¿Qué es Ciber Resiliencia?

Cómo recuperarse de un ciberataque

Santo Domingo, República Dominicana
| Noviembre 16 de 2023

iteam

Conferencista

Papá de 3

Norman Ramírez

Consultor desde 2002

nramirez@iteamgroupcorp.com

Universidad de los Andes Colombia

Ingeniero Industrial 1998
Especialista en Sistemas de Información en la Organización 2002

DRI International

- Master Business Continuity Professional (MBCP) -
- Certified Risk Manager Professional (CRMP) -
- Certified **Cyber Resilience Professional (CCRP)**
- Certified Instructor & Commissioner Representative of Latin America

Member of the Business Continuity Institute (MBCI) - BCI, UK

Lead Auditor ISO22301:2012

Authorized ICOR Training Partner

iteam

Socio fundador

Colombia 2004

Panamá 2009

México 2013

Brasil 2023

Agenda

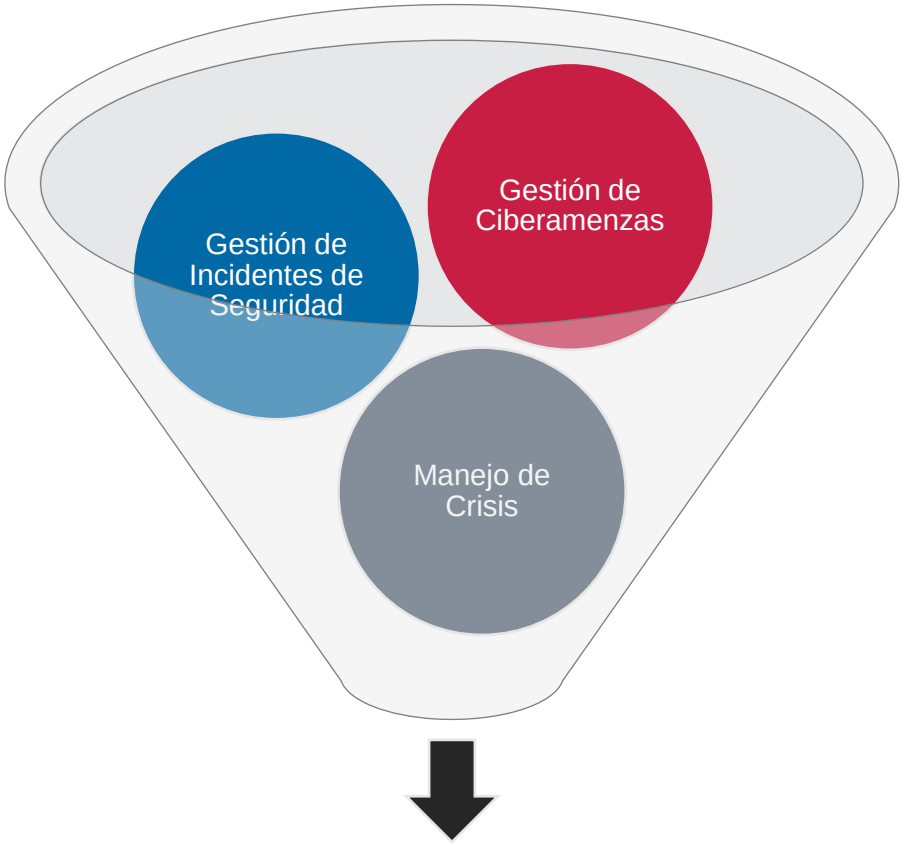
1. ¿Qué es la Ciber Resiliencia?
2. ¿Por qué es importante gestionar la Ciber Resiliencia en las organizaciones?
3. Identificación de Ciber amenazas
4. Gestión de Incidentes de Ciber seguridad
5. Realidad de DRP con respecto a Ciber ataques
6. Una solución real para recuperarse de un Ciber ataque

Marco de Resiliencia Organizacional

Resilience. Education. Credentialing. ICOR The International Consortium For Organizational Resilience

¿Qué es la Ciber Resilencia?

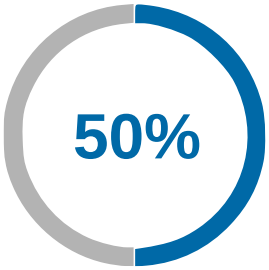
La forma con la que una compañía o entidad va a poder mantener sus operaciones ante algún tipo de ataque informático o ataque de ciber seguridad, protegiendo no sólo sus operaciones sino también su imagen corporativa



¿Por qué es importante Gestionar la Ciber Resiliencia?

Foro Económico Mundial (WEF) califica a los **ciber ataques** dentro del **Top 10 de riesgos** a nivel Global.

Principales retos de los responsables de la ciber seguridad de acuerdo con World Economic Forum

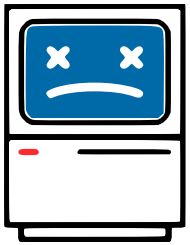


Mayor **conectividad**

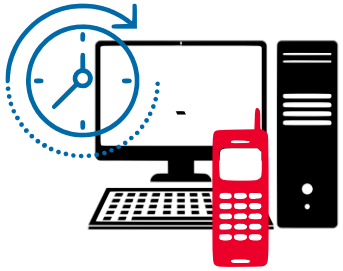
5G

Nueva Tecnología =
Nuevas amenazas

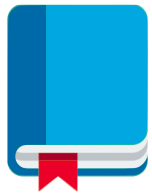
19% **Aumento de ataques** de Ransomware



Ataques a
Tecnología Crítica

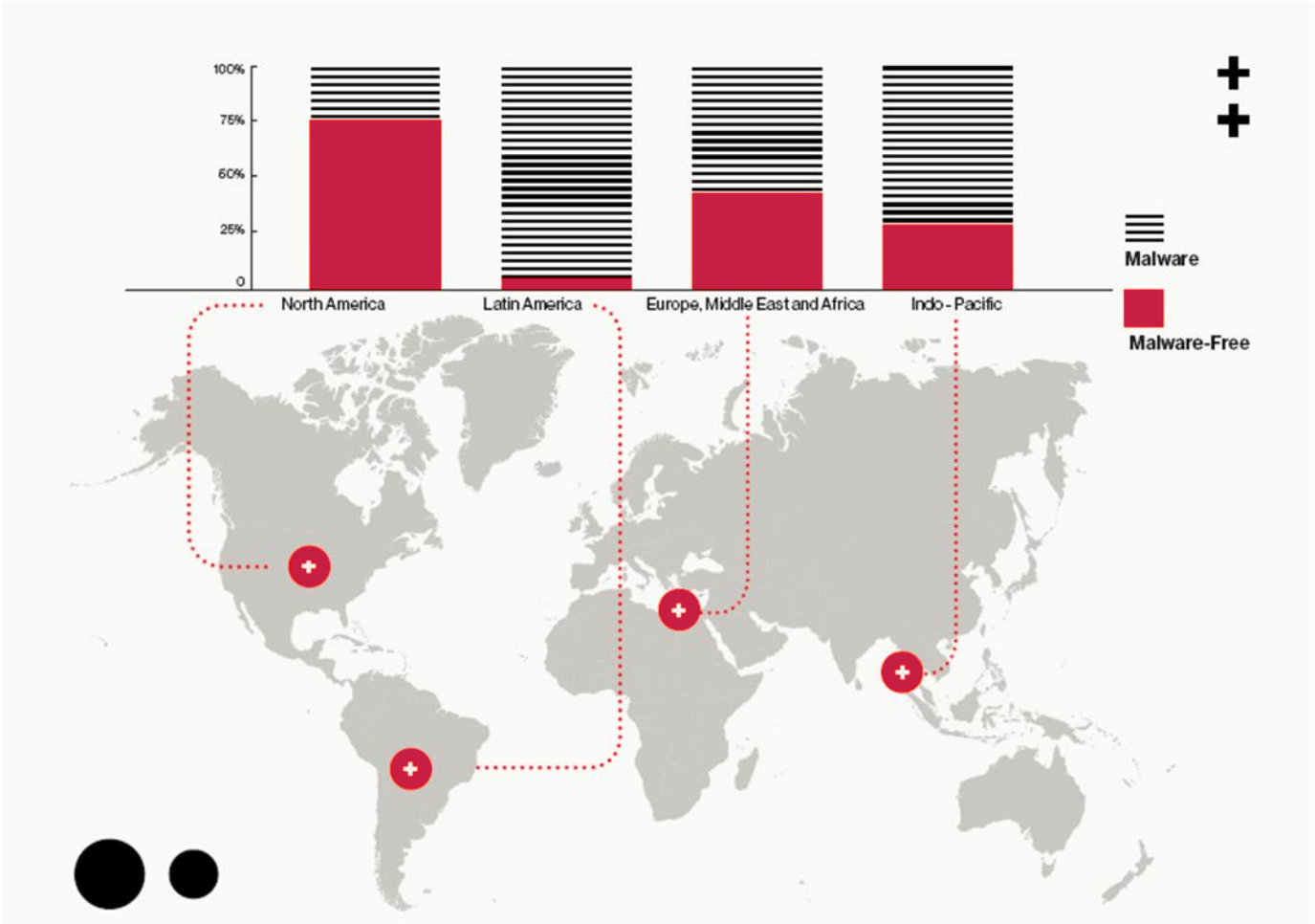


Tecnología **obsoleta**



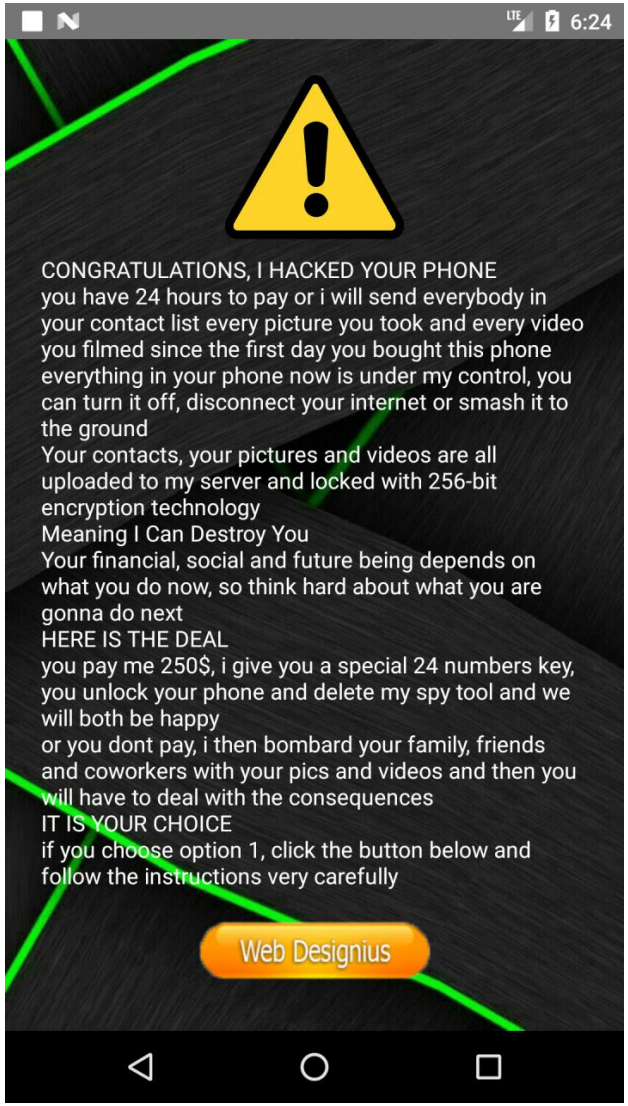
Falta de **capacitación**

En Latinoamérica +90% de los ataques son por Malware



Fuente: *CROWDSTRIKE GLOBAL THREAT REPORT 2020*

Malware y el Covid-19



Fuente: *Boletín de inteligencia del DNI de Colombia – Mayo 2020*

Ransomware:

Covidlock y Ragnar Locker

Recuperación del Incidente

Restauración del servicio.

- Gestión de incidentes TI.
- Acuerdos de niveles de servicio.
- Troubleshooting.

Continuidad a las operaciones.

- Planes de Recuperación ante desastres.
- SOP – Standard Operational Procedures – Procedimientos Operativos.
- Plan de Gestión de Crisis.

El proceso de Gestión de Ciber amenazas

- Redes Sociales
- Foros y Blogs
- Dark y Deep web
- Noticias
- Grupos de interés
- Canales internos

Amenazas conocidas

Planes de mejora sobre controles existentes

Gestión de Riesgos emergentes

Amenazas desconocidas

Conexión entre planes

Plan de Gestión de Incidentes Cibernéticos

Criterios de Activación

Plan de Gestión de Crisis

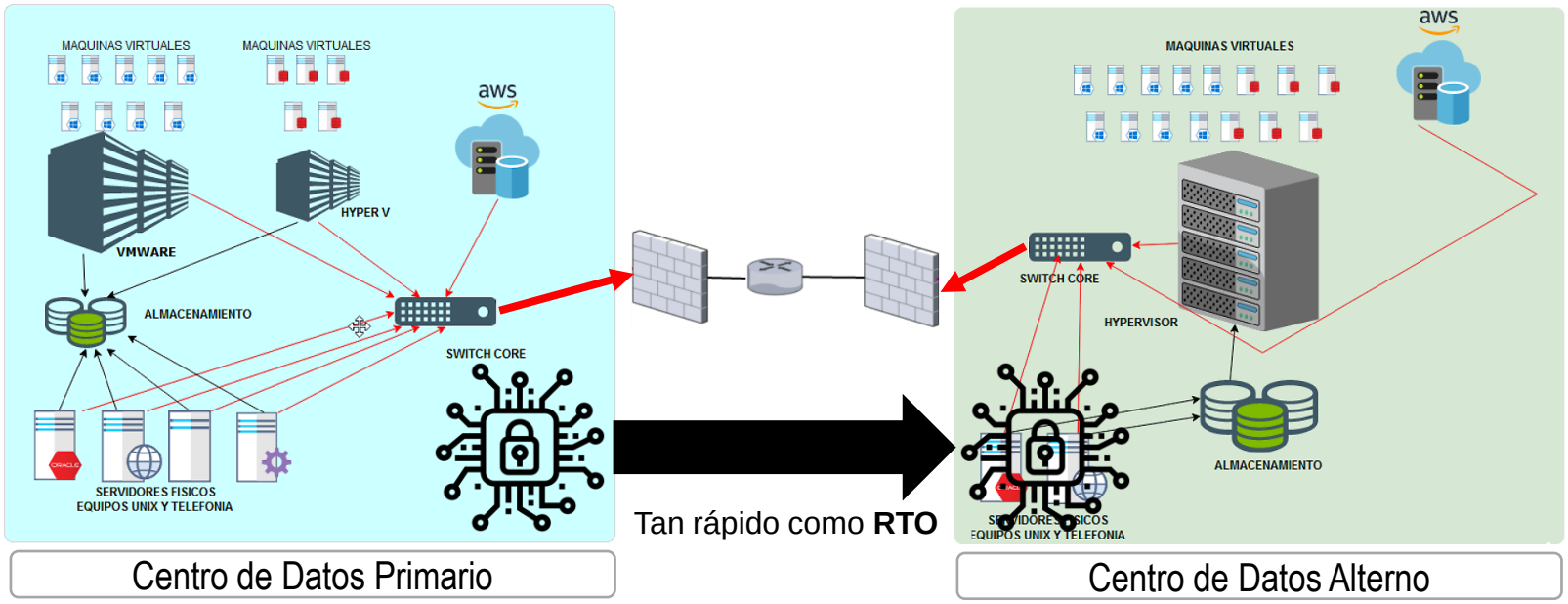
Plan de Gestión de Incidentes

Plan de Gestión de Comunicaciones

Plan de Recuperación ante desastres

Plan de Continuidad de Negocio

Realidad de DRP con respecto a Ciber ataques

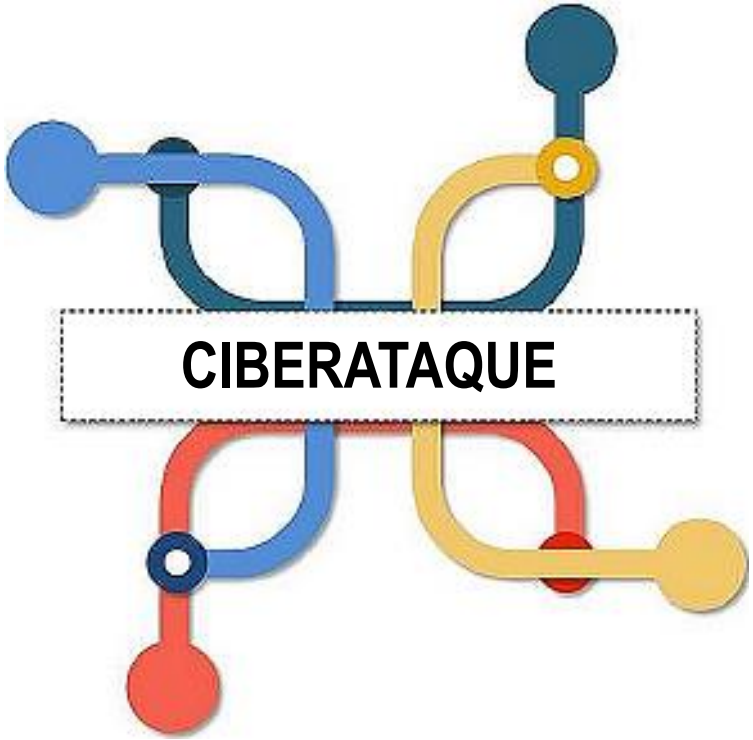


¿Qué hacer durante un ciberataque en curso?

Elementos clave de la ciberdefensa

Dar sentido y orientación

Capacidad de dar sentido rápidamente a una situación que es confusa y desconcertante.



Moverse rápidamente

Capacidad de moverse rápidamente a través de la confusión y el caos.

Actuar de forma coordinada

Activar el libro de “jugadas”: Desarrollar las actividades previstas en el “antes” y aplicar las detalladas en el “durante.

Procesar grandes volúmenes de datos

La capacidad de procesar grandes volúmenes de datos de forma rápida y fiable.

Fuente: *JCM-22 All rights reserved. @itinsecure | Basado en: Hettema, H.(2022). Agile Security Operations Engineering for agility in cyber defense, detection and response. Birmingham, UK Packt Publishing Ltd. P.71*

¿Qué hacer durante un ciberataque en curso?

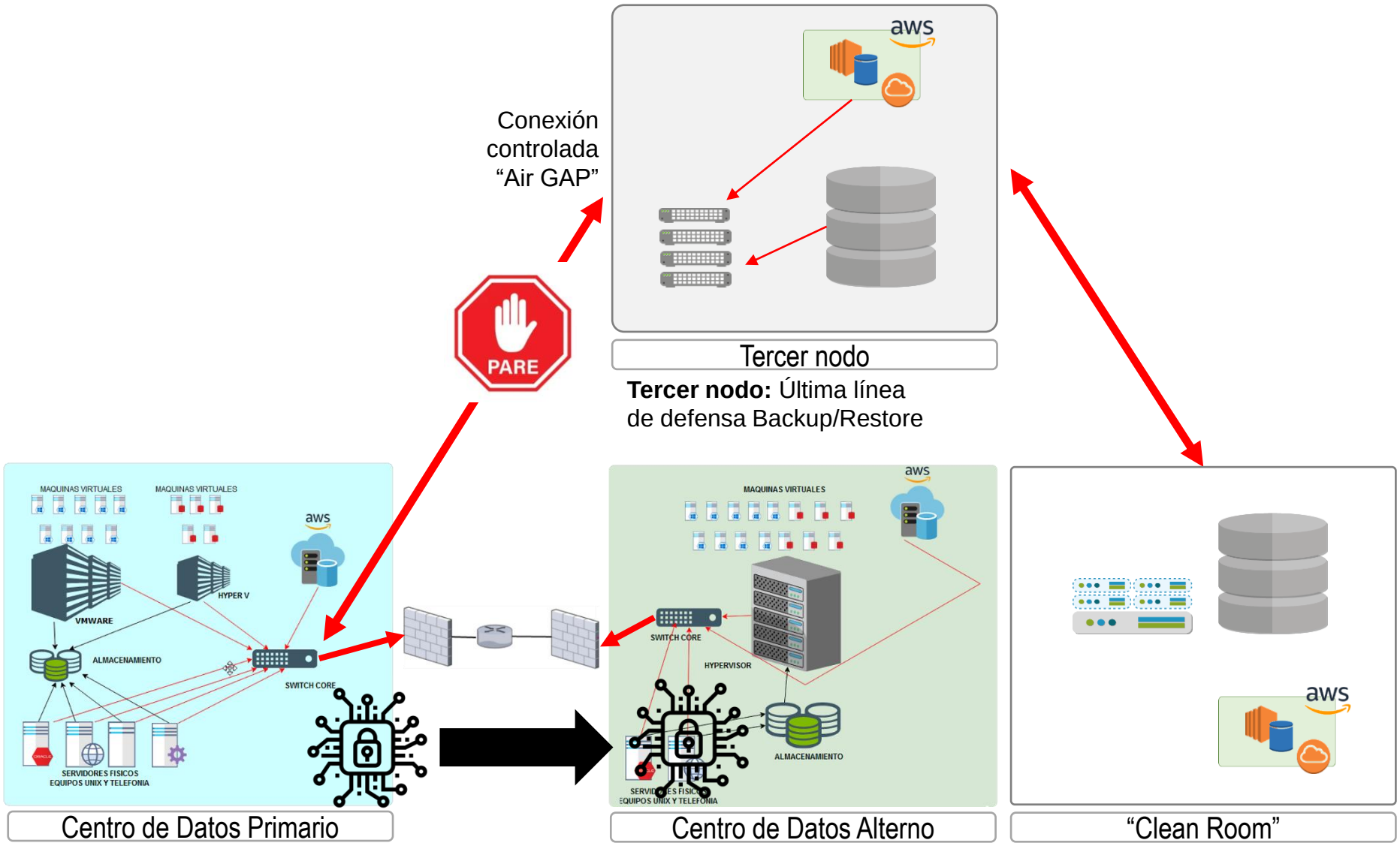
Identificar el corazón de los activos de información

- Proteger primero el “corazón” de la empresa.

- Priorizar las aplicaciones que soportan al negocio y sus datos.

- Iniciar con un modelo escalable.

Una solución real para recuperarse de un Ciber ataque



¿Preguntas?

www.iteamgroupcorp.com
info@iteamgroupcorp.com

COLOMBIA

iteam Ltda.

Dirección: Calle 103C No. 63 –39
Bogotá, D.C. Colombia

Teléfono: +57-1-770-4817

PANAMÁ

iteam Panamá S.A.

Dirección: Ave. 5ta sur.
Calle 76 San Francisco.
Edificio Ivercisco local 200-5
Panamá, República de Panamá.

Teléfono: +507-3900618

MÉXICO

Resilience Team México S de RL de CV

Dirección: Ave. Insurgentes Sur No.1898 - Pisos 12 y 14 - Col. Florida – C.P. 01030.
CDMX.
México

Teléfono: +52-55-1 56 2118 2230

BRASIL

Resilience Team Brasil Ltda.
Alameda Dos Hibiscos, 530
Cond Vitassay
Boituva - SP CEP 18553056

São Paulo, Brasil

Telefone: +55-11-984437622