KINAITECH

SWIFT

CUSTOMER SECURITY PROGRAMME - 2020

Índice

Por qué CSP ?

¿Cuáles fueron los drivers que impulsaron la creación del programa por parte de SWIFT y por qué es importante su cumplimiento?

SWIFT CSP

20 February 18

India's City Union Bank hacked via SWIFT Payment System

India's City Union Bank has released a statement that their system has suffered a security breach and a total $1.8 million was transferred in three unauthorized transactions made

Another SWIFT Hack Stole $12 Million

Heists Highlight Real-Time Payment Risks, Security Experts

Mathew J. Schwartz (euroinfosec) · May 20, 2016 · 0 Comments

Twitter Facebook LinkedIn Credit Eligi

GERMANY BREXIT WORLD BUSINESS SCIENCE ENVIRONMENT CULTURE SPORTS

TOP STORIES / BUSINESS

BUSINESS

Hackers stole $6 million in Russia bank attack via SWIFT system

Russia's central bank has admitted that hackers targeted a computer at one of its and transferred a large sum of cash. They used the SWIFT payment system, whic move trillions of dollars each day.

FINANCE • SWIFT

SWIFT Banking System Was Hacked at Least Three times This Summer

Security

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack

stomized malware apparently used

Francisco 11 Oct 2017

The NIC Asia Bank requested the support of the Central Investigation Bureau of Nepal Police to track down the crooks who hacked the SWIFT server.

SWIFT systems to steal money from a financial institution. The victim is discovered illegal fund transfer with its SWIFT server requested support n Bureau of Nepal Police to track down the crooks.

City Union Bank suffers cyber hack via SWIFT system

REUTERS

N Kamakoti, MD and CEO, CUB (file photo)

RELATED

A failure of internal controls: RBI

MUMBAI, FEB 18

City Union Bank said on Sunday that "cyber criminals" had hacked its systems and transferred nearly $2 million through three unauthorised remittances to

CNN Money Markets Economy Companies Tech Autos India Vide

If three makes a trend, then it's official: The global banking system is under attack.

The methods used by hackers to attack banks in Vietnam and Bangladesh appear to have been deployed over a year ago in a heist in Ecuador.

The January 2015 attack on Banco del Austro is described in a lawsuit filed by the bank in a New York federal court. It ended with thieves transferring $12 million to accounts in Hong Kong, Dubai, New York and Los Angeles, according to court documents.

The existence of the lawsuit was first reported Friday by the Wall Street Journal, just one week after global banking communications network SWIFT instructed clients to secure their local computer networks.

Cumplimiento

- Cambios que se dieron a partir del 2018 en materia de Cumplimiento.

SWIFT CSP

CSP Update | Modus Operandi

Customer Security Programme

Step 1	Step 2	Step 3	Step 4
Attackers compromise customer's environment	*Attackers obtain valid operator credentials*	*Attackers submit fraudulent messages*	*Attackers hide the evidence*

2020

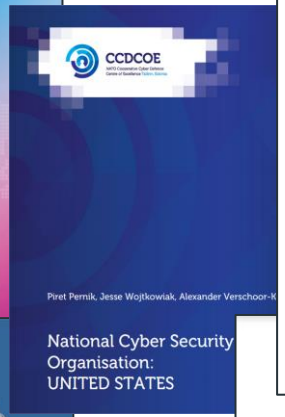
Un breve resumen de las regulaciones y de los riesgos que enfrentamos en este año.

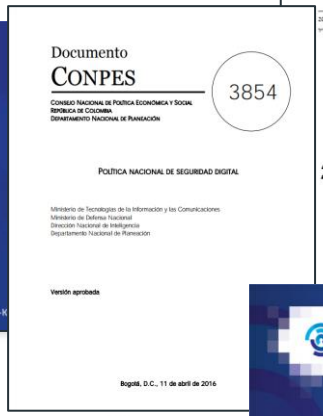
Pronósticos

- Migración en el comportamiento del Ransomware.
- El Usuario como vector de incidentes.
  - OSINT altamente automatizado.
  - Alto uso de información de Redes sociales.
- Continuamos con creciente complejidad de ataques.
  - Disponibles para cualquiera. Ataques incorporando Machine Learning.
  - IoT e Infraestructuras Críticas, crecientes objetivos.
- Estrategias DevOps empujan la necesidad de DevSecOps.

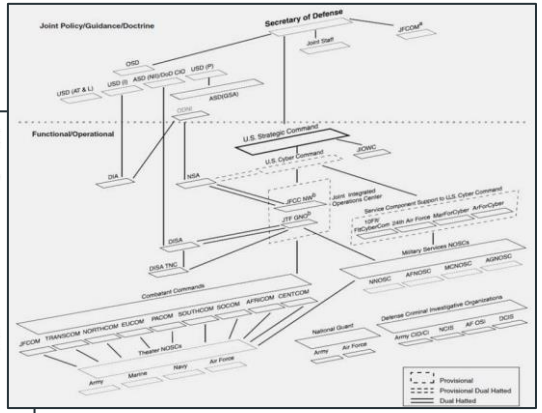
Políticas

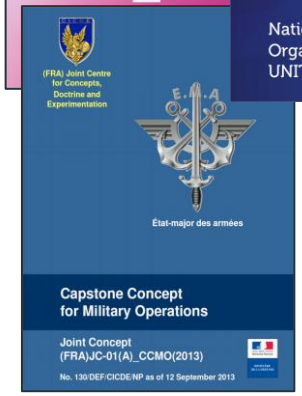

FRENCH
NATIONAL
DIGITAL SECURITY
STRATEGY

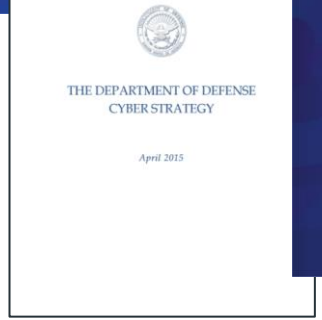

CCDCOE
Piret Pernik, Jesse Wojtkowiak, Alexander Verschoor-K
National Cyber Security
Organisation:
UNITED STATES

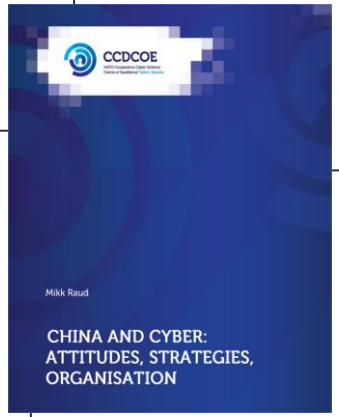

Documento
CONPES
3854
POLÍTICA NACIONAL DE SEGURIDAD DIGITAL
Bogotá, D.C., 11 de abril de 2016

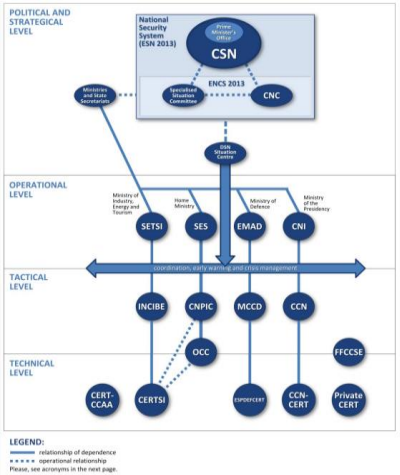

Prime Minister's Office
National Cyber Bureau
מדיניות אסדרת מקצועות
הגנת הסייבר
במדינת ישראל


Joint Policy/Guidance/Doctrine
Secretary of Defense
Functional/Operational
Provisional
Provisional Dual Hatted
Dual Hatted


(FRA) Joint Centre
for Concepts,
Doctrine and
Experimentation
État-major des armées
Capstone Concept
for Military Operations
Joint Concept
(FRA)JC-01(A)_CCMO(2013)
No. 130/DEF/CICDE/NP as of 12 September 2013


THE DEPARTMENT OF DEFENSE
CYBER STRATEGY
April 2015


CCDCOE
Mikk Raud
CHINA AND CYBER:
ATTITUDES, STRATEGIES,
ORGANISATION


POLITICAL AND
STRATEGICAL
LEVEL
National
Security
System
(ESN 2013)
CSN
ENCS 2013
CNC
OPERATIONAL
LEVEL
SETSI
SES
EMAD
CNI
TACTICAL
LEVEL
INCIBE
CNPIC
MCCD
CCN
OCC
FFCCSE
TECHNICAL
LEVEL
CERT-
CCAA
CERTSI
CCN-
CERT
Private
CERT
LEGEND:

Latinoamérica

Estrategias de Ciberseguridad

- Colombia (2011 y 2016)
- Panamá (2013)
- Paraguay (2017)
- Chile (2017)
- Costa Rica (2017)
- México (2017)
- Argentina (2019)

CUSTOMER SECURITY PROGRAMME (CSP)

Tiene como objetivo mejorar el intercambio de información en toda la red, mejorar las herramientas relacionadas con SWIFT y proporcionar un marco de control de seguridad.

https://www.swift.com/myswift/customer-security-programme-csp

SWIFT Customer Security Controls Framework

- **Objetivos**
  - Asegurar el ambiente.
  - Conocer y limitar accesos.
  - Detección y respuesta.

SWIFT Customer Security Controls Framework

Principios

Marco de controles de seguridad de CSP	
Asegurar el ambiente	1.* Restringir el acceso a Internet.
	2.* Separe los sistemas críticos del entorno general de TI.
	3. Reducir la superficie de ataque y las vulnerabilidades.
	4. Proteger físicamente el entorno.
Conocer y limitar accesos.	5. Evitar el compromiso de las credenciales
	6. Administrar identidades y segregar privilegios
Detección y respuesta.	7. Detectar actividad anómala en el sistema o en los registros de transacciones.
	8. Planificar la respuesta a incidentes y el intercambio de información.

* 1 y 2 se combinan en el CSCF

Mapping


International Organization for Standardization
ISO
27002


PCI
DSS
COMPLIANT


RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT

SWIFT Customer Security Controls Framework

Restringir el acceso a Internet y proteger los sistemas críticos del entorno general de TI.

1.1 Protección del ambiente de SWIFT

1.2 Control de cuentas privilegiadas del SO

1.3A Virtualization plataform protection

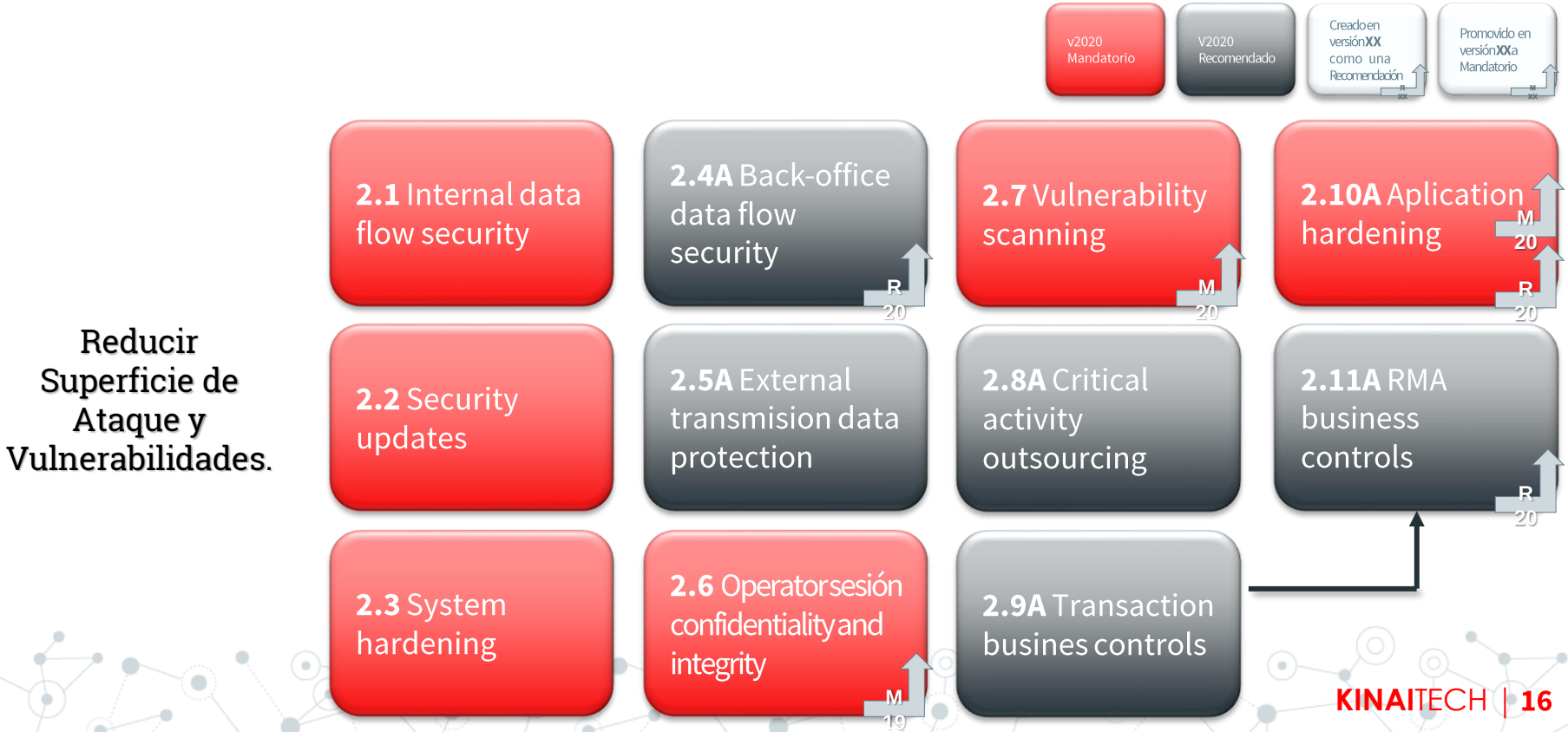
M 20

R 19

1.4A Restringir el acceso a Internet

R 20

SWIFT Customer Security Controls Framework



SWIFT Customer Security Controls Framework

Proteger físicamente el entorno

3.1 Seguridad física

Prevenir el compromiso de credenciales

.

4.1 Política de contraseñas

4.2 Multi-factor autentication

SWIFT Customer Security Controls Framework

Administrar identidades y segregar privilegios

5.1 Logical acces control

5.2 Token management

5.3A Personnel vetting process

5.4 Physical and logical password storage

M
19

SWIFT Customer Security Controls Framework

Detectar actividad anómala en el sistema o en los registros de transacciones.

- **6.1** Malware protection
- **6.2** Software integrity
- **6.3** Database integrity
- **6.4** Logging and monitoring
- **6.5A** Intrusion detection

SWIFT Customer Security Controls Framework

Planificar la respuesta a incidentes y el intercambio de información.

7.1 Cyber incident response planning

7.2 Security training and awareness

7.3A Penetration testing

7.4 Scenario risk assessment

31.12.2020

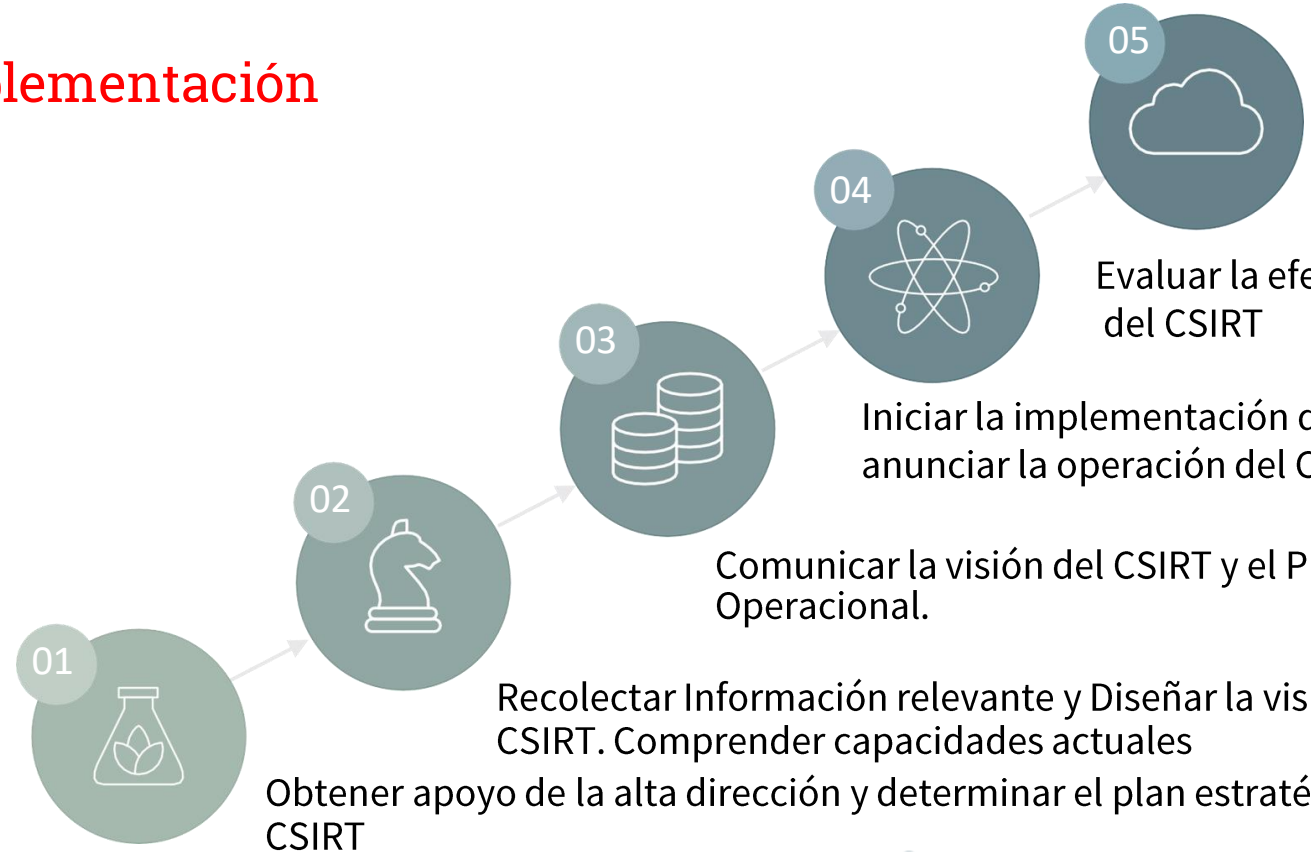
Puntos a considerar para el cumplimiento con la declaración de este año.

CSP: ¿Qué tan diferente será su declaración el 31.12.2020?

Rol de los Equipos de Respuesta ante Incidentes de Seguridad

Los equipos de respuesta especializados cumplen un rol fundamental en el proceso de defensa activa y deben ser motivadores de cambio.

Implementación



Implementación

- Analizar motivadores y requerimientos para la creación del CSIRT.
- Seleccionar el modelo de CSIRT más adecuado.
- Definición de servicios.
- Definición e implementación de procesos.
- Análisis de clientes y planes de comunicación con terceros.
- Análisis FODA y PEST.
- Definir la estructura necesaria.
- Acompañar en la selección de personal.
- Definir herramientas tecnológicas.
- Desarrollo de políticas del CSIRT.
- Búsqueda de cooperación con otros CSIRTS.
- Creación de código de conducta y de ética.
- Creación de checklist para el CSIRT.

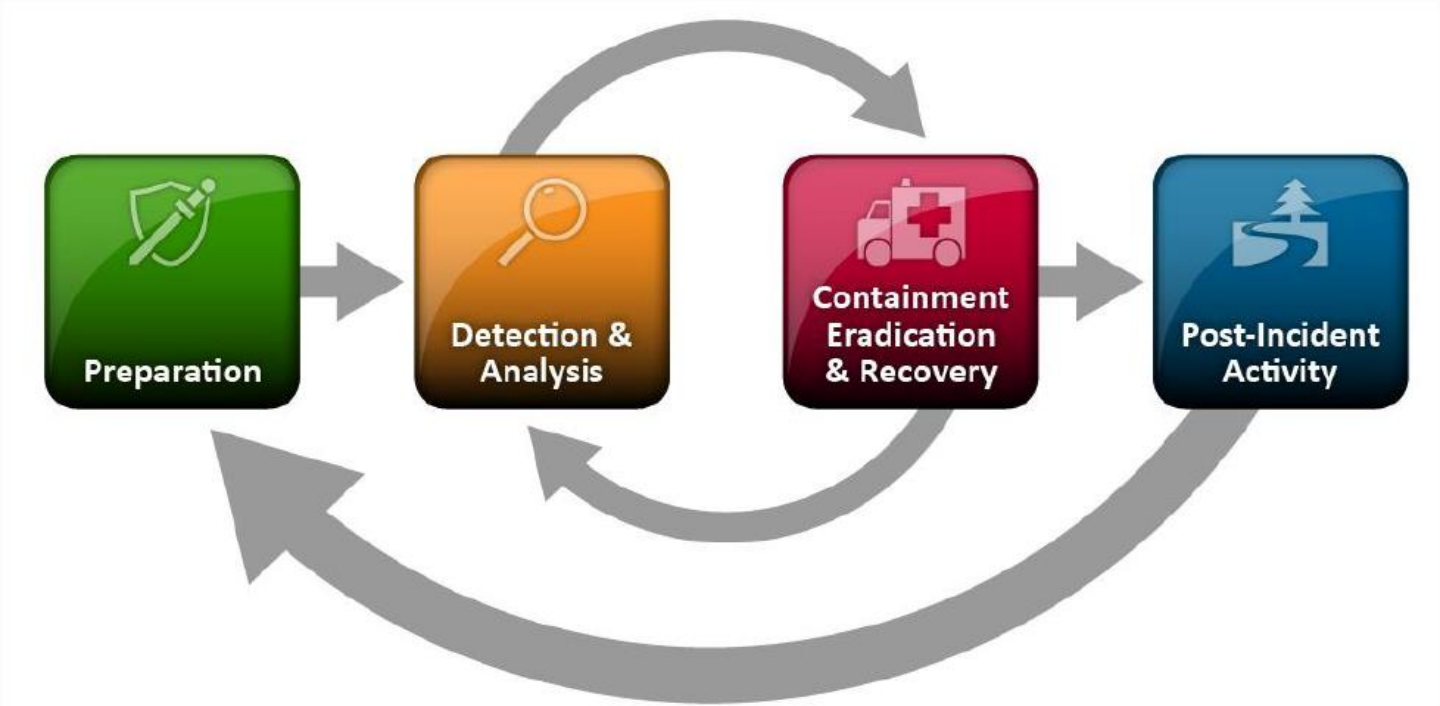
Servicios Core

- Gestión de alertas e incidentes
- Servicio 911 de respuesta a incidentes (en vivo)
- Coordinación de incidentes con terceros
- Análisis forense digital
- Gestión de vulnerabilidades y parches críticos de seguridad
- Ethical Hacking interno
- Innovación y desarrollo
- Monitoreo de sistemas críticos
- Gestión y comunicación de crisis
- Guías y auditorías de configuraciones de seguridad
- Entrenamientos y capacitación

Servicios de Colaboración

- Difusión de alertas de seguridad del mercado
- Acuerdos de colaboración con terceros
- Compartir información anónima de amenazas
- Generar lecciones aprendidas
- Monitoreo de Reputación

NIST SP800-61



Ventajas

- Disponer de una coordinación centralizada
- Reaccionar a los incidentes relacionados con las TI
- Contar con conocimientos técnicos necesarios
- Tratar las cuestiones jurídicas y proteger evidencias
- Realizar un seguimiento de los progresos conseguidos
- Fomentar la cooperación en la seguridad de las TI
- Desarrollar investigación e innovación

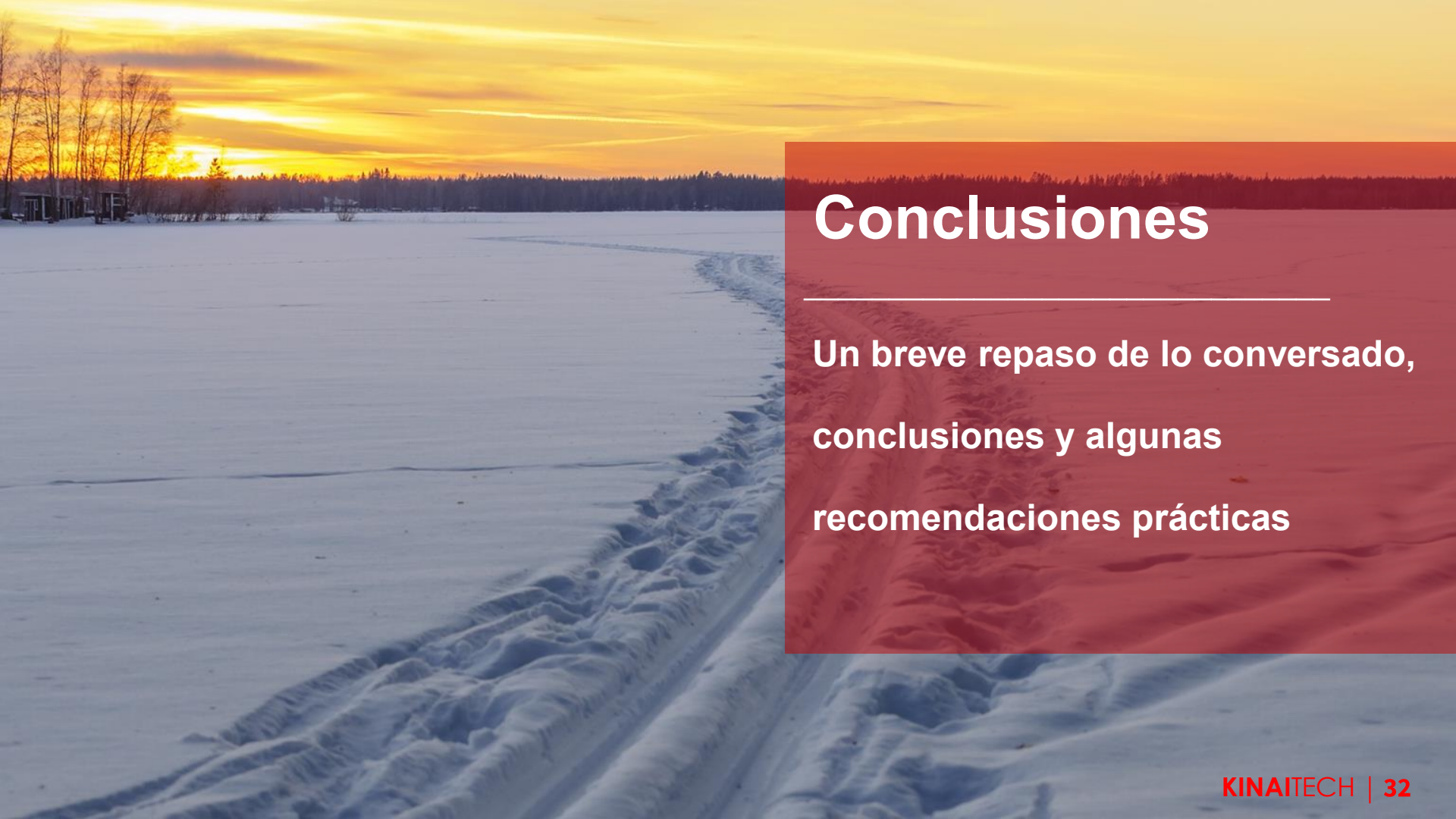
Mitigación

La mayor inversión en la capacidad de respuesta ante incidentes de ciberseguridad no radica solo en preparar la contención y respuesta sino también en prevenir y prepararse.

Prevenir

TOP 10 (Mitigar 90% de Ataques):

- Listas Blancas de Aplicaciones.
- Gestión de Parches y vulnerabilidades en sistemas operativos y aplicaciones.
- Control de Integridad y control de cambios.
- Minimizar permisos administrativos (a usuarios y administradores).
- Segmentación de la red.
- Control de dispositivos.
- Control de fuga de datos.
- Análisis de tráfico y Control de DDoS.
- Control de anomalías en estaciones de trabajo.
- Seguridad en el Desarrollo de Software.



Conclusiones

Un breve repaso de lo conversado, conclusiones y algunas recomendaciones prácticas

Conclusiones

- No esperar a diciembre 2020 para responder al SWIFT CSP.
- Trabajar en programas de respuesta ante incidentes.
- Realizar simulacros de incidentes de ciberseguridad.
- Incorporar aspectos de ciberseguridad en análisis de riesgos.
- Incorporar aspectos de mitigación del Top 10 mencionado.
- Buscar Integración entre ISO 27001, ISO 27002, ISO 27032, PCI-DSS, ISO 31000, ISO 27005, regulaciones y normativas locales para la mejora de la seguridad de su organización.

SWIFT CSCF 2020 RESUMEN

- En 2020, SWIFT promovió 2 controles de asesoramiento existentes a obligatorios e introdujo 2 nuevos controles de asesoramiento que dieron como resultado 21 controles obligatorios y 10 controles de asesoramiento en el CSCF V2020. Para 2021, SWIFT promovió 1 control a obligatorio, lo que resultó en 22 controles obligatorios y 9 controles de asesoramiento en la CSCF v2021. Todos los usuarios de SWIFT deberán realizar una “evaluación independiente”, ya que es un requisito clave de su autocertificación anual para demostrar que cumplen con SWIFT CSCF.

KINAITECH

Propuesta de servicios para

SWIFT Customer Security Controls Framework

2020

Servicios Generales para SWIFT CSCF

GAP Analysis

Ofrecemos un servicio de evaluación entre la situación actual y los controles requeridos por SWIFT CSCF.

Acompañamiento en Implementación

Generamos un plan estratégico en conjunto para la implementación de controles, acompañamos durante todo el proceso de la implementación.

Productos y Servicios para cumplimiento SWIFT CSCF

- Servicio de escaneo de vulnerabilidades periódico.
- Servicios de Penetration Testing.
- Implementación de Hardening de Sistemas.
- Chequeo de Integridad de archivos y configuraciones.
- Soluciones de MFA (multi-factor authentication).
- Soluciones de Almacenamiento de contraseñas seguras.
- Soluciones de detección de actividad maliciosa en la red.
- Soluciones de protección de Bases de Datos.
- Sistemas de consolidación y correlación de eventos (Log Management & SIEM).

Planes de Respuesta a Incidentes y Colaboración

Planes de Respuesta ante Incidentes

Proporcionamos servicios de creación de planes de respuesta a incidentes, servicio de SOC & CSIRT, servicios de forense digital y análisis de malware. Ayudamos a prepararse, prevenir, contener y recuperarse.

Entrenamientos y Campañas de Concientización

Realizamos entrenamientos técnicos y ejecutivos. Creamos, desarrollamos y comunicamos campañas de concientización en seguridad de la información.

Servicios de Penetration Testing

Nuestro equipo de consultores ofrece los mejores servicios de hacking ético, penetration testing y escaneos de vulnerabilidades tanto de infraestructura, aplicaciones web, móviles así como APIs y IoT.

Revisiones de escenarios de riesgos

Generamos escenarios de riesgos, los desafiamos y revisamos los puntos de control necesarios por la organización.

7.1 Cyber incident response planning

7.2 Security training and awareness

7.3A Penetration testing

7.4 Scenario risk assessment

Gracias!

Alejandro Benitez
+54 9 11 67562257
abenitez@kinaitech.com.ar

KINAI TECH