ibgc instituto brasileiro de governança corporativa

Papéis e Responsabilidades do Conselho na Gestão de Riscos Cibernéticos

Pocket book

orienta

Introdução

Esta publicação tem por objetivo ser um guia rápido em referência ao IBGC Orienta "Papéis e Responsabilidades do Conselho na Gestão de Riscos Cibernéticos". Desse modo, este documento pretende, de forma prática e ágil, informar e preparar o conselheiro (e demais agentes de governança) para navegar no contexto de incertezas relacionadas ao risco cibernético, permitindo assim maior capacitação para exercer a diligência neste tema dentro das empresas em que atua.

O primeiro capítulo é dedicado à governança na gestão de riscos cibernéticos e versa sobre o papel de cada agente de governança em busca da resiliência cibernética. No segundo capítulo, é traçado um panorama sobre os ataques cibernéticos na atualidade. O terceiro capítulo aponta aspectos práticos da gestão de riscos cibernéticos. Por fim, são dispostas reflexões e um *checklist* que podem auxiliar o conselheiro de administração na abordagem do tema.

Espera-se, por meio desta publicação, possibilitar maior entendimento de todos os espectros que envolvem o risco cibernético e os caminhos a serem adotados para a mitigação desse risco.

Capítulo 1
Governança na gestão de riscos cibernéticos

"Risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais.".

(International Organization of Securities Commissions. Cyber Security in Securities Markets – An International Perspective Report on IOSCO's cyber risk coordination efforts, 2016.)

Um incidente de segurança de informação pode acarretar perdas relevantes para uma empresa.

- Perda e/ou exposição de dados estratégicos ou confidenciais;
- Perda no valor da empresa;
- Perda de receita;
- Roubo de propriedade intelectual;
- Ameaças à vida ou à segurança;
- Danos à reputação;
- Perda de clientes;
- Interrupção nas operações;
- Sujeição a multas e litígios; e
- Geração de custos de diversas naturezas para reparação de danos.

Como minimizar o risco cibernético?

Para minimizar o risco cibernético, as empresas podem recorrer a várias soluções físicas, tecnológicas, humanas e processuais, mas, por se tratar de um evento externo, muitas empresas já estão buscando o seguro de riscos cibernéticos a fim de minimizar seus impactos.

A falha humana está relacionada ao sucesso de muitos dos ataques cibernéticos. Por causa disso, a promoção da cultura de segurança cibernética dentro de uma empresa é essencial.

A Gestão de Riscos aplicada à segurança da informação é uma medida importante e, quando efetivamente implementada, é capaz de trazer múltiplos benefícios:

- aumenta a compreensão e o comprometimento (*awareness and commitment*) das pessoas em relação ao papel e responsabilidade de cada indivíduo na gestão do risco da informação e nas práticas de segurança dele;
- protege os ativos, dados, informações e conhecimento;
- protege a imagem e a reputação das empresas;
- valoriza a empresa diante de parceiros, clientes, bancos, seguradoras e mercado em geral;
- propicia a continuidade do negócio em momentos de estresse operacional e crises;
- viabiliza o cumprimento de leis e regulamentações aplicáveis;
- aprimora a governança corporativa;
- contribui para a perenidade e sustentabilidade da empresa.

O risco cibernético vem galgando degraus no ranking de riscos mais prováveis a que as empresas estão sujeitas. Em pesquisa realizada pelo Fórum Econômico Mundial, o roubo e a fraude relacionados a dados ocuparam o quarto lugar como o risco mais provável nos próximos dez anos, e os ataques cibernéticos capazes de causar interrupção das operações ou infraestrutura aparecem em quinto lugar.

O papel do conselho de administração (CA)

Cabe ao conselho liderar a conscientização e o comprometimento em relação à resiliência cibernética. O conselho desempenha papel fundamental ao garantir o alinhamento da estratégia do negócio com a estratégia de segurança da informação. No desempenho de suas atribuições, o CA deve atentar às seguintes tarefas sobre a temática, e também executá-las:

Tarefas dos conselheiros de administração:

- compreender os riscos cibernéticos integrados e inerentes aos negócios da organização;
- garantir o alinhamento da estratégia do negócio com a estratégia de segurança cibernética;
- contribuir para a definição dos ativos críticos da empresa;
- ratificar o apetite a riscos da companhia em relação a riscos cibernéticos;
- aprovar a política de segurança da informação corporativa e seu efetivo modelo de governança;
- acompanhar a evolução na maturidade do ambiente de segurança cibernética da companhia;
- supervisionar a implantação da cultura voltada para a promoção da segurança cibernética;
- obter conhecimento interno ou buscar orientação externa de especialistas em riscos cibernéticos;
- informar-se sobre planos de crise e contingência para lidar com ataques cibernéticos, aprová-los e monitorá-los;
- participar de simulações periódicas sobre crises cibernéticas.

Algumas dicas que podem ajudar no entendimento da governança de riscos cibernéticos:

- A compreensão e avaliação do grau de maturidade em segurança da informação e cibernética da empresa deve ser o passo inicial.
- O modelo das três linhas do Instituto do Auditores Internos (IIA) tem sido utilizado pelas organizações para delimitar os papéis, responsabilidades e interações entre os diferentes agentes no que diz respeito à gestão de riscos, na qual se inclui a gestão do risco cibernético.
- O CA deve levar em consideração o porte, setor de atuação e estrutura da organização.
- O importante é que haja um responsável pela gestão dos riscos cibernéticos, e que ele seja qualificado para exercer essa atividade.
- O responsável pela segurança cibernética deve ser independente da função de Tecnologia da Informação e dotado de autonomia para supervisionar, monitorar, escalar e comunicar sobre qualquer tema relacionado a riscos cibernéticos e à qualidade da resiliência cibernética da organização.

Capítulo 2

Os ataques cibernéticos e as leis

Como os alvos dos ataques são escolhidos? E quais as consequências para as empresas?

Os alvos são escolhidos com base na motivação que o criminoso cibernético tem em relação à empresa. Essa motivação pode ser a de destruir, expor, modificar, roubar ou ter acesso a um ativo ou a de usá-lo sem autorização, visando prejudicar ou obter vantagens para si ou terceiros. As consequências para as empresas podem ir desde prejuízos financeiros a sérios danos a sua reputação e imagem, com o potencial de levar a empresa a sua extinção com um único evento.

Como os criminosos entram nas organizações? E que técnicas utilizam?

As técnicas mais utilizadas pelos criminosos são negação de serviços (ou ataque de força bruta), interceptação, engenharia social (agravada com a digitalização dos serviços), roubo de credenciais (incluindo senhas), manipulação de dados em sistemas e aplicação de *malwares* (*software* malicioso). Essas técnicas podem ser utilizadas de forma isolada ou de forma conjunta, dependo da complexidade e da engenhosidade do criminoso cibernético. Adiciona-se a essas técnicas a utilização de infiltração de criminosos nas empresas, seja diretamente ou por meio de aliciamento de colaboradores (oferecendo benefícios em dinheiro ou outros tipos de vantagens) ou ainda por ameaça à integridade de colaboradores ou de algum ente da sua convivência.

Proteção de dados pessoais e segurança cibernética

A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil, estabelece uma série de responsabilidades das empresas no que se refere à proteção de dados pessoais sigilosos. A Lei estabelece obrigações e penalidades que podem chegar a 2% do faturamento, limitadas a R$ 50 milhões por evento de infração.

Os criminosos cibernéticos e suas motivações

Os criminosos cibernéticos podem ser classificados em várias categorias: grupos terroristas com pautas ligadas a questões ideológicas; organizações criminosas (crime organizado); criminosos em busca de obtenção de vantagens (em geral ligadas às questões financeiras)... Um dos principais motivadores desses criminosos para cometer atos ilícitos é a possibilidade de obter êxito na sua ação sem ser identificado ou sem ter os seus bens retidos. Isso é possível por causa do aparato sistêmico de muitos deles para camuflar a sua identidade e geolocalização e, no que se refere ao recebimento de benefícios financeiros, devido ao uso de criptomoedas, que permite transferências e utilização de forma anônima.

Onde as empresas falham?

As empresas falham em questões gerenciais, como a ausência ou ineficácia de processos, procedimentos e controles que poderiam minimizar o risco de ser vítima de um ataque. Alguns exemplos dessas falhas são lapsos em atualizações de seus sistemas (*patch management*), gestão ineficiente de acessos, não rastreamento das informações e não observância da gestão de segurança da informação aplicada a fornecedores e parceiros são alguns exemplos.

Atualmente a indagação sobre o ataque cibernético não é "Se" e sim "Quando"... portanto não é uma questão de evitar o ataque e sim de preparar a empresa para ser resiliente, responder rapidamente ao incidente e ser capaz de manter e/ou restabelecer as suas operações.

Exemplos

Escopo impróprio

Incluem sistemas primários e esquecem dos secundário

Falha na atualização de sistemas

Falta de atualização de vulnerabilidades

Falha na gestão de acesso

Deficiência no processo de concessão, revogação de acesso

Falha na gestão de identidade (senhas)

Falha ao alterar as configurações padrões de fornecedores

Redução de escopo

Redução de escopo nas verificações de segurança

Falha no armazenamento de dados

Falha ao rastrear onde os dados estão armazenados

Falha na medição da eficácia da segurança cibernética

Ausência de indicadores de performance e supervisão

Gestão dos integrantes da cadeia de valor

Deficiência na gestão de acessos de terceiros aos dados e informações

Fonte: Preparado pelos autores

Capítulo 3

Aspectos práticos da gestão de riscos cibernéticos

Por onde começar?

O primeiro passo é fortalecer a conscientização e o comprometimento de todos em relação às práticas de segurança da informação e, a partir daí, realizar uma autoavaliação para conhecer o nível de maturidade da empresa no que diz respeito à gestão de segurança da informação, em que está inserido o risco cibernético.

A avaliação do modelo de maturidade permitirá que organização possa documentar, comunicar e programar melhorias no seu modelo.

Qual o nível de maturidade da organização em relação às práticas adotadas de governança corporativa?

Para efeito de gerenciamento de riscos cibernéticos, podemos dizer que as organizações podem ser classificadas em quatro estágios ou níveis de maturidade quanto à segurança da informação:

Parcial	Risco informado	Repetitivo	Adaptativo
Processo de informação *ad hoc* ou reativo. As prioridades de segurança da informação não são relacionadas aos riscos ou objetivos de negócio.	Processo de gestão dos riscos de segurança da informação é aprovado, mas não estabelecido por toda a organização.	Gestão do risco de segurança da informação é formalmente aprovada e formalizada por política. As práticas são relacionadas aos objetivos de negócio.	Processo de gestão de riscos de segurança da informação é continuamente aprimorado e incorpora as melhores práticas de mercado.

Em complemento, todo conselheiro deve conhecer também a norma ISO 27002:2015. Ela não é técnica e aborda a governança e processos de segurança da informação de forma abrangente.

Ciclo de ações na gestão de riscos cibernéticos

Para estabelecer ou aprimorar o programa, uma das alternativas é utilizar a estrutura proposta pelo National Institute of Standards and Technology (NIST), órgão do Departamento de Comércio dos Estados Unidos, que traz diretrizes sobre a segurança cibernética.

A estrutura é baseada em cinco conjuntos de temas, pilares ou "domínios" de ações que estruturam a gestão de risco cibernético: **Identificar, Proteger, Detectar, Responder e Recuperar**.

Fonte: NIST Cybersecurity Framework Core components. Source: National Institute of Standards and Technology (2018) – Version 1.1

Metodologia Bowtie

A metodologia Bowtie desenvolve uma maneira esquemática e simples de descrever e analisar os caminhos de um risco, desde as suas causas até as suas consequências e impactos.

A figura a seguir apresenta um exemplo prático do risco referente a ataques cibernéticos.

Contexto do risco cibernético (visão Bowtie)

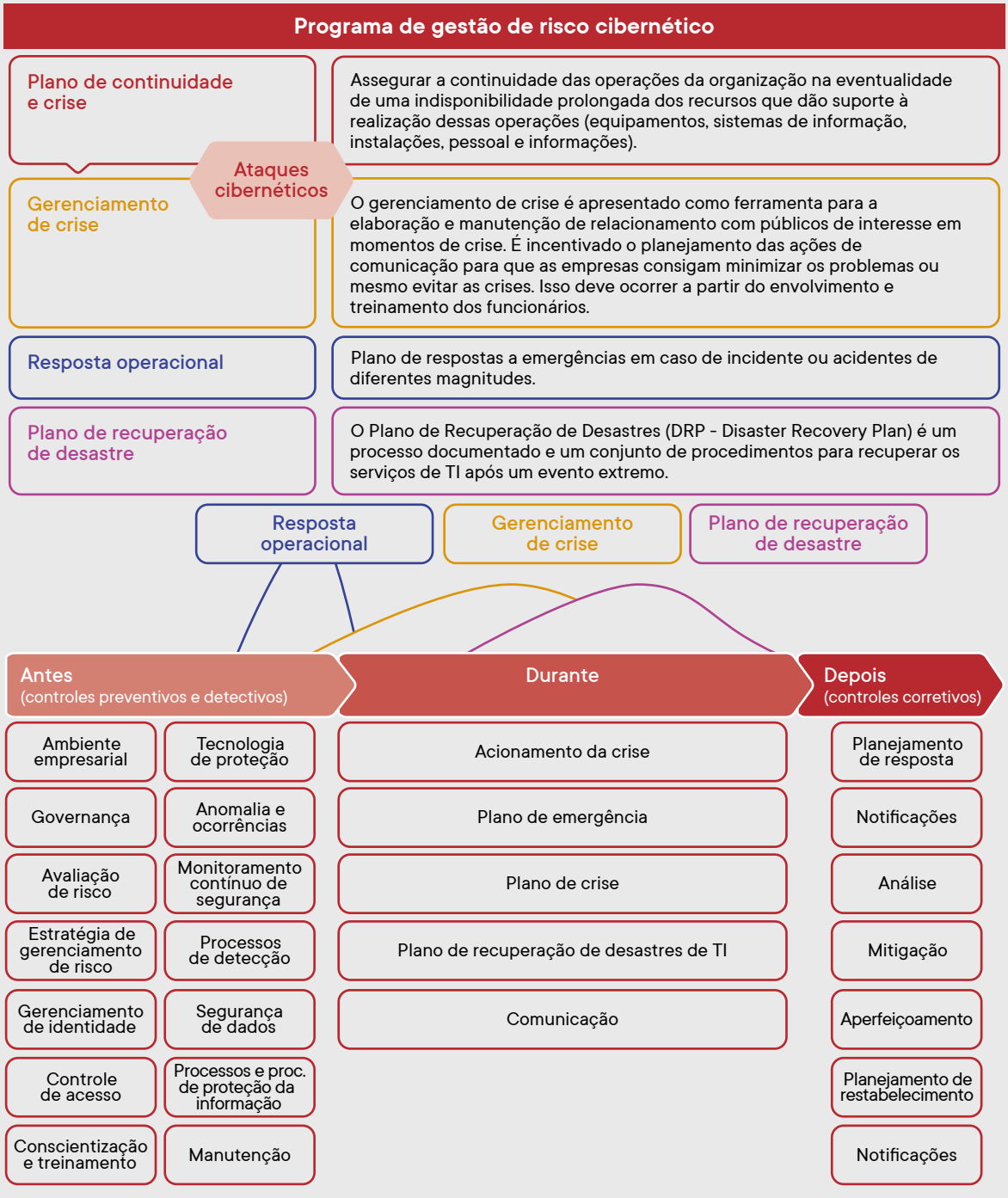
Ações				Ações
Controles preventivos	**Causas** Fato gerador do evento de riscos	**Ataques cibernéticos**	**Impactos** Consequências diretas e indiretas	**Controles corretivos**
• Ambiente empresarial; • Governança; • Avaliação de risco; • Estratégia de gerenciamento de risco; • Gerenciamento de identidade; • Controle de acesso; • Conscientização e treinamento; • Segurança de dados; • Processos e procedimentos de proteção da informação; • Manutenção; • Tecnologia de proteção; • Anomalias e ocorrências; • Monitoramento contínuo de segurança; • Processos de detecção.	• Escopo impróprio; • Falha ao atualizar sistemas regularmente; • Falha ao encerrar o acesso; • Falha ao identificar e alterar as configurações padrão do fornecedor; • Redução do escopo; • Falha ao rastrear onde os dados são armazenados; • Falha na medição da eficácia da segurnaça cibernética; • Desconsideração dos integrantes da cadeia de valor.	Risco cibernético (*) refere-se aos potenciais resultados negativos associados a ataques cibernéticos que, por sua vez, podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais. Um incidente envolvendo riscos cibernéticos inclui, mas não se limita a isto: negação de serviços, interceptação, engenharia social, *phishing* e o próprio malware ou software malicioso, entre outros.	• Perda e/ou exposição de dados estratégicos ou confidênciais; • Perda no valor da empresa; • Perda de receita; • Roubo de propriedade intelectual; • Ameaças à vida ou à segurança; • Danos à reputação; • Perda de clientes; • Interrupção nas operações; • Sujeição a multas e litígios; • Geração de custos de diversas naturezas para reparação de danos.	• Planejamento de resposta; • Notificações; • Análise; • Mitigação; • Aperfeiçoamento; • Planejamento de restabelecimento; • Notificações.

Programa de gestão de risco cibernético

Fonte: Preparado pelos autores

Programa de gestão de risco cibernético

A figura a seguir apresenta uma visão de um programa de gestão de risco cibernético que envolve 4 dimensões: (i) Plano de continuidade e crise; (ii) Gerenciamento de crise; (iii) Resposta operacional; e (iv) Plano de recuperação de desastre. Traz também uma visão sobre um evento de risco cibernético antes, durante e depois de materializado.



Fonte: Preparado pelos autores

Reflexões sobre a gestão de riscos cibernéticos

- Quanto a organização pretende “gastar” para ter “conformidade” ou investir para ter segurança?
- O que a organização deseja proteger e em que ela vai aplicar a Segurança da Informação? Por exemplo, em um processo, em uma área; em um ou mais processos e áreas; um ambiente de desenvolvimento e aplicações?
- A organização precisa de certificações corporativas, ou apenas aderência às práticas globais de Segurança da Informação? Por exemplo, PCI DSS, ISO27001...
- Os processos de sua organização estão aderentes às legislações de proteção de dados e segurança cibernética, tais como LGPD, Marco Civil da Internet?
- Qual o envolvimento de fornecedores e parceiros no processo de gestão dos riscos cibernéticos? Quais as expectativas e exigências dos clientes? Quais práticas seu negócio realmente precisa para funcionar e ter diferenciais comerciais?
- A organização está discutindo adequadamente questões de longo prazo, tanto internas quanto externas, para se manter competitiva e na vanguarda no contexto da transformação digital?
- O conselho de administração vem se preparando para enfrentar um cenário de crise e resposta a incidente?
- A organização definiu e testou o plano de gestão de crise relacionado à gestão de um incidente de risco cibernético?

Checklist do conselheiro de administração

Governança na gestão de riscos cibernéticos

- ☑ Definir papéis e responsabilidades da gestão de riscos cibernéticos da companhia (baseado no Modelo das Três Linhas do IIA), atentar para a independência do responsável pela segurança cibernética
- ☑ Promover a discussão, revisão e monitoramento do apetite a riscos alinhado à estratégia da companhia.
- ☑ Entender e supervisionar os fatores que influenciam a cultura de gestão de riscos cibernéticos.
- ☑ Discutir e aprovar as diretrizes das políticas de segurança cibernética.

Os ataques cibernéticos e as leis

- ☑ Supervisionar os indicadores de segurança cibernética.
- ☑ Entender e acompanhar o atendimento às leis de proteção de dados e segurança cibernética.

Aspectos gerais da gestão de riscos cibernéticos

- ☑ Acompanhar a evolução na maturidade do ambiente de segurança cibernética da companhia.
- ☑ Identificar os *frameworks* adotados pela empresa (NIST, PCI DSS, COBIT, ISO/IEC Standards, NERC, TY Cyber, COSO, HITTRUST CSF).
- ☑ Promover a discussão da contratação de seguro para riscos cibernéticos.
- ☑ Entender o envolvimento de fornecedores e parceiros no processo de gestão dos riscos cibernéticos.

Aspectos práticos da gestão de riscos cibernéticos

1. Identificar

- ☑ Checar a existência do mapeamento de ativos críticos.
- ☑ Definir a estratégia da gestão de risco desses ativos.

2. Proteger

- ☑ Entender o ambiente de controles para proteção a riscos cibernéticos.

3. Detectar

- ☑ Entender e supervisionar a capacidade da companhia na detecção de incidentes cibernéticos
- ☑ Estabelecer um processo de monitoramento contínuo de segurança.

4. Responder

- ☑ Entender e supervisionar a capacidade da companhia na resposta a incidentes cibernéticos.
- ☑ Conhecer e monitorar os planos de crise e de contingência para lidar com ataques cibernéticos.
- ☑ Supervisionar a implantação dos planos de ação para a promoção da segurança cibernética.

5. Recuperar

- ☑ Entender o planejamento, as melhorias e o processo de comunicação em caso de recuperação dos serviços ou operações afetados pelo ataque.

Considerações finais

A gestão do risco cibernético deve ser uma preocupação constante dos conselheiros de administração, uma vez que ela tem implicações na sustentabilidade das empresas.

Ao conselho, cabe supervisionar a gestão de riscos cibernéticos e a salvaguarda dos ativos da empresa, evitando perdas de todos os tipos e danos à reputação. Sempre consciente de que a gestão de riscos cibernéticos é parte da segurança da informação, que por sua vez deve estar inserida e alinhada às práticas de gestão de riscos da organização.

A resiliência cibernética, trazida por uma boa gestão dos riscos cibernéticos, contribui para que a empresa tenha mais segurança e qualificação para promover inovações e utilizar novas tecnologias.

Portanto, a gestão de riscos cibernéticos deve estar permanentemente em pauta para que possa ser aprimorada e enfrentar novas táticas usadas pelos perpetradores de ataques.

Referências bibliográficas

COSO (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION). Enterprise Risk Management – Integrating with Strategy and Performance: Executive Summary. Junho 2017.

IBGC (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA). Papéis e responsabilidades do Conselho na Gestão de Riscos Cibernéticos. São Paulo, IBGC, 2019 (série IBGC Orienta).

IIA (INSTITUTE OF INTERNAL AUDIT). Modelo das três linhas do IIA 2020: Uma atualização das três linhas de defesa. Julho 2020. Disponível em: <https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20072020131817.pdf>. Acesso em: 14 jan. 2022.

IOSCO (INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS). Cyber Task Force: Final Report. 2019. Disponível em: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf>. Acesso em: 14 jan. 2022.

ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION). Norma ISO/IEC 27.000:2018.

___. Norma ISO 31000:2018. Disponível em: <https://pt.scribd.com/document/371084773/Visualize-a-Nova-NBR-ISO-31000-2018-Gestao-de-RiscosDiretrizes?secret_password=Ff3Uz4g4D67be76tXreX#fullscreen&from_embed>. Acesso em: 14 jan. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. Framework for Improving Critical Infrastructure Cybersecurity. 2018. Disponível em: <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 >. Acesso em: 14 jan. 2022.

Créditos

Esta publicação foi desenvolvida por grupo de trabalho (GT) composto por membros da comissão de Gerenciamento de Riscos Corporativos do IBGC (em ordem alfabética): Corinto Lucca Arruda, Fernando Nicolau F. Ferreira, Flavia Melo, Luciana Bacci, Marcelo Toniolo, Marcos Assi e Mercedes Stinco.

Acesse a publicação completa, pelo QR code ou clique aqui

Este pocket book foi publicado em fevereiro/2022