SEGURANÇA DA INFORMAÇÃO CONTÁBIL

DICAS PARA RESGUARDAR OS DADOS DO SEU ESCRITÓRIO E DE SEUS CLIENTES

75 anos CRCSC

Nossas conexões fazem história

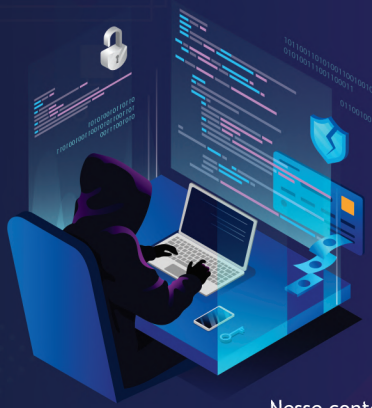
SUMÁRIO

INTRODUÇÃO

Aperfeiçoar a segurança das informações é uma medida estratégica para toda e qualquer tipo de organização, sendo uma prática fundamental para mitigar os riscos de violações quanto ao vazamento de dados, de modo a resguardar a imagem da organização e assegurar o bom funcionamento dos negócios.

Diante desse contexto, verifica-se, ainda, que as organizações que não se adequarem às diretrizes da LGPD – Lei Geral de Proteção de Dados – estarão mais suscetíveis a incidentes de segurança envolvendo dados pessoais.

Dado a relevância do assunto e seus reflexos na atuação profissional, o Conselho Regional de Contabilidade de Santa Catarina (CRCSC) elaborou o presente material contendo informações úteis sobre a tecnologia e suas aplicações no meio empresarial, com dicas voltadas especialmente às organizações contábeis, visando garantir a segurança adequada dos seus dados e de seus clientes.



NOVAS TECNOLOGIAS, NOVOS RISCOS

O avanço exponencial das tecnologias da informação provocou profundas transformações na sociedade nesses últimos tempos, sendo um dos principais fatores que mudaram o cenário social na procura pela melhoria e pela facilitação da vida e das práticas dos indivíduos, tornando-se essencial no desenvolvimento socioeconômico em nível global.

Contudo, apesar das vantagens proporcionadas, tais avanços tecnológicos requerem investimento em segurança, inclusive por parte das organizações contábeis, de modo a preservar a confidencialidade e a integridade das informações da organização e,sobretudo, de seus clientes.

Nesse contexto, observa-se que o nosso país tem sido alvo frequente de ataques cibernéticos a empresas, fato esse comprovado em um levantamento conduzido pela empresa de consultoria alemã *Roland Berger*, divulgado recentemente em reportagem do Estadão[1], o qual aponta que o Brasil é um dos principais alvos globais de ciberataques, demonstrando a fragilidade e vulnerabilidade nas redes digitais atuais.

O fato de as empresas do segmento contábil estarem conectadas à rede mundial de computadores eleva consideravelmente os riscos de violação de dados e informações confiadas ao profissional da contabilidade pelo seu cliente, principalmente quando não se estabelece um conjunto adequado de controles, políticas, procedimentos e boas práticas relacionadas à segurança da informação.

[1] *Estadão: "Brasil já é o 5º maior alvo global de ataques de hackers a empresas". 12/09/2021. Disponível em: https://economia.estadao.com.br/noticias/geral,brasil-ja-e-o-5-maior-alvo-global-de-ataques-de-hackers-a-empresas,70003837632 Acesso em: 24 set. 2021.*

PILARES DA SEGURANÇA DA INFORMAÇÃO

Cabe destacar que a segurança da informação se baseia principalmente em três pilares às quais a organização deve manter quanto aos dados, aos sistemas e à infraestrutura tecnológica:

1 CONFIDENCIALIDADE

Este princípio visa garantir que a informação estará disponível apenas para quem dela fizer uso, ou seja, impede que a informação esteja disponível a terceiros sem prévia autorização.

Para que se possa assegurar a confidencialidade, as organizações devem adotar medidas preventivas, como por exemplo, estabelecer o acesso às informações apenas para as pessoas devidamente autorizadas.

2 INTEGRIDADE

A integridade está atrelada ao conceito de preservar todas as informações originais armazenadas em um ambiente seguro, garantindo que nenhuma interferência externa irá corromper ou danificar os dados.

Assim, toda informação deve ser mantida em condição igual a que foi disponibilizada pelo seu proprietário, sem que haja modificação indevida.

3 DISPONIBILIDADE

Já a disponibilidade significa que a informação deve estar disponível para ser usada por quem necessita, ou seja, tal princípio garante o acesso à informação sempre quando solicitado, em conformidade com os requisitos de disponibilidade.

Dessa forma, mesmo que se tenha um alto nível de proteção, os dados devem ser de fácil acesso àqueles que estão autorizados a consultá-los.

Uma vez que não é possível prever incidentes relacionados à violação na segurança de dados, faz-se necessário que as empresas assegurem a proteção das informações contra acessos não desejados, disponibilizando-as no momento adequado e de maneira confiável. Assim, ter o conhecimento sobre esses três aspectos que formam a tríade da segurança da informação serve de alicerce para a implantação das melhores práticas e políticas de prevenção à proteção de dados, como forma de assegurar a confidencialidade, integridade e disponibilidade dos ativos em relação às mais variadas ameaças.

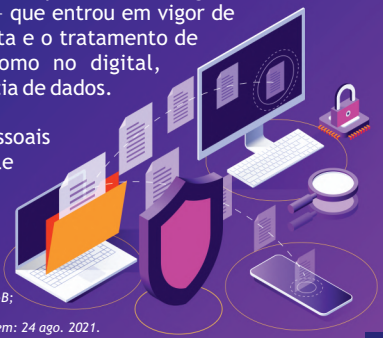
ADEQUAÇÃO DA LGPD ÀS ORGANIZAÇÕES CONTÁBEIS

Dada a rapidez do desenvolvimento da tecnologia e da dinâmica das mudanças nos mercados de produtos e serviços, a informação vem se revelando como um dos principais ativos dentro de uma organização, tendo em vista que está relacionada de forma direta com os processos organizacionais, na criação dos negócios e na tomada de decisão em todos os níveis de planejamento operacional, tático e estratégico.

Nesse sentido, é essencial que se desenvolva um conjunto de políticas de segurança da informação, com a implementação de boas práticas e comportamentos a serem adotados por toda a organização, como forma de prepará-la para um eventual ataque, seja de origem interna ou externa.

A partir das mais variadas ocorrências de vazamentos de dados, foi sancionada em nosso país, em 14 de agosto de 2018, a Lei n.º 13.709 – conhecida como Lei Geral de Proteção de Dados (LGPD) – que entrou em vigor de forma escalonada[2],sendo um dispositivo legal que veio para regulamentar a coleta e o tratamento de dados pessoais, incluindo os dados sensíveis, tanto no ambiente físico como no digital, representando, assim, um marco no que se refere ao uso, à proteção e à transferência de dados.

A LGPD foi idealizada com o enfoque de fornecer mais segurança às informações pessoais coletadas e armazenadas em todo o território nacional, o que garante maior controle dos cidadãos acerca das suas informações pessoais.



[2] Lei n.º 13.709, de 14 de agosto de 2018, estabelece em seu Art. 65 que: "Art. 65. Esta Lei entra em vigor: I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e I-A - dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos". Disponivel em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 ago. 2021.

LGPD

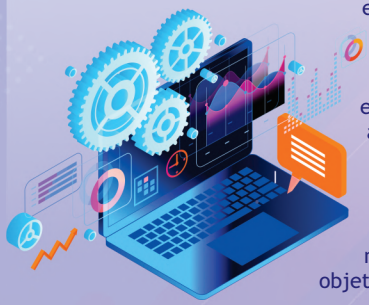
Importante ressaltar que as sanções às transgressões à LGPD já estão em vigor desde o dia 1º de agosto desse ano, podendo variar de advertências até multas que podem chegar ao montante de R$ 50 milhões por cada infração cometida, o que poderá inviabilizar as operações dos negócios para as empresas que negligenciarem a necessidade de adoção de medidas de segurança para o tratamento adequado dos dados pessoais.

Com a vigência da referida lei, as organizações contábeis precisam se adequar o quanto antes às novas regras, buscando garantir maior segurança e confiabilidade acerca dos dados e informações.

Assim, nota-se que as **organizações que possuem uma boa política de segurança da informação consequentemente estão mais próximas da conformidade com a LGPD**.

BOAS PRÁTICAS NA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Na atualidade, a Tecnologia da Informação – comumente conhecida pela sigla TI – tornou-se uma grande aliada dos ambientes corporativos, em especial, das organizações contábeis, facilitando a realização dos registros contábeis e o gerenciamento das atividades empresariais, proporcionando melhorias na operacionalização dos serviços e no atendimento aos clientes, sendo um recurso vital para a sobrevivência das empresas.



Para que uma organização se mantenha competitiva no mercado contábil, com a maximização da eficiência dos seus processos, é necessário que esteja atenta a todas as tendências a fim de criar uma boa infraestrutura de TI.

Nesse sentido, é preciso esclarecer que a segurança em TI consiste em criar estratégias de segurança eletrônica que buscam inibir, classificar e responder a acessos não autorizados a ativos da organização que exijam soluções de informática para poder acessá-las.

Ressalta-se, ainda, que as informações são ativos preciosos para as organizações, sendo primordial prover meios que garantam a sua proteção, a fim de que se possa mitigar os vazamentos, perdas ou ação de pessoas mal-intencionadas, que tenham o objetivo de furtar, destruir ou modificar os dados para fins ilícitos.

As organizações precisam assegurar a integridade das informações que estão sob sua responsabilidade, evitando danos à imagem da empresa que possam prejudicar seus negócios. Por isso, preparamos algumas dicas de boas práticas de TI que podem ser implementadas por qualquer organização, de acordo com as suas necessidades:

DOCUMENTE SEU TI

É fundamental que seja realizada a descrição da estrutura de rede, mantendo sempre atualizado o inventário dos equipamentos de informática e licenças de *software* e etc.

ELABORE INSTRUÇÕES DE TRABALHO DAS ROTINAS E PROCEDIMENTOS

Realize instruções de trabalho das rotinas e procedimentos importantes de modo que as informações não fiquem centralizadas junto ao setor de TI.

ESTABELEÇA UMA AGENDA DE MANUTENÇÃO PREVENTIVA

A manutenção preventiva caracteriza-se por ser uma ação contínua de controle e monitoramento de computadores, bem como de outros dispositivos semelhantes, objetivando antever e impedir problemas que não permitam o bom funcionamento tanto na parte de *hardware* (partes, peças e demais acessórios), quanto na de *software* (sistemas e aplicativos). Assim, o ideal é que se tenha um calendário de manutenção preventiva com visão de curto, médio e longo prazos, para ser aplicada em *hardware*, incluindo limpeza de poeira interna, troca de pasta térmica, limpeza de contatos dos componentes (memória e/ou placa de vídeo quando existente); e em *software*, englobando cuidados com as atualizações dos sistemas operacionais, limpeza de arquivos, de cache dos principais navegadores, entre outros procedimentos.

RESERVE UM ESPAÇO PARA OS EQUIPAMENTOS

É importante que a organização tenha uma área reservada para alocar seus servidores, *nobreaks* e outros equipamentos que compõem a estrutura de *Data Center*.
Considere segurança, boa refrigeração, condições de organização e espaço para realizar as devidas manutenções.

MANTENHA UMA CONFIGURAÇÃO MÍNIMA DAS MÁQUINAS

Mantenha uma configuração mínima das máquinas de forma que suporte as aplicações utilizadas.

DEFINA UMA JANELA DE MANUTENÇÃO

Estabeleça uma janela de manutenção, com a definição de datas e horários, para que a equipe de TI faça melhorias e correções nos sistemas do escritório. Em tempos de pandemia, geralmente as equipes não possuem um horário fixo de trabalho por estarem em teletrabalho, fato esse que dificulta a realização dos procedimentos de manutenção.

UTILIZE OS ANTIVÍRUS E *FIREWALLS* ATUALIZADOS

Por meio do *firewall* é que passa todo o tráfego de dados originados da *internet*, sendo um item básico de segurança para as redes de computadores. Assim, procure manter antivírus e *firewalls* atualizados, bem como busque navegar e efetuar o *download* de arquivos por meio de *sites* confiáveis.

AVALIE TERCEIRIZAR A EQUIPE DE TI

Entende-se que a terceirização ou *outsourcing* de TI implica em transferir de forma total ou parcial a função de TI para um fornecedor externo, de modo que a gestão da infraestrutura, bem como a equipe de profissionais fica a cargo da empresa prestadora do serviço. Além da manutenção da estrutura interna, deve ser avaliada a contratação de uma empresa terceirizada, já que o *outsourcing* de TI proporciona inúmeras vantagens para a organização contábil, tais como: aumenta a eficiência dos serviços de TI; reduz custos; auxilia nas ações de segurança; gera maior foco nos negócios; dentre outros benefícios.

CRIE POLÍTICA DE SENHAS

Para evitar o vazamento de dados e informações, faz-se necessário que a organização estabeleça uma política de senhas e oriente seus funcionários a criar combinações que dificultem a ação de invasores de sistemas. A equipe de trabalho deve procurar não utilizar senhas óbvias e fáceis de serem descobertas, já que os cibercriminosos têm facilidade para identificar os dados e decodificar as credenciais de acesso, principalmente em razão da difusão das informações pessoais nas redes sociais.

VIRTUALIZE OS SERVIDORES

Entende-se que a virtualização de servidores consiste na técnica de execução de múltiplos sistemas operacionais virtuais interdependentes em apenas um servidor físico. Dentre as vantagens dos servidores virtuais, podemos citar: redução de custos em espaço físico, energia e pessoal; maior segurança em relação às informações sensíveis; manutenção e suporte simplificado. Além disso, a aplicação de servidores virtuais proporciona maior produtividade entre a equipe de Tecnologia da Informação, o que gera ganho de tempo, agilidade e eficiência para a equipe de TI, possibilitando a realização de outras tarefas mais produtivas.

DEFINA UMA POLÍTICA DE *BACKUP*

Para que se tenha uma proteção de dados eficiente é de suma importância que se estabeleça uma política de *backup*, que é um documento onde são registradas todas as decisões a respeito do armazenamento dos dados corporativos.
Dessa forma, deve ser definida uma política de *backup* para que a rotina ocorra de forma segura e seja aplicada nos servidores, sistemas de contabilidade, dados e e-mails. Nesse tipo de procedimento é importante considerar os seguintes elementos: periodicidade; formato (em disco ou *cloud*); redundância; guarda (prazo e local); capacidade de armazenamento e agilidade na recuperação dos dados.

UTILIZE APENAS *SOFTWARES* LICENCIADOS OU DE CÓDIGO ABERTO

Nas organizações contábeis, assim como em qualquer outra empresa ou entidade, é necessário que se utilize apenas softwares licenciados – que recebem autorização do fornecedor para sua utilização – ou de código aberto (*open source*) – que são livres para qualquer usuário sem a necessidade da compra de uma licença.

ADOTE UMA POLÍTICA DE DESCARTE DE EQUIPAMENTOS

A organização deve avaliar o estado dos seus equipamentos ao estabelecer critérios de desfazimento de bens de informática quando estes estiverem ociosos e/ou obsoletos. Nesse sentido, defina e aplique uma política descarte de equipamentos, com atenção especial aos discos rígidos (*HDs*) com dados salvos.

ADEQUE SUA EMPRESA À LGPD E INVISTA NA SEGURANÇA DA INFORMAÇÃO

As organizações contábeis que ainda não se adaptaram à LGPD devem fazê-lo de imediato, considerando que a lei já está em vigor, bem como devem realizar investimentos em segurança da informação.

IMPLEMENTE UM SERVIÇO DE *HELP DESK*

A implantação de um serviço de *help desk* permite centralizar o recebimento de demandas, otimizando o tempo de respostas e a resolução de problemas de baixa complexidade. Com essa ferramenta é possível gerenciar e controlar os chamados e criar uma base de conhecimento. Nesse caso, considere a gestão de mudanças, o inventário de ativos, *software* e licenças.

CRIE UM COMITÊ DE INOVAÇÃO MULTIDISCIPLINAR

A constituição de um comitê de inovação multidisciplinar possibilita obter ganhos no processo de tomada de decisão, além da integração com membros de outras áreas funcionais da organização, bem como na gestão de recursos. Uma das principais contribuições do comitê é a de permitir o gerenciamento do TI com o intuito de buscar soluções em RPA (*Robotic Process Automation*), AI (*Artificial Intelligence*), integração etc.

ESTABELEÇA UM ORÇAMENTO ANUAL PARA O TI

Apesar de não ser uma prática usual nas organizações contábeis, definir um orçamento anual para o TI ajuda o gestor na hora de realizar o planejamento e o estabelecimento de prioridades das ações para o alcance dos objetivos propostos.

PROTEJA A SUA REDE *WI-FI*

Uma conexão *wireless* em um ambiente corporativo está sujeita a entrada de invasores ou de pessoas não autorizadas quando não se tem os devidos cuidados com a segurança da informação. Nesse sentido, algumas pequenas ações são importantes para proteger sua rede, tais como: utilize uma senha forte e conexão com encriptação dos dados; modifique as configurações padrão do roteador utilizado pela empresa, ao alterar a senha de acesso ao painel de configurações do aparelho; e mantenha um *firewall* ativo como forma de assegurar a integridade da rede *Wi-Fi*. Além disso, a criação de *voucher* temporário de acesso é uma ferramenta necessária para o monitoramento dos visitantes da rede, já que nessa situação, quando a rede de internet está aberta, os dados inseridos no sistema ficam expostos de forma vulnerável a ações maliciosas.

DISPONIBILIZE OS DADOS EM NUVEM

Avalie a disponibilidade de realizar o armazenamento de dados, documentos, e aplicativos em nuvem. Esse recurso vem sendo amplamente difundido nos últimos tempos, inclusive entre as organizações contábeis, sendo uma solução eficiente para a realização do trabalho de forma remota. Esse tipo de ferramenta proporciona inúmeros benefícios à empresa, como por exemplo: aumento da eficiência do trabalho; redução dos custos das operações; segurança dos dados; entre outros.

CONSIDERAÇÕES FINAIS

Ao longo do tempo a profissão contábil vem se modificando graças à otimização da produtividade disponível por meio dos recursos tecnológicos, sendo uma eficiente ferramenta de auxílio no trabalho do profissional da contabilidade. Contudo, tais avanços trouxeram à tona questões importantes no que se refere à segurança da informação no âmbito contábil.

Nesse cenário, o investimento em segurança digital na contabilidade precisa ser tratado como um elemento prioritário e estratégico, como forma de resguardar os dados do escritório e dos seus clientes, assim como propiciar um ambiente mais seguro às áreas de atuação profissional.

Cabe lembrar que é um dever do profissional da contabilidade, conforme consta na NBC PG 01 – Código de Ética Profissional do Contador –, guardar sigilo sobre o que souber em razão do exercício da profissão, ressalvados os casos previstos em lei ou quando solicitado por autoridades competentes. Portanto, é imprescindível que o profissional adote medidas de segurança da informação na contabilidade de modo que assegure o sigilo profissional, como forma de respeitar a confidencialidade das informações obtidas em decorrência de relações profissionais e comerciais.

Assim sendo, o CRC de Santa Catarina, por meio desse trabalho, cumpre seu propósito de levar conhecimento de forma clara e objetiva à toda classe contábil catarinense, contribuindo na promoção do exercício ético e qualificado da profissão.

EXPEDIENTE

Projeto e Redação:
Contador **Carlos Vinícius Gonçalves** (CRCSC-036778/O-7)
Design gráfico:
Ana Cláudia Antunes Vallejos

DIRETORIA EXECUTIVA – BIÊNIO 2020/2021

Rúbia Albers Magalhães
Presidente

Raquel de Cássia Souza Souto
Vice-Presidente Câmara de Administração e Finanças

Ranieri Angioletti
Vice-Presidente Câmara de Fiscalização, Ética e Disciplina

Hermeliano de Oliveira
Vice-Presidente Câmara de Registro

Adriano de Souza Pereira
Vice-Presidente Câmara de Controle Interno

José Mateus Hoffmann
Vice-Presidente Câmara de Desenvolvimento Profissional

Roberto Aurélio Merlo
Vice-Presidente Câmara Técnica

Marcello Alexandre Seemann
Vice-Presidente Institucional e de Relação com os Profissionais

CÂMARA DE REGISTRO

TITULARES	SUPLENTES
Hermeliano de Oliveira	Ivan Gabriel Coutinho
Édio Silveira	John Kennedy Lara da Costa
Solange Rejane Schroder	Bruna Linzmeier
Péricles de Oliveira Borges	Gislei Hemsing
Cassiano Bambinetti	José Carlos de Souza

CÂMARA DE ADMINISTRAÇÃO E FINANÇAS

TITULARES	SUPLENTES
Raquel de Cássia Souza Souto	Marcelo Burg
Adilson Pagani Ramos	José Carlos de Faveri
Édio Silveira	José Carlos de Souza

CÂMARA DE CONTROLE INTERNO

TITULARES	SUPLENTES
Adriano de Souza Pereira	Neusa Ivete Muller
John Carlos Zoschke	Tadeu Pedro Vieira
Guilherme Corbellini	Vladimir Arthur Fey
Hermeliano de Oliveira	Ivan Gabriel Coutinho
Valdeci Sagaz	Luiz Ricardo Espíndola

CÂMARA DE DESENVOLVIMENTO PROFISSIONAL

TITULARES	SUPLENTES
José Mateus Hoffmann	Marlise Alves Silva Teixeira
Adilson Bachtold	Asdir Elton Kratz
Marcos Alexandre Emilio	Daniela Zimmermann Schmitt
Adriano de Souza Pereira	Neusa Ivete Muller
Maria Denize H. Casagrande	

CÂMARA TÉCNICA

TITULARES	SUPLENTES
Roberto Aurélio Merlo	Marcia Regina Mendes da Silva Dias
Cassiano Bambinetti	Walmor Mafra
Péricles de Oliveira Borges	Valdecir José Nunes da Silva

CÂMARA DE ÉTICA E DISCIPLINA

TITULARES	SUPLENTES
Ranieri Angioletti	Marcelo Machado de Freitas
Sérgio da Silva	Giselle Varela Serpa
Marcos Alexandre Emilio	Valdecir José Nunes da Silva
Adilson Bachtold	Asdir Elton Kratz
Solange Rejane Schroder	Bruna Linzmeier
Maria Denize Henrique Casagrande	
José Mateus Hoffmann	Marlise Alves Silva Teixeira
John Carlos Zoschke	Tadeu Pedro Vieira
Raquel de Cássia Souza Souto	Marcelo Burg
Roberto Aurélio Merlo	Márcia Regina Mendes da Silva Dias
Guilherme Corbellini	Dayana Fernandes da Silva
Ilário Bruch	John Kennedy Lara da Costa

CÂMARA DE RECURSOS DE ÉTICA E DISCIPLINA

TITULARES	SUPLENTES
Ilário Bruch	Marcelo Machado de Freitas
Marcos Alexandre Emilio	Daniela Zimmermann Schmitt
Ranieri Angioletti	Walmor Mafra
Adilson Pagani Ramos	José Carlos de Faveri
Sérgio da Silva	Giselle Varela Serpa
Valdeci Sagaz	Luiz Ricardo Espíndola

CÂMARA DE RECURSOS DE FISCALIZAÇÃO

TITULARES	SUPLENTES
Ilário Bruch	Marcelo Machado de Freitas
Marcos Alexandre Emilio	Daniela Zimmermann Schmitt
Ranieri Angioletti	Walmor Mafra
Adilson Pagani Ramos	José Carlos de Faveri
Sérgio da Silva	Giselle Varela Serpa
Valdeci Sagaz	Luiz Ricardo Espíndola

75 anos CRCSC — Novas conexões fazem história

FICHA CATALOGRÁFICA

Conselho Regional de Contabilidade de Santa Catarina

Segurança da Informação Contábil: dicas para resguardar os dados do seu escritório e de seus clientes / Conselho Regional de Contabilidade de Santa Catarina. Florianópolis: CRCSC, 2021.
19 p.

Publicação online.

1. Segurança da Informação. 2. Contabilidade. 3. Lei Geral de Proteção de Dados. I. Título.

CDU 657:004.056.53

Ficha Catalográfica elaborada pelo Bibliotecário Leandro Pinheiro CRB-14/1340

SEGURANÇA DA INFORMAÇÃO CONTÁBIL

75 anos CRCSC

Nossas conexões fazem história