ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Panel Continuidad del negocio .. Los nuevos retos de la ciberseguridad

Mayo 26, 2020

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Agenda

Continuidad y Resiliencia – Marcos de Referencia

Resultados de la encuesta

Reflexiones

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Aviso de Privacidad – Eventos

En cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) le informamos que ISACA Capitulo Ciudad de México, A.C. con dirección en WTC, Montecito N° 38, piso 28, Col. Nápoles, Ciudad de México, C.P. 03810, es una asociación civil sin fines de lucro, y que los datos personales en su poder serán tratados con la finalidad de proveer información relacionada con mejores prácticas internacionales desarrolladas por el IT Governance Institute a sus asociados e interesados, así como para realizar el registro de interesados en eventos promovidos por la asociación.

Se han implantado las medidas de seguridad necesarias para evitar el uso por personal no autorizado y la divulgación a terceros.

ISACA Capitulo Ciudad de México, A.C. tratará estos datos con la máxima confidencialidad siendo el destinatario único y exclusivo de los mismos, y no efectuando cesiones o comunicaciones a terceros al margen de las señaladas por la normativa vigente.

Para el ejercicio de derechos de acceso a los datos, rectificación, cancelación y oposición a partir de enero 2016 dirigir solicitud a la dirección antes señalada con los requisitos establecidos por la LFPDPPP.

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Cultura de control y prevención

+

# Buenas prácticas en materia de Continuidad

# Plan de Continuidad del Negocio (PCN / BCP)

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Percepción general de que el PCN:

- No se revisa y actualiza con la frecuencia que dictan las buenas prácticas
- No considera todos los escenarios factibles de ocurrir
- No se realizan los simulacros necesarios

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

Covid-19
tomó por sorpresa a muchos,
no obstante que estuvo
acompañada por mucha
información,
generada en los países
donde el brote inicio antes
que en México

La COVID-19 es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. Tanto el nuevo virus como la enfermedad eran desconocidos antes de que estallara el brote en Wuhan (China) en diciembre de 2019 (Foto: Shutterstock)

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter


Fuente:
E&Y
La crisis del COVID-19
Abril 2020

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# “Ahogado el niño … ”

Existencia de Organizaciones no pusieron atención a las recomendaciones emitidas por parte de las áreas encargadas del control: *no fue prioritario y no contó con los recursos necesarios*

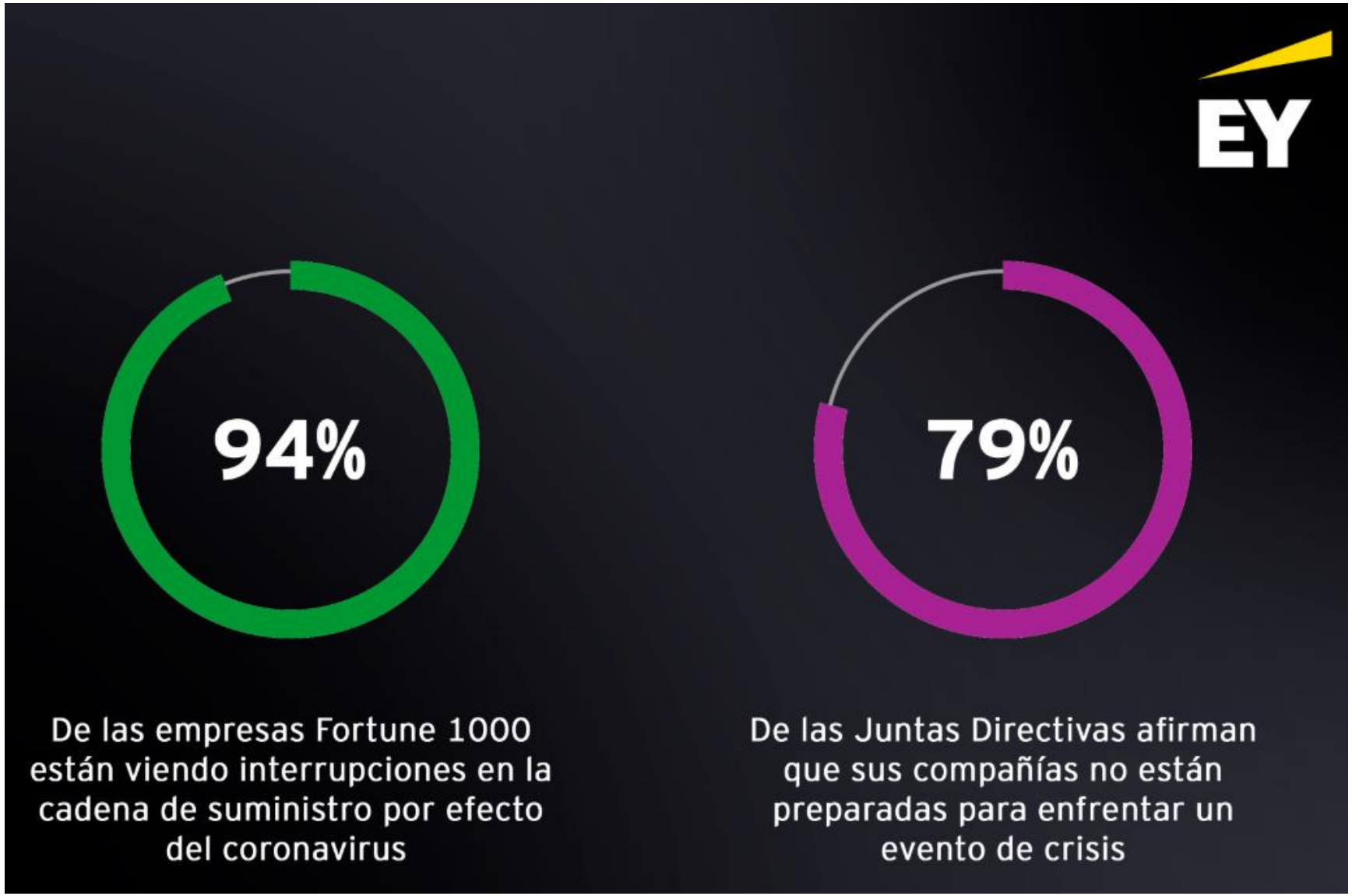
… ahora sufriendo las consecuencias

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

Fuente:
E&Y
La crisis del COVID-19
Abril 2020



ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

A los que respondieron la encuesta … ***muchas gracias***

Esta información de primera mano fue importante para darnos una idea de cómo se está gestionando este importante hecho

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

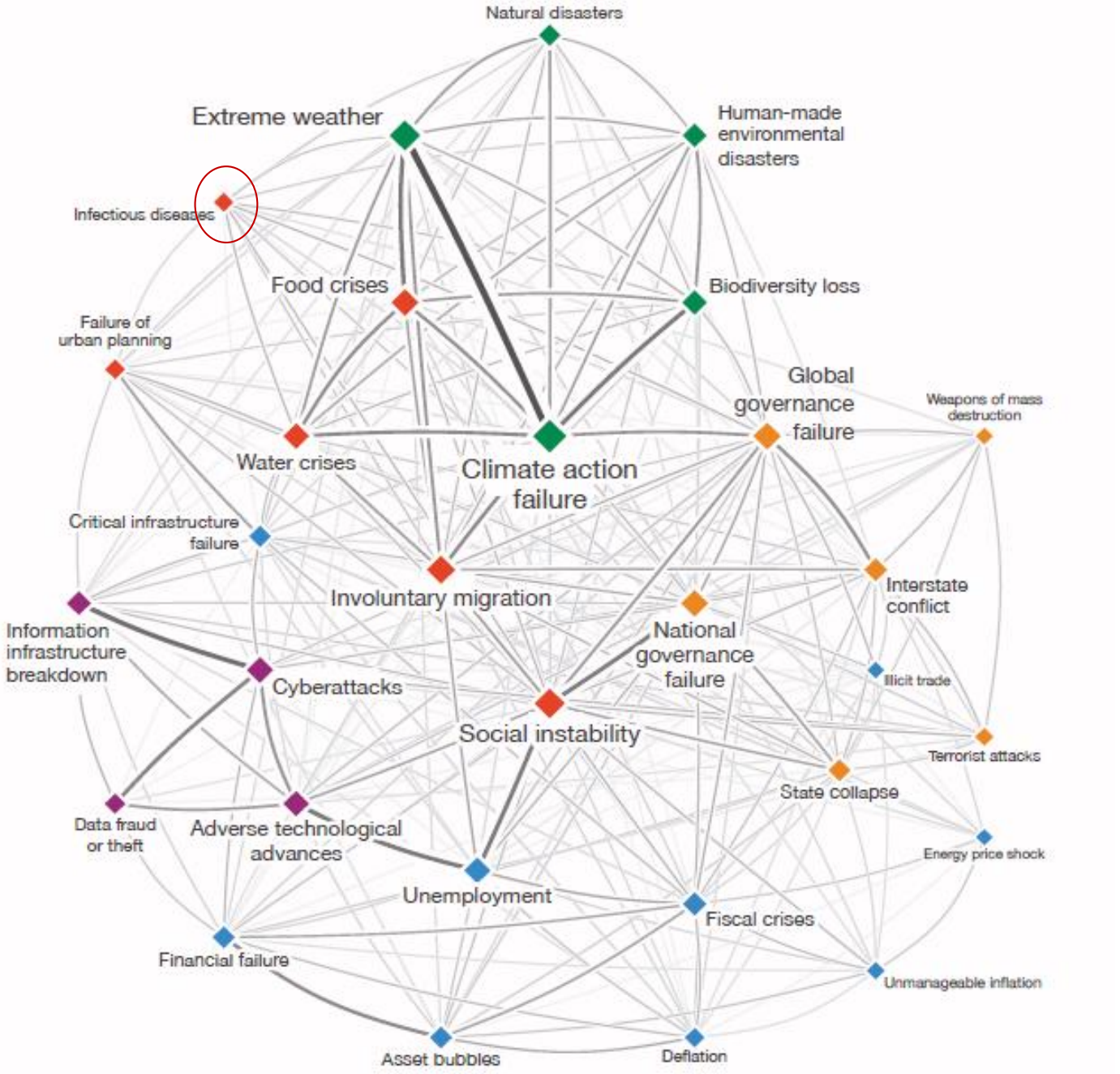
# Principales marcos de referencia en materia de Riesgo (Global Risk Landscape 2020=)

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Riesgo (Global Risk Landscape 2020)



ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

ISO

NIST National Institute of Standards and Technology U.S. Department of Commerce

ISACA

ts mitigation™

open

HITRUST CSF®

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

## ISO/IEC 27000: Sistema de Gestión de la Seguridad de la Información (35 referencias)

ISO/IEC 27001: Sistema de Gestión de la Seguridad de la Información – Requisitos
ISO/IEC 27002: Código de prácticas para controles de la seguridad de la información
ISO/IEC 27005: Gestión de riesgos de seguridad de la información
**ISO/IEC 27031 Guías para la preparación tecnologías de la información y comunicaciones para la continuidad del negocio**l
SO/IEC 27032 Guías para la ciberseguridad

## ISO 22300 Series

ISO 22300:2012 Societal security – Terminology
**ISO 22301:2019 Security and Resilience – Business continuity management systems – Requirements**
ISO 22311:2012 Societal security – Video-surveillance – Export interoperability
ISO 22313:2012 Societal security – Business continuity management systems – Guidance
ISO 22315:2014 Societal security – Mass evacuation – Guidelines for planning
ISO 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)
**ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes**
ISO 22320:2011 Societal security – Emergency management – Requirements for incident response
ISO 22322:2015 Societal security – Emergency management – Guidelines for public warning
ISO 22324:2015 Societal security – Emergency management – Guidelines for colour-coded alert
ISO 22397:2014 Societal security – Guidelines for establishing partnering arrangements
ISO 22398:2013 Societal security – Guidelines for exercises

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

## ISO 22301:2019 Security and Resilience – Business continuity management systems – Requirements

Está compuesta por 10 secciones. las secciones 4 a 10 son obligatorias y están alineadas al ciclo de mejora continua Planear, Actuar, Verificar y Actuar (PDCA)

**4. Contexto de la organiza**

**5. Liderazgo**.

**6. Planificación**

**7. Soporte**:

**8. Operación**: define la im
evaluación y tratamiento
planes y procedimientos,
documentación, y capacic
continuidad del negocio.

**9. Evaluación del desemp**

**10. Mejora**:

**Planes de Continuidad del Negocio**

**8.4.4.1.** La organización debe documentar y mantener los planes y procedimientos de continuidad del negocio. Los planes de continuidad del negocio deben proveer guías e información para asistir a los equipos para responder a una **disrupción** y asistir a la organización con la respuesta y recuperación

**Disrupción**

Incidente, ya sea anticipado o no, que causa una desviación negativa no planeada, de la entrega esperada de productos y servicios acorde a los objetivos del negocio.

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

NIST National Institute of Standards and Technology U.S. Department of Commerce

## NIST (183 referencias)

| | |
|---|---|
| **800-171 Rev. 2** | Protección de información no clasificada controlada en sistemas y organizaciones no federales |
| **800-160 vol. 2** | **Desarrollo de sistemas ciber resilientes: un enfoque de ingeniería de seguridad de sistemas** |
| **800-53 Rev. 4** | Controles de seguridad y privacidad para organizaciones y sistemas de información federales |
| **800-37 Rev. 2** | Marco de gestión de riesgos para sistemas y organizaciones de información: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad |
| **800-34 Rev. 1** | **Guía de planificación de contingencia para sistemas de información federales** |
| **800-30 Rev. 1** | Guía para realizar evaluaciones de riesgos |
| **NIST (CSF)** | Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Marco de Ciberseguridad |

ISACA Guadalajara Chapter

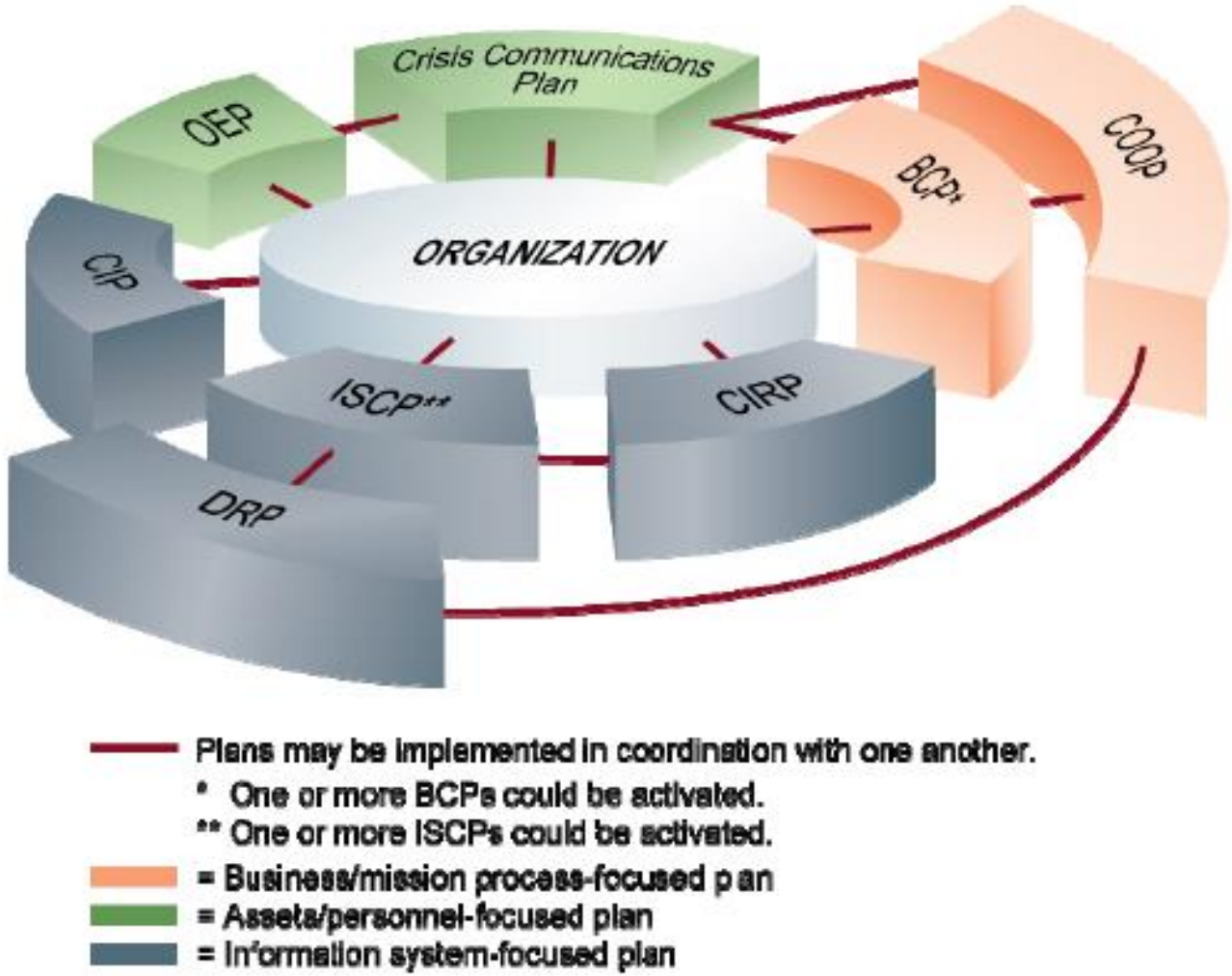
infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

NIST National Institute of Standards and Technology U.S. Department of Commerce

**NIST 800 160 Guía de planificación de contingencia para sistemas de información federales**



# Principales marcos de referencia en materia de Continuidad y Resiliencia

## NIST 800 160 Guía de planificación de contingencia para sistemas de información federales

**Personnel Health**

Pandemic Influenza (PI) is a global outbreak of disease that occurs when a new influenza virus emerges in human populations and causes serious illness. Because there is little natural immunity, the disease can spread easily from person to person, rapidly moving across the country and around the world. The Homeland Security Council, *The National Strategy for Pandemic Influenza Implementation Plan*, May 2006, requires federal organizations to develop plans to address how the organization will:

- Protect employees during a pandemic;
- Sustain essential functions during significant times of absenteeism;
- Support the overall federal response during a pandemic; and
- Communicate guidance to stakeholders during a pandemic.

Common strategies to protect personnel health during a pandemic outbreak include stricter hygiene precautions and reducing the number of personnel working in close contact with one another through implementation of "social distancing." Approved telework arrangements facilitate social distancing through working at home while sustaining productivity. Government-run telework sites are also available to federal employees who cannot work from home or the office. The Office of Personnel Management provides guidance and resources for developing Pandemic Influenza plans in coordination with the organization's Continuity of Operations Plan, human capital policy and strategies during a pandemic, and telework arrangements.

*The World Health Organization provides fact sheets on Avian Influenza at http://www.who.int/mediacentre/factsheets/avian_influenza/en/.*
*OPM provides information and guidance on Pandemic Influenza planning at http://www.opm.gov/pandemic/index.asp. The Web site also provides human capital guidance on issues including pay, leave, hiring, and alternate work arrangements.*
*OPM and GSA provide information and guidance on federal telework programs from the manager, employee, and Telework coordinator perspectives at www.telework.gov. Telework centers are also listed on this site.*

ISACA Guadalajara Chapter

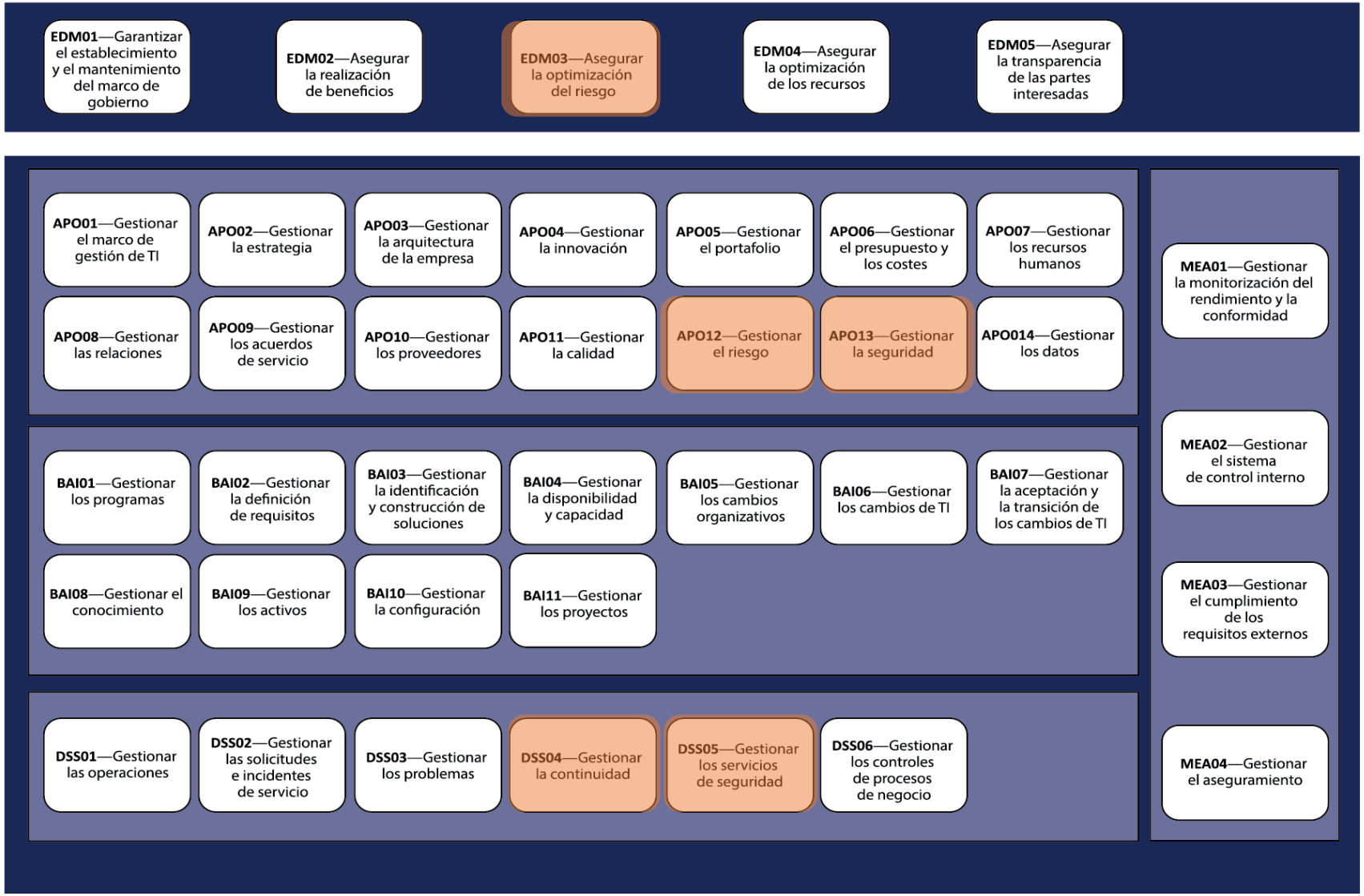
infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

ISACA

COBIT 2019



ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

COBIT 2019

| Domain: Deliver, Service and Support<br>Management Objective: DSS04 - Managed Continuity | Focus Area: COBIT Core Model |
|---|---|
| **Description** | |
| Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise. | |
| **Purpose** | |
| Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands). | |

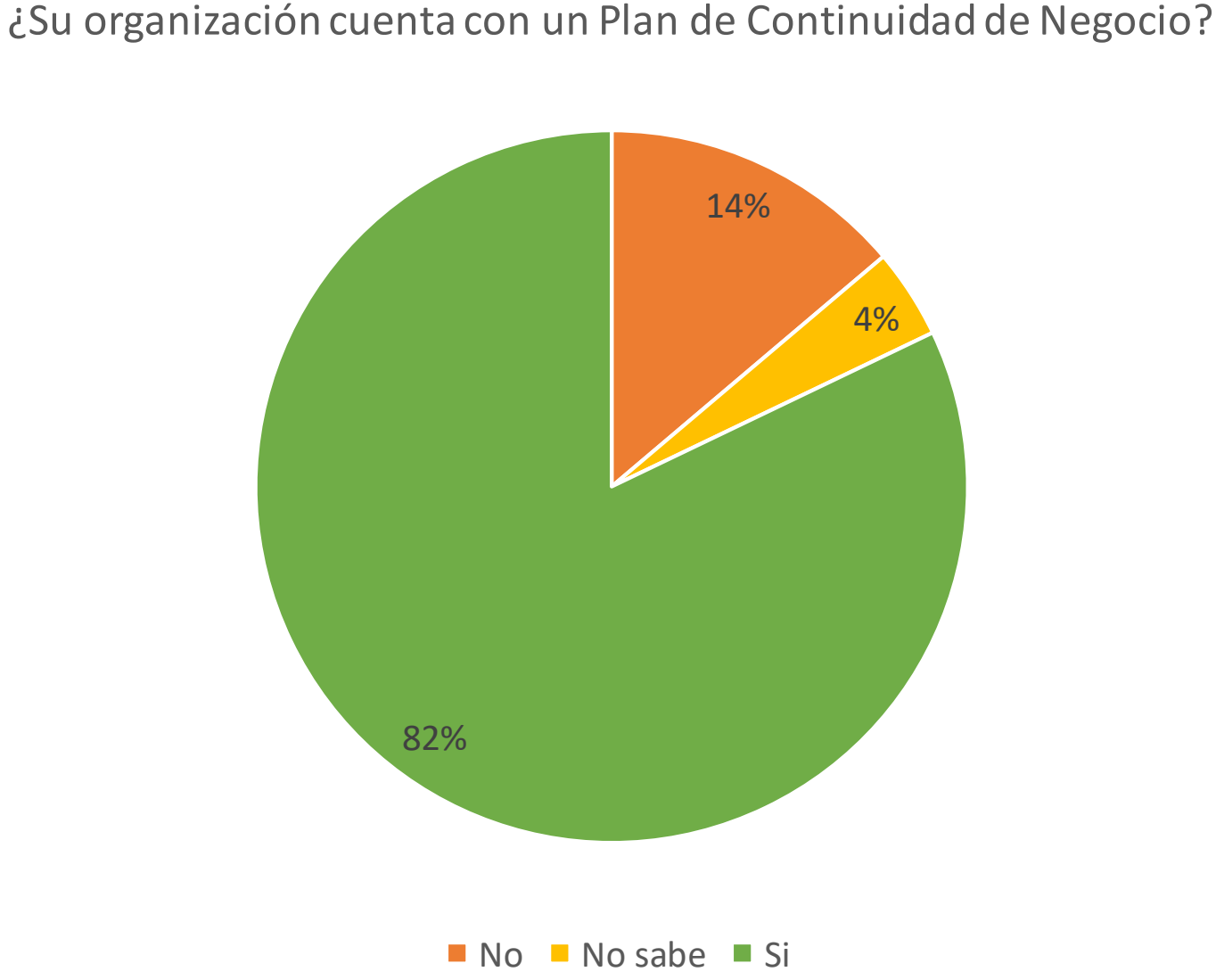
| | |
|---|---|
| DSS04.01 | Define the business continuity policy, objectives and scope. |
| DSS04.02 | Maintain business resilience. |
| DSS04.03 | Develop and implement a business continuity response. |
| DSS04.04 | Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). |
| DSS04.05 | Review, maintain and improve the continuity plans. |
| DSS04.06 | Conduct continuity plan training. |
| DSS04.07 | Manage backup arrangements. |
| DSS04.08 | Conduct post-resumption review. |

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Al respecto ¿ nuestros encuestados que dicen … ?

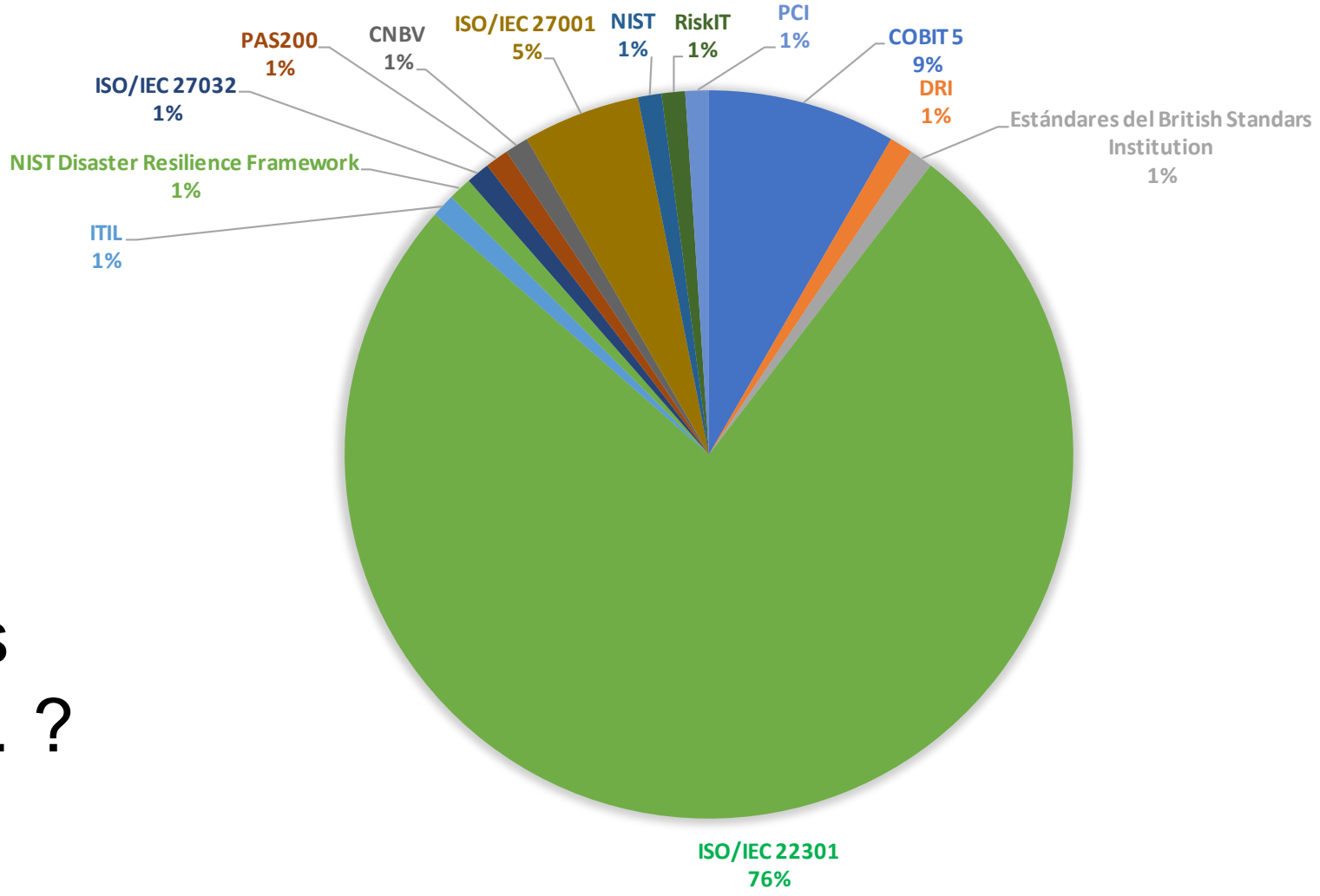


ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

## MENCIONA ALGUNOS ESTÁNDARES O BUENAS PRÁCTICAS EN LOS QUE EL PLAN DE CONTINUIDAD DE NEGOCIO SE BASÓ PARA SU DEFINICIÓN.




Al respecto ¿ nuestros encuestados que dicen … ?

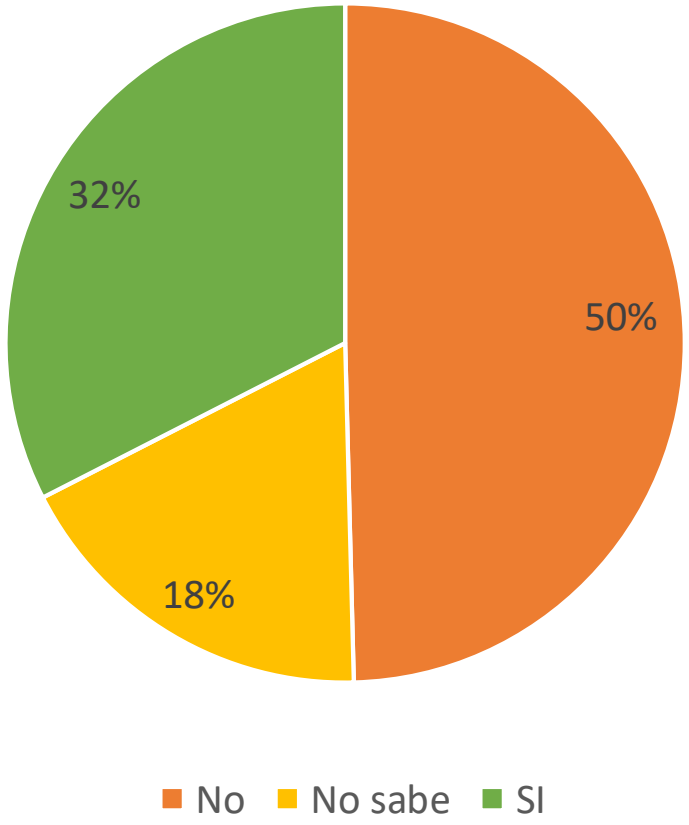
ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Al respecto ¿ nuestros encuestados que dicen … ?

¿Considerando el actual Plan de Continuidad de Negocio de la organización, el escenario relacionado a Pandemia, se encontraba incluido?

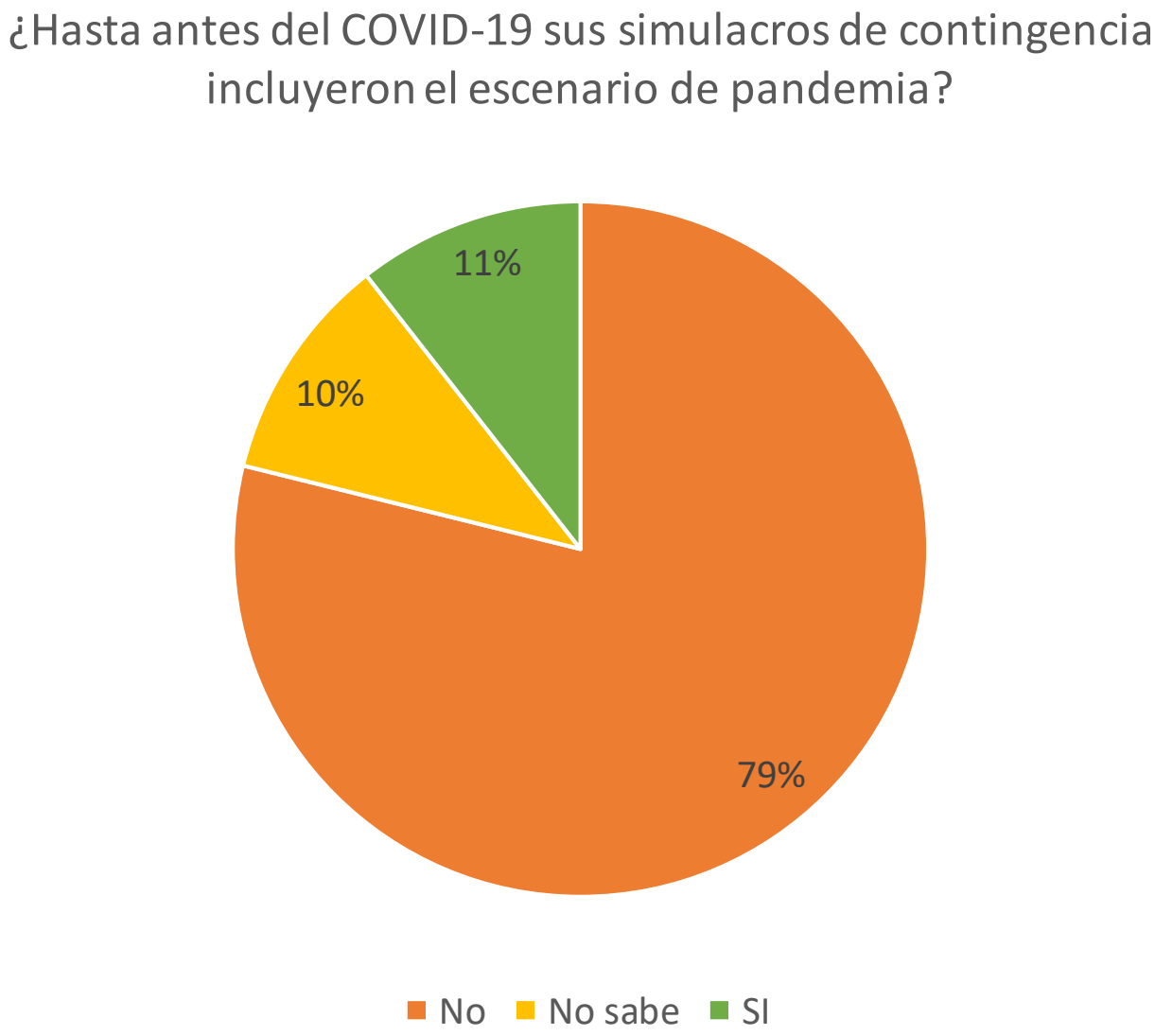


ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

Al respecto ¿ nuestros encuestados que dicen … ?



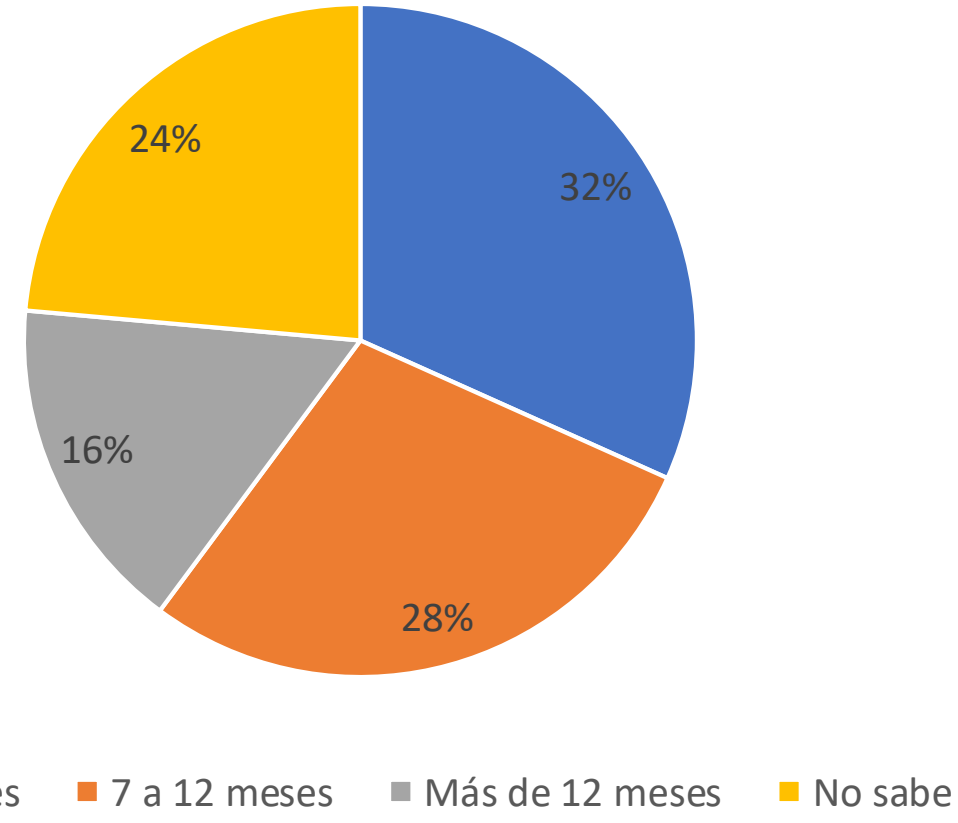
ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

¿Cuándo fue la última actualización del Plan de Continuidad del Negocio de la organización tomando como referencia el inicio del confinamiento?

Al respecto ¿ nuestros encuestados que dicen … ?



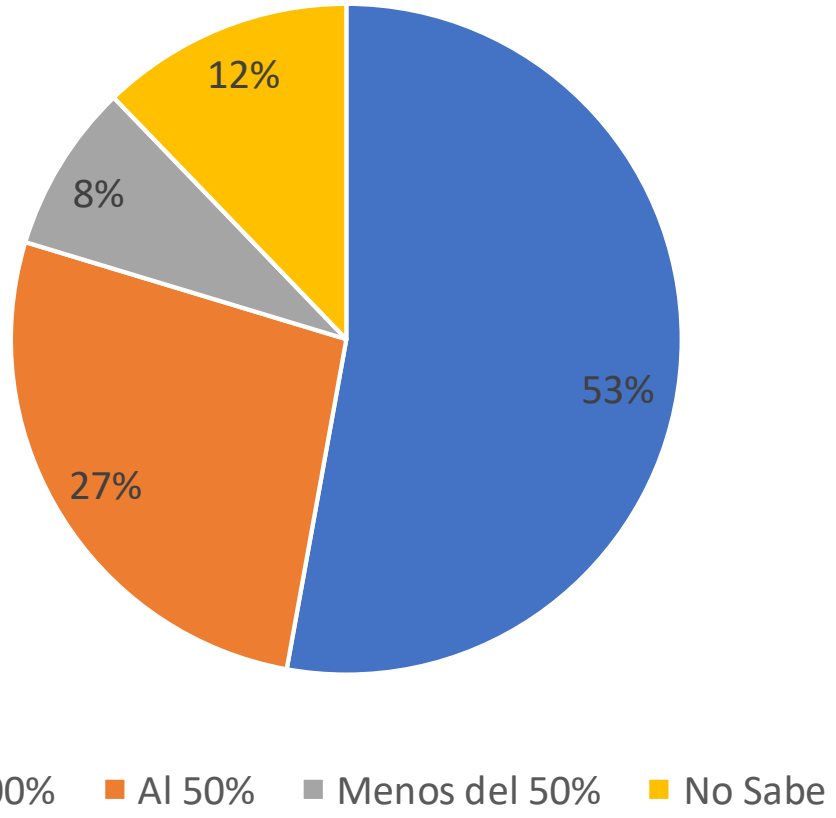
ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

Considerando el porcentaje de cobertura de los procesos críticos dentro del Plan de Continuidad del Negocio, ¿Qué porcentaje de cobertura incluye su actual BCP?

Al respecto ¿ nuestros encuestados que dicen … ?

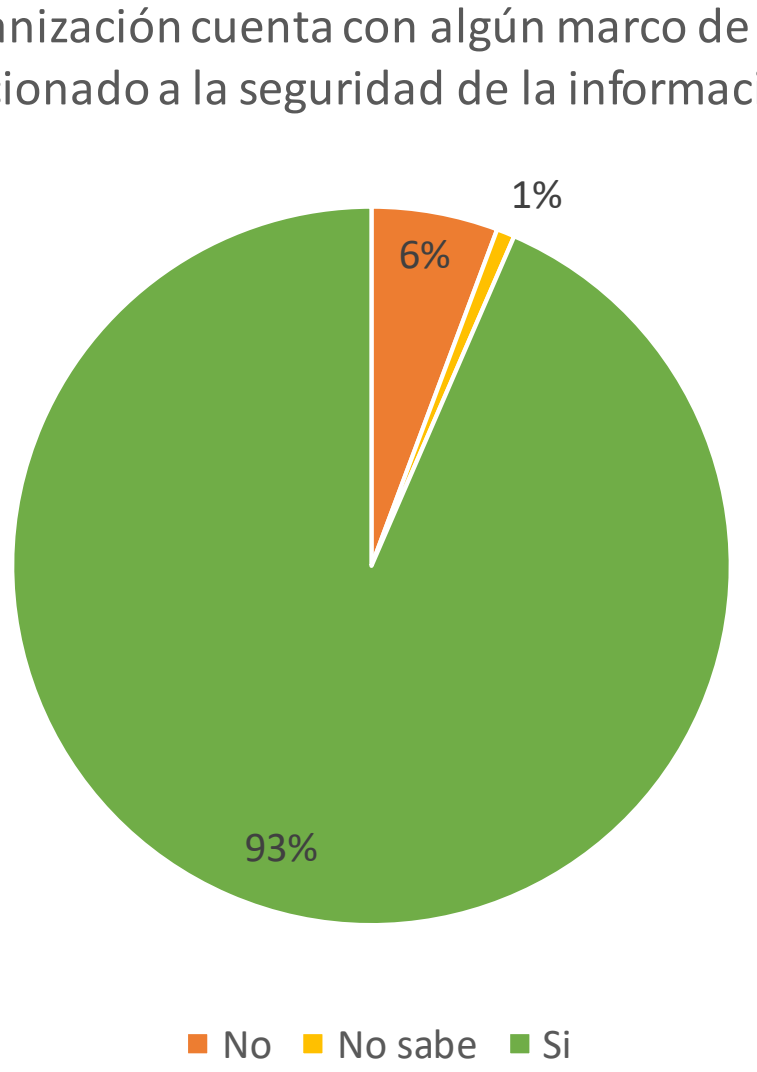


ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

Al respecto ¿ nuestros encuestados que dicen … ?

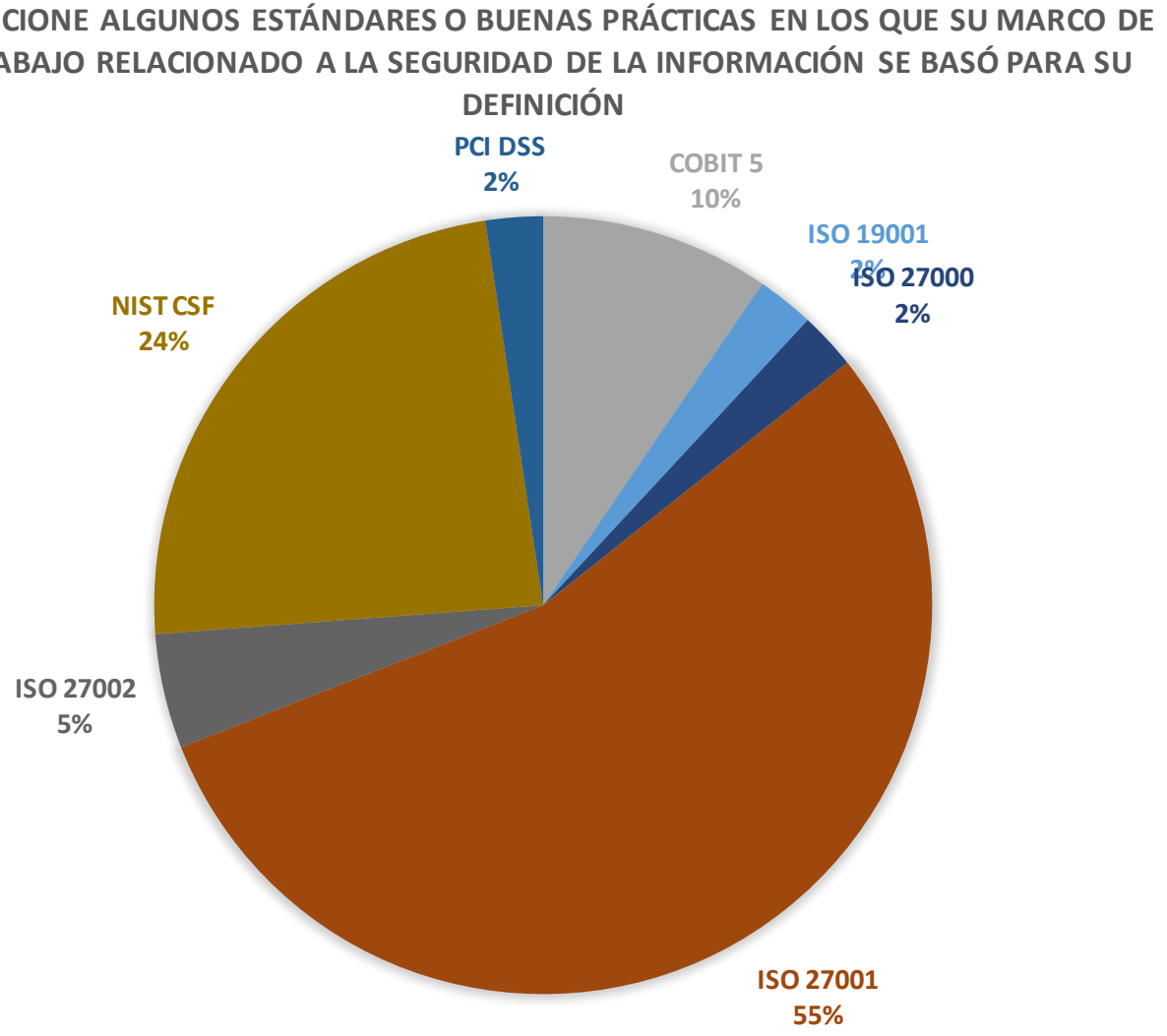


ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

Al respecto ¿ nuestros encuestados que dicen … ?



ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

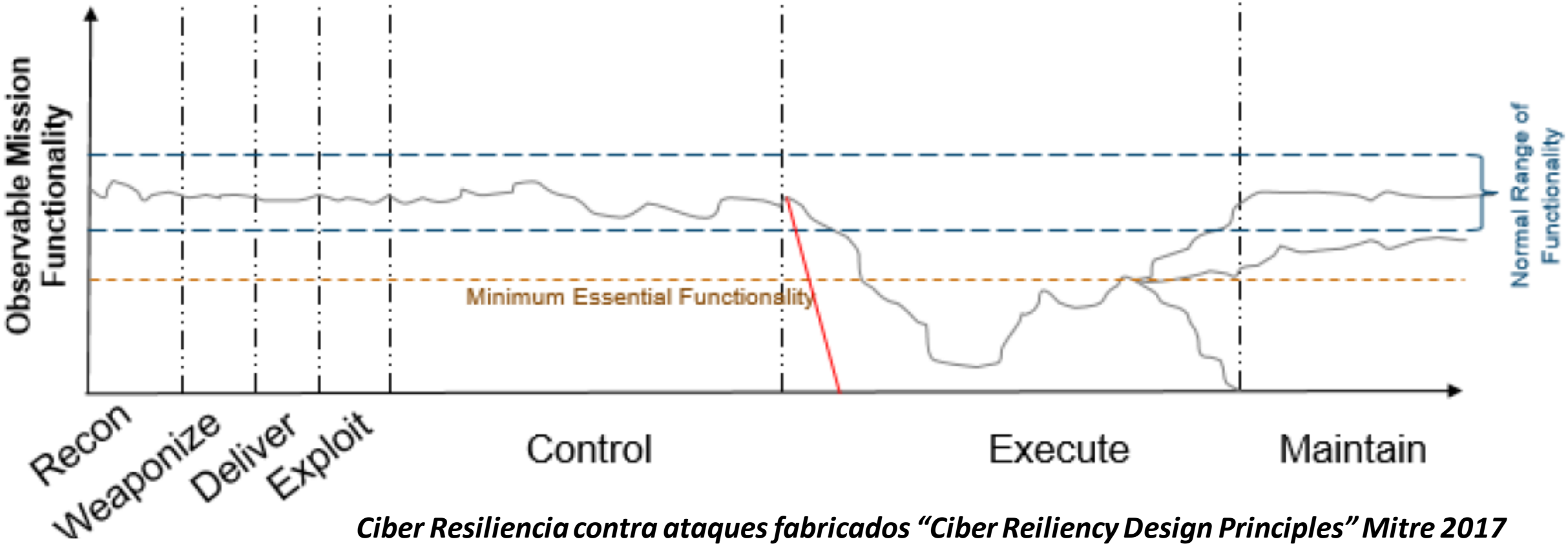
¿ La contingencia sanitaria provocada por el Covid-19 debe ser considerada como un desastre bajo los términos en los que ha sido conceptualizada dentro de los PCN ?

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia



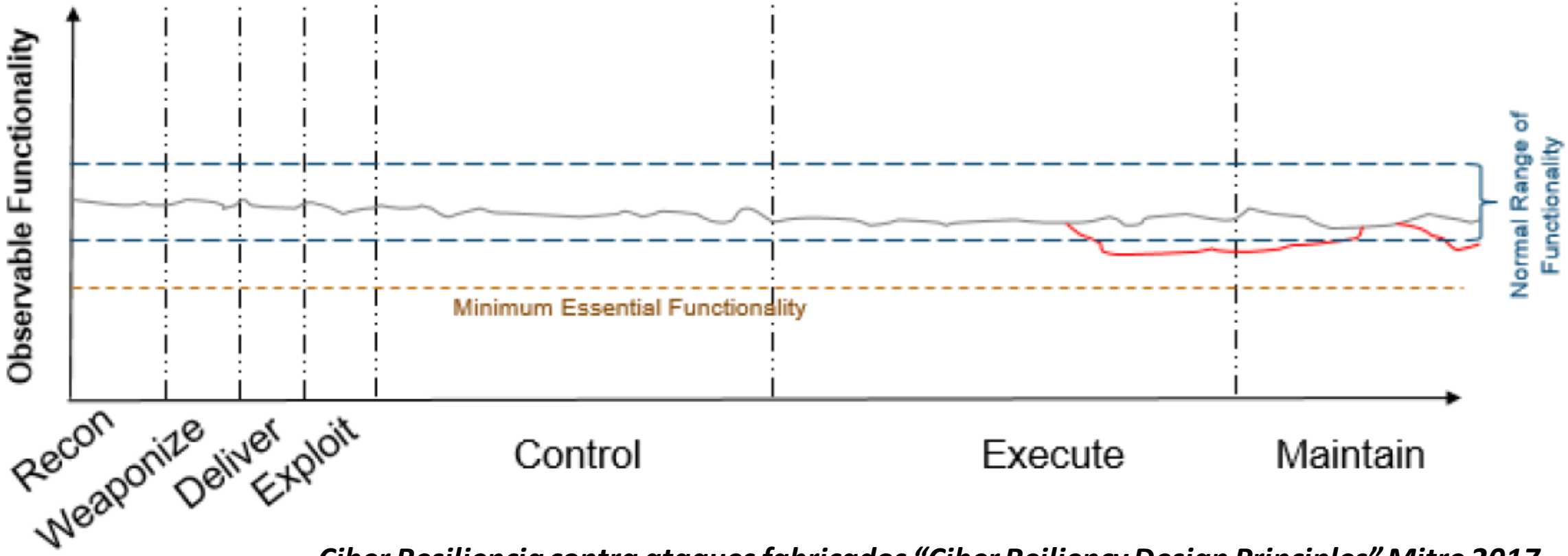

***Ciber Resiliencia contra ataques fabricados "Ciber Reiliency Design Principles" Mitre 2017***

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia




***Ciber Resiliencia contra ataques fabricados "Ciber Reiliency Design Principles" Mitre 2017***

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

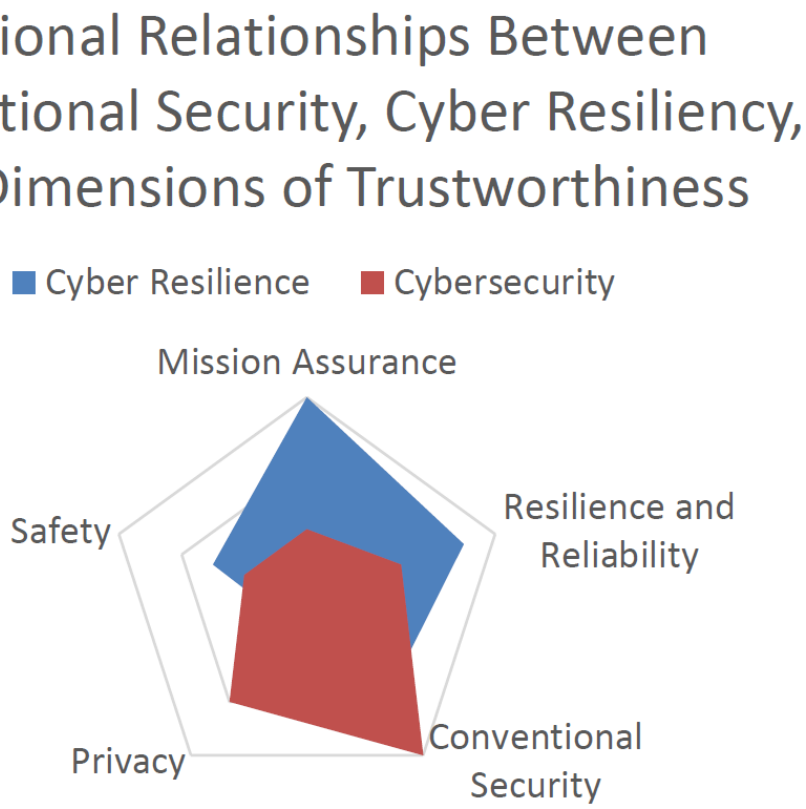
# Principales marcos de referencia en materia de Continuidad y Resiliencia

## Ciber Resiliencia

**NIST**

"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources."

This definition can be applied to a system; to a mechanism, component, or system element; to a shared service, common infrastructure, or system-of-systems identified with a mission or business function; to an organization; to a critical infrastructure sector or a region; to a system-of-systems in a critical infrastructure sector or sub-sector; and to the Nation.

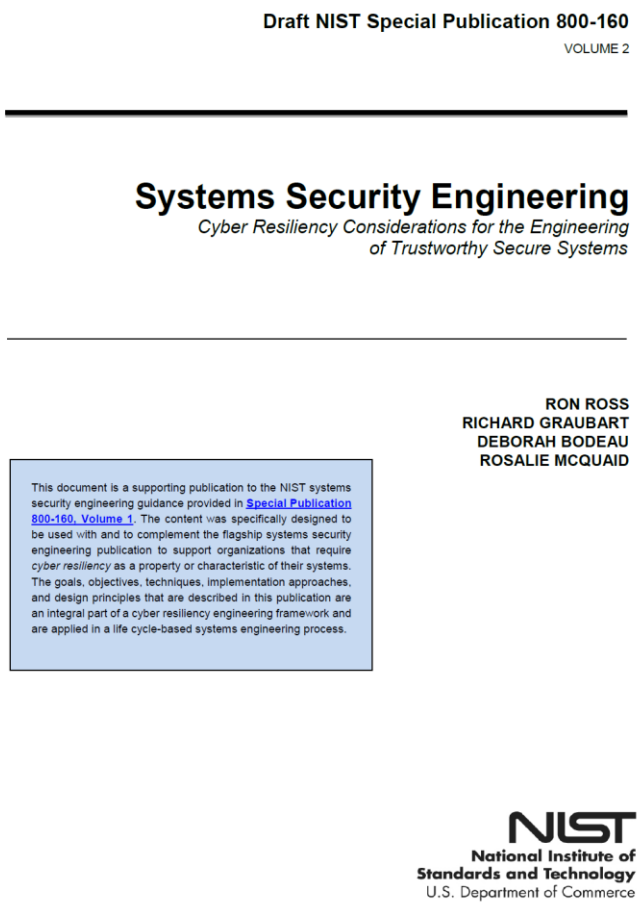


ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia



Draft NIST Special Publication 800-160

VOLUME 2

**Systems Security Engineering**

*Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*

RON ROSS
RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID

This document is a supporting publication to the NIST systems security engineering guidance provided in Special Publication 800-160, Volume 1. The content was specifically designed to be used with and to complement the flagship systems security engineering publication to support organizations that require *cyber resiliency* as a property or characteristic of their systems. The goals, objectives, techniques, implementation approaches, and design principles that are described in this publication are an integral part of a cyber resiliency engineering framework and are applied in a life cycle-based systems engineering process.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

| | Focus on common critical assets | Support agility and architect for adaptability | Reduce attack surfaces | Assume compromised resources | Expect adversaries to evolve |
|---|---|---|---|---|---|
| Limit the need for trust. | | | X | X | |
| Control visibility and use. | X | | X | X | |
| Contain and exclude behaviors. | X | | | X | X |
| Layer defenses and partition resources. | X | | | X | |
| Plan and manage diversity. | X | X | | X | |
| Maintain redundancy. | X | X | | X | |
| Make resources location-versatile. | X | X | | | X |
| Leverage health and status data. | X | X | | X | X |
| Maintain situational awareness. | X | | | | X |
| Manage resources (risk-) adaptively. | X | X | | | X |
| Maximize transience. | | | X | X | X |
| Determine ongoing trustworthiness. | X | | | X | X |
| Change or disrupt the attack surface. | | | X | X | X |
| Make the effects of deception and unpredictability user-transparent. | | X | X | | |

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Principales marcos de referencia en materia de Continuidad y Resiliencia

| | | | |
|---|---|---|---|
| Adaptive response | Analytic monitoring | Coordinated protection | Deception |
| Diversity | Dynamic positioning | Dynamic representation | Non-persistence |
| Privilege restriction | Realignment | Redundancy | Segmentation |
| | Substantiated integrity | Unpredictability | |

# Principales marcos de referencia en materia de Continuidad y Resiliencia

## ISO 22300 Series

### ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes

**Organizational resilience** is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.

More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context.

Enhancing resilience can be a strategic organizational goal, and is the outcome of good business practice and effectively managing risk.

**Annex A**

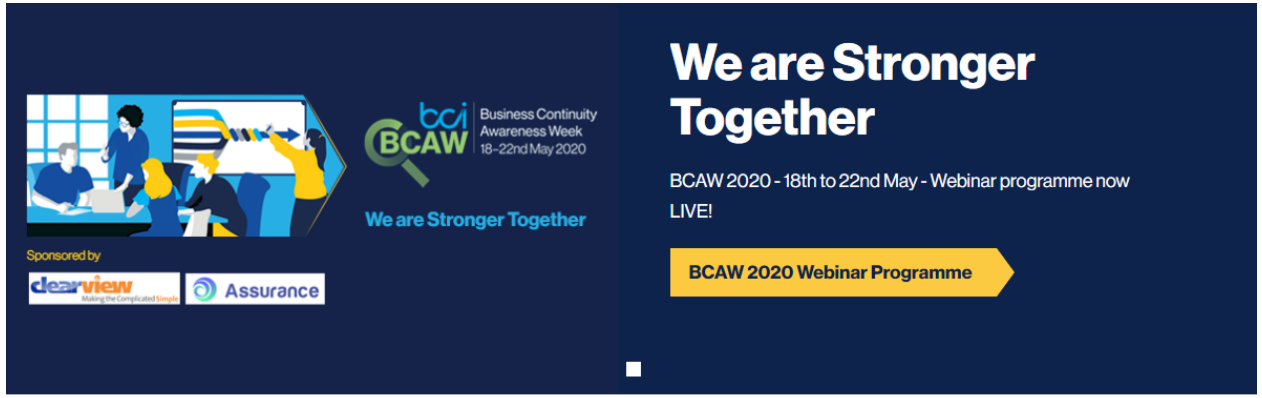
**Relevant management disciplines**

- **asset management;**
- **business continuity management;**
- **crisis management;**
- **cyber security management;**
- **communications management;**
- **emergency management;**
- **environmental management;**
- **facilities management;**
- **financial control;**
- **fraud control;**
- **governance;**
- **health and safety management;**
- **human resources management;**
- **information security management;**
- **information, communications and technology;**
- **physical security management;**
- **quality management;**
- **risk management;**
- **supply chain management;**
- **strategic planning.**

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter




Welcome | Webinar Programme | Downloads | Blogs | Discounts | Sponsors

The BCAW 2020 Webinar Programme is now live, with three engaging streams and packed with insightful sessions led by experts in business continuity and resilience.

**Start browsing the programme now and register your place in the webinars that most interest you! All times are in BST.**

**All webinars will be recorded and will be available on our Knowledge Library.**

**18 May** | **19 May** | **20 May** | **21 May** | **22 May**

Los expertos en el tema de continuidad y resiliencia, uno de ellos, el ***Business Continuity Institute***, ya están trabajando para marcar los nuevos lineamientos a partir del Covid-19

## COVID-19 – A black swan event for Business Continuity Planning?

60 mins | Stream #3 - COVID-19 & Pandemic Planning | **Speaker:** Brett Wilson, Director of Data Centre & Business Continuity

## Will the COVID-19 Pandemic Change Business Continuity Management for Ever?

60 mins | Stream #3 - COVID-19 & Pandemic Planning

## COVID-19: Business Resilience in the Face of the Unexpected

60 mins | Stream #3 - COVID-19 & Pandemic Planning

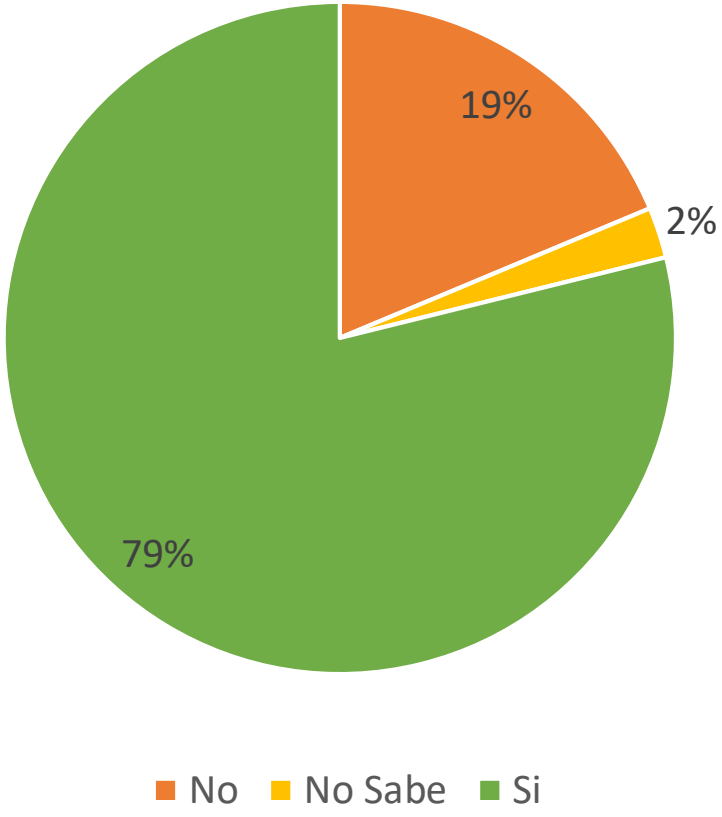
ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

¿Al momento de iniciar el confinamiento, contaba con la infraestructura suficiente para trabajar vía remota (Equipos, VPN) y atender al menos los procesos críticos)?

Al respecto ¿ nuestros encuestados que dicen … ?



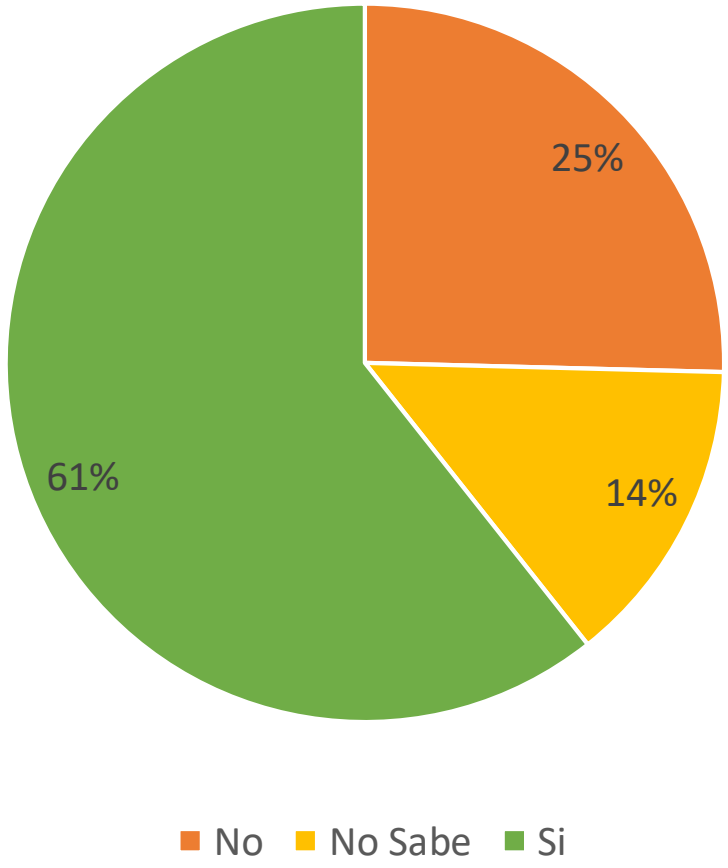
ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

¿Hasta antes de la contingencia sanitaria sabe si los controles de seguridad para el trabajo remoto habían sido evaluados?

Al respecto ¿ nuestros encuestados que dicen … ?



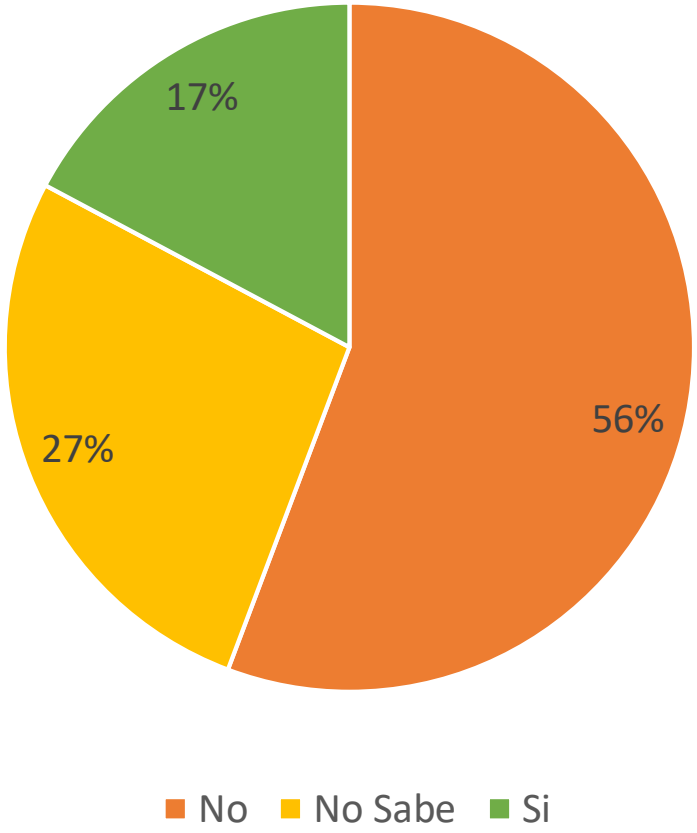
ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

¿Durante la etapa de confinamiento, los usuarios de su empresa han registrado incidentes de seguridad de la información trabajando desde sus hogares?

Al respecto ¿ nuestros encuestados que dicen … ?

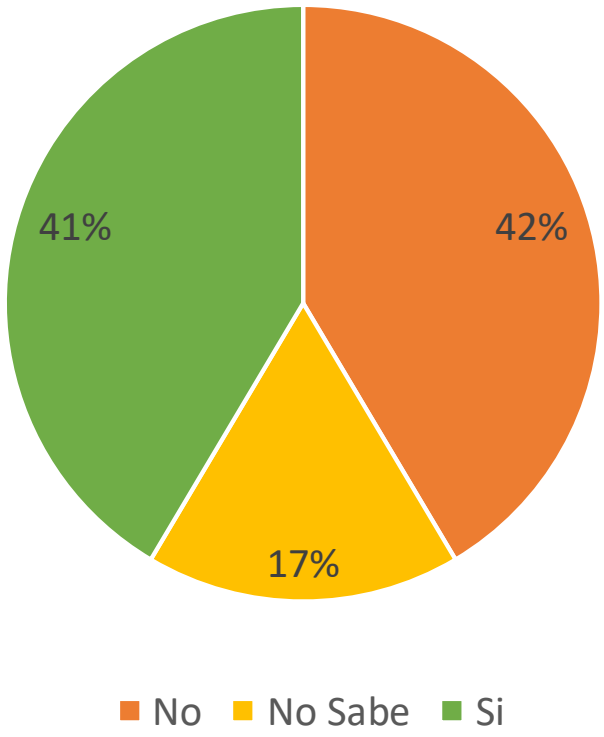


ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Al respecto ¿ nuestros encuestados que dicen … ?



ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# ¿ Cómo saber que tan Resiliente fue nuestra organización, bajo el escenario de confinamiento provocado por el Covid-19, considerando además, aspectos de Seguridad de la Información ?

ISACA Guadalajara Chapter

infosecurity MEXICO

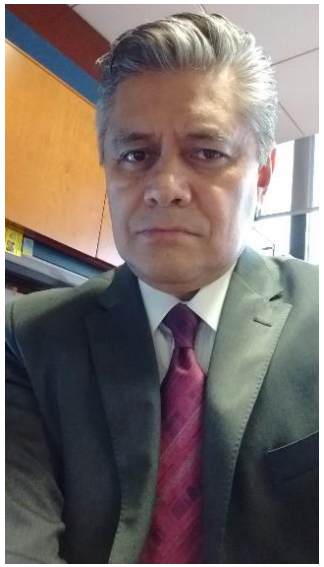
ISACA Mexico City Chapter

# ¿Preguntas?

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter



**Rubén Quintero Ubando**
Vicepresidente de ISACA Capítulo Ciudad de México
r.quinterou@gmail.com

**Roberto Hernández Rojas Valderrama**
Presidente de ISACA capítulo Ciudad de México
roberto.hernandezrv@dyasys.com.mx


**Hugo Enrique Santamaría Martínez**
Presidente de ISACA Capítulo Guadalajara
presidente@isacagdl.org.mx

ISACA Guadalajara Chapter

infosecurity MEXICO

ISACA Mexico City Chapter

# Panel Continuidad del negocio .. Los nuevos retos de la ciberseguridad

## Gracias

Mayo 26, 2020