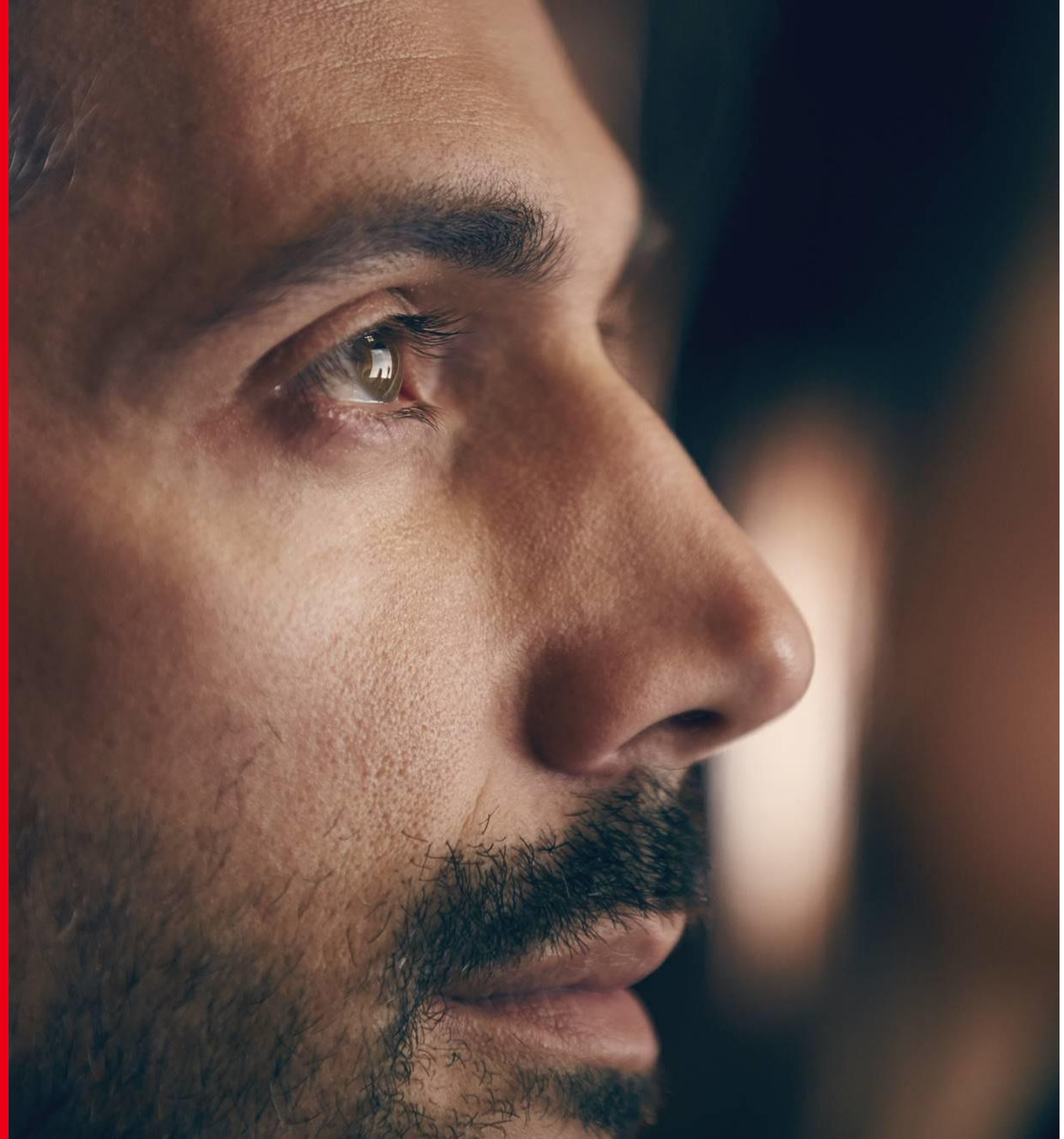
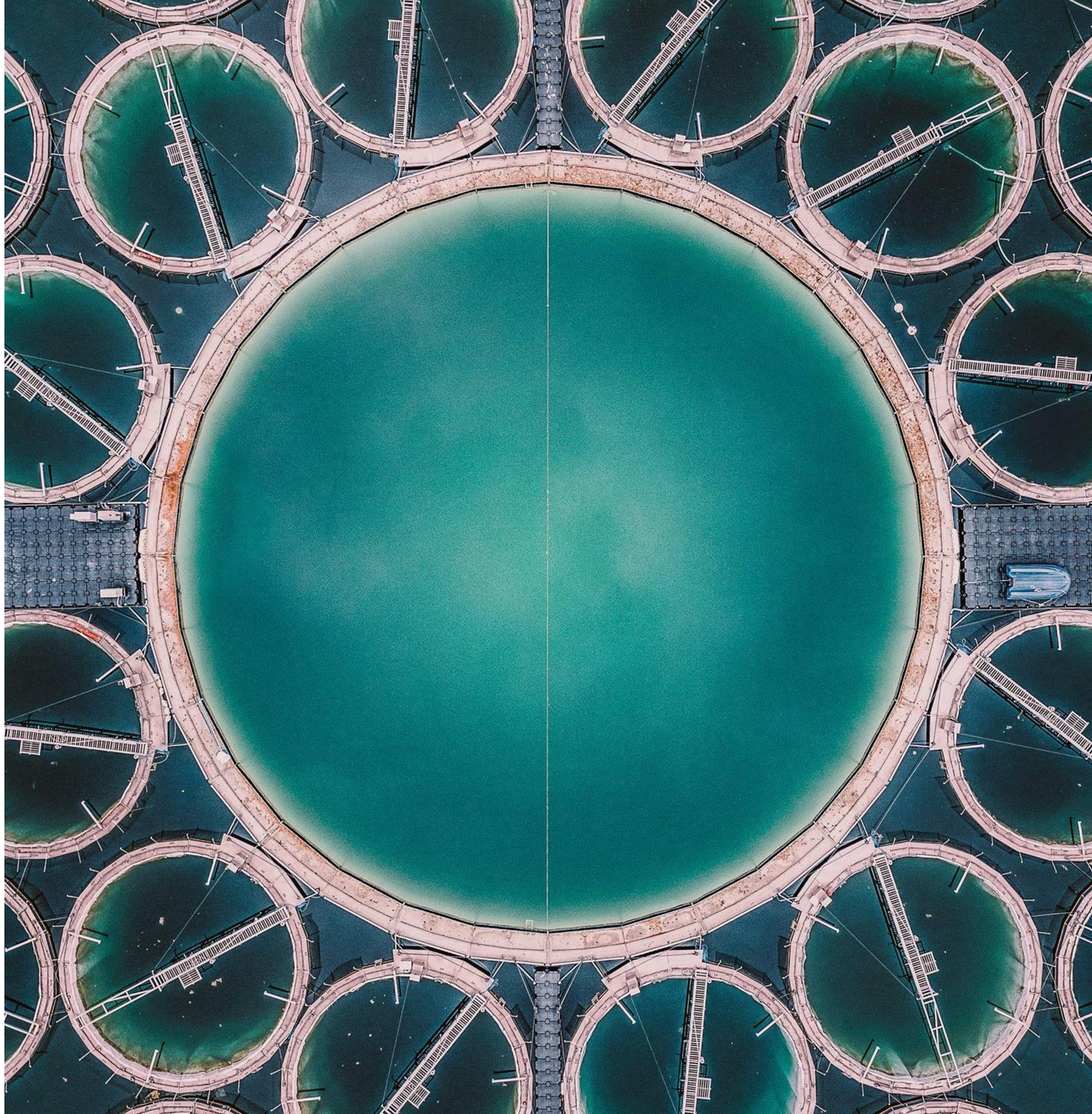


Avaliação de Fornecedor por Aon Global Risk Consulting

Avaliação: Sinqia Scafplustnet
Para: Unileverprev

Sumário



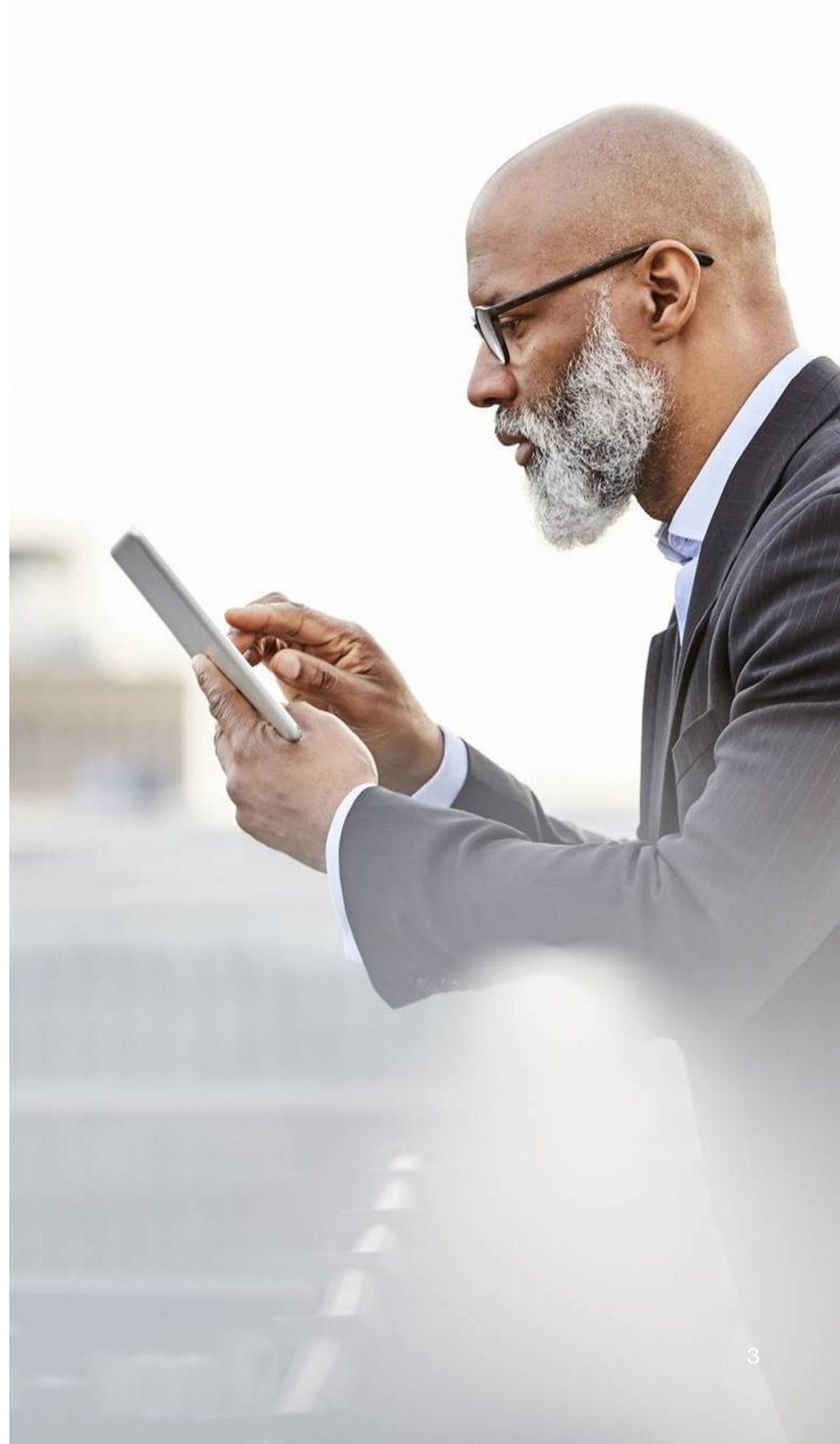
Introdução

De acordo com a mais recente pesquisa global de riscos da Aon, a GRMS 2023, gestores e gestoras do mundo inteiro apontam o risco cibernético e a falha na cadeia de suprimento como algumas das principais preocupações para a gestão das companhias. Respectivamente esses riscos ocupam a primeira e a sexta posição, e há mais de dez anos figuram entre os dez principais riscos que preocupam as empresas.

O risco cibernético pode ser definido como a exposição gerada a partir de uma forte interação com tecnologia e dados. Enquanto o risco da falha na cadeia de suprimento pode ser definido pela alta dependência de produtos e serviços externos para realização das entregas da própria companhia.

Quando analisamos mais profundamente ambas as ameaças entendemos que estas estão intrinsecamente ligadas, isto é, é possível haver uma falha na cadeia de suprimento por conta de riscos cibernéticos aos quais nossos fornecedores estão expostos, da mesma forma que é possível sofrer um ataque cibernético em função de uma porta de entrada encontrada por criminosos via fornecedores.

Assim, é fundamental que companhias estejam preparadas para avaliar seus fornecedores, estabelecendo SLAs de segurança e privacidade a fim de que seja criada uma linha base para gestão de risco nestes dois âmbitos. Uma vez que a empresa entende seu próprio nível de maturidade, entende a profundidade em que está exposta perante seus fornecedores, entende o impacto causado por problemas de segurança e privacidade, estará melhor preparada para lidar com as adversidades de eventos ocorridos que envolvam essas duas esferas de risco.



Introdução

Neste relatório a Aon irá apresentar o resultado de sua análise de maturidade para fornecedores baseada no CyQu. O CyQu, ou Cyber Quotient Evaluation, é uma ferramenta proprietária, desenvolvida pela Aon para a avaliação de Riscos cibernéticos com base na NIST (framework de segurança).

Através da análise de 97 perguntas, 35 áreas de controle, e 9 domínios de segurança a Aon determina um perfil de higiene cibernética baseado na NIST. As notas são estabelecidas de 1 a 4, sendo 1 o menor nível de maturidade e higiene cibernética, considerado básico; e 4 o maior nível, definido o perfil em avançado.

Empresas em níveis mais baixos de governança e higiene cibernética, seja geral, ou individualmente nas áreas de controle, são consideradas empresas reativas, de perfil básico, mais sucetiveis a desdobramentos mais catastroficos de ataques cibernéticos e vazamento de dados. Já empresas em níveis mais altos são consideradas proativas, sujeitas a melhor contenção de danos e prejuízos, e uma maior taxa de sucesso na execução de seus planos de recuperação e resposta.

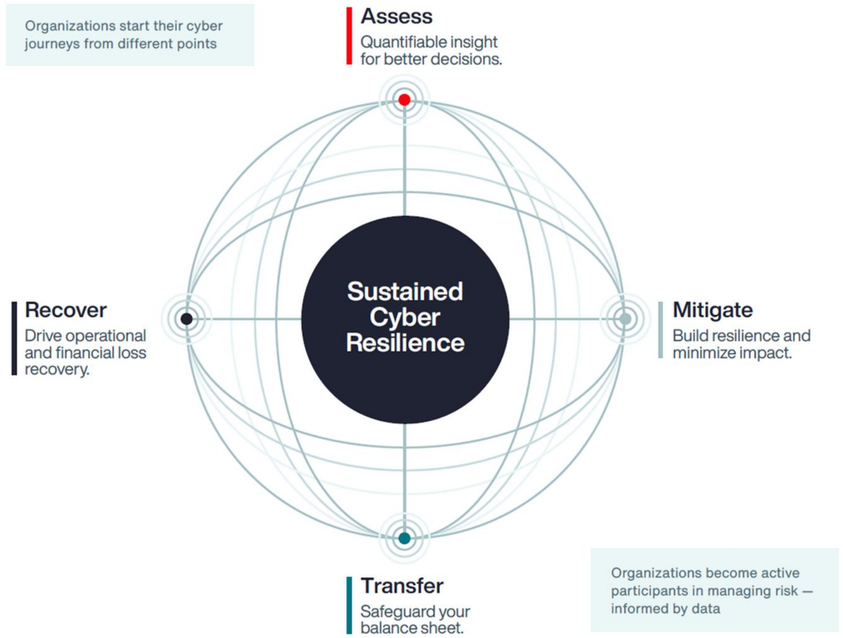
Assim, através desta avaliação, é possível determinar focos de trabalho e correção, bem como focos de investimento para a companhia baseado naquilo que possui maior impacto para as operações.

Cyber Loop

Metodologia

- O **Aon Cyber Loop** é a estratégia da **Aon** para a abordagem dos riscos cibernéticos. Trata-se de uma estratégia cíclica e holística, possível de se aderir a qualquer momento. Acreditamos que a gestão de riscos cibernéticos é uma ação constante e contínua, e que somente o acompanhamento próximo e a regularidade podem nos colocar a frente das ameaças que surgem todos os dias.

- O primeiro passo é a realização de um diagnóstico da gestão de risco cibernético, pela aplicação da ferramenta analítica ***Cyber Quotient Evaluation*** (**CyQu**), pelo qual a organização através de 9 domínios tem um claro entendimento de suas práticas preventivas e protecionais.



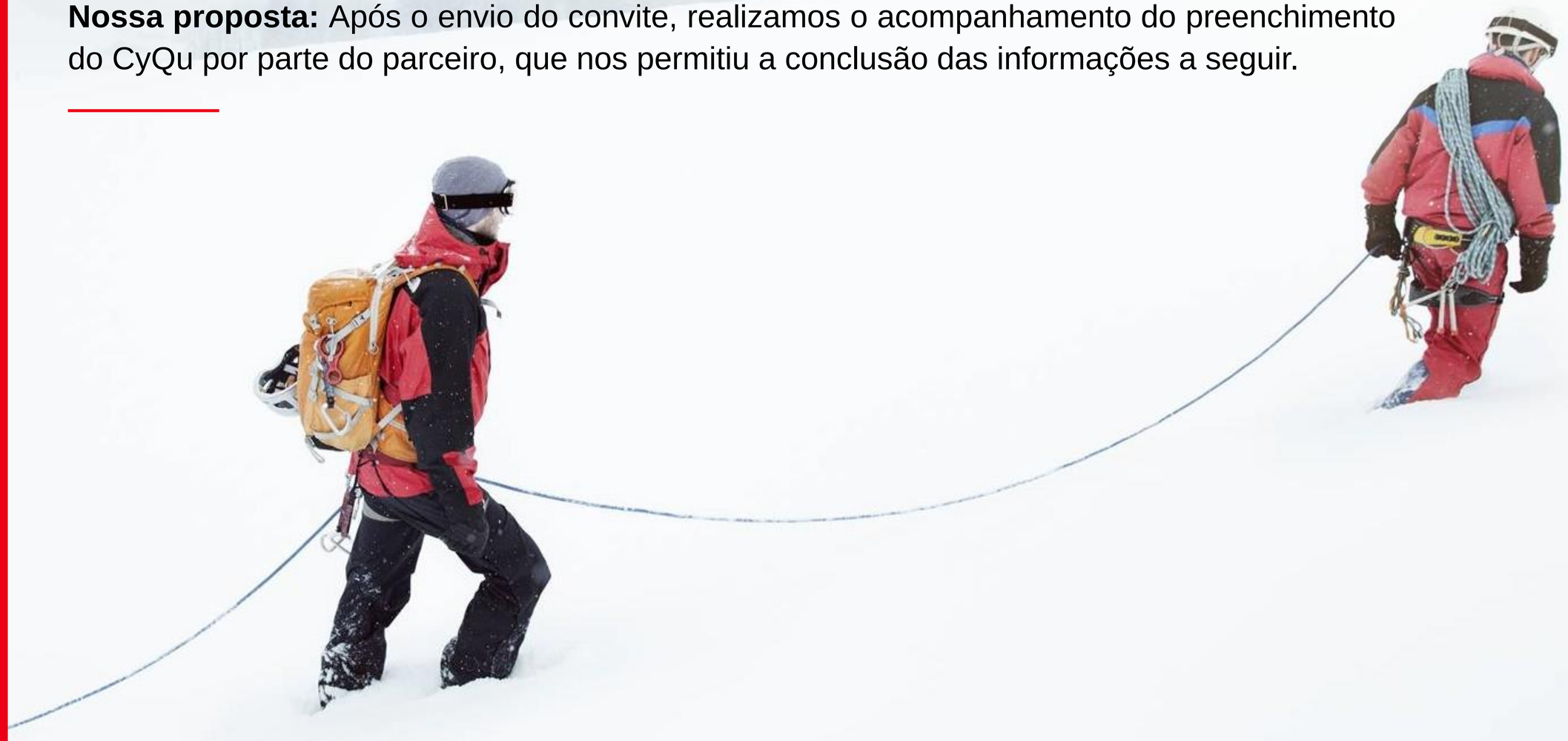
What is next?

- Benchmark: o CyQu oferece completo benchmark, incluindo notas comparativas gerais, por dominio de segurança, por área de controle.
- Avaliação: tenha visibilidade instantânea dos níveis de maturidade por área de controle, estabeleça focos e responsabilidades.
- Roadmap: baseado na avaliação do CyQu determine o curso das próximas ações para a companhia.

Sumário Executivo

Objetivo do trabalho: O escopo consiste em fazer uma avaliação de perfil de risco de parceiros críticos elencados pela UnileverPrev. Juntos, estabelecemos o modelo de trabalho, assim como o convite que foi encaminhado ao parceiro selecionado.

Nossa proposta: Após o envio do convite, realizamos o acompanhamento do preenchimento do CyQu por parte do parceiro, que nos permitiu a conclusão das informações a seguir.



Sinqia

At a glance

Resumo

Encontre abaixo o resultado CyQu para Sinqia no projeto Scafplusnet. A Nota Geral do Sinqia Scafplusnet foi 3,4. Após revisão da versão um, houve melhoria significativa considerando que este relatório se refere apenas a uma fração da operação dedicada ao suporte à Unilever e com controles específicos ao seu ambiente personalizado. A nota anterior havia sido 2,5.

CyQu Domínios

- Segurança de Dados
- Controles de Acesso
- Endpoint e Segurança
- Segurança em Redes
- Segurança Física
- Segurança em Aplicações
- Terceiros e prestadores de serviço
- Resiliência do Negócio
- Trabalho Remoto

ATENÇÃO!

As avaliações do risco cibernético, pela sua natureza complexa, podem ser muito subjetivas. Existirão lacunas e incertezas devido à variabilidade na integralidade, precisão e atualidade dos dados e análises referenciados nesta revisão. A Pontuação de Avaliação do Quociente Cibernético acima é uma pontuação produzida exclusivamente a partir das respostas submetidas às questões. Representa uma suposição e opinião baseada em fatos e circunstâncias relatados no momento da submissão. As respostas sobre a postura e os mecanismos de segurança cibernética não foram validadas e/ou testadas externamente. Posteriormente, todas as informações deverão ser revisadas e validadas pela empresa. A precisão dos resultados permanecerá dependente da precisão das informações fornecidas pela empresa, e as suposições feitas podem variar significativamente.

Nenhuma representação ou garantia é feita no fornecimento da Pontuação de Avaliação do Quociente Cibernético e ela é fornecida apenas para fins informativos e não pode ser confiável ou de qualquer forma usada na tomada de decisões sobre segurança cibernética ou para determinar a vulnerabilidade de sua organização a um ataque cibernético ou outra ameaça semelhante.

Caso a organização deseje usar os resultados do CyQu para facilitar uma conversa com um corretor de seguros, um relatório separado está disponível mediante solicitação, onde todas as pontuações são removidas e as respostas às perguntas do CyQu permanecem. Quaisquer respostas deverão ser validadas e ajustadas em reunião com seu corretor de seguros.

Relatório detalhado

1. Sobre a UnileverPrev

Sobre a companhia

A UnileverPrev é uma empresa inovadora no ramo de previdência privada, comprometida em prover soluções financeiras sólidas e personalizadas para seus clientes. Tem se destacado no mercado por sua abordagem centrada no cliente, transparência e excelência em gestão de investimentos.

Seu propósito é cuidar de seus participantes e seus beneficiários, administrando os seus benefícios previdenciários para garantir no futuro, durante a aposentadoria, a mesma qualidade de vida que têm hoje.

Com uma equipe de especialistas altamente qualificados e experientes, a UnileverPrev se destaca pela qualidade de seus serviços e pelo compromisso em proporcionar segurança e tranquilidade para o futuro financeiro de seus clientes.

Na UnileverPrev, o planejamento previdenciário é fundamental para garantir uma aposentadoria tranquila e estável. Por isso, o trabalho é incansável para oferecer as melhores opções de investimento, combinadas com um atendimento personalizado e eficiente.

Relatório detalhado

1. Grandes marcos

1981

A UnileverPrev ou antiga Previgel, foi constituída para administrar o Plano de Benefício Definido oferecido aos empregados da Unilever.

2003

Criação do Plano de Previdência Complementar UnileverPrev - PPCU (na modalidade de Contribuição Definida) com opção de migração voluntária pelos participantes do Plano de Benefício Definido e fechamento deste para futuras adesões.

2017

Alteração regulamentar que eliminou os benefícios de risco do plano PPCU, fazendo dele um plano 100% Contribuição Definida.

2022

Estamos entre as 25 maiores entidades fechadas de previdência complementar não públicas do Brasil, e nosso plano PPCU está entre os 15 maiores planos de Contribuição Definida do país segundo o relatório Consolidado Estatístico ABRAPP de 09/2021.

Relatório detalhado

3 – Parceiro indicado pela UnileverPrev

sinqia

Especialista no sistema financeiro, a Sinqia é uma das empresas que mais crescem no Brasil. Eleita diversas vezes como uma das 100 maiores Fintechs do Mundo, seus softwares estão presentes em 8 a cada 10 instituições financeiras do país. Iniciou sua operação pequena ainda no fim da década de 1990 em uma cafeteria das ruas de São Paulo, e hoje, após um aumento vertiginoso da sua capacidade produtiva, se consolida como líder em softwares e inovação para o sistema financeiro brasileiro e uma das maiores provedoras de tecnologia e serviços para essa indústria.

Foi com o objetivo de migrar de um modelo de negócios baseado exclusivamente em serviços para um modelo mais completo que abarcava também o desenvolvimento de produtos, que o primeiro software de prateleira foi lançado já nos anos 2000. Dois anos depois, a empresa foi contemplada com recursos do BNDES Prosoft acelerando a mudança e modernizando seu modelo de negócios.

2004 marca o lançamento do SBS (Senior Banking Solution), que se tornou o principal produto da Companhia por ser um dos primeiros aplicativos brasileiros para tesouraria de instituições financeiras. Já em 2005, mais investimentos foram recebidos com a venda de participação acionária para o BNDESPAR e para o FMIEE Stratus GC.

AON

Relatório detalhado

3 – Parceiro indicado pela UnileverPrev

sinqia

Ampliou-se, então, a abrangência do SBS, desenvolvendo módulos para câmbio, derivativos e renda fixa, e iniciou-se a estratégia de crescimento via aquisições com a incorporação da NetAge (software SIAN para tesouraria e investimentos), em 2005. Desde então deu-se início a uma estratégia de consolidação muito bem sucedida, que resultou na liderança do setor.

A Sinqia está presente no seleto grupo de empresas com capital aberto na B3 desde 2013, conhecida como SQIA3 pelos investidores.

Hoje, com mais de 26 anos de experiência, a empresa oferece plataformas de softwares voltadas para bancos, fundos, previdência e consórcios, além dos serviços de outsourcing e consulting.

Em 2021, com as recentes aquisições, criou-se uma unidade de negócios voltada para soluções digitais que complementam todos os segmentos de softwares e de serviços. Essa estrutura coloca foco em cada segmento, potencializando soluções que impulsionam o sistema financeiro.

AON

Relatório Detalhado

4. Diagnóstico – 4.1. Cyber Quotient Evaluation (CyQu)

O ***CyQu*** é uma ferramenta desenvolvida pela **Aon** para ajudar a organização a entender o seu grau de maturidade quanto a riscos cibernéticos. A ferramenta foi construída com base no framework NIST e na ISO 27001. Através da análise de 9 domínios de segurança e suas respectivas 35 áreas de controle críticos, a organização poderá entender melhor seus pontos fortes e aqueles a melhorar de sua gestão de segurança.

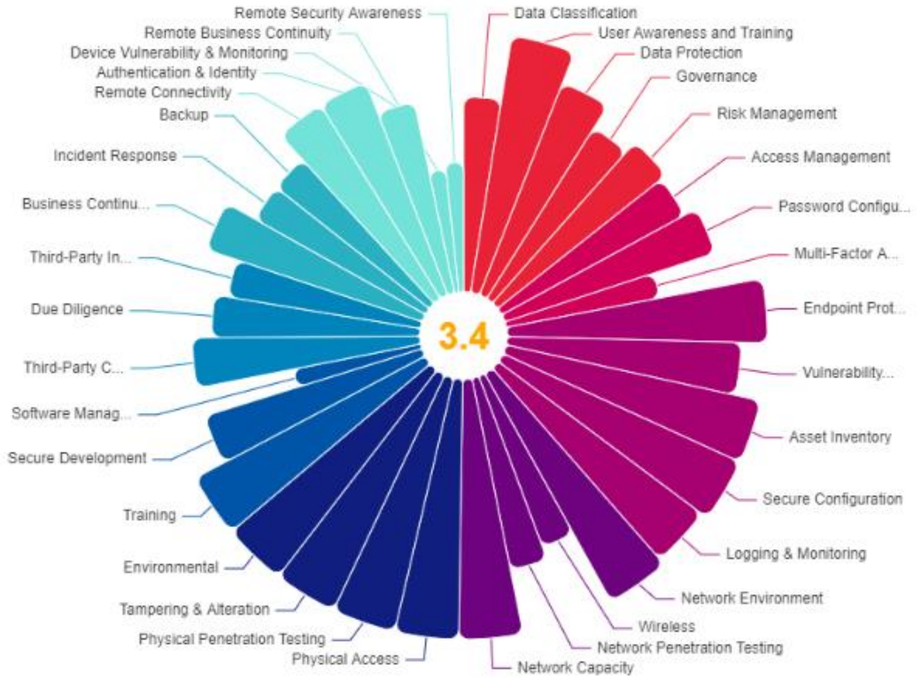
O relatório também é capaz de oferecer à organização comparativos de suas notas com as demais empresas do mercado que se assemelham em termos de faturamento e indústria, isso ajuda a estabelecer objetivos de curto e longo prazo, e priorizar investimentos de acordo com as necessidades específicas da indústria e, obviamente, da empresa.

Relatório Detalhado

4.2. Resultado do CyQu

Key Findings

- A Sinqia apresenta um ambiente robusto e seguro para gerenciar o risco cibernético a nível do contrato que possui com a UnileverPrev
- Destacamos as notas dos domínios de seguraça de sistemas e endpoints, bem como segurança de rede, que são de extrema importância para esta relação e possuem notas altas, estabelecendo um alto grau de maturidade por parte da Sinqia.
- Recomendamos o acompanhamento de implementação do projeto de SSO.



1	Initial

CONTROL AREAS

- Remote Business Continuity

2	Basic

CONTROL AREAS

- Multi-Factor Authentication
- Software Management
- Remote Security Awareness

3	Managed

CONTROL AREAS

- Data Classification
- Governance
- Risk Management
- Access Management
- Password Configuration
- Wireless
- Network Penetration Testing
- Due Diligence
- Third-Party Inventory
- Incident Response
- Backup
- Device Vulnerability & Monitoring

4	Advanced

CONTROL AREAS

- User Awareness and Training
- Data Protection
- Endpoint Protection
- Vulnerability Management
- Asset Inventory
- Secure Configuration
- Logging & Monitoring
- Network Environment
- Network Capacity
- Physical Access
- Physical Penetration Testing
- Tampering & Alteration
- Environmental
- Training
- Secure Development
- Third-Party Contracts
- Business Continuity/DR
- Remote Connectivity
- Authentication & Identity

Relatório Detalhado

4.3. Resultado consolidado do CyQu

1 – 1,8	1,9 – 2,6	2,7 – 3,2	3,3 – 4
1 Inicial	**2 Básico**	**3 Gerenciada**	**4 Avançado**
Práticas de gestão de riscos de segurança cibernética organizacional não são realizadas Se a empresa identifica e trata riscos, isso é feito apenas dentro de silos. Os componentes e atividades do processo de gestão de riscos têm escopo limitado e são implementados de maneira ad hoc	As práticas e tecnologias de gestão de riscos de segurança cibernética organizacional não foram formalizadas, e o risco é gerenciado de maneira ad hoc e, às vezes, reativa As práticas e tecnologias de gestão de riscos não são estabelecidas em toda a empresa	As práticas e tecnologias de gestão de riscos são desenvolvidas e estabelecidas na maioria da empresa Adapta suas práticas de segurança cibernética de acordo com as práticas recomendadas e indicadores preditivos na maioria da empresa Políticas, processos e procedimentos são definidos, implementados como planejado e revisados. Métodos compatíveis são aplicados para responder efetivamente a mudanças nos riscos	Adota uma abordagem em toda a organização para gerenciar riscos de segurança cibernética As práticas de segurança cibernética organizacional são atualizadas regularmente com base na aplicação de processos de gerenciamento de risco para mudanças nos requisitos de negócios/missão e um cenário de ameaças e tecnologia em constante mudança Processo de melhoria contínua incorporando tecnologias e práticas avançadas de segurança cibernética

Visão Geral

De acordo com os dados contidos em nossos sistemas, e de acordo com os resultados obtidos pela Sinqia no CyQu, a empresa está classificada, em 02/12/2024, como empresa de risco avançado. Uma empresa que possui um perfil de risco avançado pode ser entendida como uma empresa voltada para o futuro em segurança e privacidade, proativa, que possui processos e procedimentos adequadamente documentados e testados. É também uma empresa que considera a participação (e possível falha de fornecedores críticos) nos seus testes.

Considerações

Ambientes seguros podem ser caros e exigir monitoramento e investimento contínuos. Recomendamos fortemente a criação de uma rotina periódica de avaliação de riscos, incluindo avaliações comparativas ao longo do tempo. Recomendamos revisão periódica das cláusulas de Responsabilidade Civil e que o contratante exija seguros Cibernéticos, E&O e Crime, como garantias adicionais ao contrato.

Relatório Detalhado

Classificação por área de controle

Control Areas	Your CyQu	Peer
Data Security *Manages safeguards to protect the confidentiality, integrity, and availability of information.*	3.4	2.9
Data Classification *Manages classification of data to determine appropriate technical safeguards.*	3.0	2.6
User Awareness and Training *Delivers education for employees on security best practices and common threats that could compromise the confidentiality, availability, integrity of information.*	4.0	3.3
Data Protection *Manages the protection of sensitive data using data encryption and loss-monitoring tools.*	3.5	2.9
Governance *Board / Executive Management ownership and commitment to cyber security as a critical factor for achieving business objectives and protecting value*	3.1	2.9
Risk Management *Integration of cyber security into the risk management framework to achieve alignment on risk metrics and improve decision making processes*	3.3	2.7
Access Control *Grants authorized users the right to use a service while preventing access to non-authorized users.*	3.1	2.9
Access Management *Prevents compromise of confidential data by ensuring least privileged access rights.*	3.2	2.8
Password Configuration *Prevents compromise of confidential data by ensuring password configuration settings.*	3.4	3.3
Multi-Factor Authentication *Prevents compromise of confidential data by providing an extra layer of security where the first layer mechanism may be at risk or compromised.*	2.5	2.9
Endpoint and Systems Security *Delivery and administration of infrastructure services, systems monitoring, endpoint protection, configuration management, storage management, infrastructure operations.*	3.9	2.9
Endpoint Protection *Manages endpoint security software to limit viruses, trojans and other malware that could result in unauthorized access to sensitive information, data exfiltration and/or noncompliance.*	4.0	3.0
Vulnerability Management *Manages process to identify, rate, prioritize, report on information system vulnerabilities and recommend an appropriate treatment response.*	3.8	2.8
Asset Inventory *Maintains information and relationships for a collection of assets in order to provide visibility into an organization's environment and drive key decisions based on risk.*	4.0	2.6
Secure Configuration *Manages a process to identify, rate and track gaps in critical information system compliance against a pre-defined standard.*	4.0	2.8
Logging & Monitoring *Delivers centralized security logging, monitoring, and analytics capabilities to support incident response efforts and regulatory/compliance mandates.*	3.9	3.0
Network Security *Delivers infrastructure services including enterprise defense for network, compute, physical presence, cloud, storage management and operations.*	3.7	3.0

Relatório Detalhado

Classificação por área de controle

Network Environment *Provides network based detective and preventive control capabilities to stop unwanted traffic and offer visibility for investigation and remediation.*	4.0	3.0
Wireless *Manages a process to identify, rate and track gaps in critical wireless devices against a pre-defined standard.*	2.8	2.7
Network Penetration Testing *Manages process to identify, rate, prioritize, report on network vulnerabilities and recommend an appropriate treatment response.*	3.0	3.2
Network Capacity *Manages system capacity and resourcing to limit denial of service and other availability issues.*	4.0	2.9
Physical Security *Protects facilities, equipment, resources, and personnel from unauthorized access, damage or harm.*	4.0	2.9
Physical Access *Manages appropriate access to key physical locations.*	4.0	3.3
Physical Penetration Testing *Manages process to identify, rate, prioritize, report on physical vulnerabilities and recommend an appropriate treatment response.*	4.0	1.9
Tampering & Alteration *Manages appropriate access to key physical infrastructure equipment or systems.*	4.0	2.1
Environmental *Plans for securing key physical infrastructure against environmental threats.*	4.0	3.3
Application Security *Protects applications from threats by requiring measures or checks during each stage of the application development life cycle.*	3.1	2.5
Training *Provides software security training to development community including a structured approach to identify, quantify, and address the security risks associated with an application.*	4.0	2.7
Secure Development *Delivers dynamic analysis and penetration testing for applications including correlation of application vulnerabilities, assessment of the level of risk, and recommendations on appropriate remediation and mitigation.*	3.5	2.8
Software Management *Manages process for authorizing and allow listing applications.*	2.0	2.0
Third Party *Monitors relationships with third parties to ensure provided services adhere to defined security policies.*	3.3	2.4
Third-Party Contracts *Manages third-party risk through formal legal agreements.*	3.5	2.5
Due Diligence *Prevents and detects third-party risk through standard security assessments.*	3.2	2.3
Third-Party Inventory *Manages list of key vendors with access to system or data.*	3.0	3.0
Business Resilience *Plans for prompt and effective continuation of business critical services in the event of a disruption.*	3.2	2.6
Business Continuity/DR *Plans for prompt and effective continuation of business critical services in the event of a disruption.*	3.5	2.6
Incident Response *Allows for recovery of critical applications and business process in the event of a failure.*	3.0	2.7
Backup *Allows for recovery from an unplanned security or operational event.*	3.0	2.7

Relatório Detalhado

Classificação por área de controle

Remote Work *Enabling users to remotely access corporate systems and data securely to deliver on their roles and responsibilities when outside of corporate working environments.*	3.0	2.9
Remote Connectivity *Providing the ability to connect from non-corporate locations to business information systems, applications and data.*	3.5	3.4
Authentication & Identity *Enabling the business to identify and control access where appropriate and allowing users to connect to the required and relevant systems, data and domains to perform their specific duties.*	3.5	3.0
Device Vulnerability & Monitoring *Securing remote devices from the latest known vulnerabilities with regular updates and security monitoring.*	3.0	2.6
Remote Business Continuity *Providing organizations the ability to backup information from remote clients and maintain business continuity in the event of large scale remote working.*	1.9	2.3
Remote Security Awareness *Educating business and technology users on relevant cyber security attacks, threats and risks based on their remote working environments, and how to safeguard themselves appropriately.*	2.0	2.3

Relatório Detalhado

4.4. Recomendações

De forma geral, o projeto Scafplusnet da Sinqia atende as melhores práticas de governança corporativa, segurança da informação e privacidade com base no modelo NIST. Apresentando uma nota de 3,4 a empresa se encontra em nível avançado de higiene cibernética.

Em nossa perspectiva, este é um risco transferível e segurável. Não apresentando apontamentos que poderiam restringir o appetite da seguradora. Assim, recomendamos que a UnileverPrev considere solicitar a contratação de seguros de Responsabilidade civil profissional, Fraude e Responsabilidade Civil Cibernética, a fim de garantir melhor colateralização.

A ferramenta CyQu não aponta redflags ou nenhuma preocupação específica. A empresa se encontra, atualmente, no projeto Scafplusnet, em conformidade. A Aon recomenda que este relatório seja refeito duas vezes ao ano para acompanhamento dos resultados e controles.

Lembramos que todas as avaliações e análises foram feitas com base nas respostas dadas pelo Sinqia, não houve a apresentação de evidências, coleta de respostas via entrevista/reunião, nem nenhum tipo de verificação remota de vulnerabilidades.

Ainda recomendamos a análise do risco mediante ferramentas como Security Score Card e Bitsight, porém acreditamos que estas ferramentas não consigam fazer uma análise granularizada, de forma a segregar o projeto Scafplusnet dos demais ambientes.

Atenção!

Apesar de nenhum apontamento por parte da ferramenta usada para a avaliação do risco, nossos consultores acreditam existir pontos a serem debatidos

1 **Gestão de Fornecedores**

Recomendamos que a UnileverPrev solicite à Sinqia uma apresentação complete e detalhada sobre suas políticas de gestão de fornecedores. A dependência de fornecedores por parte da Sinqia pode resultar em um impacto considerável para a UnileverPrev.

2 **Projetos de Segurança**

Gestão de acesso é um ponto crítico para esta relação considerando a natureza das operações. Acompanhar projetos como a implementação do SSO e outras medidas de automação para concessão e revogação de acessos são primordiais.

3 **Gestão de aplicações e desenvolvimento**

Sugerimos que sejam esclarecidos os controles e medidas protetivas aplicadas para a execução e uso de softwares não autorizados.

Relatório Detalhado

4.5 – Análise de Risco e Potenciais Impactos

Diante do escopo da prestação de serviços, a análise de risco é crucial para identificar vulnerabilidades que podem impactar a operação. Destacamos, a seguir, critérios que estão diretamente ligados à operação e seus potenciais impactos.

Potenciais Riscos e seus impactos:

- **Interrupção dos Serviços – Sinqia (Scafplusnet)**

A falha de segurança de controles existentes pode resultar em interrupções significativas nos serviços prestados, impactando diretamente o cliente final da UnileverPrev, além de contar com o próprio programa de seguros e gerenciamento de riscos, recomendamos que a UnileverPrev considere:

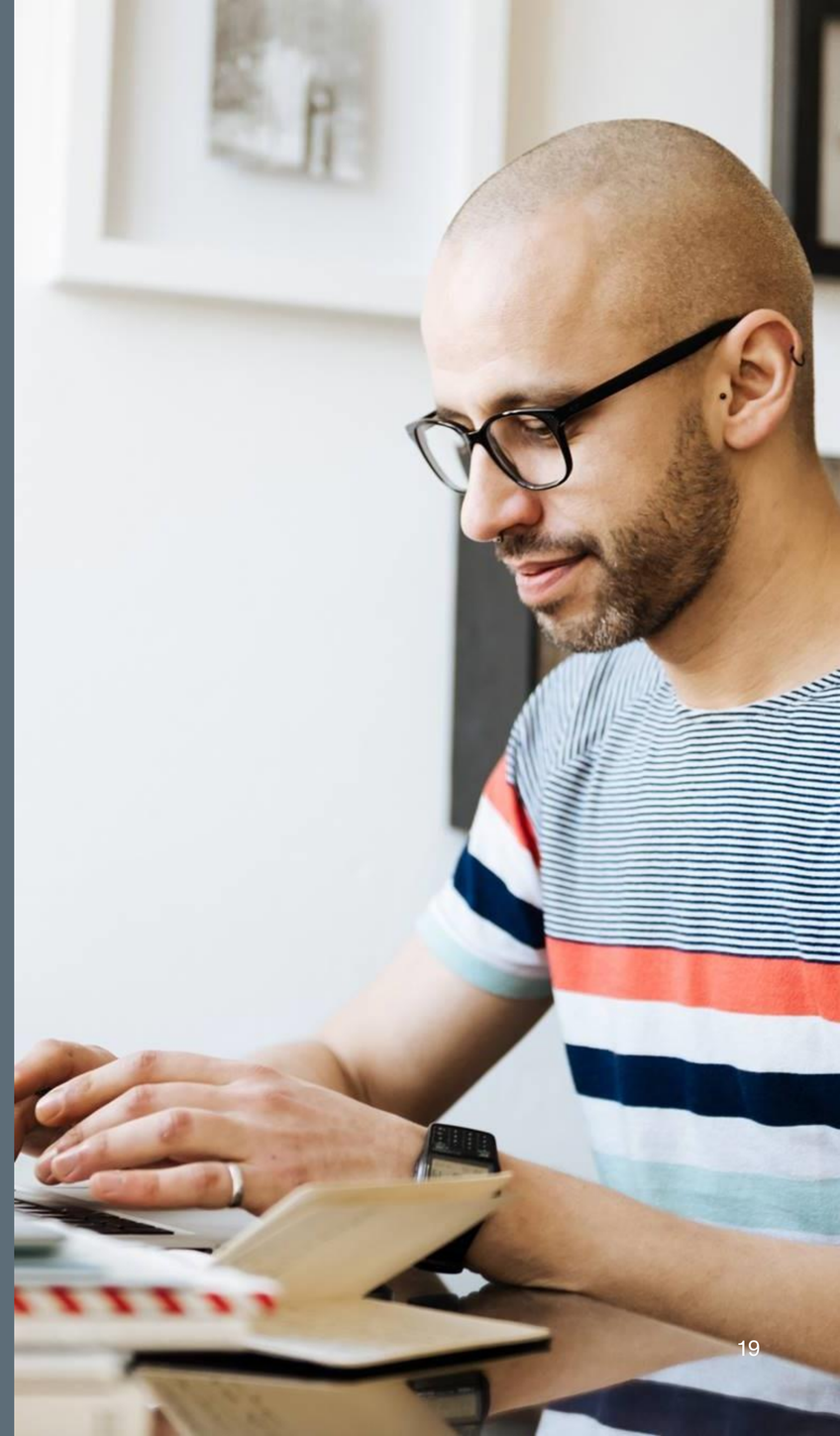
a. Considere se inteirar do plano de resposta ao incidente e recuperação de desastres da Sinqia, defina seu papel e avalie impactos. Nesse sentido, considere também participar de exercícios de execução destes planos e simulações. Ainda, compreenda as redundâncias envolvidas e os tempos de recuperação para consideração em seu próprio plano de resposta ao incidente.

- **Perda de Dados**

Dados de clientes da UnileverPrev podem estar expostos, ainda que o armazenamento, a coleta e o processamento não ocorram necessariamente na mãos da UnileverPrev, perante reguladores a responsabilidade poderá ser determinada de forma diferente. Assim esteja preparados para possíveis discussões em âmbito administrativo a respeito das responsabilidades da Unilever quanto a contratação e dependência de seus terceiros.

- **Reputação e Confiança**

Clientes podem se sentir inclinados a buscar alternativas se não sentirem que suas informações e seus ativos estão adequadamente tratados e cuidados.



Relatório detalhado

4.5 – Análise de Risco e Potenciais Impactos

Gestão da cadeia de suprimento

A boa relação com fornecedores é fundamental, e entender como essa cadeia se desenvolve ainda mais adiante é imprescindivel. Recomendamos:

- Solicitar apresentação de controles de segurança e garantias dadas por fornecedores críticos da Sinqia ligados ao projeto Scafplusnet.
- Solicitar explicações adicionais sobre controles e protecionais para acesso físico à fornecedores de infraestrutura crítica da Sinqia, relacionados ao projeto Scafplusnet.
- Recomendamos exigir de fornecedores Seguro de Erros e Omissões, Cyber e Fraude.
- Recomendamos incentivar e participar de testes e exercícios de crise.

Projetos de segurança

Gestão de segurança e privacidade é uma tarefa constante e necessita de um investimento continuo, de tempo e recursos financeiros. Recomendamos:

- Acompanhar o desenvolvimento dos projetos de implementação de projetos de segurança e ferramentas adicionais.
- Acompanhar a implementação de estratégias alternativas de segurnaça para domínios e áreas de controle que caminham em direção a um maior patamar de maturidade.

Gestão de softawares e APIs

O desenvolvimento de softaware é uma tarefa de muita responsabilidade e exposição. Recomendamos:

- Solicitar apresentação sobre o processo de desenvolvimento. Indagando questões relacionadas ao desenvolvimento e o uso controlado de ferramentas, como inteligência artificial, pool de códigos, softwares não previamente autorizados, etc.

Gestão de acessos

A gestão de acessos pode ser uma grande vulnerabilidade da companhia em termos de capacidade de criminosos e agentes mal intencionados subverterem valores e acessos em benefício próprio, criando exposições desconhecidas e de difícil rastreabilidade. Recomendamos:

- Exigir clareza no processo de avaliação, concessão e revogação de acessos. Questionar a implementação de automaticidade a estes processos, ou em contrapartida demandar explicação detalhada do processo com exemplificação e apresentação de evidencia.

Conclusão

Identificamos que a empresa Sinqia, para o projeto Scafplusnet, está classificada como empresa “Avançada”.

Acreditamos que todos os controles apresentados estão em conformidade com os padrões necessários para o estabelecimento de uma relação sustentável e segura com a UnileverPrev.

Recomendamos que sejam criadas rotinas de acompanhamento para os pontos deixados em aberto, bem como rotinas de integração mais eficientes entre as duas emrpesas.

Assumptions

Durante a preparação do nosso relatório, assumimos e confiamos nas respostas fornecidas pelo destinatário e responsável pelo questionário CyQu. Não validamos a precisão, integridade e confiabilidade dessas respostas recebidas e/ou o perfil real e atual da estrutura de segurança cibernética da organização. As informações incluídas no relatório de avaliação são baseadas nos dados e condições que nos foram comunicados, e que podem ser sujeitas a mudanças rápidas e materiais. Embora essa mudança possa ter um impacto sobre nossas suposições e resultados, não temos obrigação de atualizar, revisar ou reafirmar nossa revisão, suposições ou opiniões. Ninguém deve agir com base em tais informações sem aconselhamento profissional adequado após um exame completo da situação particular. O Relatório de Avaliação não pode ser distribuído, reproduzido ou usado sem o consentimento prévio expresso por escrito da Aon.

A Aon não terá nenhuma responsabilidade para o destinatário ou qualquer outra parte resultante do uso deste informações do destinatário ou dessa outra parte.