Una guía metodológica para la elaboración de libros de jugadas (playbooks) para riesgos cibernéticos.

Jeimy J. Cano M.
Universidad de los Andes
Colombia

Agenda

- ✓ Introducción
- ✓ Riesgos de tecnología de información y los riesgos cibernéticos
- ✓ Libros de jugadas. Conceptos y estructura general
- ✓ Guía metodológica para construir libros de jugadas para riesgos cibernéticos específicos
- ✓ Aplicación de la guía metodológica para construir libros de jugadas para riesgos cibernéticos específicos
- ✓ Conclusiones
- ✓ Referencias

Introducción

Contexto global. *Inestabilidad e incierto*

1 Everything goes digital
The pandemic accelerated digital transformation of business, government, and social interaction.

2 Work becomes riskier
The rise of a remote or freelance workforce multiplies risks from the use of more devices outside corporate perimeters.

3 Organizations morph into ecosystems
Businesses and cities become elaborate networks of partners and suppliers as the platform economy takes shape.

4 Physical and digital worlds collide
Digitally connected physical assets expose strategic infrastructure to greater attack.

5 New technologies emerge
AI, IoT, multi-cloud, and 5G create cyber vulnerabilities for organizations and provide more advanced weapons for criminals.

6 Cyber adversaries up their game
Cybercrime becomes a big business through ransomware; threat actors become smarter, better organized, and more institutionalized.

7 Cyber warfare ushers in a new risk era
Russia's attack on Ukraine marks a new wave of geopolitical volatility, making cyber warfare a greater threat in the free world.

8 Regulations become more complex
Cybersecurity worries prompt a maze of new regulations around the world, from the US to the EU and Asia.

Tomado de: ThoughtLab (2022). Cybersecurity Solutions for a Riskier World. How business and government can protect themselves in the emerging risk landscape. *Report*. https://thoughtlabgroup.com/wp-content/uploads/2022/05/Cybersecurity-Solutions-for-a-Riskier-World-eBook_FINAL-2-1.pdf

Contexto global. *Fundamentos del adversario*

INTELIGENCIA
(*Perfilación de las organización y las personas objetivo*)

DISTRACCIÓN
(*Ataques conocidos*)

ENGAÑO
(*Creación de historia creíble*)

Contexto global. *Incremento de ataques*

Ataques visibles de alcance nacional e internacional

Aquellos cuya visibilidad e impacto es nacional e internacional.

Ataques visibles en el sector de industria

Aquellos cuya visibilidad ha sido manifiesta en medios de comunicación y reportes de industria.

Ataques a empresas similares

Aquellos que afectan a empresas del mismo sector de negocio.

Ataques directos

Aquellos que afectan directamente los procesos, sistemas e infraestructura propia.

Ataques contra terceros estratégicos

Aquellos dirigidos contra aliados estratégicos que soportan el modelo de negocio.

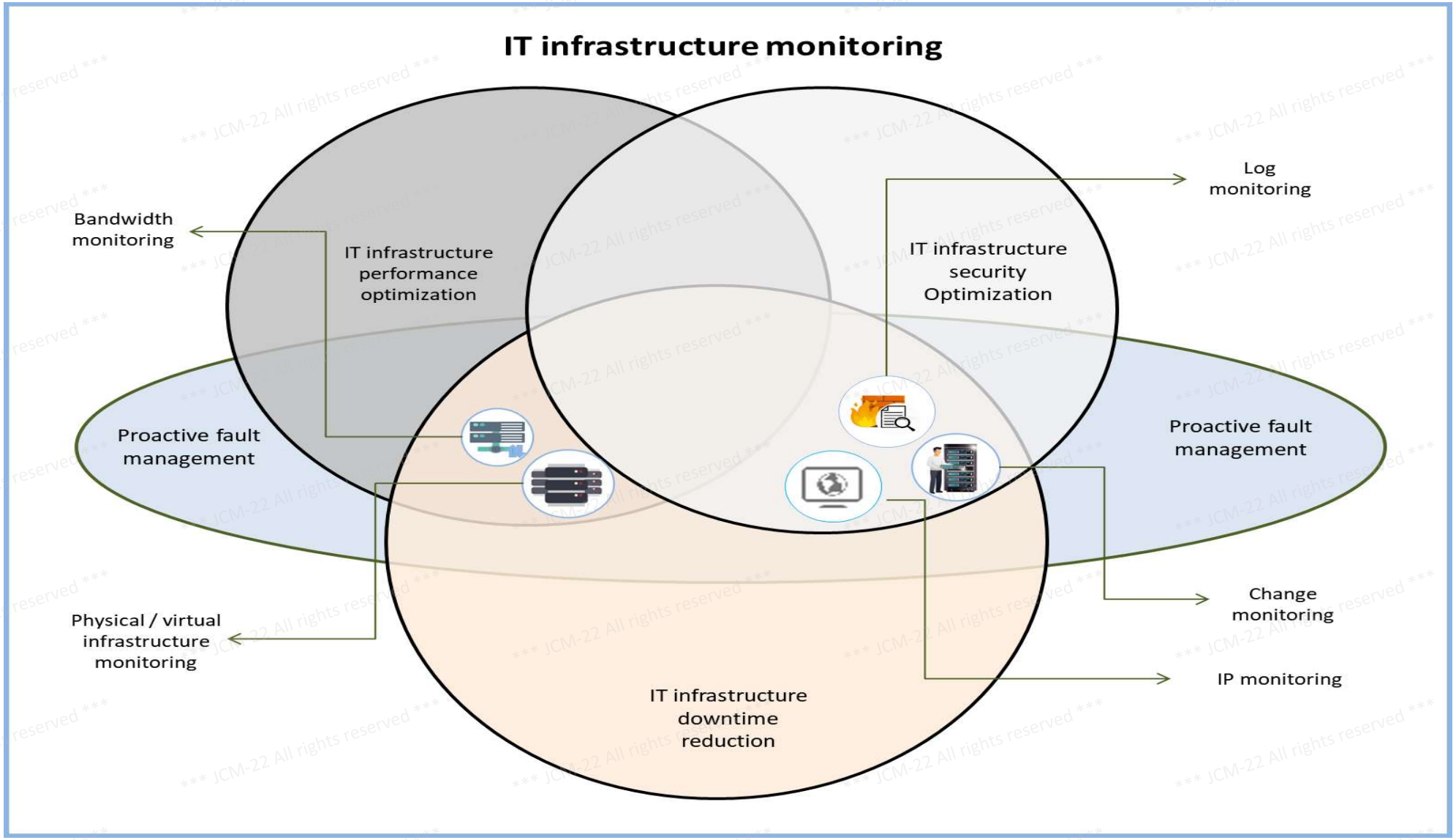
Adaptado de: Zeijlemaker, S. (2022). *Managing the dynamic nature of cyber security. A future-proof strategy, this is how it works*. Netherlands. Disem Institute. P. 85-86

Pregunta central

¿Cómo desarrollar un "libro de jugadas" (*playbook*) en el contexto del gobierno y gestión de la ciberseguridad/seguridad de la información de las empresas?

Riesgos de tecnología de información y los riesgos cibernéticos

Riesgo de tecnología de información (TI)



Fuente: https://manageengine.com.mx/opmanager-plus/supervision-de-la-infraestructura-de-ti

Riesgo cibernético

Es un riesgo que se *expande y cambia* frecuente y rápidamente

Es un riesgo sistémico, donde una *pequeña falla* puede *alcanzar todo el sistema*

Es un riesgo *de alta complejidad* para entender sus impactos

Es un riesgo cuya mitigación *implica abarcar distintas tecnologías y proveedores*

Es un riesgo donde las *personas y los procesos son parte fundamental*

Es un riesgo cuyo efectos se evidencian en *las interconexiones e interdependencias de los sistemas*

Es un riesgo en el cual se tiene *poca experiencia a nivel ejecutivo*

Basado en: Zukis, B., Ferrillo, P. & Veltos, C. (2020). *The great reboot. Succeeding in a world of catastrophic risk and opportunity*. USA: DDN Press. P. 98-99

Riesgo TI y Riesgo Cibernético

	Riesgos de Tecnología de Información	*Riesgos Cibernéticos*
Fundamento:	Reducción de costos	*Apetito al riesgo*
Foco:	Operación/Proceso	*Negocio/Promesa de valor*
Tipo:	Conocidos	*Sistémicos*
Gestión:	Estándares y prácticas	*Capacidades y patrones*
Orientación:	Continuidad del negocio	*Resiliencia del negocio*
Estrategia:	Mitigación	*Umbrales de operación*
Objetivo:	Proteger y asegurar	*Defender y anticipar*

Basado en: Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas. 63-73. https://doi.org/10.29236/sistemas.n151a5

Libros de jugadas.

Conceptos y estructura general

¿Qué son?

Una *estrategia* para actuar de forma coordinada

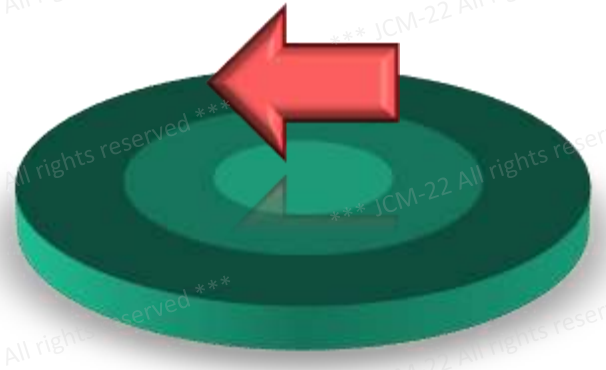
Una *estructura* para la toma de decisiones

Una *respuesta* a escenarios conocidos y latentes

Una *forma de gestionar* riesgos

¿Qué estructura tienen?

ANTES

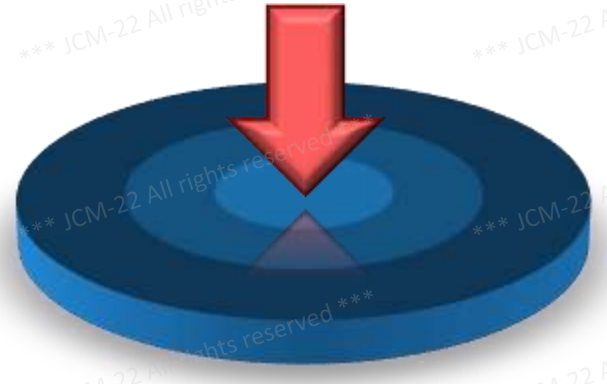


Preparación:
- Puntos de contacto y áreas requeridas
- Plan legal definido

Detección:
- Alertas identificadas

Análisis:
- Posibles consecuencias y efectos

DURANTE

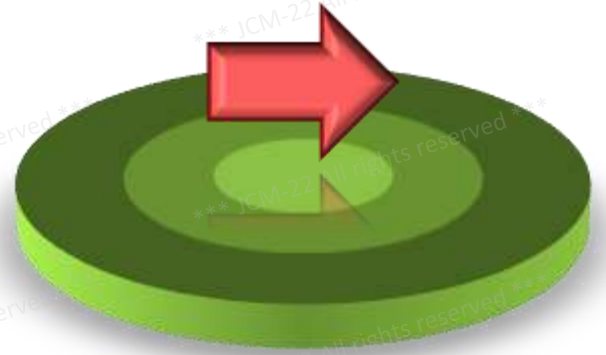


Contención:
- Prevención de daños

Erradicación:
- Inhabilitar fuente de ataque

Remediación:
- Reconfigurar y actualizar

DESPUÉS



Recuperación:
- Plan de vuelta a la "nueva normalidad"
- Activación plan legal

Lecciones aprendidas:
- ¿Qué se deja de hacer?
- ¿Qué se mantiene?
- ¿Qué se va a hacer diferente?

Basado en: Vasella, T. (2020). Incident response playbooks. Indispensable in future crisis situation. De: https://www.scip.ch/en/?labs.20190103

¿Cuáles son los resultados esperados?

01 Comunicaciones

Internas y externas. Tono y foco de los mensajes.

02 Coordinación

De las operaciones y equipos de trabajo.

03 Comprensión

Del evento o eventos y sus relaciones.

04 Calidad

De las respuestas y resultados.

05 Conciencia

De las situaciones y sus implicaciones a nivel organizacional.

Guía metodológica para construir libros de jugadas para riesgos cibernéticos específicos

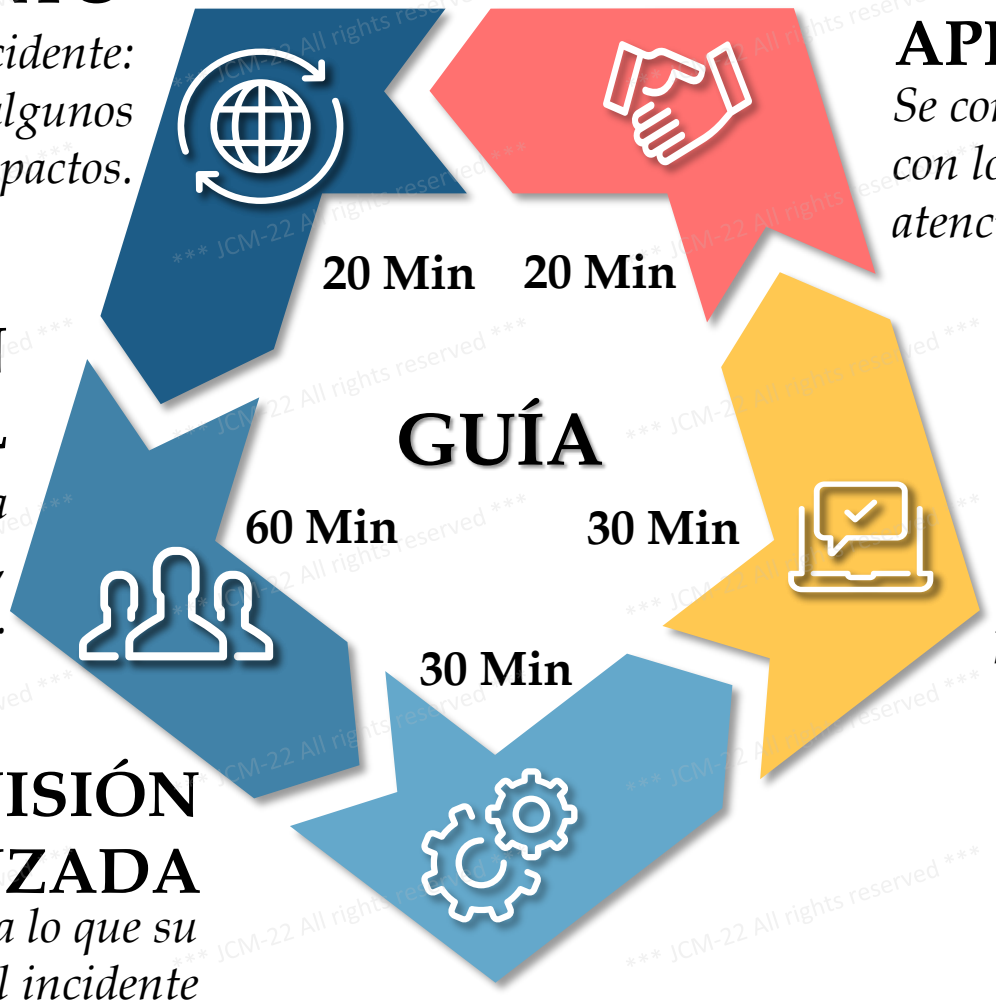
Guía metodológica

CONTEXTO

Presentación conceptual del incidente: definición, características, algunos indicadores y posibles impactos.

RESUMEN DE APRENDIZAJES

Se consolidan las reflexiones y aprendizajes con los elementos de ajuste requeridos en la atención del incidente.



PARTICIPACIÓN INDIVIDUAL

Cada uno de los participantes detalla según su realidad qué haría antes, durante y después del incidente.

CONSTRUCCIÓN CONJUNTA

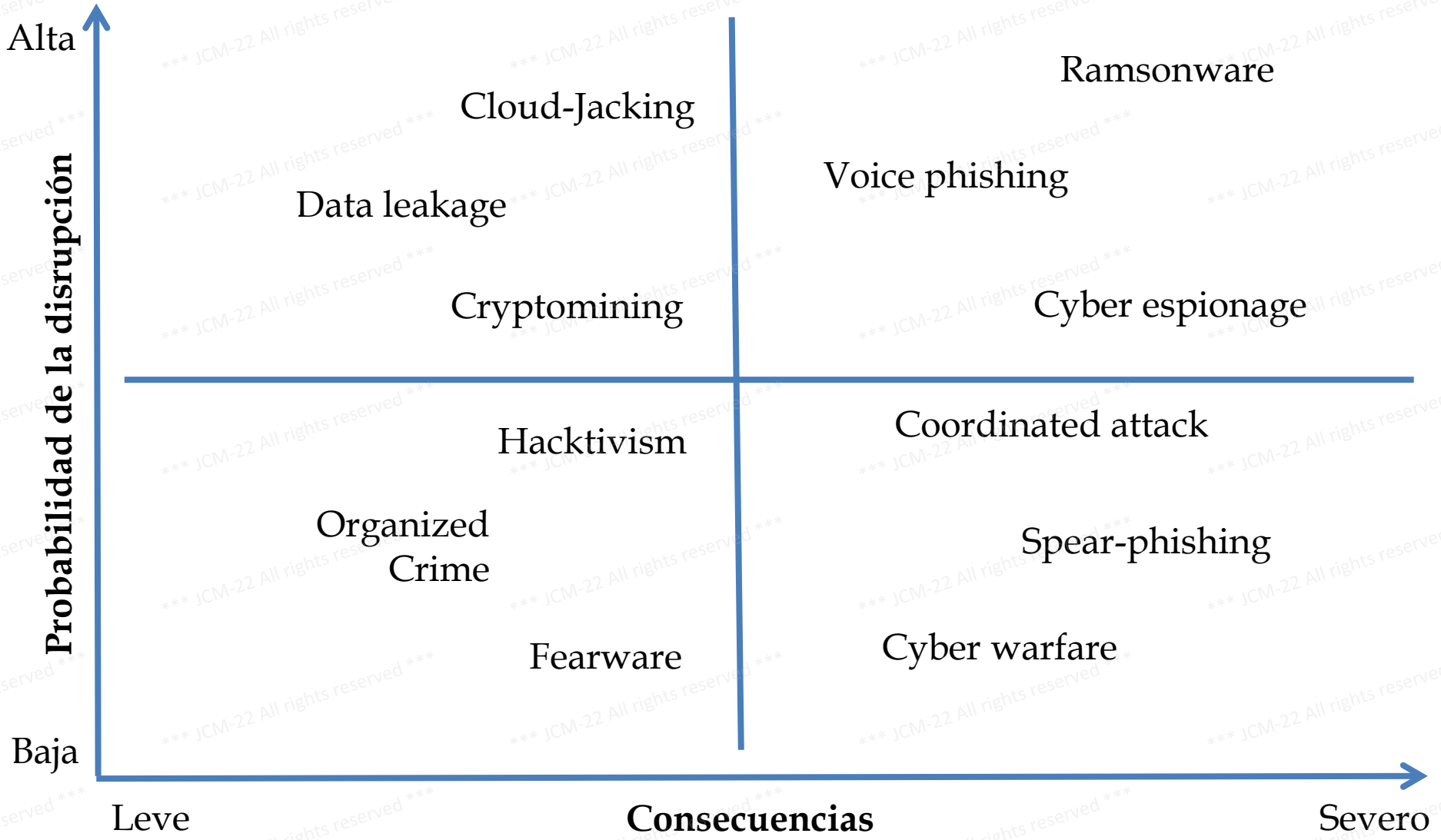
Espacio de reflexión para compartir puntos de encuentro, desencuentro y brechas.

REVISIÓN CRUZADA

Cada participantes revisa y analiza lo que su par efectúa en cada momento del incidente (antes, durante y después).

Aplicación de la guía metodológica para construir libros de jugadas para riesgos cibernéticos específicos

Aplicación de guía metodológica. *Valoración de riesgos cibernéticos*



Aplicación de guía metodológica. *Contexto*

Despliegue	Instalación	Ejecución
• Ingeniería social • Sitios web • Macros en documentos • Infección autónoma • Descargas • Botnets • Mensajes fraudulentos	Payload Creación de carpetas Ocultamiento Inyección de procesos Ofuscamiento Deshabilitar servicios Elevación de privilegios Comando & Control	Archivos cifrados Mensaje de recuperación Exigencia de pago

Definición: Tipo de **malware** que **secuestra y cifra** los **archivos** en un sistema de almacenamiento, para luego pedir un **rescate**, generalmente a través de **pagos mediante criptomonedas**, sin la garantía de que todos los archivos puedan ser descifrados o sean devueltos con las mismas condiciones

Tomado de: Osorio, A., Mateus, M. & Vargas, H. (2020) Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*. 13(3). 131-142. doi: 10.18273/revuin.v19n3-2020013

Aplicación de guía metodológica. *Participación individual*

Aplicación de guía metodológica. *Revisión cruzada*

Aplicación de guía metodológica. *Construcción conjunta*

Aplicación de guía metodológica. *Resumen de aprendizajes*

Conclusiones

Reflexiones finales

- El **riesgo cibernético** se caracteriza por ser *incierto, inestable y no lineal*, evoluciona y se transforma de forma permanente.
- La **construcción de un LJ/PB** se convierte en un reto empresarial para fundar una vista conjunta y holística de las actividades que se requieren para orquestar un incidente.
- **Un LJ/PB** habilita lugares comunes de conversación entre las diferentes áreas de la organización: confianza, coordinación, cooperación, colaboración y comunicación.
- **La guía metodológica** ofrece una intervención abierta, activa y transparente de cada uno de los participantes del ejercicio:
  - Representación real
  - Revelación de posibles puntos ciegos vigentes
  - Músculo de memoria colectiva

Referencias

Referencias

- [1] EY: "Are you reframing your future or is the future reframing you? Megatrends 2020 and beyond". EY Megatrends. https://assets.ey.com/content/dam/ey-sites/eycom/en_gl/topics/megatrends/ey-megatrends-2020-report.pdf, 2020.
- [2] Vasella, T: "Incident response playbooks. Indispensable in future crisis situation". https://www.scip.ch/en/?labs.20190103, 2020.
- [3] Caltagirone, S., Pendergast, A. & Betz, C.: "The Diamond Model of Intrusion Analysis". US Department of Defense. Technical Report. https://apps.dtic.mil/sti/pdfs/ADA586960.pdf, 2013.
- [4] Cano, J.: "De las incertidumbres claves, los "libros de jugadas" y la gestión dinámica de riesgos. Conceptos que retan el statu quo de la ciberseguridad empresarial". Global Strategy. Global Strategy Report. No.8. https://global-strategy.org/de-las-incertidumbres-claves-los-librosde-jugadas-y-la-gestion-dinamica-de-riesgos-conceptos-que-retan-elstatu-quo-de-la-ciberseguridad-empresarial/, 2021.
- [5] Hoffman, W. & Levite, A.: "Private sector cyberdefense. Can active measures help stabilize cyberspace". Washington, D.C., USA Carnegie Endowment for International Peace. https://carnegieendowment.org/2017/06/14/private-sector-cyber-defensecan-active-measures-help-stabilize-cyberspace-pub-71236, 2017.
- [6] W. Stallings, Effective cybersecurity. A guide to using best practices and standards. New York, USA: Addison Wesley, 2018.
- [7] Cano, J., "Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo". Revista SISTEMAS. Asociación Colombiana de Ingenieros de Sistemas. 63-73. https://doi.org/10.29236/sistemas.n151a5, 2019.
- [8] Donaldson, S., Siegel, S., Williams, C. & Aslam, A., Enterprise Security. How to build a successful cyberdefense program against advanced threats. New York, USA: Apress, 2015
- [9] Eling, M. & Schnell, W., "What do we know about cyber risk and cyber risk insurance?" The Journal of Risk Finance. 17(5). 474-491. Doi: https://doi.org/10.1108/JRF-09-2016-0122, 2016.
- [10] Bollinger, J., Enright, B. & Valites, M., Crafting the InfoSec Playbook. Sebastopol, CA. USA: O'Reilly, 2015.
- [11]Espejo, R. & Reyes, A., Sistemas organizacionales. El manejo de la complejidad con el modelo del sistema viable. Bogotá, Colombia: Universidad de los Andes-Universidad de Ibagué, 2016.
- [12] Angafor, G., Yevseyeva, I. & He, Y., "Game-based learning: A review of tabletop exercises for cybersecurity incident response training". Security and Privacy. 3:e126. https://doi.org/10.1002/spy2.126, 2020.
- [13] Sheffi, Y., The Resilient Enterprise. Overcoming Vulnerability for Competitive Advantage. Cambridge, MA. USA. MIT Press, 2005.

Referencias

- [14] Daniel, M., “Why Is Cybersecurity So Hard?” Harvard Business Review. https://hbr.org/2017/05/why-is-cybersecurity-so-hard, 2017.
- [15] Sieber, S. & Zamora, J., “The Cybersecurity Challenge in a High Digital Density World”. European Business Review. November. https://www.europeanbusinessreview.com/the-cybersecurity-challengein-a-high-digital-density-world/, 2018.

Una guía metodológica para la elaboración de libros de jugadas (playbooks) para riesgos cibernéticos.

Jeimy J. Cano M.
Universidad de los Andes
Colombia