempre que possível, com o suporte de um time de Segurança da Informação. Mas lembre-se que a responsabilidade é de todos, colaboradores e departamentos que cumprem um papel importantíssimo nos esforços para fortalecer a resiliência em Segurança da Informação.

4. CREDENCIAL E SENHA DE ACESSO A SISTEMAS DE INFORMAÇÃO

As suas credenciais e senhas te identificam na Unimed e concedem acesso aos ambientes físicos, servidores, sistemas e dispositivos para a melhor execução do seu trabalho. Devido aos privilégios de acesso que suas credenciais e senhas garantem, protegê-las é um dos focos desta cartilha.

A maioria das tentativas de invasão a sistemas e roubo/interceptação de dados mira as credenciais e senhas como grandes "diamantes", pois tendo acesso às mesmas, é possível explorar diversas vulnerabilidades intrínsecas aos sistemas de informação — como a disponibilidade dos dados, por exemplo.

Não se trata aqui somente de segredos comerciais, mas de vidas: endereços das casas e numeração de documentos de clientes podem colocar vidas e famílias inteiras em risco, devendo realmente ser protegidas como o que são: um bem maior e estruturante da sociedade.

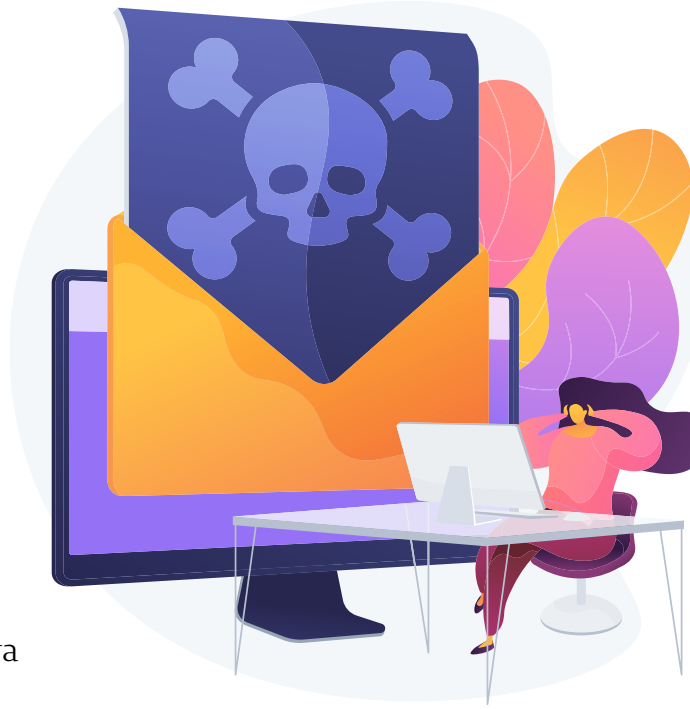
São vidas como a de quem escreve esse texto e a de quem o lê; vidas como as de quem contrata produtos e serviços e como as de quem trabalha para que eles sejam fabricados e entregues, girando as engrenagens da sociedade.

Por isso, proteger suas credenciais e senhas é fundamental.

5. PROTEÇÃO EM AMBIENTES FÍSICOS

A proteção dos ambientes físicos é uma preocupação para garantir a segurança de pessoas, ativos e informações, siga as recomendações abaixo:

- Nunca anote informações sigilosas em post-its;
- Guarde documentos em local seguro;
- Bloqueie o computador/ celular ao se afastar;
- Ao descartá-los, fragmente ou rasgue os documentos físicos até impossibilitar a leitura;
- Colocou o arquivo na lixeira do computador? Esvazie a lixeira em seguida;
- Ao descartar mídias removíveis, destrua-as até que sejam irrecuperáveis;
- Mantenha a posse exclusiva de suas credenciais;
- Evite conversar sobre assuntos de trabalho nos ambientes comuns da empresa e/ou fora dela.



6. SENHAS FORTES

Para criar senhas fortes, siga as recomendações abaixo:

- Misture números, letras (maiúsculas e minúsculas) e caracteres especiais;
- Utilize mais de 10 caracteres;
- Crie frases sem lógica e troque letras por números e caracteres especiais;
- Crie sempre uma senha nova e única para cada serviço;
- Evite padrões óbvios, como 'DPSP@123' ou 'Senha#2022';
- Ative sempre o duplo autenticação (também conhecida como autenticação em duas etapas/fatores).

7. USO DE DISPOSITIVOS MÓVEIS

O uso de dispositivos móveis deve ser feito sempre com muito cuidado. Por serem portáteis, há vários riscos básicos envolvidos que tocam o tema da Segurança da Informação:

- Sempre garanta a posse do seu dispositivo, evitando deixá-lo desprotegido sobre mesas em locais de livre acesso;
- Mantenha o seu dispositivo móvel sempre protegido contra impactos — lembre-se: qualquer acesso ao seu aparelho, mesmo que para reparos, é uma brecha possível para vazamentos de dados;
- Ative sempre o bloqueio automático de tela, garantindo que apenas você possa acessar o sistema operacional e os dados ali armazenados;
- Evite conceder acesso de terceiros ao seu dispositivo;
- Ative a geolocalização somente quando necessário — e lembre sempre de desativá-la após o uso;

- Nunca use o seu dispositivo para receber arquivos desnecessários ou acessar conteúdo alheio às funções desempenhadas, minimizando o risco de infecções e vazamentos.

8. GOLPES E FRAUDES

O conhecimento qualificado é a vacina contra falhas de Segurança da Informação.

As diferentes modalidades de golpe não se limitam ao telefone, e-mail, whatsapp, redes sociais e websites, mas podem ocorrer também em bares, restaurantes e outros locais públicos, com os ataques de engenharia social sendo cada vez mais sofisticados, eficazes e difíceis de detectar.

Como evitar os golpes mais comuns através de:

- E-mails: não abra mensagens de destinatários desconhecidos, verifique se há erros de português no texto (caso comum em golpes) ou imagens;
- Arquivos: não faça download de documentos desconhecidos e evite os downloads automáticos;
- Instruções: jamais siga cegamente as instruções contidas em e-mails, procurando sempre confirmar a procedência da mensagem e a identidade de remetente (tem sido comum a clonagem de endereços corporativos);
- Links: nunca clique em links suspeitos, mesmo que de fontes confiáveis.

9. REDUZINDO RISCOS AO NAVEGAR PELA INTERNET

Aprenda a diferenciar sites falsos de sites seguros. Como os dois são muito parecidos visualmente, algumas dicas podem te ajudar na identificação:
Verifique a URL: veja se o endereço do site é o correto. Algumas pequenas diferenças podem ser fáceis de ignorar, como "go0gle.com.br" ao invés de "google.com.br", por exemplo.

Pesquise: se estiver em dúvida, pesquise o site que você quer no Google. Os sites verdadeiros costumam aparecer no topo dos resultados, enquanto os falsos têm dificuldade para serem validados pelo buscador;

Verifique a segurança: se a conexão for segura, o endereço do site começará com "https://". Além disso, o navegador exibirá um pequeno cadeado logo ao lado do endereço do site.

Acesse somente endereços necessários às rotinas de trabalho e utilize dispositivos separados para o uso pessoal e o uso profissional.

10. PHISHING

Phishings são mensagens falsas enviadas amplamente por e-mail, chats e outros meios. A palavra é uma derivação de *Fish* ("Peixe", em Inglês) e tenta passar o espírito do golpe: "pescar" dados enganando pessoas com iscas que pareçam atrativas.

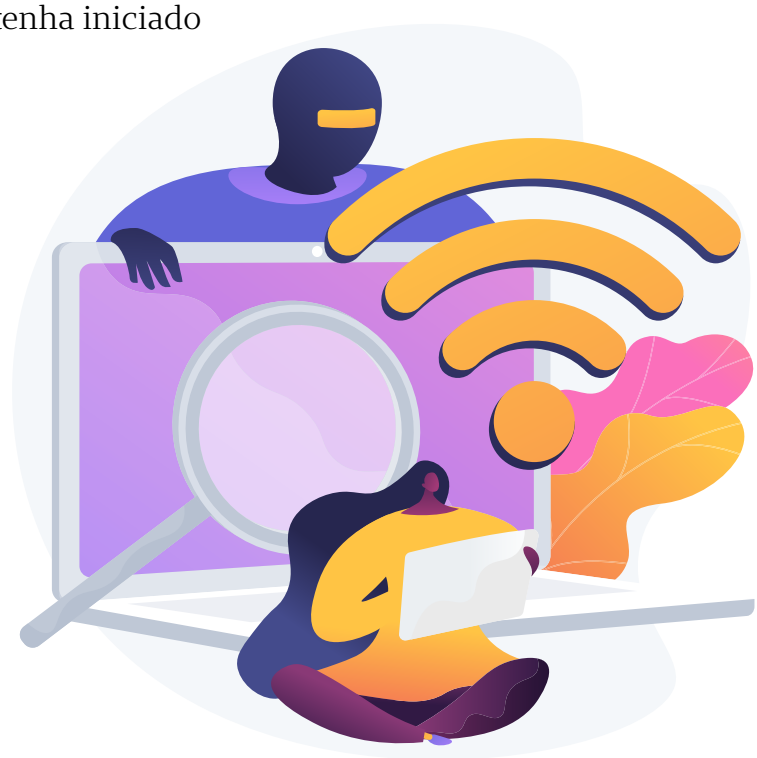
Por essa característica, o *phishing* está sempre em transformação, ora oferecendo uma grande viagem de Natal com um desconto bom demais para ser real, ora oferecendo ingressos gratuitos para show, teatros e filmes, com tudo pago, em troca do cadastro dos dados do seu cartão de crédito "apenas para confirmar a sua identidade".

O que pode ocorrer caso você caia em um phishing:

- Roubo de identidade para uso em outros golpes;
- Vazamento de dados sensíveis;
- Invasão a sistemas e dispositivos;
- Paralisação das atividades e prejuízos financeiros.

Como se proteger:

- Não clique em links contidos em mensagens de remetentes desconhecidos;
- Verifique a identidade do remetente;
- Nunca realize downloads sem a certeza de que são seguros;
- Evite fornecer dados e informações solicitados por aplicativos de mensagens ou ligações telefônicas sem que você tenha iniciado o contato.



11. COMO REPORTAR INCIDENTES

Caso testemunhe incidentes de Segurança da Informação, entre em contato imediatamente com o time responsável pela Segurança da Informação da sua Unimed. O tempo é o fator mais importante em eventos dessa natureza, muitas vezes fazendo a diferença na proteção dos dados.

Caso os eventos ocorram em sua vida íntima — como senhas vazadas ou informações íntimas expostas —, é fundamental que você troque as suas senhas e, se julgar necessário, comunique às autoridades, registrando boletim de ocorrência caso se trate de crime previsto em lei.

Agradecemos pela sua atenção até aqui. Esperamos que esta cartilha seja útil na proteção dos dados e informações da Unimed.

Em caso de dúvida ou ocorrências ligadas a SI, procure a equipe de **SEGURANÇA DA INFORMAÇÃO**!

Para mais dicas sobre Segurança da Informação, fiquem atentos às dicas que a Unimed do Brasil envia mensalmente.

Unimed
Brasil

Alameda Santos, 1827 – 10º andar – Cerqueira César
01419-909 – São Paulo – SP – Tel: (11) 3265-4000
www.unimed.coop.br