RELATÓRIO DE VIAGEM

DADOS DO EVENTO

DATA DE INÍCIO	DATA DE TÉRMINO	NOME DO EVENTO	CIDADE/PAÍS
2 de setembro de 2024	5 de setembro de 2024	ISACA Conferência Latino-americana 2024	Buenos Aires - Argentina

RESUMO DO EVENTO

ENTIDADE ORGANIZADORA	PROCESSO	PARTICIPANTES
Information Systems Audit and Control Association – ISACA	TC-018.287/2024-7	Helton Garcia

JUSTIFICATIVA (RESUMO)

[Neste campo demonstre a relevância do trabalho desempenhado na cidade de realização do evento, para a obtenção da autorização de viagem. Procure ser objetivo (a), apresentando apenas o que for importante para análise do pleito. Lembre-se que este relatório será publicado]

Trata-se da principal conferência realizada anualmente no âmbito da América Latina patrocinada pela ISACA - Information Systems Audit and Control Association.

A ISACA é uma organização internacional sem fins lucrativos que promove auditoria, segurança da informação, governança, gestão de riscos e tecnologias emergentes. Fundada em 1969, a ISACA desempenha um papel fundamental no desenvolvimento de padrões e certificações globais, como CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager) e COBIT (Control Objectives for Information and Related Technologies).

Sua importância no cenário global está no reconhecimento pelo mercado acerca da sua atuação, na qualidade de profissionais certificados pela Associação. E nesse sentido, o evento reveste-se de catalisador para promover compartilhamento de conhecimentos de borda na linha do conhecimento acerca de temas de interesse.

E no que tange especificamente à Sesouv (Secretaria de Ouvidoria e Segurança da Informação), a temática de segurança da informação reveste-se de foco em vários círculos de discussão apresentados no evento, onde questões como ameaças cibernéticas, gestão de segurança da informação, riscos de segurança, continuidade de negócios, tecnologias emergentes e sua aplicabilidade em cenário de confiança digital, ransomware, entre outros, foram temáticas amplamente discutidas.

RELATO

[Descreva o evento de forma sucinta, destacando aquilo que posa ser útil a outros colegas, como transferência de conhecimento. Evite elogios e juízo de valor, tais como: “O evento foi muito proveitoso”, “Os anfitriões são muito acolhedores”, “O evento não foi bem organizado” etc.

Caso o evento deixe de trazer algo de novo, causando frustação em termos de expectativas, relate os pontos considerados altos em relação ao conhecimento transferido, ou faça um paralelo daquilo que foi apresentado e a situação do TCU]

O evento da Conferência Latinoamericana da ISACA 2024 destacou temas cruciais em segurança da informação, gestão de riscos e governança de TI, alinhando-se ao lema "Riscos digitais, estratégias profissionais" (""Riesgos digitales, estrategias profesionales"). A programação foi dividida em palestras e oficinas ("talleres") que abordaram desde cibersegurança, ameaças digitais, estudos de caso reais até tecnologias emergentes, como aspectos de inteligência artificial aplicados, com foco em desafios de borda nas áreas de conhecimentos enfatizadas no evento..

Entre os principais tópicos, destacam-se palestras sobre estratégias de segurança da informação e cultura de segurança organizacional, com ênfase na proteção contra ameaças como phishing e ransomware.

Também incluem a realizada pela Interpol sobre ciberameaças globais e sobre estudos de caso empregando frameworks como NIST CSF 2.0 (National Institute of Standards and Technology Cybersecurity Framework v2.0), CIS Critical Security Controls.

Os temas ransomware e phishing foram amplamente debatidos, com foco nas estratégias de resposta a ataques e na análise de casos reais. Inclusive umas das oficinas abordou estudo de caso prático, procurando trazer realismo ao exercício. Em outro, houve a apresentação de estudo de caso real envolvendo inclusive processo negociação (ransom).

Também foi apresentado estudo de caso envolvendo implementação de plano de continuidade de negócio empregando framework de mercado, bem como outra relacionada ao emprego de boas práticas para aprimoramento de resiliência organizacional.

Nas oficinas, foram abordados temas como o papel do profissional de cibersegurança na nova era digital e simulações de ataques cibernéticos com a oficina "CyberWar". Outra oficina importante foi "Hacking Culture", que abordou a necessidade de minimização de superfície de ataques pela atuação no fator comportamental de usuários, destacando a necessidade de uma forte cultura de segurança, como elemento chave para promover conduta pró-ativa na mitigação de riscos de segurança da informação.

Por fim, e não menos importante, o evento foi marcado pela presença de palestrantes referenciados internacionalmente em suas respectivas áreas de atuação. Houve oficinas preparadas por outras representações da ISACA internacional como outro diferencial de conhecimento. Outro ponto forte foi a possibilidade de acesso a casos reais e na oportunidade de discuti-los não somente com os instrutores, mas também de contam com importantes insights de profissionais de mercado inscritos no evento, tendo em vista que a maioria do público é formada por profissionais contendo certificações ISACA internacionalmente reconhecidas como padrões de excelência de mercado.

Diante do exposto, a utilidade do evento se mostra inequívoca.

ENCAMINHAMENTOS POSSÍVEIS, NO ÂMBITO DO TCU, DECORRENTES DESTA AÇÃO

[Baseado em sua experiência e as novas informações/os novos conteúdos assimilados, proponha pontos de melhoria para o Tribunal atingir a sua missão precípua ou para sua Unidade, caso a ação seja específica para o seu trabalho.]

Esta é uma parte que se mostra mais objetiva para discorrer.

Já que a aplicação do conhecimento está sendo IMEDIATA.

Mas para isso, é preciso trazer o contexto de atuação da Sesouv. O norte geral baseado em nosso artigo principal, previsto no Resolução-TCU nº347/2022, mais especificamente no art. 23, incisos I cc XX:

"...art. 23 [...] Compete à Sesouv [...] coordenar a implementação e o funcionamento do Sistema de Gestão de Segurança da
Informação (SGSI/TCU), incluindo a gestão da continuidade de negócio do Tribunal [sob a perspectiva tecnológica], e da Política Corporativa de Segurança da Informação (PCSI/TCU), bem como a aplicação da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no âmbito do TCU;..."

No mesmo sentido, temos a Resolução-TCU nº 342/2022, que dispõe sobre a Política Corporativa de Segurança da Informação (PCSI/TCU) e sobre o Sistema de Gestão de Segurança da Informação do Tribunal de Contas da União (SGSI/TCU).

"...art. 12. Compete à Unidade responsável pela coordenação da Segurança da Informação do TCU [Sesouv]: [...] I - coordenar a implementação e o funcionamento do Sistema de Gestão de Segurança da Informação (SGSI/TCU) e da Política Corporativa de Segurança da Informação (PCSI/TCU), bem como a aplicação da Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e da Lei no 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no âmbito do TCU..."

Então, a Sesouv dispõe da incumbência na coordenação de dois sistemas de gestão:
- Segurança da Informação e
- Continuidade de Negócios

Mencionando alguns projetos da unidade, como exemplo, em que o servidor atua diretamente, temos alguns exemplos acerca da aplicabilidade IMEDIATA do conhecimento adquirido. Na forma de importantes insights e conhecimentos para agregar valor a projetos conduzidos pela unidade, fora a possibilidade de aprofundamento e contatos realizados com outros profissionais certificados ISACA atuantes no mercado global:

- NORMATIZA-SI: trata-se de iniciativa de responsabilidade da Sesouv para modernização do arcabouço normativo de segurança da informação no TCU. Seu primeiro ciclo ocorreu em 2021. Várias normas foram modernizadas. E materialmente mais de dez políticas de SI. Este tipo de trabalho está diretamente relacionado a temáticas de boas práticas, frameworks de mercado, estudo de caso reais, implementação de modelos. E importantes percepções práticas foram trazidas para melhorar nosso arcabouço normativo, sob ponto de vista dos sistemas de gestão coordenados pela Sesouv.

- EDUCA-SI: trata-se de rol de iniciativas relacionadas a competências acerca de fatores comportamentais, cuja responsabilidade encontra-se no escopo de competências da Sesouv. Importante destacar também estar prevista no programa TCU+SEGURO, publicada pela Portaria-TCU nº 74, de 02 de junho de 2021, que institui o Programa Especial de Segurança da Informação do Tribunal de Contas da União (Programa TCU+Seguro). No art. 3º, II, consta a Sesouv como sendo responsável pelo EIXO COMPORTAMENTAL. Nesse sentido, os conhecimentos estão sendo diretamente aplicados em iniciativas educacionais, uma delas inclusive previstas para ter início nesta semana - Conscientização de usuários em segurança cibernética - uma abordagem prática contra phishing. Aliás phishing e

ransomware foram temas AMPLAMENTE discutidos. Disponível: https://contas.tcu.gov.br/ords/f?p=706144:106:15425817648416::NO:106:P106_COD:221730. Há 83 (oitenta e três) inscritos e momento bastante oportuno para compartilhar conhecimentos e trazer conhecimento de borda advindo do Evento ISACA.

- PROTEJA-SI: no mesmo sentido do item anterior, o PROTEJA-SI é um treinamento autoinstrucional de aproximadamente que traz as boas práticas fundamentais sobre segurança da informação. O módulo 1 conta com mais de 600 inscritos em espaço de menos de 2 anos. O treinamento aborda temas fundamentais como phishing, Duplo Fator de Autenticação, Engenharia Social, temas amplamente abordados no evento ISACA. Link https://contas.tcu.gov.br/ords/f?p=ISCNET2_PAR:106:::NO:106:P106_COD:206275

- CONTINUA-SI: trata-se de iniciativa relacionada à Sesouv, com a publicação da Res-TCU nº342/2022. Tem como objetivo assegurar a resiliência organizacional, relacionada a atividades consideradas críticas para o negócio. E nesse sentido, o evento ISACA proporcionou a discussão de casos com aplicação de boas práticas de mercado. Nosso link para a temática de continuidade de negócios. https://tcucloud.sharepoint.com/sites/SI/SitePages/GCN.aspx

- Gestão de incidentes de segurança da informação: A Sesouv é responsável por coordenar o sistema de gestão de segurança da informação (SGSI). E nesse sentido, o inciso V do art. 3º da Res-TCU nº 342/2022 prevê que a gestão de incidentes de SI é um dos processos do SGSI a cargo da Sesouv. Incidentes de segurança, envolvendo ataques de ransomware, phishing e tecnologias emergentes foram AMPLAMENTE discutidas, inclusive sob a apresentação de casos reais. E aqui, é inequívoca a aplicabilidade do conhecimento, particularmente na necessidade de mitigação de riscos de segurança da informação.