Infraestructura Crítica Ciberseguridad en Chile

Marco Antonio Zúñiga
marco@maz.cl – www.maz.cl

Diciembre 2019

Contenidos

- **Presentación de Modelos de Infraestructura Crítica (Contenido Público de Microsoft)**
- **CSIRT de Gobierno**
- **Política Nacional de Ciberseguridad**

Asegurando Infraestructuras Críticas

Marco A. Zúñiga

Gerente de Desarrollo Negocios Sector Público
Microsoft Chile

maz@microsoft.com

Microsoft
Your potential. Our passion.™

En su opinión, en el terremoto de 1960 en Chile, el principal impacto inicial fue:

1. *Alimento y Vivienda*
2. *Comunicaciones*
3. *Energía*
4. *Obras Civiles y Conectividad Terrestre*
5. *Servicios Básicos*

En su opinión, en el terremoto de 2010 en Chile, el principal impacto inicial fue:

1. *Alimento y Vivienda*
2. *Comunicaciones*
3. *Energía*
4. *Obras Civiles y Conectividad Terrestre*
5. *Servicios Básicos*

¿ Qué cambió ?

¿Cómo? ¿Por qué?

Características de la Nueva Economía

Digitalización	Activos Físicos v/s Información y Datos
Virtualización	En sector Financiero, Comercial, de Información, de Soporte, tanto Públicos como Privados
Información en Tiempo Real	Comunicación e Información en línea vital para la operación personal y de la sociedad
Sociedad de Servicios	Servicios Físicos y Virtuales

Nuevas Acciones en una Nueva Economía

Reducción de Costos	• Mejoras a la administración de energía • Amigables con el ambiente
Liderazgo del Ecosistema	• Socialización de formas innovadoras de pensar y usar la tecnología • Generar percepciones y deseos de adoptar nuevas tecnologías (confianza)
Consideraciones Geo-Políticas	• Aumento de dependencia tecnológica • Cyber-warfare • Sistemas de identificacion y ciudadanía
Impacto Económico	• Impacto devastador de actividades no chequeadas, resultado del aumento creciente de la “rapidez de entrega” (efecto “run-away”)

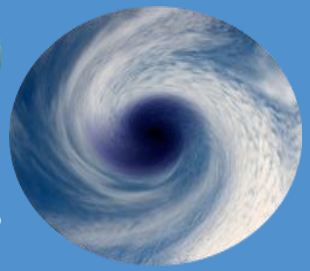
Los modelos de riesgo cambian

Porque las amenazas son múltiples y diversas …

Protección de Infraestructura

Preocupaciones de la Política


Cyber-ataques


Desastres Naturales


Convergencia


Terrorismo


Guerra


Globalización

Respuestas de la Política

Estrategias Nacionales
Directivas/Políticas
Planes de Respuesta a Emergencias

Asegurando Infraestructuras Críticas

Resilient

Innovative

Trustworthy

Microsoft

Trustworthy Infrastructure Programs and Policy

Infraestructura Crítica Global

- *Infrastructura Crítica* se entiende generalmente como los sistemas clave, servicios y funciones cuya disrupción o destrucción tiene un impacto que debilita la salud y seguridad pública, el comercio y/o la seguridad nacional. Esto incluye:
  - Comunicaciones
  - Energía
  - Servicios Financieros
  - Transporte
  - Salud y Seguridad Pública
  - Servicios esenciales del Gobierno

Ejemplos de Infraestructuras Críticas

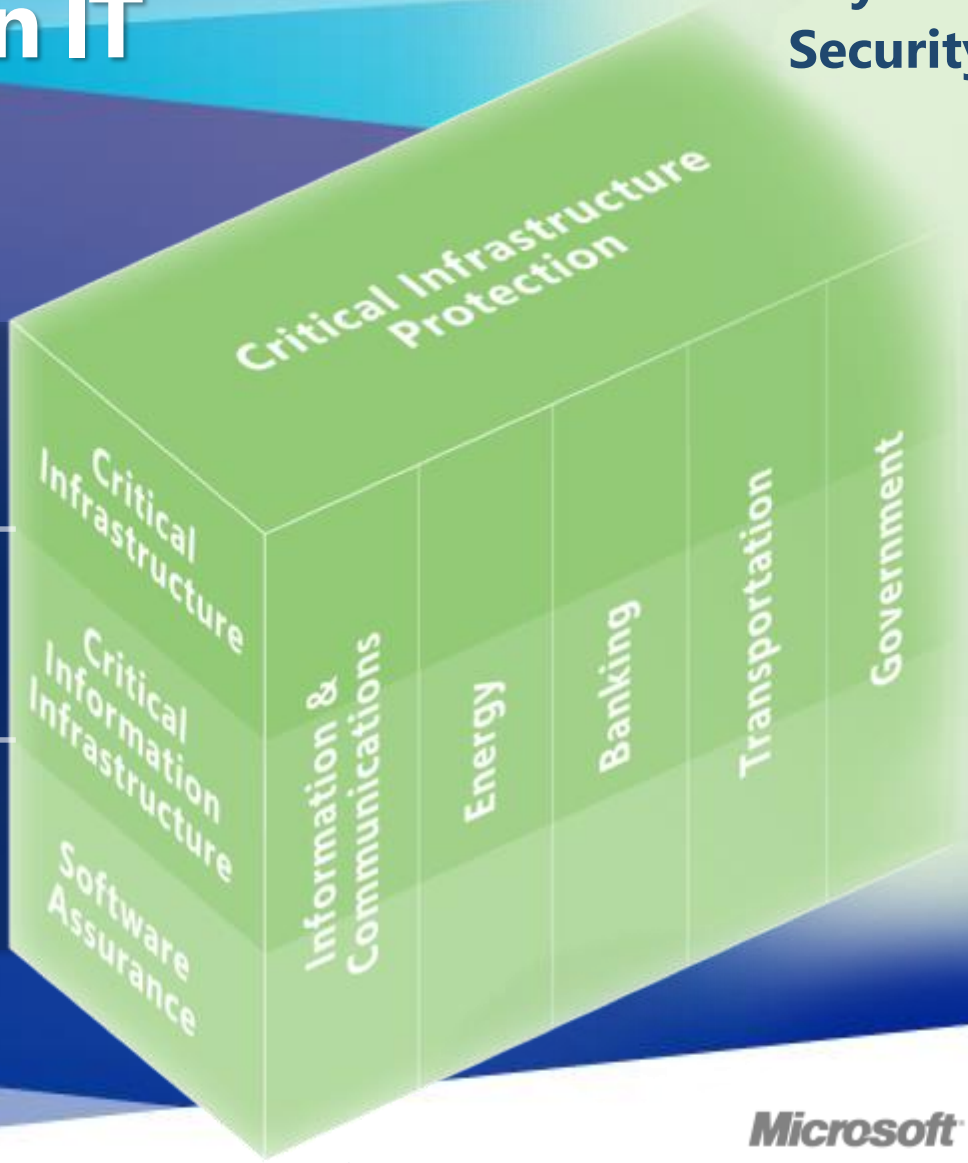
Infraestructura Crítica
Soporte confiable en IT

Cyber Security

Aseguramiento de sistemas clave físicos y virtuales, servicios y funciones

Sistemas Virtuales Críticos

Software, hardware, y servicios funcionando en forma predictible



Microsoft

Trustworthy Infrastructure Programs and Policy

La visión para Protección de Infraestructura Crítica

Apoyar al ecosistema estratégico y el cambio interno que fortalezca la infraestructura de seguridad y la resiliencia, construya confianza y permita el alineamiento de acciones con los gobiernos y proveedores de infraestructura crítica

Secure

Trustworthy Computing

Resilient

Trustworthy Computing

Trustworthy

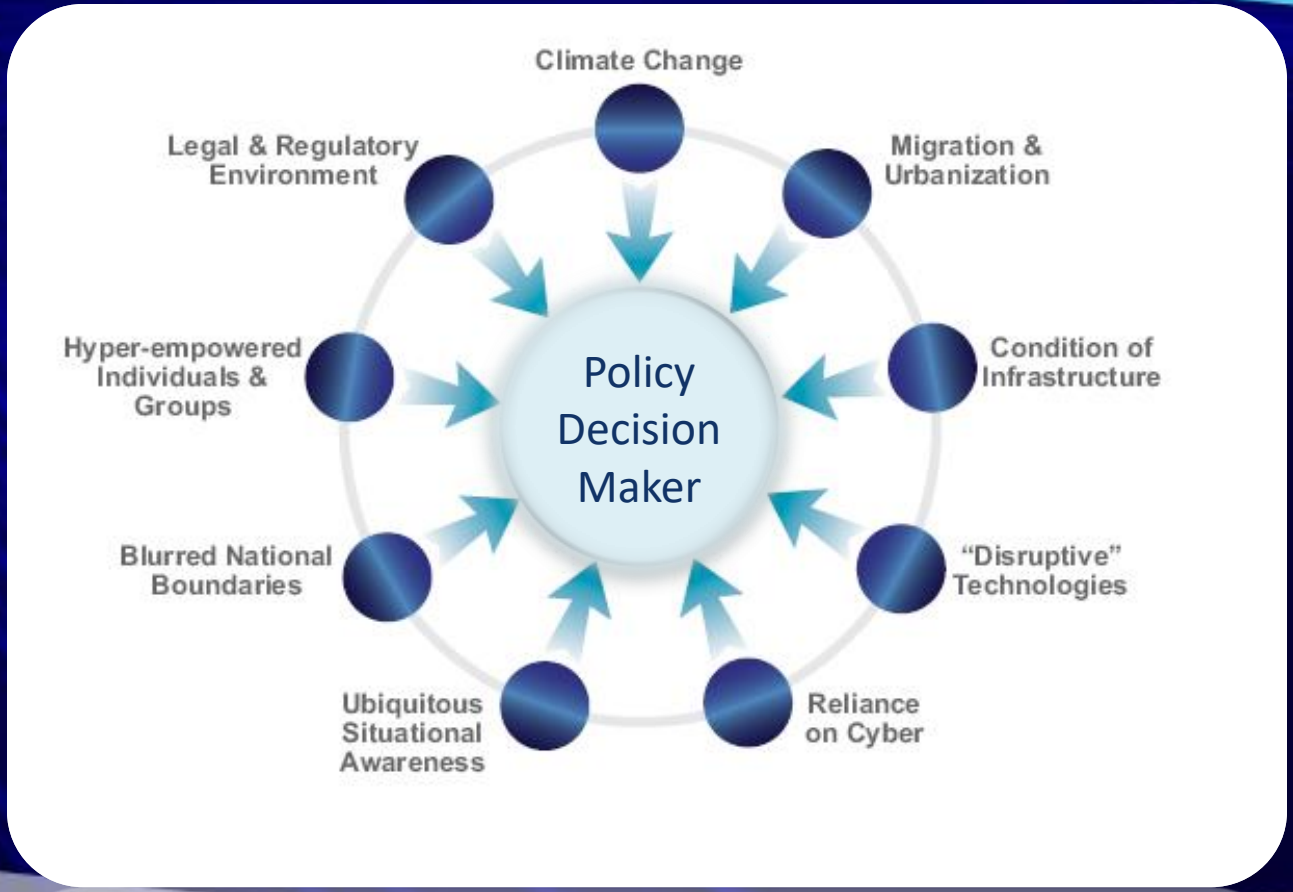
Trustworthy Computing

Innovative

Trustworthy Computing

Protección de Infraestructura

Complejidad de las Infraestructuras Críticas



Source: modified from *Guarding Our Future Protecting Our Nation 's Infrastructure* Toffler Associates 2008

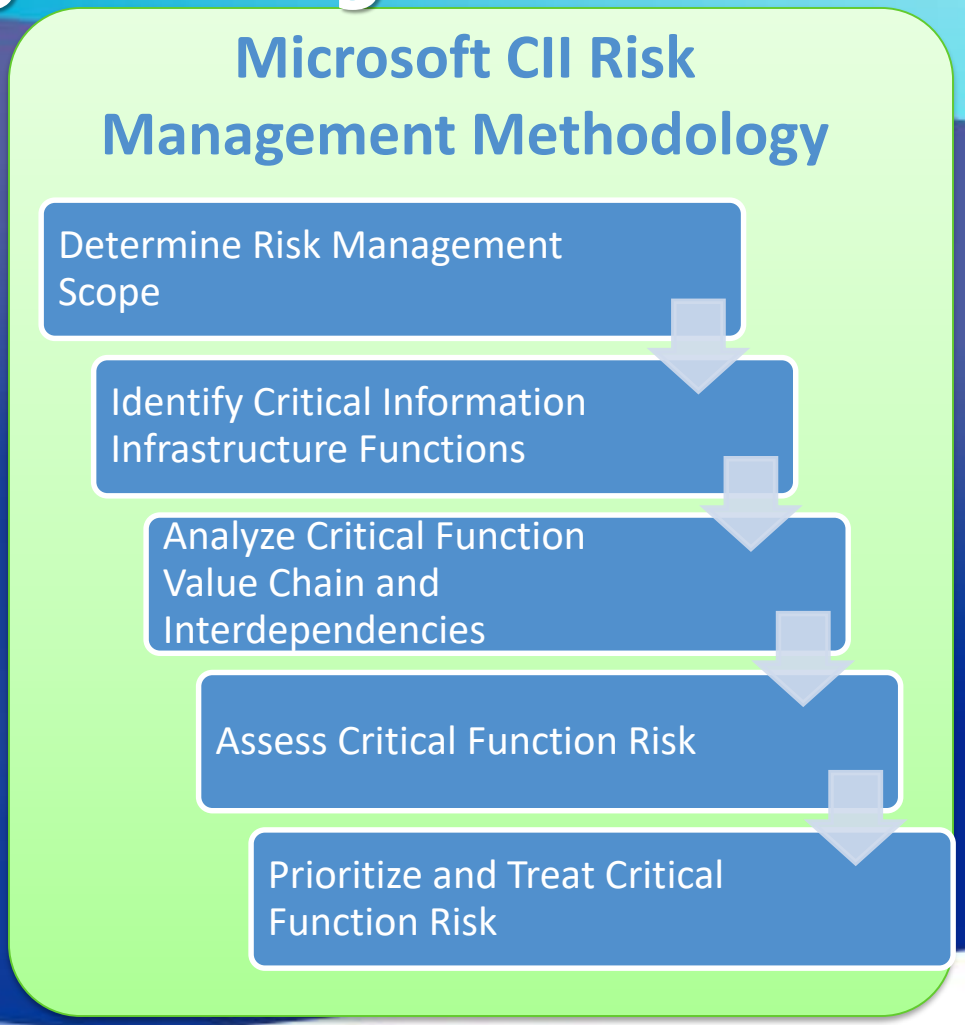
CIP Continuum
Un modelo continuo

- Identifica tres funciones distintas para crear una capacidad de protección de infaestructura crítica
- Enfatiza la importancia de coordinación efectiva y compromiso con el sector privado para un plan efectivo, gestión, respuesta y protección
- Define el desarrollo de programas que evolucionan en un entorno dinámico

Operaciones Resilientes

Operaciones Resilientes–
Administración de Riesgo Estratégico

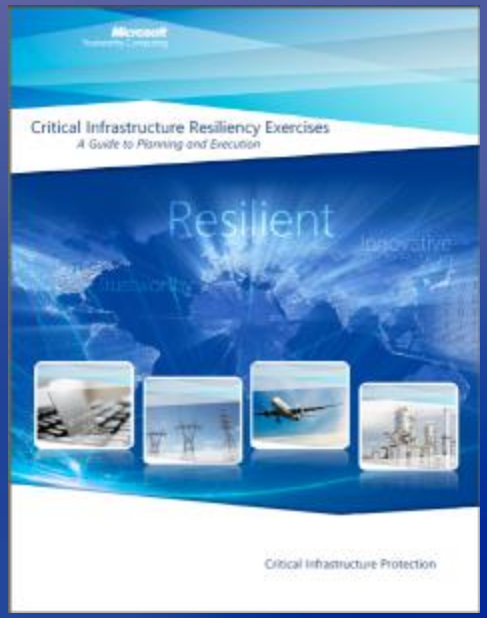
- Optimiza recursos limitados para proteger la infraestructura más crítica
- Se focaliza en objetos de infraestructura
  - Bienes
  - Localizaciones
  - Sistemas
  - Funciones
- Basada en estrategias metodológicas definidas
  - Bottom up
  - Top-down



Operaciones Resilientes – Administración del Riesgo Operacional

Operacione Resilientes – Ejercicios de Infraestructura Crítica

- **Valor**
  - Construye Confianza
  - Promueve Alianzas
  - Mejora el compartir información
  - Identifica brechas de preparación
  - Resuelve brechas mediante colaboración
- **Microsoft's Critical Infrastructure Resiliency Exercise Guide**
  - Una guía detallada, paso a paso, proceso "how-to" para planificar, conducir y aprender a partir de los ejercicios de infraesructura crítica
  - Sugerencias para enfrentar cada etapa del ejercicio
  - Material de apoyo, referencias, templates, y presentaciones ejecutivas PowerPoint relacionadas con cada etapa del proceso del ejercicio.



Algunas experiencias globales …

Cómo se prepara el mundo en la globalidad

Trustworthy Plans and Policies

International Telecommunications Union

A national approach to cybersecurity includes raising awareness about existing cyber risks, creating national structures to address cybersecurity, and establishing the necessary relationships that may be utilized to address events that occur. Assessing risk, implementing mitigation measures, and managing consequences are also part of a national cybersecurity program. A good national cybersecurity program will help protect a nation's economy from disruption by contributing to continuity planning across sectors, protecting the information that is stored in information systems, preserving public confidence, maintaining national security, and ensuring public health and safety.

International Telecommunications Union
January 2008

Five Elements of a National Cyber Security Capability

- Developing a National Strategy for Cybersecurity
- Establishing National Government–Industry Collaboration
- Deterring Cybercrime
- Creating National Incident Management Capabilities
- Promoting a National Culture of Cybersecurity

Trustworthy Plans and Policies

European Union

[…] ICT systems, services, networks and infrastructures […] form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.

European Commission Communication on CIIP
March 2009

Challenge and Action Plan

- Preparedness and prevention
  - Baseline of [CERT] capabilities and services for pan-European cooperation
  - European Public Private Partnership for Resilience (EP3R)
  - European Forum for information sharing between Member States
- Detection and response
  - European Information Sharing and Alert System (EISAS)
- Mitigation and recovery
  - National contingency planning and exercises.
  - Pan-European exercises on large-scale network security incidents
  - Reinforced cooperation between National/Governmental CERTs
- International cooperation
  - Internet resilience and stability
  - Global exercises on recovery and mitigation of large scale Internet incidents
- Criteria for the ICT sector
  - ICT sector specific criteria

Trustworthy Plans and Policies

United States

The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. This technology has transformed the global economy and connected people in ways never imagined. Yet, cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. [...] It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution.

White House Cyberspace Policy Review
May 2009

Action Plan

- Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
- Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
- Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
- Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
- .....
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation

Cibersecurity in Chile

Dec 2018

Marco A. Zuniga
marco@maz.cl
@mazuniga

https://ncsi.ega.ee/

Context

- 2017:
- Chile in Budapest Convention about Cybercrime
- National Cybersecurity Policy (Defense vs. Interior)
- Still pending: new Privacy Law (last release 1999)

- 2018:
- Security breaches in Financial Sector (Q1)
- Credit Cards (carding) (Q2)
- Banco de Chile breach (Q2)
- Banco Consorcio breach (Q4)
- Appointment of National Cybersecurity Coordinator (Q2)
  - President DR
  - New legislative initiatives
  - Governance Model for Cyber in Government

Business environment

New political sponsors in Government and Parlament

16% of national companies have Cybersecurity as a priority in Boards (still slow)

Cibersecurity Alliance (multisectorial) conformed in May 2018

Specific regulations and initiatives for specific industries

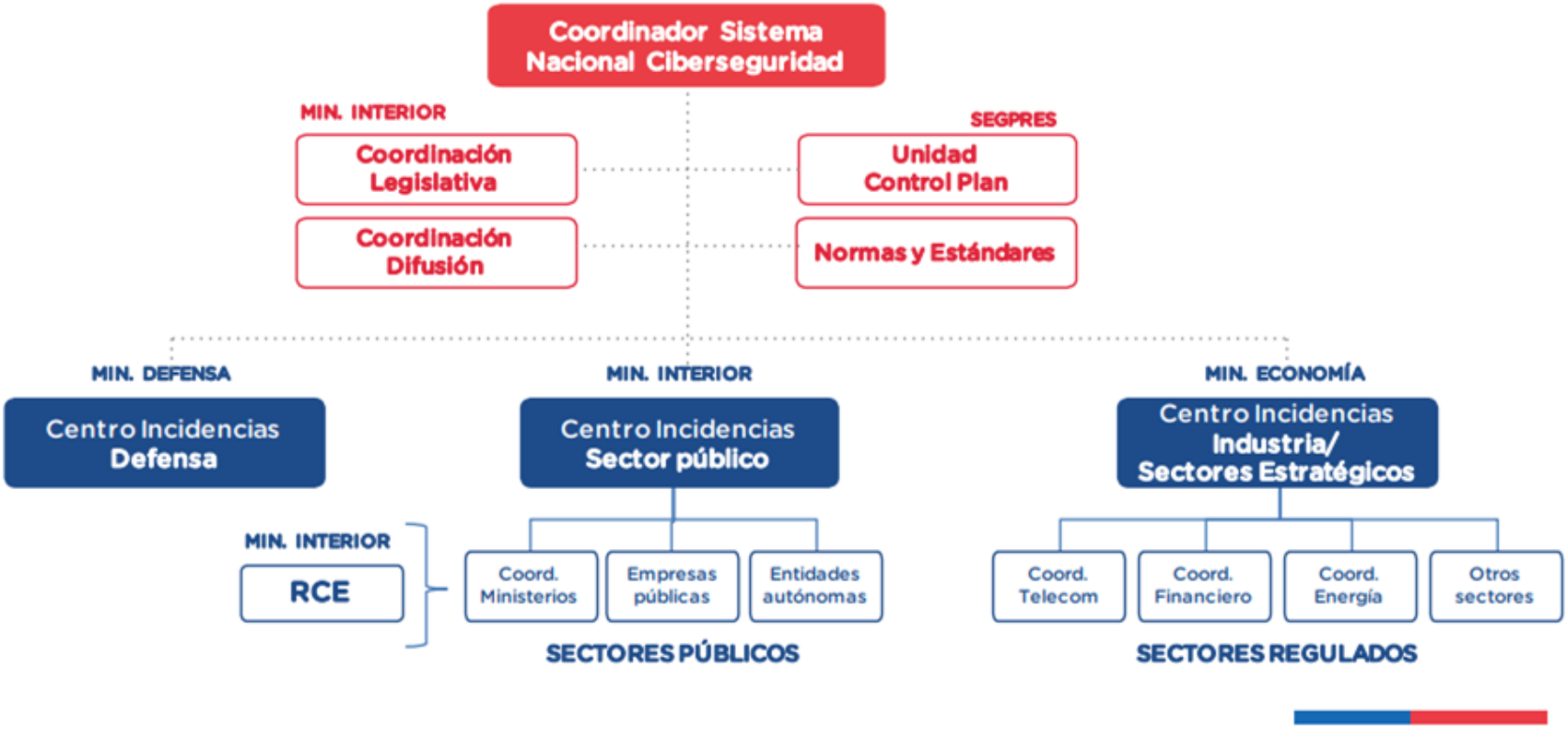
No stoppers for Cloud usage

Cloud first policy for Govenment institutions

Few companies specialized, lack of professionals

Lack of international experience

GOBERNANZA PROVISORIA DE CIBERSEGURIDAD



AGENDA LEGISLATIVA

Proyecto de Ley General de Banco (LGB)

- Proyecto de Ley en trámite.
- Ley Corta para incorporar exigencias de Ciberseguridad mercado financiero.

Proyecto Ley de Datos Personales

- En trámite. Una buena protección de los datos personales es clave.

Nueva Ley de Delitos Informáticos

- Tipificación de Nuevos Delitos.
- (Convención de Budapest)
- Mejora procesal de la prueba del delito.

Ley Marco de Ciberseguridad

- Definiciones y responsabilidades sobre Ciberseguridad.
- Creación de Centros de Respuesta ante Incidencias/Emergencias Informáticas en sectores público y privado.

Proyecto Ley Registro de Celulares Prepago

- Presentar proyecto ley para el registro de teléfonos de prepago. Este tema tiene beneficios para prevención del delito, disminuir el fraude en Portabilidad y minimizar los delitos de Ciberseguridad.

Ley de Infraestructura crítica para Sistemas de Información

- Definición de Instituciones Públicas y Empresas Privadas estratégicas para los sistemas de Información.
- Regulación de ellas para evitar y mejorar incidentes de emergencias Informáticas.

ALIANZA CHILENA DE CIBERSEGURIDAD

Infraestructura Crítica: Las Preguntas Pendientes

06 junio 2019

Marco A. Zúñiga
Consejero de la Alianza Chilena de Ciberseguridad
Director Ejecutivo de Chiletec

Qué hemos aprendido

Desde diciembre 2018

- Las diferencias entre Seguridad, Ciberseguridad, SGSI, Infraestructura Crítica, Gestión del Riesgo, ¿Continuidad del Negocio?
  - Si usted no sabe las diferencias → preocúpese y ocúpese
  - Si su Directorio no sabe las diferencias → [preocúpese y ocúpese] x 10
- Colaboración del ecosistema es la única vía
- Se establece mediante Alianzas Público – Privadas
- Son procesos de mejora continua
  - Ciclo de Deming: Planificar, Hacer, Verificar, Actuar

ALIANZA CHILENA DE CIBERSEGURIDAD

Ciclo de Deming (ISO)

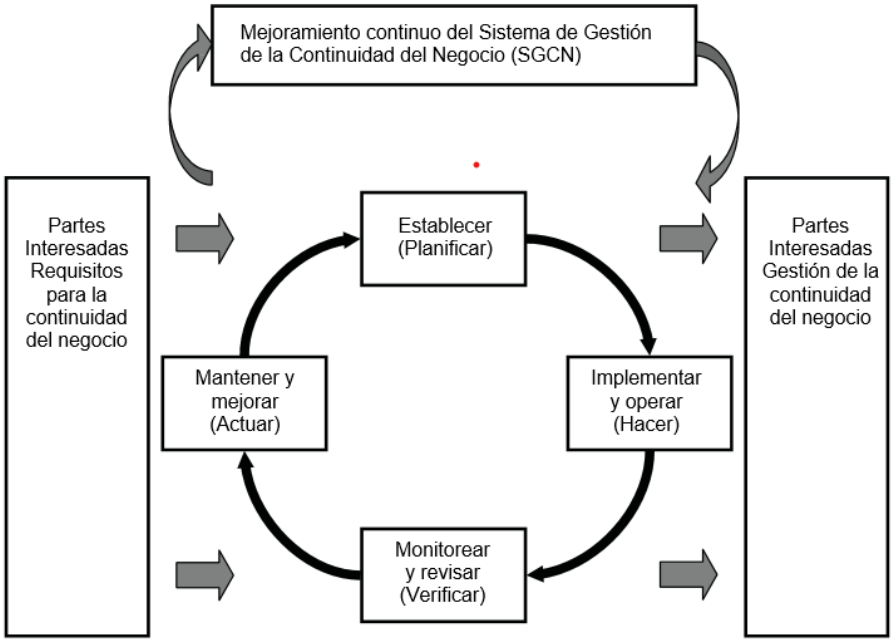
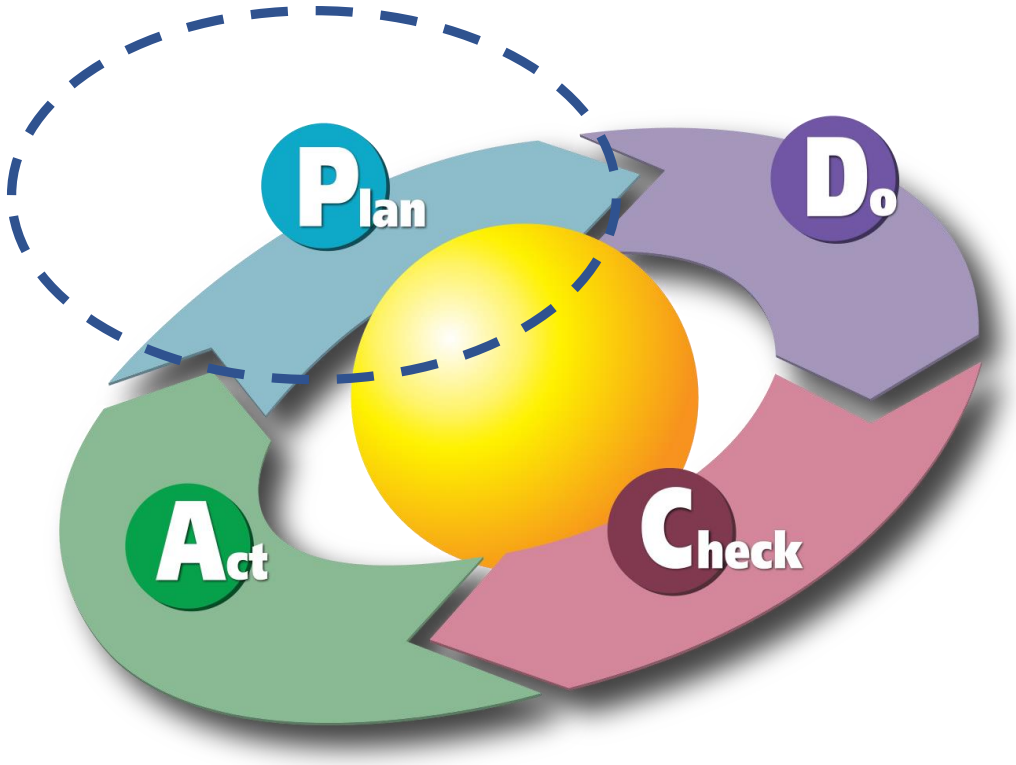


Figura 1 - Modelo PHVA aplicado a los procesos SGCN

ALIANZA CHILENA DE CIBERSEGURIDAD

Ciclo de Deming (Wikipedia)



ALIANZA CHILENA DE CIBERSEGURIDAD

Desafío Pendiente: La Alta Gerencia

- La Gestión del Riesgo es un tema instalado en muchas organizaciones
  - Pero los riesgos tecnológicos no están bien conectados
- La Gestión de Continuidad del Negocio no es aún un tema instalado
  - La Seguridad en todas sus variantes es componente fundamental del Negocio
    - Seguridad de la sociedad
    - Sistemas de gestión de la continuidad del negocio
- La Seguridad y sus variantes ya no es responsabilidad de la Administración, es responsabilidad del Directorio
- ¿Cuál es el modelo de gobernanza adecuado?

ALIANZA CHILENA DE CIBERSEGURIDAD

Preguntas y tareas pendientes
para Chile

- ¿Qué componentes consideramos en Chile como parte de nuestra Infraestructura Crítica?
  - No es una discusión técnica. Es una discusión política que considera historia, cultura, modelo país, tecnología, capacidades, prioridades.
- No más intuiciones o wishful thinking. ¿Cuáles es la base de estándares sobre los cuales nos basaremos?
  - ISO ¿23xxx?, ¿27xxx?, ¿38xxx?
- ¿Cómo coordinamos actores relevantes en nuestro país para la estrategia y respuesta a la emergencia?
- ¿Cuál es nuestro Manual de Procedimientos frente a la emergencia?
- ¿Cuál es el procedimiento de mejora continua de nuestras políticas?

ALIANZA CHILENA DE CIBERSEGURIDAD

Ciberseguridad

Un desafío para la Transformación Digital de la Pymes

Recursos y Herramientas Prácticas para Afrontar la Ciberseguridad

Marco A. Zúñiga
Director Ejecutivo CHILETEC
@mazuniga

#CiberseguridadParaPymes

CORFO

@Corfo

CHILETEC

@ChiletecOrg

CAPACITACIÓN usach
UNIVERSIDAD DE SANTIAGO DE CHILE

@Usach_Capacita

Las duras cifras …

Un 34,6% de las pymes de Valparaíso, Santiago y Concepción han sufrido algún tipo de incidente relacionado con la ciberseguridad. Este porcentaje fue obtenido gracias al estudio "Vulnerabilidad de Empresas en Ciberseguridad", realizado por el Observatorio del Comercio Ilícito (OCI), iniciativa de la Cámara Nacional de Comercio, Servicios y Turismo (CNC).

De acuerdo con sus resultados, las vulneraciones informáticas van desde infecciones de virus, en un 28%, hasta el robo de información de bases de datos y phishing, en donde las víctimas sufren la sustracción de sus claves bancarias y con ello, los delincuentes pueden acceder a su dinero sin mayores dificultades.

La investigación arrojó que, del total de las pymes afectadas, un 27% no tomó medidas de seguridad digital luego del problema. "Este dato nos parece especialmente preocupante", sostuvo Bernardita Silva, Directora Ejecutiva del Observatorio del Comercio Ilícito de la Cámara Nacional de Comercio. "Si bien hay situaciones en las que no vale la pena denunciar el caso ante las autoridades, creo que siempre debe ser prudente que se hagan revisiones exhaustivas de los equipos, cuando se han descubierto intrusiones, porque muchas veces depende de ellos el éxito o fracaso de los negocios", agregó la ejecutiva.

Estudio Observatorio Comercio Ilícito CNC, Octubre 2016

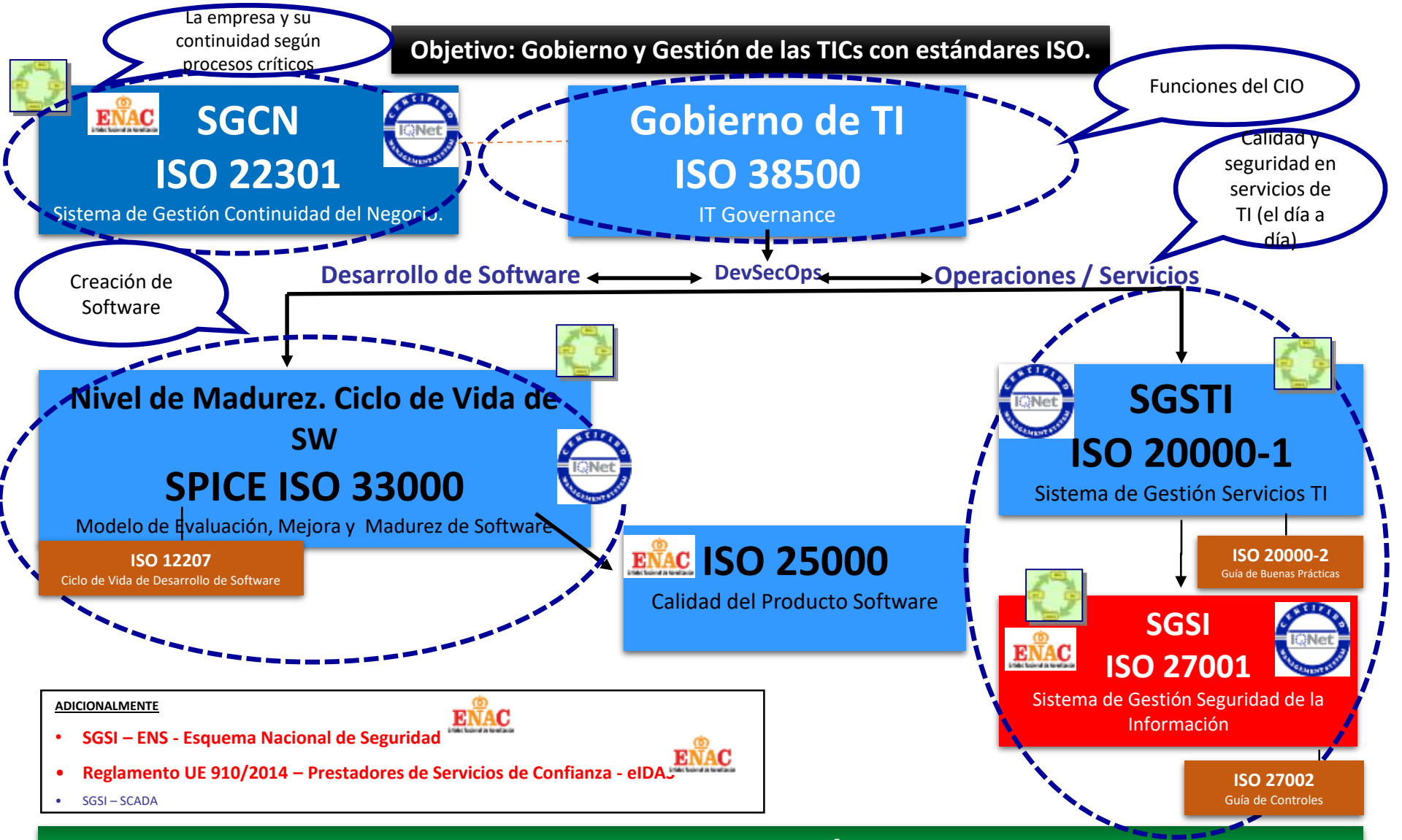
Yo soy PYME … es preocupante …

¿Cómo enfrentamos esto?

Le tenemos la solución …

Yo no vengo a vender, vengo a regalar …

3. MODELO DINAMICO DE GOB. Y GESTION DE LAS TIC CON ISO



El resultado …

Les voy a contar dos secretos …

Por razones de seguridad del conferencista y los asistentes, este slide explícitamente no registra contenido de lo hablado durante esta sección de la conferencia.

Cualquier referencia o comentario a lo expresado en los próximos minutos por el conferencista tendrá como respuesta ***"Nunca lo dije. Y si lo dije, no me acuerdo".***

Secreto 1

Secreto 2

Reboot …

Ciberseguridad

Un desafío para la Transformación Digital de la Pymes

Recursos y Herramientas Prácticas para Afrontar la Ciberseguridad

Marco A. Zúñiga
Director Ejecutivo CHILETEC
@mazuniga

#CiberseguridadParaPymes

CORFO

@Corfo

CHILETEC

@ChiletecOrg

CAPACITACIÓN usach
UNIVERSIDAD DE SANTIAGO DE CHILE

@Usach_Capacita

Las duras cifras …

Un 34,6% de las pymes de Valparaíso, Santiago y Concepción han sufrido algún tipo de incidente relacionado con la ciberseguridad. Este porcentaje fue obtenido gracias al estudio "Vulnerabilidad de Empresas en Ciberseguridad", realizado por el Observatorio del Comercio Ilícito (OCI), iniciativa de la Cámara Nacional de Comercio, Servicios y Turismo (CNC).

De acuerdo con sus resultados, las vulneraciones informáticas van desde infecciones de virus, en un 28%, hasta el robo de información de bases de datos y phishing, en donde las víctimas sufren la sustracción de sus claves bancarias y con ello, los delincuentes pueden acceder a su dinero sin mayores dificultades.

La investigación arrojó que, del total de las pymes afectadas, un 27% no tomó medidas de seguridad digital luego del problema. "Este dato nos parece especialmente preocupante", sostuvo Bernardita Silva, Directora Ejecutiva del Observatorio del Comercio Ilícito de la Cámara Nacional de Comercio. "Si bien hay situaciones en las que no vale la pena denunciar el caso ante las autoridades, creo que siempre debe ser prudente que se hagan revisiones exhaustivas de los equipos, cuando se han descubierto intrusiones, porque muchas veces depende de ellos el éxito o fracaso de los negocios", agregó la ejecutiva.

Estudio Observatorio Comercio Ilícito CNC, Octubre 2016

Yo soy PYME … es preocupante …

¿Cómo enfrentamos esto?

Chile y su Historia

“Porque no tenemos nada, queremos hacerlo todo”

Carlos Dittborn, 1956
Presidente Comité Organizador
Mundial de Fútbol 1962

La Tendencia Mundial

McKinsey & Company

Desde

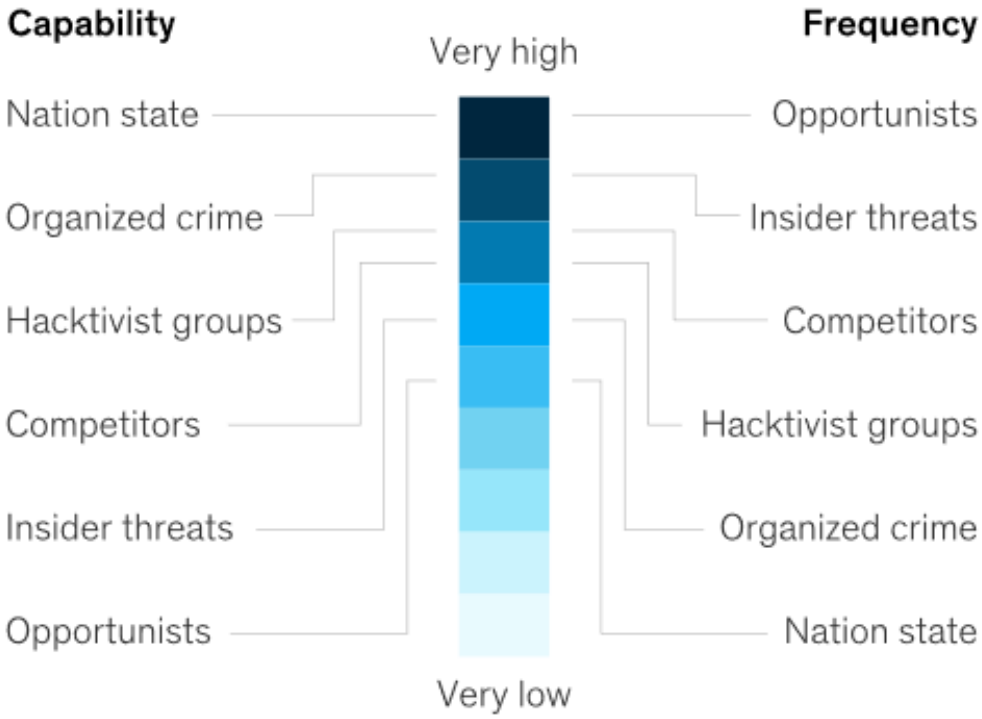
"modelos de madurez"

hacia

"gestión de los ciber-riesgos"

Cyberthreats are growing in severity and frequency.

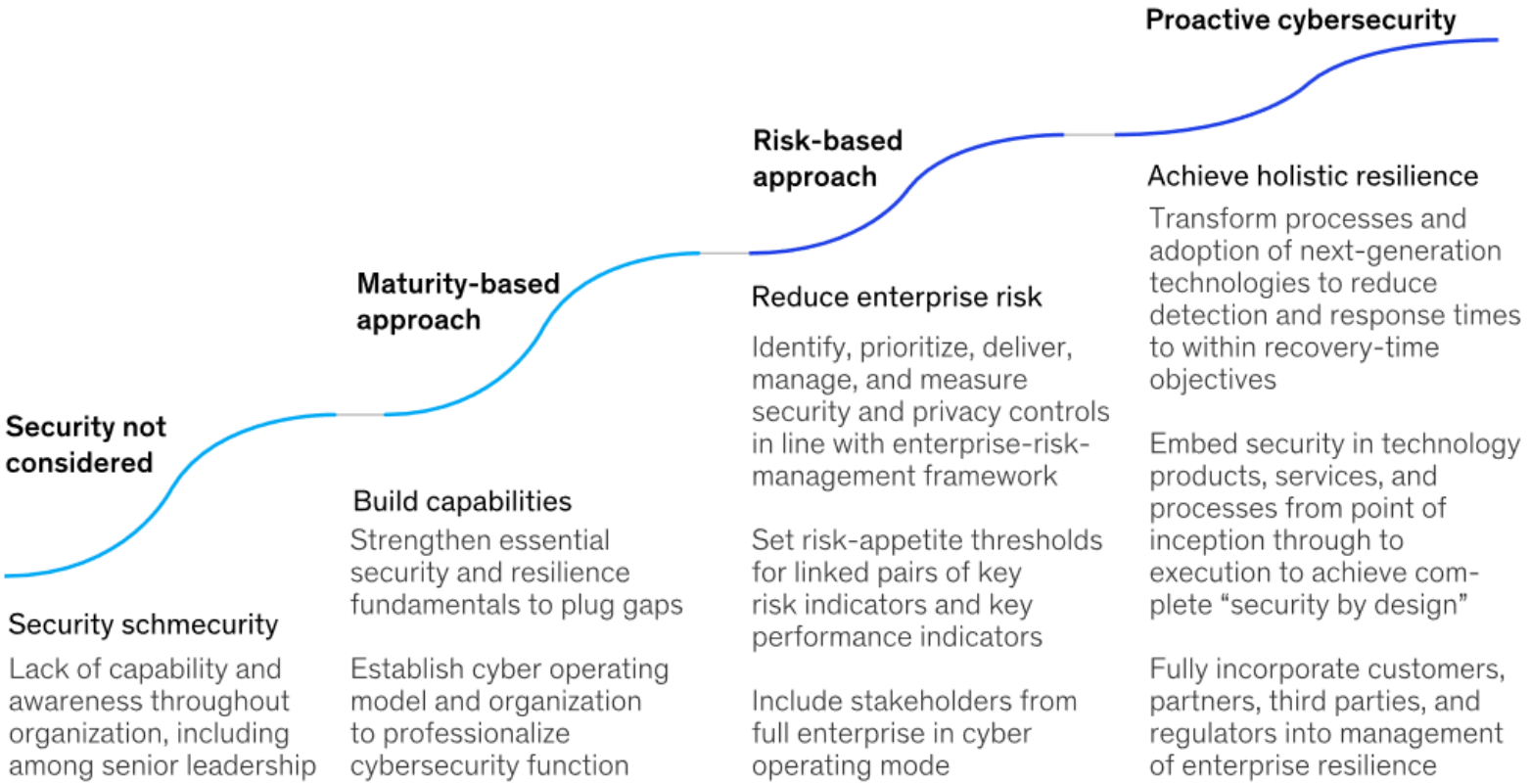
Cyberthreat capability and frequency today, by threat actor



McKinsey & Company

Fuente: McKinsey, 2019

For most companies, the risk-based approach is the next stage in their cybersecurity journey.



Fuente: McKinsey, 2019

Ya … me tincó eso de “gestión del riesgo”. Peroooo …

¿De dónde saco recursos? (Soy PYME)

¿Cómo podemos partir?
¿Alguna papita …..?

Recomendación inicial

Aplicar el modelo de Gestión de Riesgos del NIST

- Identificar
- Defender
- Detectar
- Responder
- Recuperar

Matriz de Gestión de Riesgo

Identificar	Defender	Detectar	Responder	Recuperar

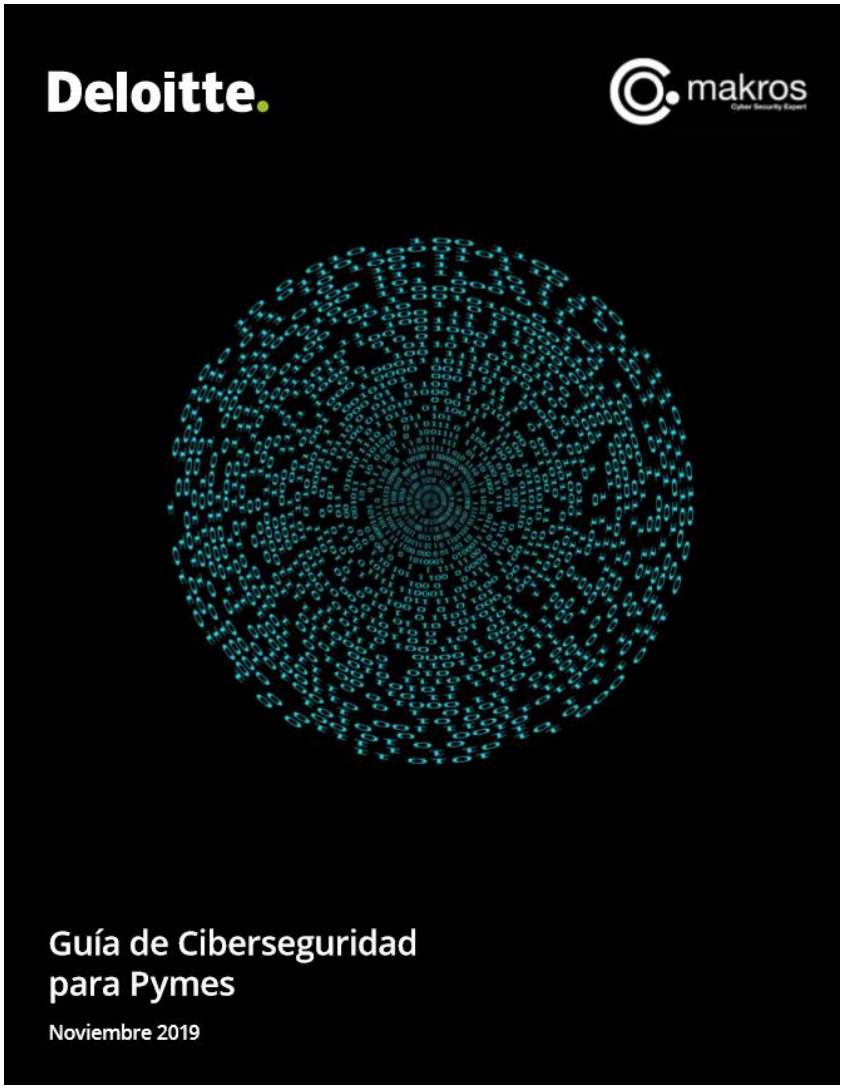
Ejemplo 1

Identificar	Defender	Detectar	Responder	Recuperar
Tengo riesgo de que me roben plata de la tarjeta de crédito de la empresa	Sistema de autenticación de dos factores Tener dos tarjetas: una para operaciones en línea y otra física	Activar avisos automáticos de transacciones del banco (mail y SMS) Revisar los movimientos de cuenta corriente y tarjeta de crédito una vez al día	En caso de identificar una transacción no reconocida, bloquear de inmediato la tarjeta correspondiente Avisar a las jefaturas	Solicitar devolución inmediata del dinero al Banco Activar seguro de fraude

Ejemplo

Identificar	Defender	Detectar	Responder	Recuperar
Tengo terror a perder los archivos de planos de los proyectos de los quinchos de mis clientes, por virus o ransomware, porque no puedo seguir operando el negocio	Todos los archivos de los directorios de trabajo de los proyectos y los discos de computadores personales son respaldados automáticamente en la nube Todo empleado de la empresa tiene el antivirus instalado y actualizado automáticamente	Revisar y estar alerta a cualquier cambio no autorizado en los archivos de trabajo personales Chequear una vez a la semana que los archivos de responsabilidad de cada uno estén correctamente sincronizados Verificar diariamente estado del antivirus	En caso de un ataque de ransomware o virus detectado, se apagan todos los computadores de inmediato Se ubica al soporte informático de la empresa Los que puedan, continúan operando desde sus teléfonos móviles con los archivos en la nube	Se limpian todos los equipos y red interna por personal especializado Se reinstalan todos los computadores con la versión vigente de los archivos 24 horas antes del incidente

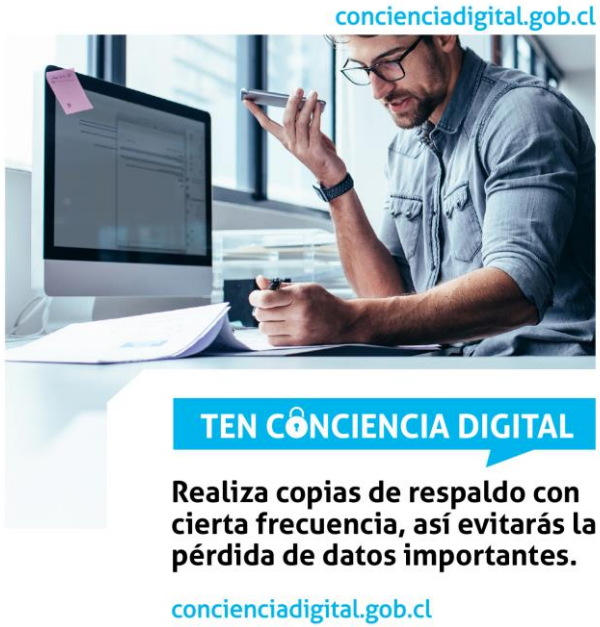
Y por el mismo precio le traemos …



Un buen aporte

Una guía de recomendaciones específicas para las PYMEs

Basado en el Framework del NIST



Recursos del Estado gratuitos!!!!

Sitio de Ciberseguridad del Ministerio del Interior, correo de consultas y call center !!!

www.concienciadigital.gob.cl

Autoevaluación!!!

Sitio de la Cámara Nacional e Comercio con respaldo de la Alianza Chilena de Ciberseguridad

www.pymecibersegura.cl

Ejemplos de Ambitos de Trabajo Iniciales

Manejo de residuos y basura
- Picar información en papel
- Eliminación segura de dispos

Procedimientos
- Manejo información crítica
- Cómo operar en emergencia

Capacitar al personal
- Evitar conductas riesgosas
- No bajar software pirata
- Manejo de claves

Respaldos
- Nube
- Dispositivos seguros

Seguridad de Dispositivos
- Actualizaciones de SO
- Respaldos
- Antivirus

Identificar dónde están los datos críticos de la organización
- Correos
- Sistemas
- Archivos
- Bases de Datos

Imagen
- Protección de marca
- Propiedad intelectual

Aplicaciones
- Optar por soluciones en la Nube vs. On Premise
- Actualización de versiones
- No usar software pirateado
- Incorporar sólo aplicaciones gratuitas autorizadas

Conectividad
- No conectarse en cualquier parte
- "Más vale diablo conocido que por conocer“
- Uso de VPN
- Bloqueo de puertos riesgosos

@Corfo

@ChiletecOrg

@Usach_Capacita

Marco A. Zúñiga
Director Ejecutivo CHILETEC
@mazuniga

#CiberseguridadParaPymes

Muchas Gracias

Gracias por su atención

Material Adicional en:

http://www.maz.cl

marco@maz.cl