RELATÓRIO DE VIAGEM

DADOS DO EVENTO

DATA DE INÍCIO	DATA DE TÉRMINO	NOME DO EVENTO	CIDADE/PAÍS
26 de agosto de 2019	29 de agosto de 2019	Conferência Latinoamericana de Segurança da Informação e Gerenciamento de Riscos (Latin America CACS 2019) e Curso sobre a Certificação CSXF (Certified Cybersecurity Fundamentals)	Santiago/Chile

RESUMO DO EVENTO

ENTIDADE ORGANIZADORA	PROCESSO	PARTICIPANTES
Information System Auditor and Control Association (Isaca)	VIAJAR 460/2019	Harley Alves Ferreira

JUSTIFICATIVA (RESUMO)

Trata-se de relatório circunstanciado referente à minha participação na Conferência Latinoamericana de Segurança da Informação e Gerenciamento de Riscos (Latin America CACS 2019) e no Curso sobre a Certificação CSXF (Certified Cybersecurity Fundamentals), ambos realizados em sequência na cidade de Santiago/Chile, entre 26/8/2019 e 29/8/2019.

O programa do evento foi voltado à atualização de conhecimento, certificações e aperfeiçoamento profissional para auditores de Tecnologia da Informação envolvendo sistemas, segurança cibernética, governança, riscos e compliance. Esse ano foram abordados 3 temas principais, organizados nas seguintes trilhas: Segurança Cibernética e Resiliência; Auditoria de TI; Governo e Riscos de TI.

RELATO

A conferência LatinCacs 2019, que contou com 300 participantes de 19 países, 36 palestrantes e 168 horas de palestras, teve início no dia 26/8/2019, com uma palestra de boas-vindas/abertura que exaltou os 50 anos de existência da Isaca, mostrando sua origem e desenvolvimento ao longo do tempo, atuando na disseminação de boas práticas de auditoria de sistemas, exames de certificação, promoção de eventos e publicação de documentos e frameworks relacionados ao tema. Foi ressaltado que a Isaca conta atualmente com mais de 140.000 membros divididos em 221 capítulos em 188 países ao redor do mundo.

A seguir foi proferida uma palestra inaugural da empresa Delloite abordando aspectos de cyber defesa e respostas a incidentes, na qual foram abordados os seguintes tópicos:

- destacou-se que o custo médio de ataques cibernéticos contra as organizações é de 3.86 milhões de dólares, fora os custos extras de imagem, reputação, legais, etc;
- o sequestro de dados e a extorsão não somente de empresas, mas de órgãos governamentais, como prefeituras, por exemplo, vêm crescendo muito ultimamente;
- a forma como as organizações respondem aos ataques é tão importante quanto os controles de segurança aplicados, pois não existe defesa 100% segura e os incidentes em algum momento podem acontecer, devendo as organizações estarem preparadas para minimizar os danos;
- efetividade, acurácia e velocidade das respostas são essenciais para reduzir os impactos dos incidentes;
- os ataques cibernéticos dependem da conjunção de 3 fatores: criatividade, conhecimento técnico e motivação. Nesse contexto, é preciso que a equipe de defesa trabalhe com os mesmos fatores para ser efetiva.

Na sequência foram assistidas as seguintes palestras técnicas nos dias 26 e 27/8/2019:

- La Inteligencia Artificial avanza, auditoría la alcanza?
- Cybersafety y su impacto en la sociedad. Niños, adolescentes y adultos en peligro
- Eficaz, eficiente y efectivo: auditando agilmente
- Consolidando una cultura de ciberseguridad
- Modelando al atacante. Ataques asímetricos y desaprendizajes
- Ciberinteligencia: Describiendo la naturaleza del desafio
- Ciberseguridad em Chile – CSIRT: Equipo de Respuesta ante Incidentes de Seguridad Informática
- Mejorando la Ciberdefensa, lecciones aprendidas de los ataques al Sistema de Pagos Bancario Mexicano
- Auditoría de Ciberseguridad utilizando los Controles de Seguridad Críticos – CSC definidos por el Center for Internet Security – CIS
- Innovación y Ciberseguridad Blended
- Ciberauditoría práctica con NIST Framework
- Ciberseguridad en el desarrollo de software en tiempos de metodologías ágiles
- Cuantificando la Exposición al Riesgo Cibernético
- Blockchain y criptoactivos, la revolución tecnológica

No bojo dessas palestras, cabe apontar os seguintes tópicos:

- Existência da norma ISO/IEC 27032:2012, internalizada pela ABNT em 2015 (https://www.abntcatalogo.com.br/norma.aspx?ID=334079), que contém diretrizes para melhorar o estado de Segurança Cibernética, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança da informação (recomendo que seja adquirida pelo Tribunal);
- A Segurança Cibernética no Chile está num estágio mais avançado do que no Brasil, com a existência de:
  - uma Equipe Federal de Respostas a Incidentes de Segurança da Informação (CSIRT - https://www.csirt.gob.cl), com possibilidade de registro de incidentes de cyber seguridade por qualquer cidadão;
  - Lei Federal de Tipificação de Delitos Cibernéticos;
  - Lei do Marco de Proteção da Infraestrutura Crítica;
  - Diversos decretos regulamentando: sítios web, sistemas de correio eletrônico, Comitê Interministerial de Segurança Cibernética, padrões de segurança da informação e regulamentação de Lei de telecomunicações;
  - Acordos de cooperação técnica com diversos países, como EUA, Israel, Argentina, Colômbia entre outros (não foi citado o Brasil);
  - Plano de ação para fortalecimento da Segurança Cibernética no país;
  - Promoção de programas nacionais de coinscientização para o setor privado, governo, jovens, idosos, etc.
- Existência da publicação especial NIST SP 800-53 Rev. 4 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) que descreve Controles de segurança e privacidade para Sistemas de Informação e Organizações Federais americanas;
- Existência do CIS CSAT (https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/), ferramenta gratuita para avaliar a implementação de controles CIS, com a atribuição de uma nota de avaliação com pontuação para cada controle e um painel de controle que mostra o nível de maturidade da organização para esse conjunto de controles. Essa nota poderia ser utilizada como um dos componentes do ranking de segurança cibernética que deverá ser criado em Levantamento a ser promovido pela Sefti. Os controles CIS são

um conjunto de controles de segurança criados pela comunidade internacional com base em diretrizes de segurança cibernética priorizadas. Link para download: https://learn.cisecurity.org/cis-controls-download;

- Divulgação do ranking com as Top 10 principais vulnerabilidades da OWASP – Projeto Aberto de Segurança em Aplicações Web (https://www.owasp.org/index.php/Main_Page), que é uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web. O Top 10 OWASP é um ranking que traz as principais vulnerabilidades de segurança em aplicações web e que mais impactaram as empresas no decorrer do período analisado. Realizada periodicamente pela comunidade OWASP, que é a maior referência mundial em segurança web, a análise mostra quais são as falhas críticas que mais possibilitam ataques de pessoas mal-intencionadas e também o que são cada uma destas vulnerabilidades. Confira abaixo o ranking:

1 – Injection (Injeção de Código)

2 – Broken Authentication and Session Management (Quebra de Autenticação e Gerenciamento de Sessão)

3 – Cross-Site Scripting (XSS)

4 – Insecure Direct Object References (Referência Insegura e Direta a Objetos)

5 – Security Misconfiguration (Configuração Incorreta de Segurança)

6 – Sensitive Data Expousure (Exposição de Dados Sensíveis)

7 – Missing Function Level Access Control (Falta de Função para Controle do Nível de Acesso)

8 – Cross-Site Request Forgery (CSRF)

9 – Using Known Vulnerable Components (Utilização de Componentes Vulneráveis Conhecidos)

10 – Unvalidated Redirects and Fowards (Redirecionamentos e Encaminhamentos Inválidos)

- Apresentação de alguns dados preocupantes:
  - 4.4 bilhões de usuários de internet no mundo, navegando num ambiente com mais de 60 mil vulnerabilidades mapeadas, sendo o seguinte cenário nos principais fabricantes: 3.800 nos sistemas SAP, 2.934 na Microsoft, 1.927 na Apple, 1.531 na Oracle, 1.457 na IBM, 1.384 na SUN, 1.147 na Cisco, 1.195 no Mozilla, 944no Linux, 925 na HP e 818 na Adobe;
  - 37% das pessoas já acessaram acidentalmente informação confidencial de colegas de trabalho ou de outros setores;
  - 33% das pessoas afirmam ter acesso a arquivos e documentos de locais de trabalho anteriores;
  - 80% das pessoas não acreditam que são responsáveis por garantir que os documentos institucionais tenham os controles e restrições de acesso adequados;
  - 72% dos empregados armazenam arquivos no trabalho que contém informação pessoal identificada ou dados confidenciais;
  - 6 bilhões de dólares é o custo estimado por danos causados por cyber crimes em 2021.
- Com a evolução e utilização cada vez maior das tecnologias emergentes, surgiram novas portas de entrada para os cyber criminosos: Cloud, Internet das Coisas (IoT), Dispositivos Móveis/BYOD (Bring Your Own Device) e Processos de Automação Robótica. Nesse cenário os desafios das equipes de segurança estão se tornando maiores e mais complexos;
- O uso do Blockchain – tecnologia para habilitar bases de dados distribuídas que admitem vários escritores cujas entradas ocorrem por validação consensual e formam um registro imutável das transações – tem crescido bastante e pode aumentar os níveis de segurança da informação nas organizações. Possui as seguintes características: Descentralização, Múltiplos Atores, Confiabilidade Nativa obtida por meio de seus Protocolos e Regras de Negócio, Imutabilidade dos Registros, Múltipla Propriedade dos Ativos, Sincronização em Tempo Real, Autenticação Baseada em Consenso e Cadeia Cronológica de Atividades.
- A tecnologia de Blockchain pode trazer avanços em diversas áreas, dentre as quais destacam-se:
  - Setor Energético – possibilita a criação de redes elétricas inteligentes com livre mercado e sem a necessidade do uso de baterias e agentes contaminantes, contribuindo para um futuro mais ecológico;
  - Setor de Seguros – contratos inteligentes para uma gestão de demandas mais personalizada, transparente e responsável, possibilitando ativação de cláusulas de maneira automática;
  - Setor Público – votações digitais para fortalecer a democracia; registros ágeis e transparentes dos atos governamentais; finanças públicas visíveis para diminuição da corrupção;
  - Setor de Saúde – registros e prontuários médicos globais e descentralizados, incluindo histórico e antecedentes familiares. Medicina genética acessível na palma da mão;
  - Setor Financeiro – realização de transações interbancárias e internacionais de maneira imediata com baixos custos de comissões e tempos de resposta;

- Setor de Consumo – rastreamento da cadeia de suprimentos para gerar transparência e confiança aos consumidores, com produtos certificados desde a origem da matéria prima até a venda.

- Auditorias de Segurança da Informação, assim como outros tipos de auditoria, podem usar métodos ágeis para imprimir velocidade e efetividade aos trabalhos. Quando se deve usar Ágil:

Ágil	Tradicional
Plano de auditorias extenso e pouco tempo para execução	Auditorias estritamente de conformidade
Necessidade de melhorar as relações com as partes interessadas	Processos muito padronizados e previamente auditados
Necessidade de relatórios de maior impacto e valor agregado ao negócio	Auditorias forenses

Principais diferenças entre auditorias ágeis e tradicionais:

Ágil	Tradicional
Comunicação frequente durante todo o processo	Comunicação completa após um longo processo
Atividades rápidas e iterativas	Atividades planificadas e rígidas
Documentação relevante e oportuna	Documentação completa e exaustiva
Papéis designados em um sistema flexível	Papéis estabelecidos em um sistema hierárquico
Respostas a riscos emergentes	Segue o plano da auditoria
Transparência plena em todo o processo	Controle da transparência em todo o processo

- Marcos de referência e regulamentação específica imaturos, bem como a falta de um guia específico para auditoria em Inteligência Artificial (IA) dificultam a execução de auditorias nessa tecnologia emergente, que deve:
  - Concentrar-se nos controles e segurança dos dados, evitando focar nos algoritmos;
  - Preparar a equipe para uma curva pronunciada de aprendizagem sobre auditoria de IA;
  - Contratar especialistas em IA se for necessário;
  - Atentar para os riscos dos provedores causados pela terceirização das atividades de IA;
  - Documentar as lições aprendidas e fomentar compartilhamento das informações entre as equipes.
- Existência do framework 'Guia de Auditoria de Cyber Seguridade' da Isaca, que prevê as seguintes funções para uma gestão de riscos de segurança cibernética nas organizações:
  - Identificar os ativos/serviços críticos para o negócio e suas ameaças;
  - Proteger a infraestrutura tecnológica que suporta esses ativos/serviços;
  - Detectar a ocorrência de eventos de Cyber seguridade;
  - Responder aos eventos detectados;
  - Recuperar os ativos/serviços afetados e sua infraestrutura tecnológica.
- O guia da Isaca prevê os seguintes níveis de implementação do Marco, do menor para o maior: Parcial, Risco Informado, Repetível e Adaptável.

Posteriormente, nos dias 28 e 29/8/2019 foi ministrado Curso sobre a Certificação CSXF (Certified Cybersecurity Fundamentals), que abordou conceitos relacionados à Segurança Cibernética e uma preparação inicial para o exame de certificação. O material do curso está disponível no _sarq_prod\Unidades\sefti\Eventos\LatinCacs2019.

Durante o curso também foram acessados diversos links com materiais de apoio importantes relacionados ao tema:

https://www.us-cert.gov/resources/assessments

https://www.nist.gov/cyberframework/assessment-auditing-resources

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx

https://www.nacdonline.org/files/NACD%20Cyber-Risk%20Oversight%20Executive%20Summary.pdf

http://www.isaca.org/Knowledge-Center/Research/Documents/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask_res_Eng_0814.pdf

https://www.isaca.org/info/state-of-cybersecurity-2019/index.html

https://apt.securelist.com/

https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

https://es.khanacademy.org/computing/computer-science/cryptography

https://www.youtube.com/channel/UCAUGS3VUpTF9FRdg10BThuw/videos?view=0&sort=dd&shelf_id=1&view_as=subscriber

http://www.isaca.org/cyber/pages/self-assessment.aspx?id=100000&utm_referrer

https://cybersecurity.isaca.org/csx-resources

https://cybersecurity.isaca.org/csx-nexus

https://cybersecurity.isaca.org/info/pathways/index.html?cid=pr_1237248&appeal=pr

https://nexus.isaca.org/products

https://cybersecurity.isaca.org/csx-learning/csx-foundations-series-course-bundle

https://cybersecurity.isaca.org/csx-certifications/csx-fundamentals-certificate

https://cybersecurity.isaca.org/csx-certifications/csx-practitioner-certification

http://www.isaca.org/info/cybersecurity-audit/index.html

Informações mais detalhadas sobre o evento podem ser consultadas por meio do endereço eletrônico http://latincacs2019.com.

ENCAMINHAMENTOS POSSÍVEIS, NO ÂMBITO DO TCU, DECORRENTES DESTA AÇÃO

Considera-se importante realizar as seguintes ações no âmbito do Tribunal em decorrência da participação no LatinCacs 2019:

Compartilhamento deste relatório e das apresentações realizadas no encontro com os demais colegas da Secretaria de Fiscalização de Tecnologia da Informação (Sefti), que é a unidade do TCU especializada em auditorias de TI;

Utilização do conhecimento adquirido na Supervisão do trabalho previsto no planejamento da Sefti que fará um Levantamento da situação da segurança cibernética na APF e propor uma Estratégia de atuação do Tribunal para induzir as melhorias necessárias.