El rol de la auditoría interna en la gestión de incidentes de ciberseguridad

Andrés Casas

Jornada 2022

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Andrés Casas

andres.casas@brakk.us

Jornada 2022

BRAKK nearshore cyber security

CQBIT 2019 Foundation An ISACA® Certificate

CISA CRISC CISM CGEIT CSX-P CDPSE

CISSP® Certified Information Systems Security Professional

AXELOS ITIL MANAGING PROFESSIONAL

PMP

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Agenda

Jornada 2022

- El hostil mundo de los ciber-ataques
- Conceptos clave
- Ciclo de vida de la gestión de incidentes

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Agenda

Jornada 2022

- **EL HOSTIL MUNDO DE LOS CIBER-ATAQUES**
- Conceptos clave
- Ciclo de vida de la gestión de incidentes

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Jornada 2022

1960

Término “hacker” nació

La única intención era experimentar, e incluso mejorar, las opciones de los programas que existían

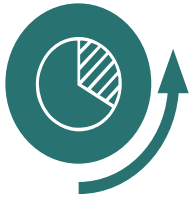
01

1970

Phreaker

Personas que se especializan en ataques al sistema telefónico.

02



1980

Edad de Oro del Hacking

pequeños delitos, pirateando software, creando virus y hackeando sistemas para robar información valiosa. Primer Gusano.

03

1990

Crackers

Robo de software de grandes empresas, fraude a una estación de radio para ganar un coche a sorteo y por el primer robo digital a una institución financiera.

04

2000

Germinación

correo electrónico con el asunto “ILOVEYOU”. Ataques masivos a grandes empresas como Microsoft, eBay, Yahoo y Amazon

05

Actual

Personas y el Internet

La comunidad de piratas informáticos se está volviendo más sofisticada, compleja y difícil de controlar que nunca

06

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Jornada 2022

USD$ 400,000,000,000

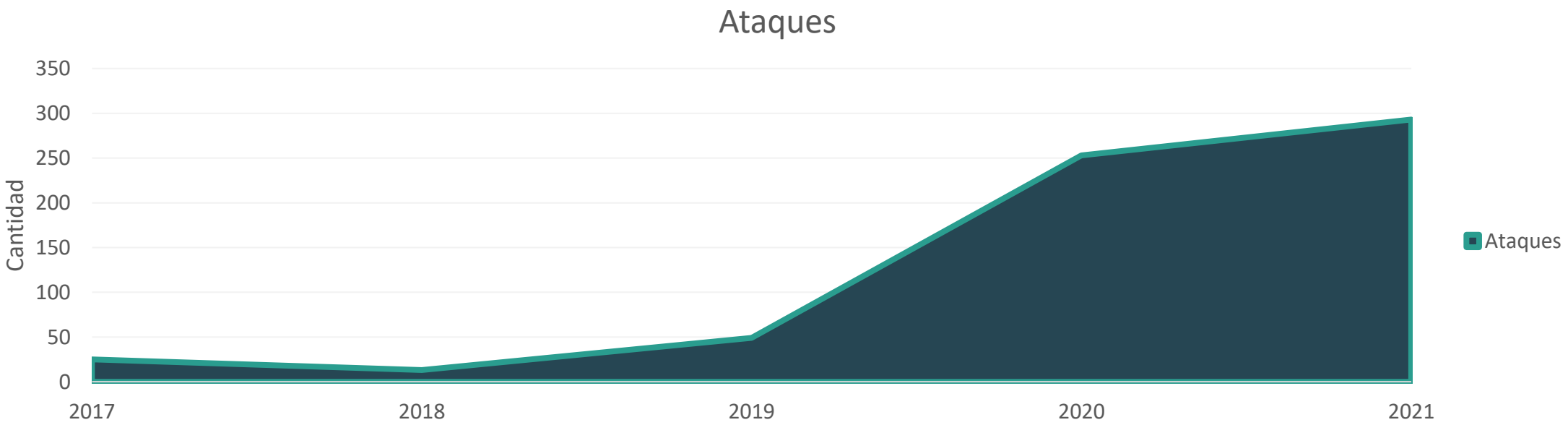
USD$ 6,000,000,000,000

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Jornada 2022

Incremento de ataques ransomware



Fuente: Five Lessons Learned from Over 600 Ransomware Attacks, RiskRecon MasterCard

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

¿Cuál es su mayor preocupación por el crimen cibernético?

Jornada 2022

El FBI presentó informes de casi $ 2.4 mil millones en pérdidas de víctimas por estafas BEC en 2021. Eso fue 49 veces más que el rendimiento del ransomware reportado al FBI ($ 49.2 millones), y más de un tercio del total de delitos cibernéticos ($ 6.9 mil millones).

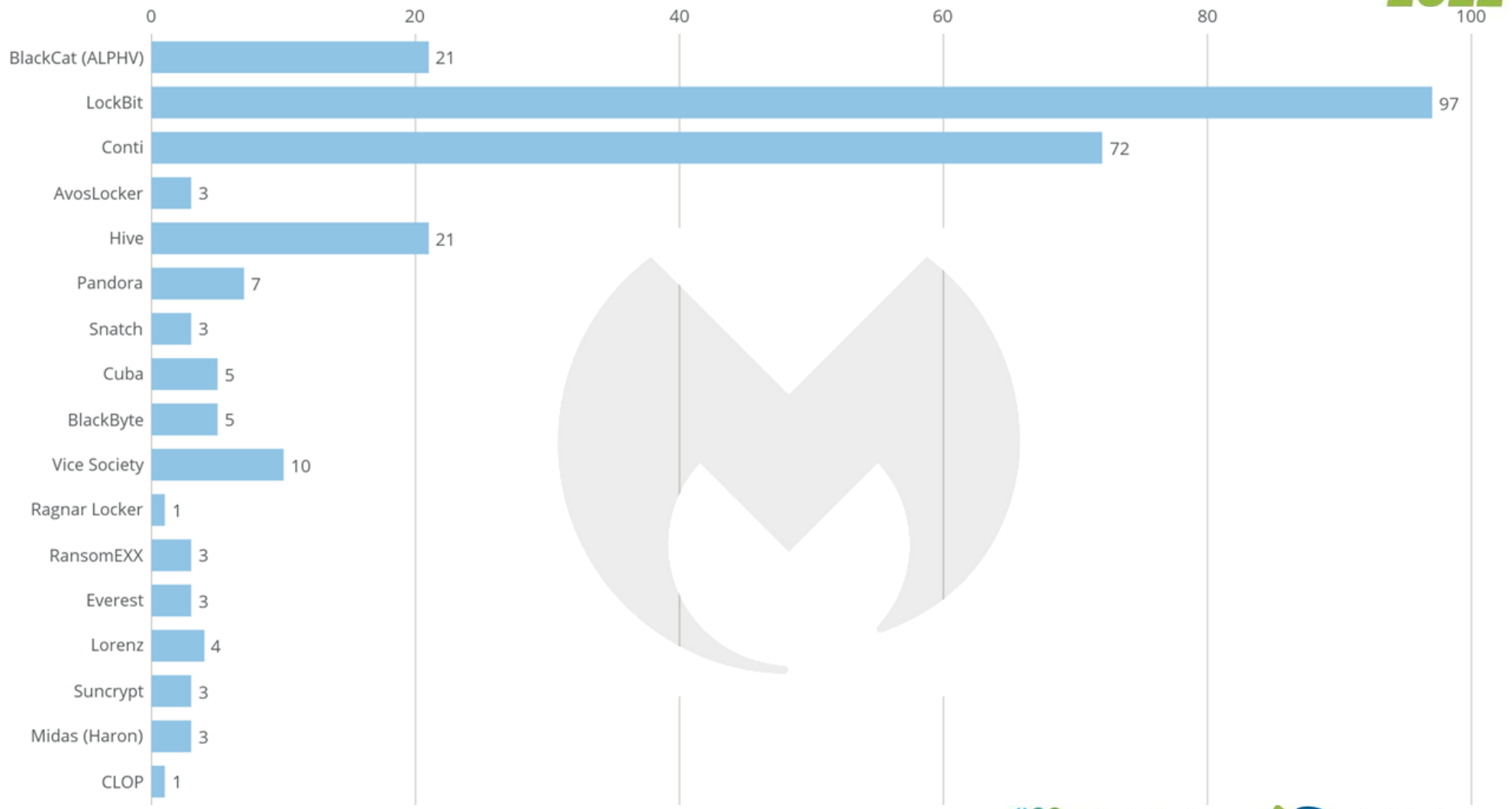
Fuente: Internet Crime report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ataques de ransomware por banda

Jornada 2022

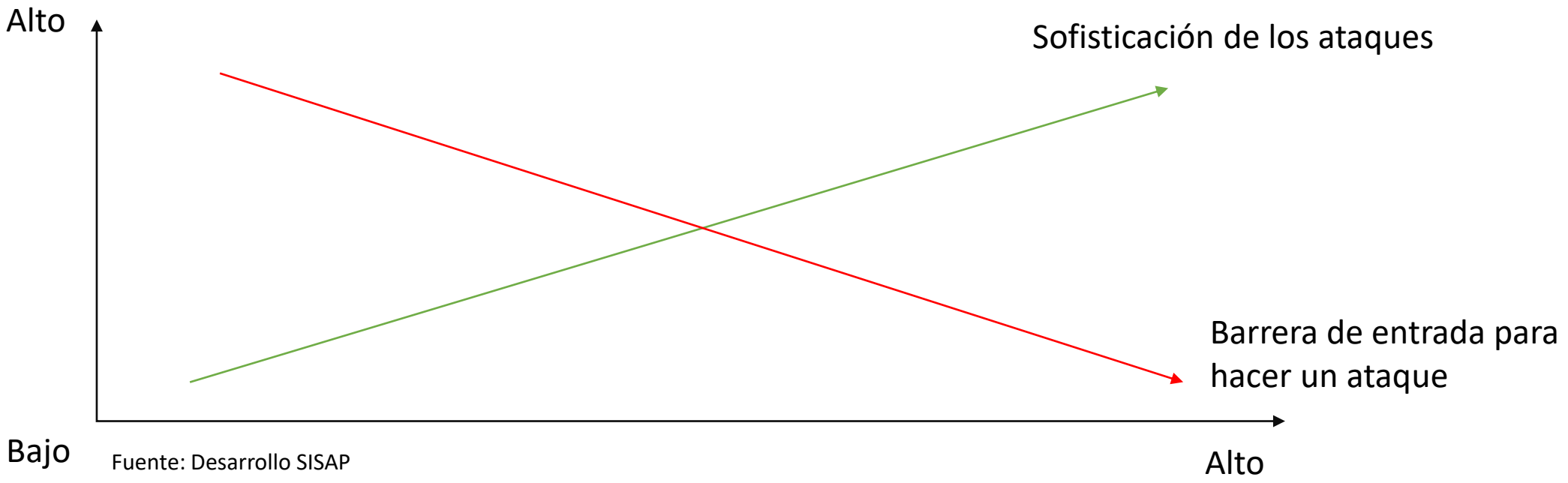


ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ingreso al mercado

Jornada 2022



Fuente: Desarrollo SISAP

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ingreso al mercado

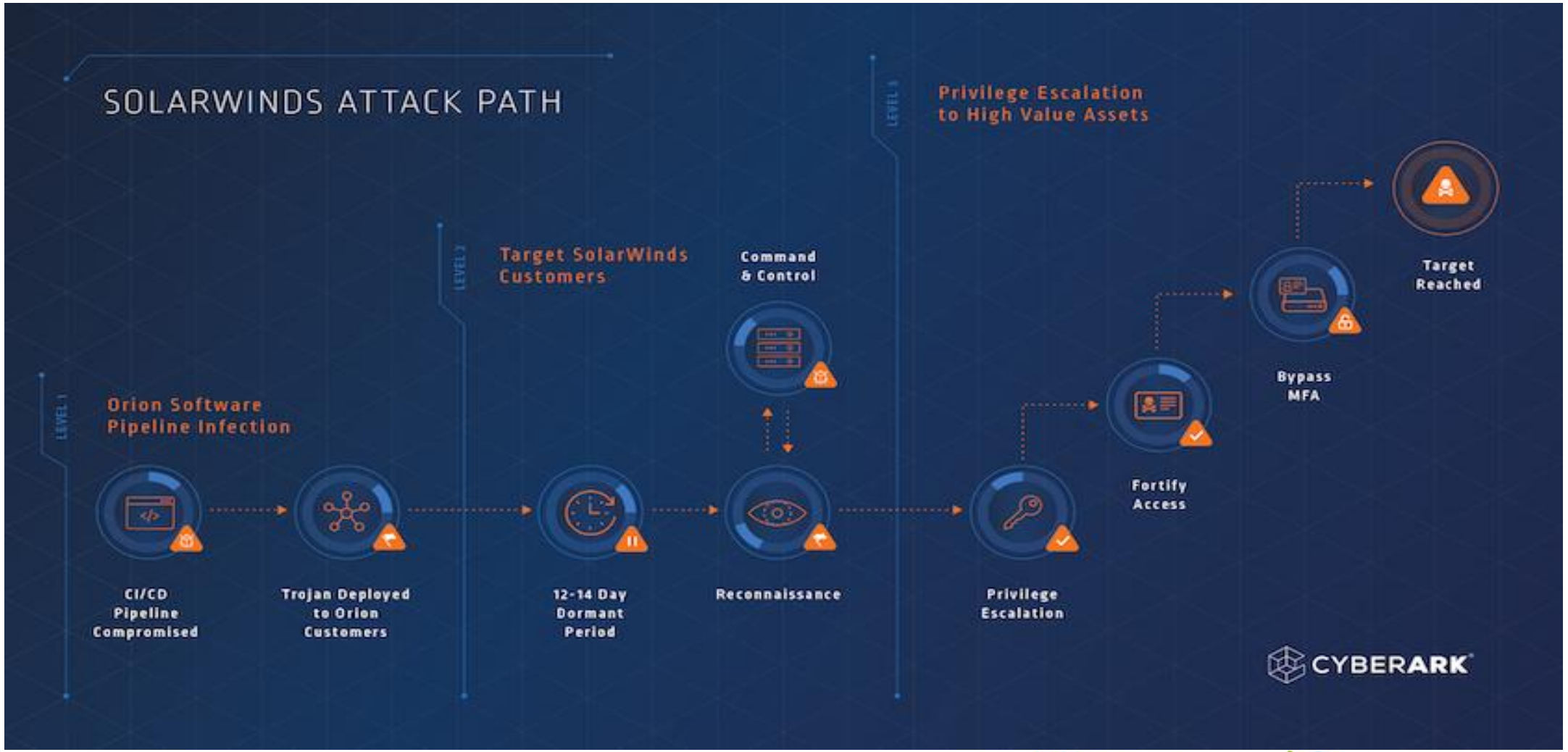
Jornada 2022

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Caso SolarWinds

Jornada 2022



ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Agenda

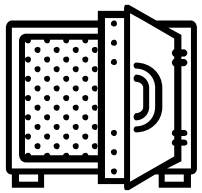
Jornada 2022

- El hostil mundo de los ciber-ataques
- **CONCEPTOS CLAVE**
- Ciclo de vida de la gestión de incidentes

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Jornada 2022

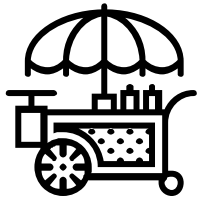


Confidencialidad

Garantizar la privacidad de los datos.

Integridad

Garantizar que la información sea precisa y confiable.



Disponibilidad

Garantizar que la información esté disponible a las personas autorizadas.

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Amenaza

Vulnerabilidad

Evento/Alerta

Incidente

Activo de Información

Incidente

Fuente: ISO 27035 – Técnicas de seguridad Gestión de incidentes de seguridad de la información

Jornada 2022

Amenazas

Causa **potencial** de un **incidente no deseado**, el cual puede ocasionar daño a un sistema o a una organización.

Vulnerabilidad

Debilidad de un activo o de un **control** que puede ser explotada por una o más **amenazas.**

Fuente: ISO 27035 – Técnicas de seguridad Gestión de incidentes de seguridad de la información

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Criterios

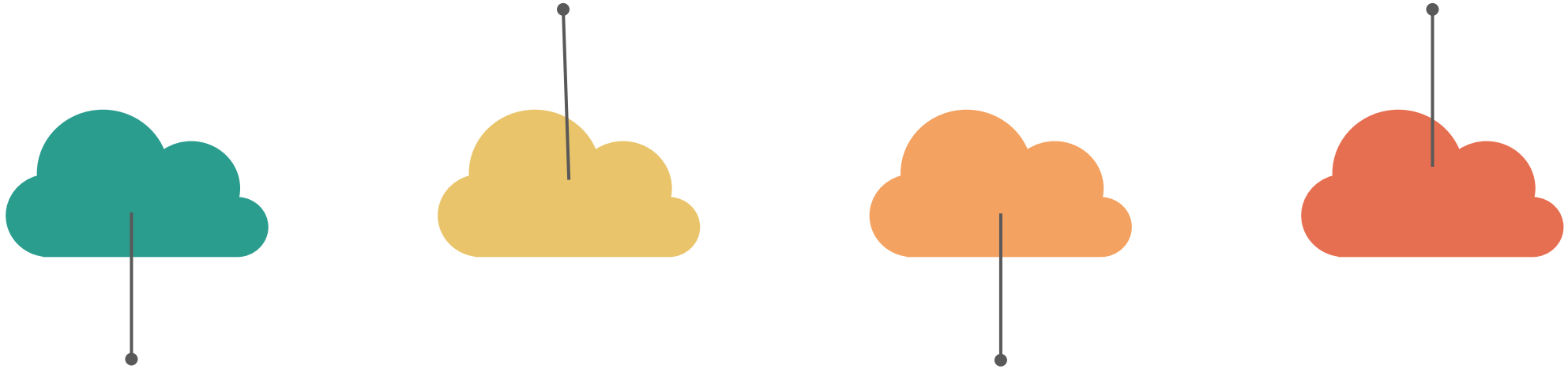
Jornada 2022

COBIT 2019

Marco: Objetivos de gobierno y gestión

NIST CSF

Cyber Security Framework



ISO 27035

Técnicas de seguridad
Gestión de incidentes de seguridad de la información

NIST.SP.800

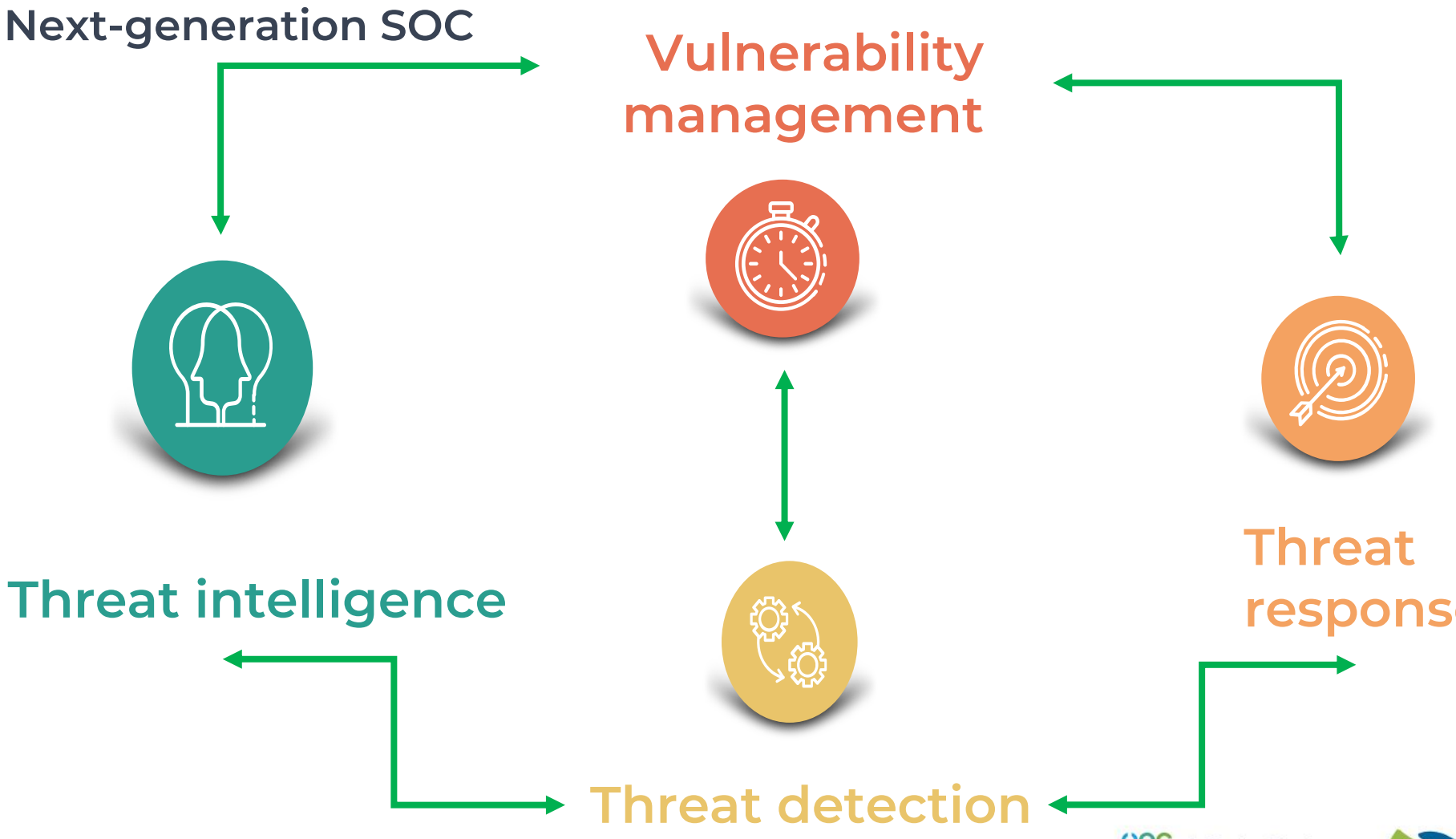
Incident Handling Guide

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Cyber Fusion Center

Jornada 2022



ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Agenda

Jornada 2022

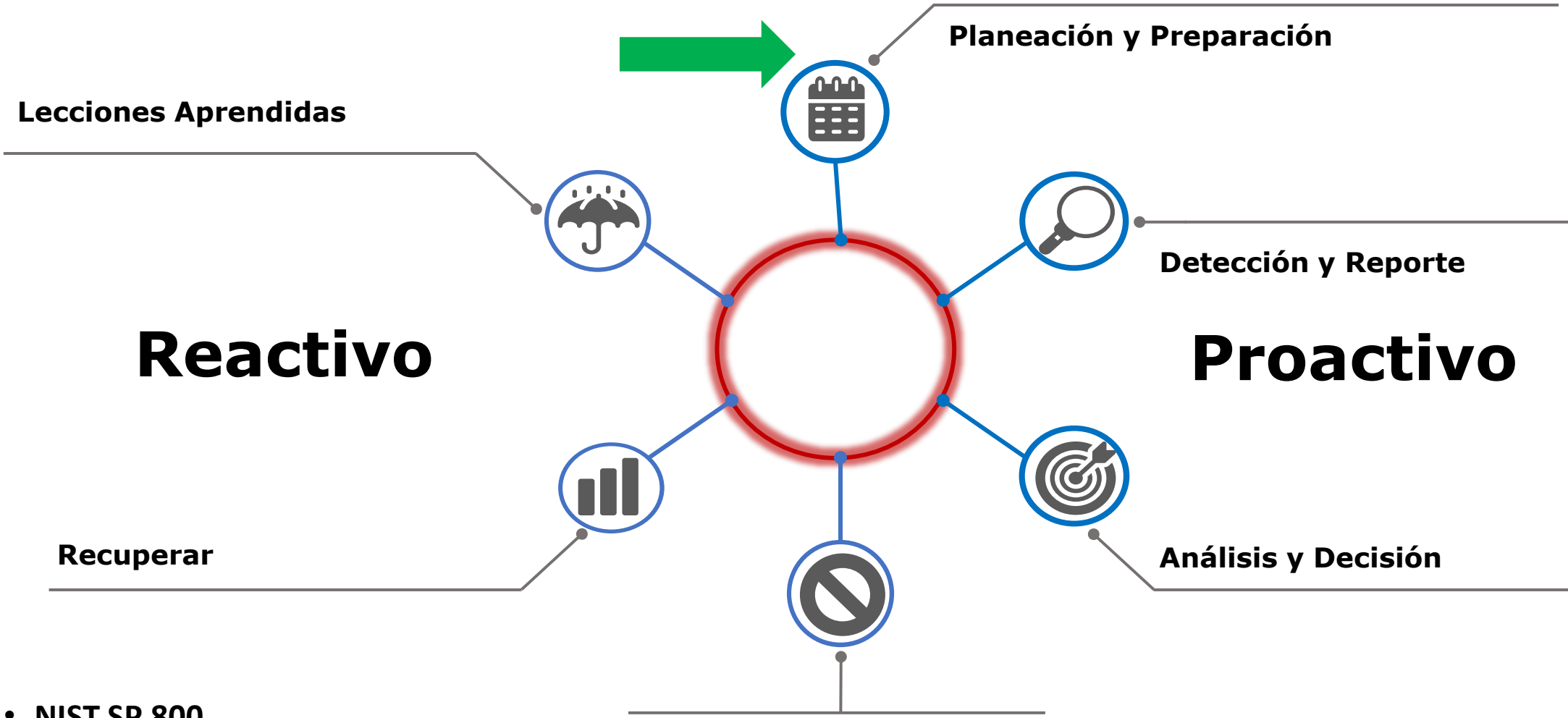
- El hostil mundo de los ciber-ataques
- Conceptos clave
- **CICLO DE VIDA DE LA GESTIÓN DE INCIDENTES**

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida

Jornada 2022



- NIST SP 800
- ISO 27035

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida - Planeación y preparación

Jornada 2022

01 **Alinear la estrategia del negocio con los objetivos de seguridad Para la gestión de incidentes.**

02 **Definir políticas y procedimientos de seguridad.**

03 **Ejecutar un análisis de riesgos de seguridad.**

04 **Establecer un plan de gestión de incidentes de seguridad.**

05 **Definir los equipos de respuesta a incidentes.**

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida - Planeación y preparación

Jornada 2022

06 **Establecer relaciones y conexiones.**

Definir el soporte técnico y otros. 07

08 **Definir el soporte técnico y otros.**

Pruebas. 09

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida - Planeación y preparación

Jornada 2022

06 **Establecer relaciones y conexiones.**

Definir el soporte técnico y otros. 07

08 **Definir el soporte técnico y otros.**

Pruebas. 09

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida - Planeación y preparación

Jornada 2022

Cada organización debería documentar una política para la gestión de eventos, incidentes o vulnerabilidades de seguridad, como parte de su política holística para la gestión de seguridad de la información. Algunos de sus componentes clave son:

- Debe ser documentada a alto nivel.
- Debe establecer el propósito, objetivos y alcance de la política.
- Debe establecer la importancia de la gestión de incidentes para la organización.
- Debe establecer qué se considera como un incidente de seguridad para la organización.
- Debe incluir una descripción de las categorías de incidentes de seguridad.
- Debe definir las responsabilidades de las partes interesadas.
- Debe establecer las autoridades y líneas de reporte y comunicación.
- Debe establecer cualquier iniciativa de concientización y capacitación que requiera el personal.
- **Debe estar aprobada por la alta gerencia.**

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Gestión de riesgos

Jornada 2022

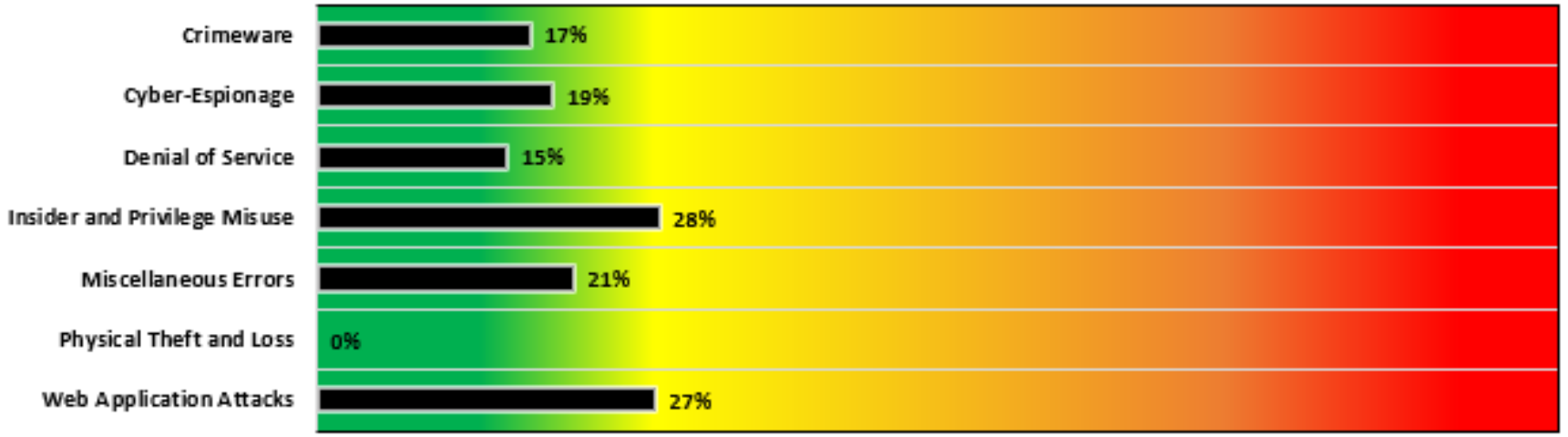
Octubre 13 2022

¿Cuál es el factor de exposición de mi organización según el DBIR?

SISAP Sistemas Aplicativos

Top ataques que afectan a mi industria	Motivos detrás de cada ataque	Tipo de datos comprometidos
Aplicaciones Web Errores diversos Todo lo demás	Financiero (91%) Espionaje (3%) Represalia (3%)	Personal (77%) Otros (35%) Credenciales (35%) Banca (32%)

En esta medición, la organización debe buscar acercarse a 0%.
Debido a que estamos determinando el nivel de exposición de 1% a 100%.



Ciclo de vida – Gestión de riesgos

Jornada 2022

Octubre 13 2022

Hipótesis de cuantificación de interrupción causada por ciberataques

SISAP Sistemas Aplicativos

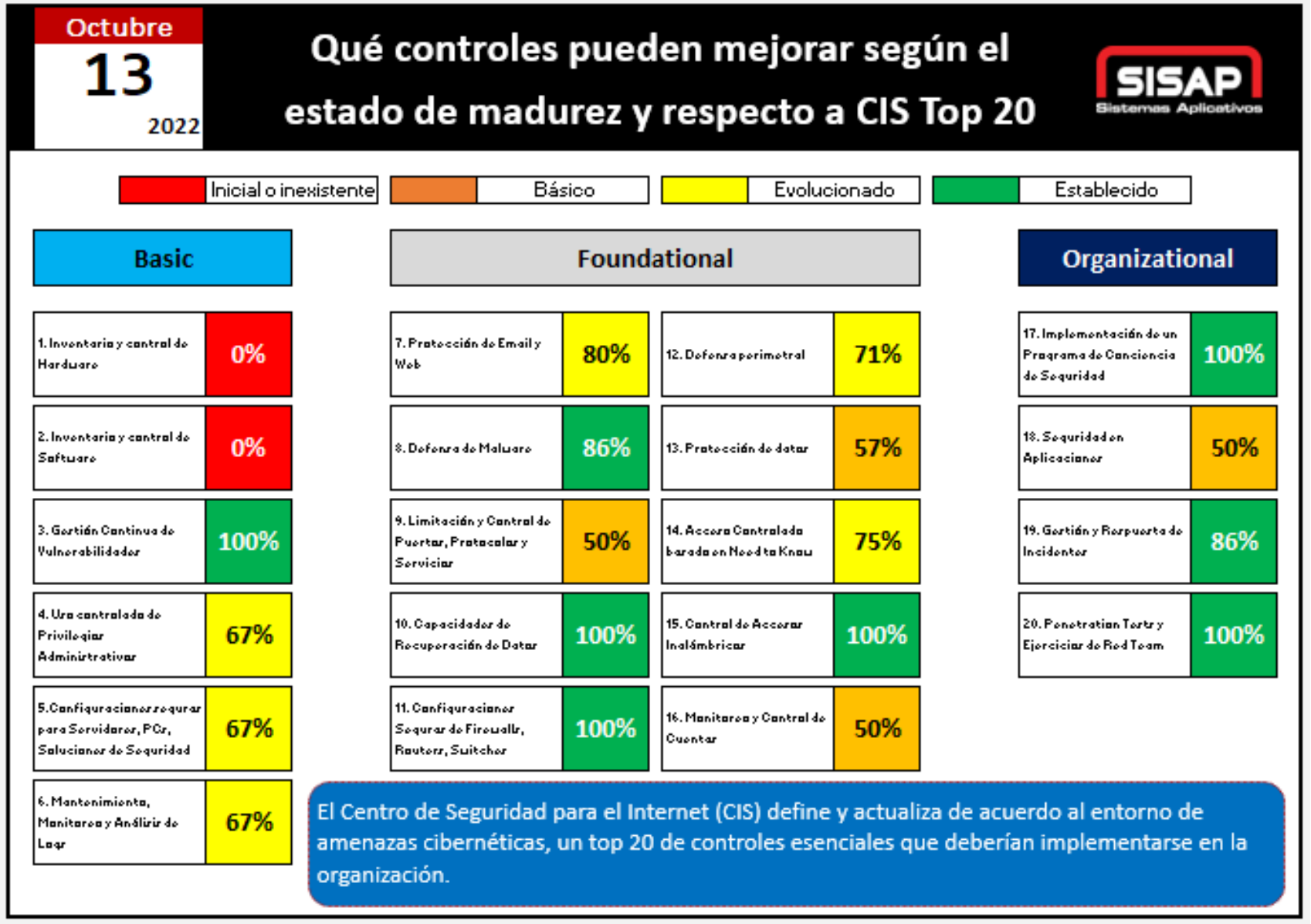
Uno de los mayores retos que todo CISO afronta es poder traducir el ciber-riesgo a una pérdida esperada en dinero. Para esto se puede utilizar una fórmula **CCR (Costo Ciber Riesgo)** con los siguientes parámetros:

- Revenue del último año (RN)
- Porcentaje de dependencia tecnológica del negocio (%DT)
- Factor de exposición en porcentaje (%FE)
- Efectividad de la estrategia actual de ciberseguridad (ECS)

Revenue del último año	$ 158.000.000,00
% dependencia tecnológica	99%
% factor de exposición	18%
% efectividad de estrategia actual	85%

Ciclo de vida – Gestión de riesgos

Jornada 2022



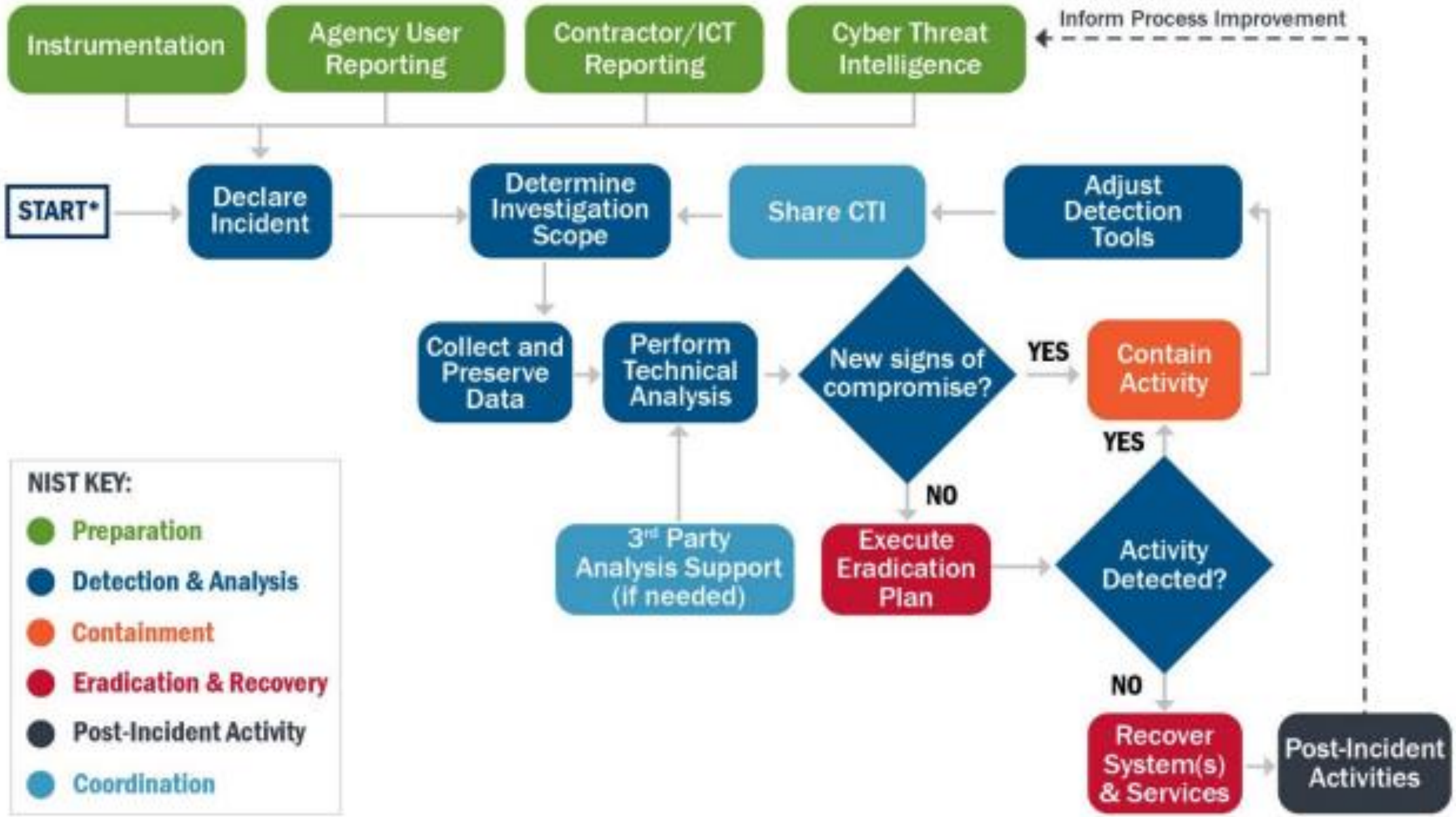
Ciclo de vida – Plan de gestión de incidentes

Jornada 2022

- Creación de manuales y protocolos.
- Determinación de herramientas para la detección y respuesta.
- Métodos para el análisis y toma de decisiones sobre un incidente.
- Procesos para la identificación de lecciones aprendidas post-incidente

Instituto de Auditores Internos de Costa Rica

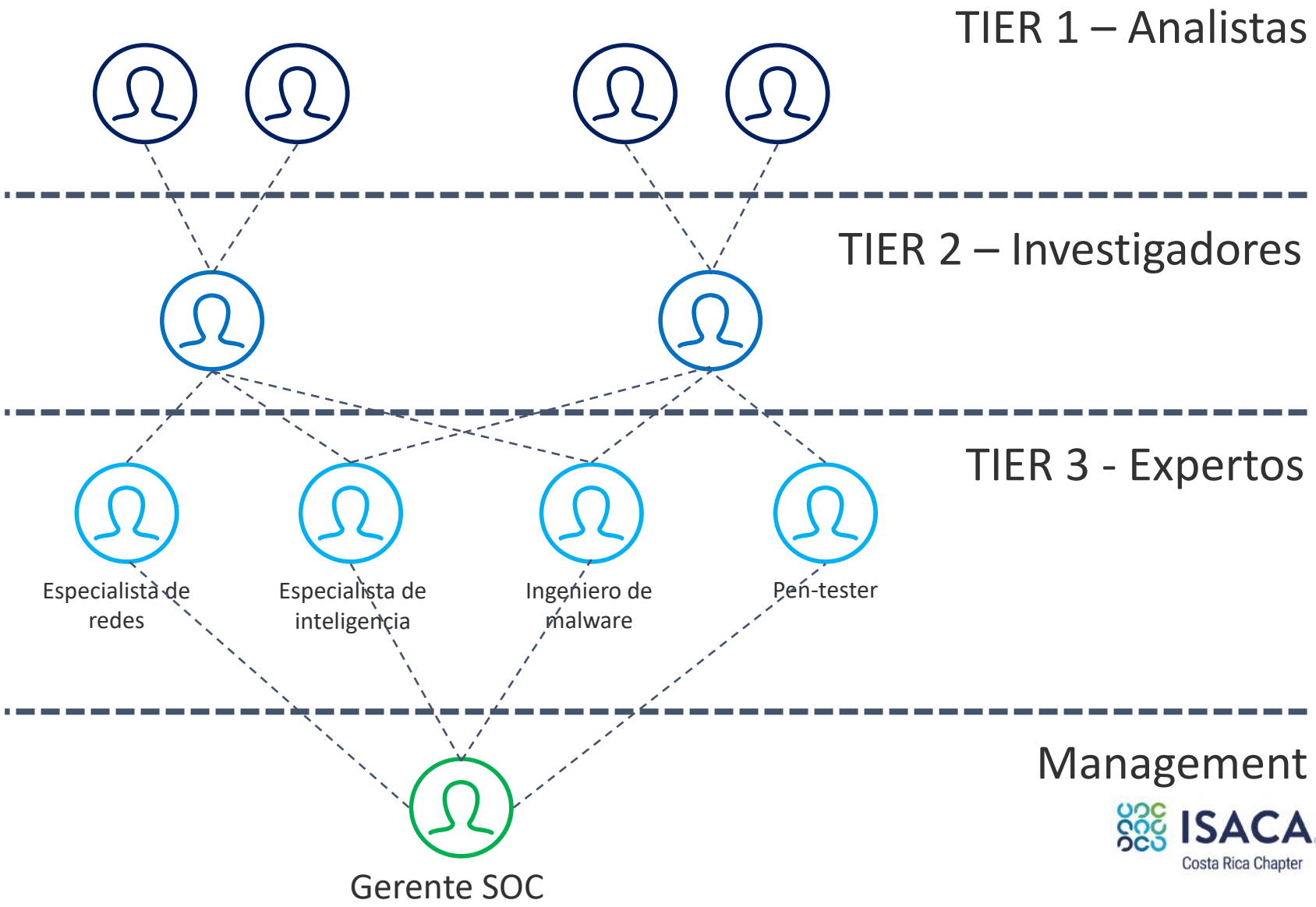
Ciclo de vida – Proceso



Fuente: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Ciclo de vida – Equipo de respuesta

Jornada 2022



ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Detección y reporte

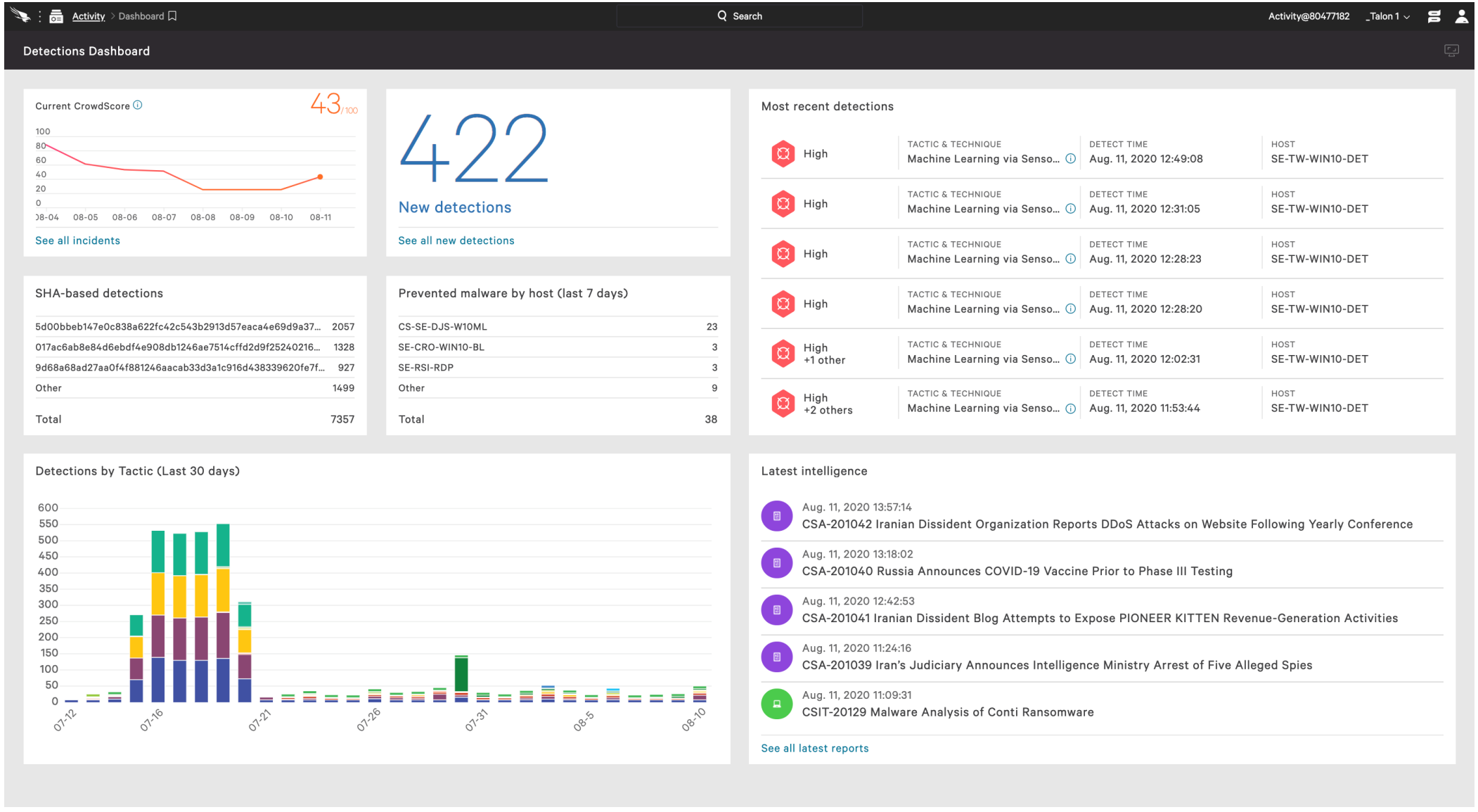
Jornada 2022

¿Cómo detectar un incidente de seguridad? ¿Cuáles son las fuentes?

- Plataforma SIEM.
- Usuarios finales.
- Equipos de seguridad perimetral (Firewall, IPS, IDS, WAF, etc).
- Clientes.
- Sub-unidades de TIC.
- NOCs (Network Operation Center).
- Organizaciones de investigación.
- SOCs (Security Operation Center).
- Proveedores de servicio.
- CERTs externos o internacionales.
- Unidades de negocio o departamentos internos.
- Medios de comunicación.
- Sitios Web.

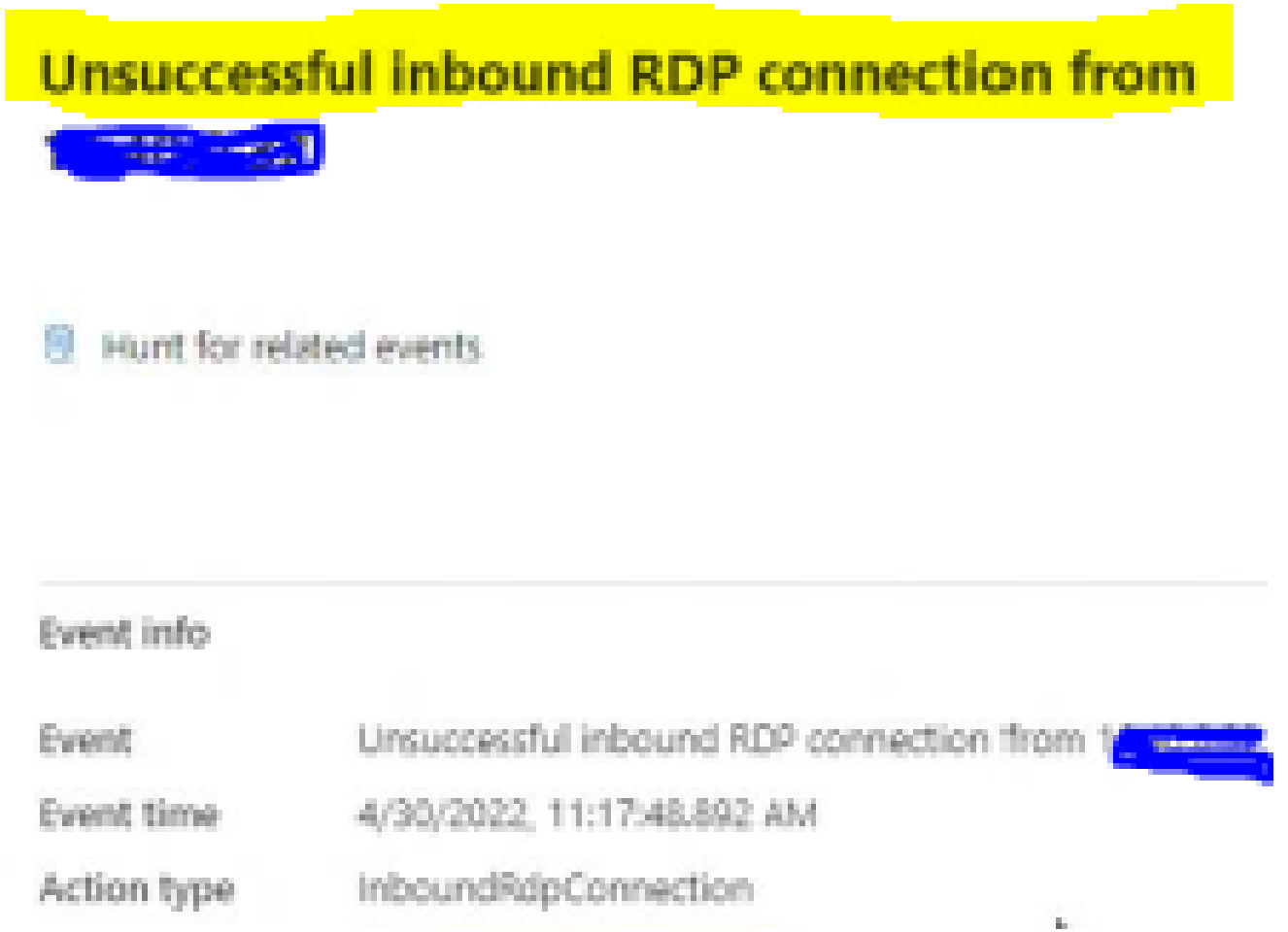
Ciclo de vida – Detección y reporte

Jornada 2022



Ciclo de vida – Detección y reporte

Jornada 2022

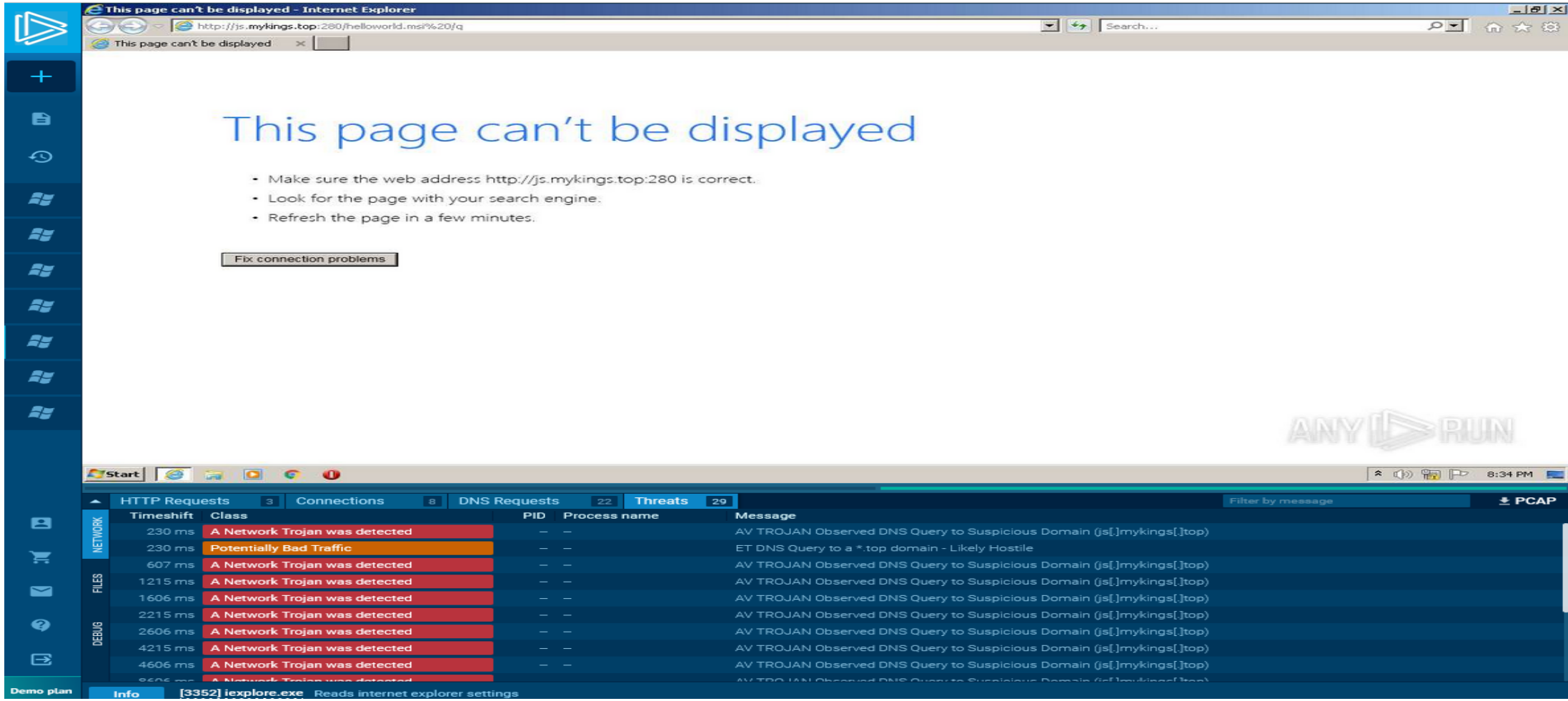


ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Detección y reporte

Jornada 2022

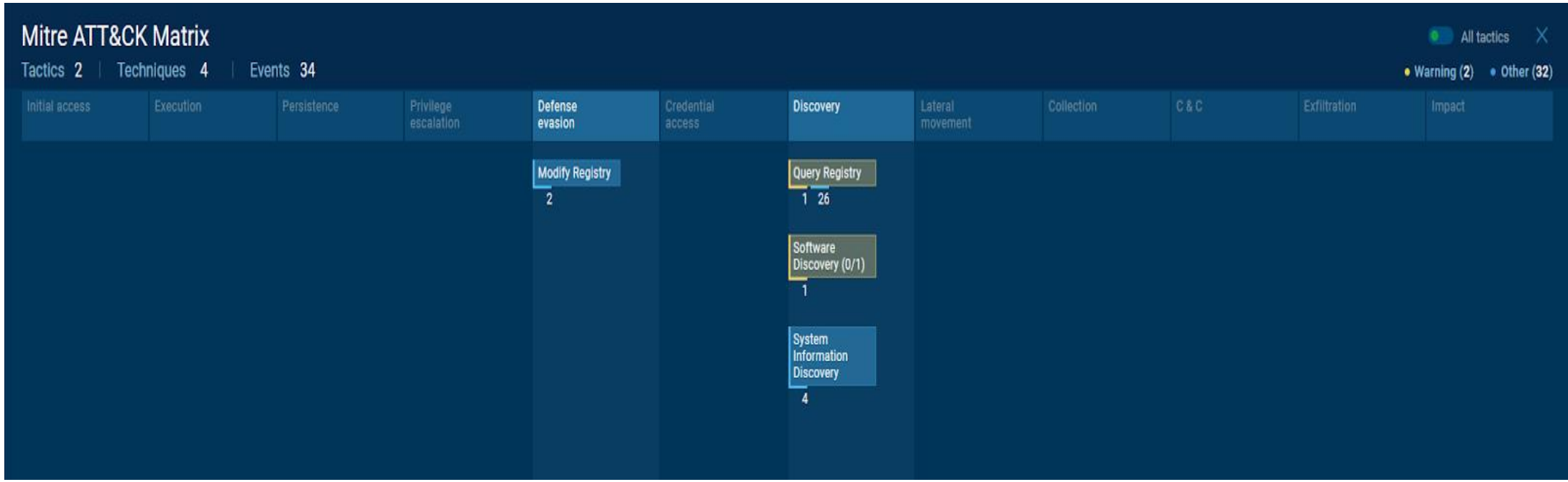


ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Detección y reporte

Jornada 2022

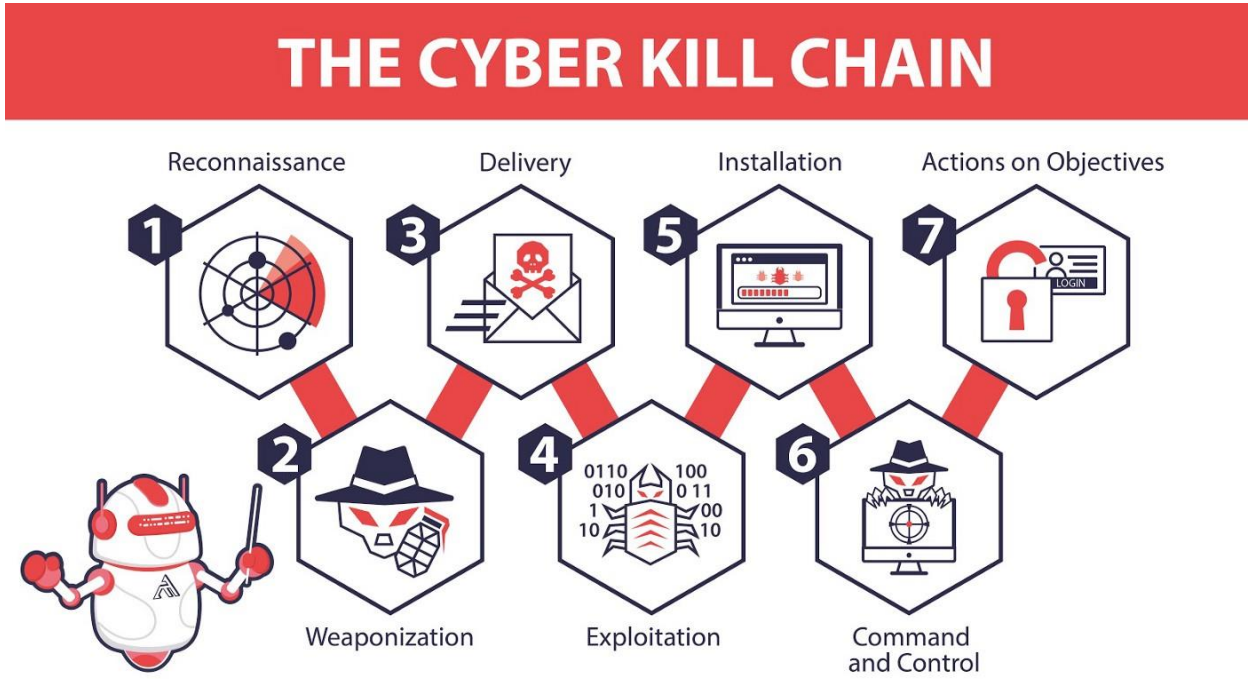


ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Detección y reporte

Jornada 2022



MITRE ATT&CK™

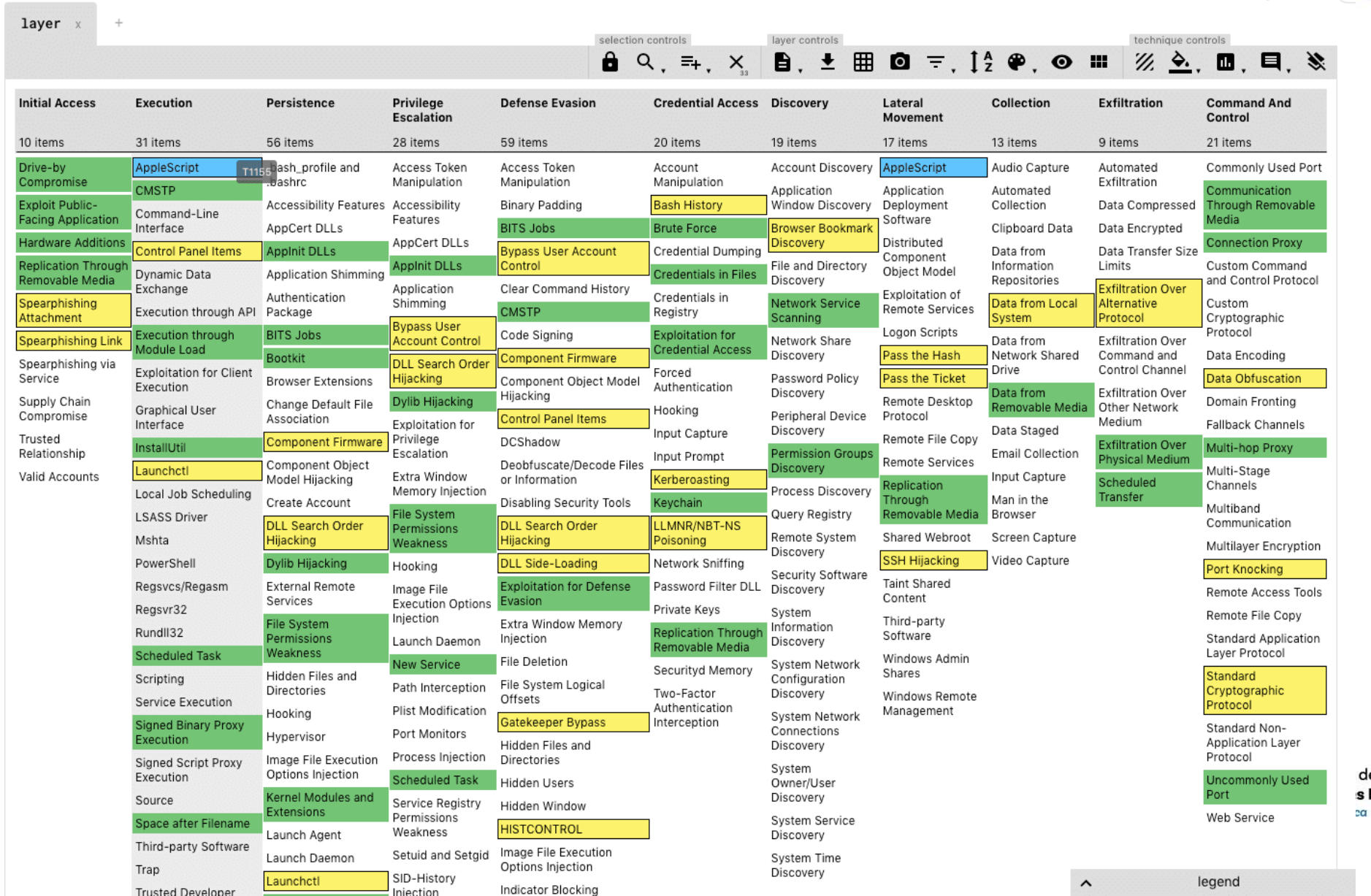
ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Detección y reporte

Jornada 2022

MITRE ATT&CK™ Navigator



Ciclo de vida – Detección y reporte

Jornada 2022

Ciclo de vida – Detección y reporte

Jornada 2022

Para la mayoría de las organizaciones, el mayor reto en el proceso de respuesta a incidentes de seguridad es detectar y evaluar los posibles incidentes, así como determinar lo que sea que haya pasado, el tipo, la extensión y la magnitud del problema.

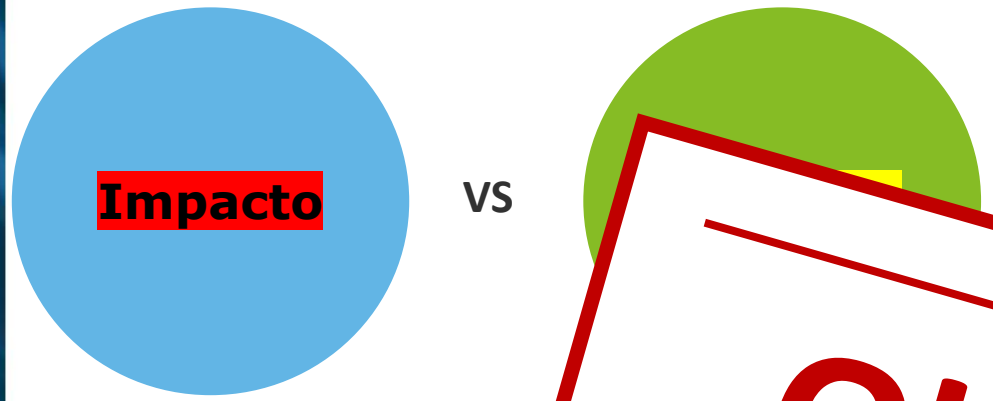
ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Análisis y decisión

Jornada 2022

¿Cómo clasificar un Incidente?



Obsoleto

Mapa de Calor Cuantitati					
Urgencia	Valor	1	2	3	4
Urgente	4	4	8	12	16
Significativa	3	3	6	9	12
Moderada	2	2	4	6	8
Leve	1	1	2	3	4

Impacto		
Nivel	Descripción Cualitativa	Grado de Escala
Bajo	• No representa mayor impacto en la operación de los servicios críticos del negocio. • Afectación leve en el rendimiento de las aplicaciones críticas. • Existen soluciones alternativas. • El impacto es transparente para los clientes. • No representa un impacto significativo sobre la operación del	1
		2
Muy Alto	• Afectación grave en el rendimiento de las aplicaciones críticas. • Afecta a muchos clientes. • Se requiere el involucramiento del	4

Urgencia		
Nivel	Descripción Cualitativa	Grado de Escala
Leve	• Representa la incorporación de ciertas mejoras a nivel de aplicación, automatización de procesos o nuevas configuraciones. • Requiere de previa planificación. • El incidente puede ser fácilmente controlado, aislado y resuelto.	1
Moderada	• Requiere atención a fin de resolver problemas recurrentes o fallas detectadas. • La atención debe ser planificada con anticipación y notificada a las unidades de negocio respectivas. • El incidente se encuentra parcialmente controlado.	2
	• Requiere atención en el menor tiempo posible con el fin de prevenir un posible impacto en la operación del negocio. • El incidente debe ser notificado a la Dirección Institucional. • El incidente requiere esfuerzos significativos para ser controlado, aislado y resuelto.	3
Urgente	• Requiere atención de manera inmediata a fin de prevenir un posible y severo impacto sobre la operación del negocio. • El incidente debe ser presentado ante la Dirección Institucional y	4

Ciclo de vida – Análisis y decisión

Jornada 2022

Triage

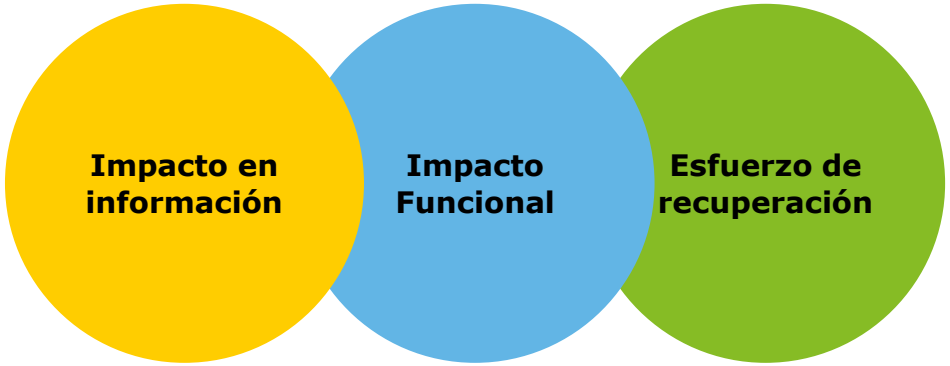
Se le conoce como el arte de clasificar, categorizar y priorizar eventos de seguridad; con el fin de determinar cuáles serán las acciones contención y respuesta a ejecutar.

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

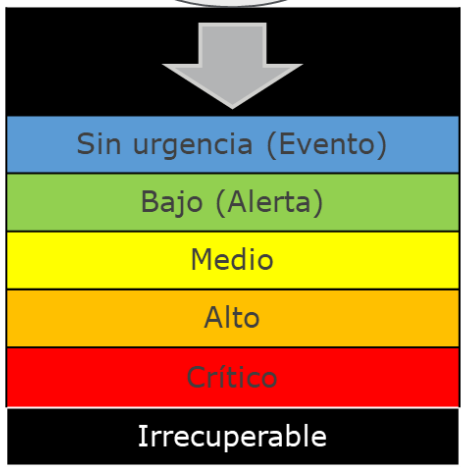
Ciclo de vida – Análisis y decisión

Jornada 2022



Nivel	Valor Cuantitativo	Valor Cualitativo	Descripción
Ninguno	0		Sin efectos potenciales en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización.
Bajo	1		Efecto potencial leve en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización. La organización podría entregar los servicios críticos, pero con perdida de eficiencia.
Medio	2		Efecto potencial moderado en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización. La organización podría perder la capacidad de entregar servicios críticos a un sub-conjunto de usuarios o por un lapso determinado de tiempo.
Alto			Efecto potencial severo en la capacidad de entregar servicios críticos a los usuarios o

Nivel	Valor Cuantitativo	Valor Cualitativo	Descripción
Ninguno	0		No requiere ningún esfuerzo.
Regular	1		El tiempo para la recuperación es predecible con los recursos existentes.
Adicional	2		El tiempo de recuperación es predecible con recursos adicionales a los actuales.
Extendido	3		El tiempo de recuperación es impredecible, recursos adicionales y apoyo externo podrías ser necesario.



ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Cyber

Ciclo de vida – Ejercicio grupal

Jornada 2022

Durante las últimas 24 horas, muchos empleados han llamado a la mesa de soporte de seguridad para consultar sobre la validez de un correo que recibieron proveniente de "SkyFinancial S.A".

El correo indica que se dio una posible filtración de datos financieros y que se requiere acceder a sitio web mediante un link para crear una nueva contraseña, después de proveer su contraseña actual para validar la identidad del usuario y los datos de la cuenta.

1- ¿Indique cuál activo de información se vio afectado?

2- ¿Indique cuál fue una posible vulnerabilidad explotada?

3- Clasifique, categorice y priorice el caso.

4- ¿Indique qué impacto potencial tuvo este incidente?

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Contención y erradicación

Jornada 2022

El objetivo principal de esta fase es limitar el alcance y la magnitud del incidente, es decir, evitar que el incidente se expanda y empeore.

No es posible erradicar un problema de seguridad que ha comprometido la organización si no se conoce qué pasó.

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Contención y erradicación

Jornada 2022

Contención

- Respuesta inmediata para minimizar el impacto.
- Vigilancia al atacante o incidente.
- Preservación de la evidencia.
- Mantener la cadena de custodia (De ser necesario).
- Identificar la fuente del incidente (No al atacante).

Erradicación

- Aplicar estrategias y protocolos de erradicación.
- Escalamiento.
- Eliminar rastro del incidente.
- Activar el DRP o BCP (De ser necesario).
- Comunicación interna/externa.

"El enfoque principal al responder ante un incidente debería ser la minimización de impactos adversos al negocio, mientras que la identificación del atacante debería ser considerada como un **objetivo secundario**".

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Cyber

Ciclo de vida – Contención y erradicación

Jornada 2022

Restablecer Respaldos

Cambio masivo de contraseñas

Aislar equipos infectados

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Ejercicio grupal

Jornada 2022

Su servidor “Core financiero” fue comprometido, su archivo de contraseñas, dirección IP y la información del sistema operativo podría haber sido compartida en un foro de ciber-delincuentes en la Dark Web. Su servidor ha sido repetidamente atacado durante las siguientes 2 semanas y se han detectado comportamientos sospechosos en su red.

1- ¿Indique cómo contendría el ataque?

2- ¿Indique cómo mejoraría sus defensas?

3- ¿Indique su proceder para determinar la causa?

4- ¿Indique su proceder para erradicar la causa?

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Recuperación

Jornada 2022

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Ciclo de vida – Lecciones aprendidas

Jornada 2022

La documentación de lecciones aprendidas permite:

- Determinar exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Mantener los documentados los procedimientos realizados.
- Determinar si se tomaron medidas o acciones que podrían haber impedido la recuperación.
- Identificar que debería hacerse la próxima vez que ocurra un incidente similar.
- Determinar acciones correctivas que pueden prevenir incidentes similares en el futuro.
- Identificar herramientas, recursos o mejoras al proceso que son necesarias para detectar, analizar y mitigar los incidentes en el futuro.

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Palabras de clausura

Jornada 2022

01 El monitoreo de red es la peor pesadilla de un atacante, prepárese cada segundo cuenta

02 Una buena seguridad tiene que ver con la resiliencia, no con ser a prueba de balas

03 Habilitar la preservación de la evidencia en todas sus herramientas le ahorrará mucho tiempo a su organización

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Palabras de clausura

Jornada 2022

04 Conozca a su adversario para detener los ataques modernos

05 Elimine las configuraciones erróneas y deshabilite los servicios no seguros

06 Construir una cultura de ciberseguridad

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica