



CIBERSEGURIDAD

¿cómo obtener mayor protección contra ataques y robo de información?



C O N T E N I D O

01 %

INTRODUCCIÓN



02 %

TÉCNICAS PARA EL
ANÁLISIS



03 

HALLAZGOS
PRINCIPALES



04 

CRONOLOGÍA DEL
INCIDENTE
INVESTIGADO



05 

RIESGOS



06 

RECOMENDACIONES





CIBERSEGURIDAD

INTRODUCCIÓN

SEGURIDAD DE LA INFORMACIÓN.

Es la práctica de proteger sistemas, redes y programas de ataques digitales.

"La seguridad de la información se ha convertido en una agenda prioritaria, tanto para los gobiernos, como para las empresas"

Lo anterior parte de la premisa de que los datos son el nuevo gran valor y tesoro de la nueva realidad y en México existen regulaciones respecto a su acceso, manejo y gestión.

Información a proteger:

Crítica : indispensable para la operación.

Valiosa : evitar riesgos futuros de las empresas.

Sensible : aquella que solo deben conocer determinadas personas.

MÁS DE 22.000 MILLONES DE ARCHIVOS FUERON
EXPUESTOS COMO CONSECUENCIA DE FILTRACIONES
DE DATOS EN TODO EL MUNDO EN 2020, A PARTIR
DE 730 FILTRACIONES REVELADAS PÚBLICAMENTE

—Informe retrospectivo sobre el panorama de las amenazas en 2020 de Tenable



IDENTIFICAR



CUMPLIR



PÉRDIDAS



Riesgos : materialización de las vulnerabilidades que están identificadas en CADA EMPRESA que resulta de la combinación de la probabilidad que suceda un evento no deseable y su impacto negativo a la organización.

Seguridad: forma en que la empresa se protege de los riesgos

BUSCANDO LA RELACIÓN COSTO VS. BENEFICIO

Disponibilidad: información siempre accesible

Confidencialidad: acceso a la información solo a quien debe tenerlo

Integridad: la información no debe ser modificada

A. Información

B. Dinero

C. Confianza de los clientes

D. Ventaja frente a la competencia





Se prevé que, en los próximos 50 años, la demanda de alimentos aumentará un 70 por ciento.

DURANTE LA PANDEMIA LOS SECTORES MÁS ATACADOS FUERON:

- 1) HOSPITALES
- 2) LABORATORIOS
- 3) TECNOLOGIA
- 4) BANCOS
- 5) GOBIERNO MX: LOTENAL, ISSSTE, BANXICO, SAT, PEMEX

VISIÓN DE LA CIBERSEGURIDAD EN MÉXICO

¿Será suficiente un antivirus?

¿Control de acceso físico y lógico?

En el año 2021 se detectaron más de **360 mil archivos maliciosos** generados por día, un crecimiento del ataque de redes de acceso remoto de 242% siendo **México el segundo lugar a nivel mundial.**

El COVID-19 trajo dos vertientes, nos cambió la vida física y digital,

¿qué generó esto en las empresas?, las empresas con el fin de mantener la operación, adaptaron sus sistemas de acceso rápidamente y **esto los ciberdelincuentes lo aprovecharon al máximo.**

Entidades públicas y privadas están haciendo lo siguiente:

- a) Reforzando sus políticas, procesos e infraestructura.
- b) Capacitando y concientizando a su personal.
- c) Implementando los Marcos de Ciberseguridad y creando sus propios sistemas de gestión de seguridad de la información.
- d) Elaborando políticas de protección de datos.

+ INFO

+ INFO



GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702



CIO- CIBERSEGURIDAD

TÉCNICAS UTILIZADAS

MARCO METODOLÓGICO NIST (INSTITUTO NACIONAL DE
ESTÁNDARES Y TECNOLOGÍA)

Pilares de la Seguridad

01

PROCESOS

NIST 800-86 y 61

MARCO METODOLÓGICO NIST
(INSTITUTO NACIONAL DE
ESTÁNDARES Y TECNOLOGÍA)
Adecuado a cada giro de empresa

02

TECNOLOGÍA

HARDWARE & SOFTWARE

Software para prevenir el acceso a
archivos, links, sitios web.
Hardware
Firewall, cctv, biométricos para control
de acceso, switches, tokens

03

PERSONAL

Capacitado

y

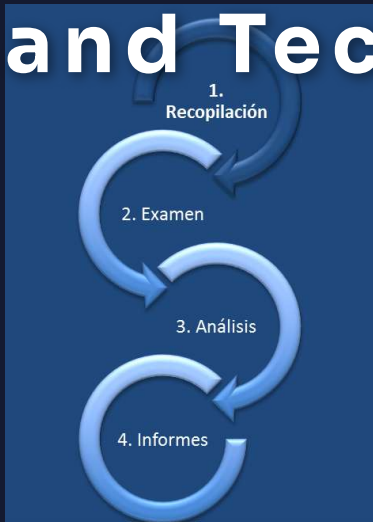
Concientizado

Recomendamos capacitación
periódica libre de marcas para el total
del personal

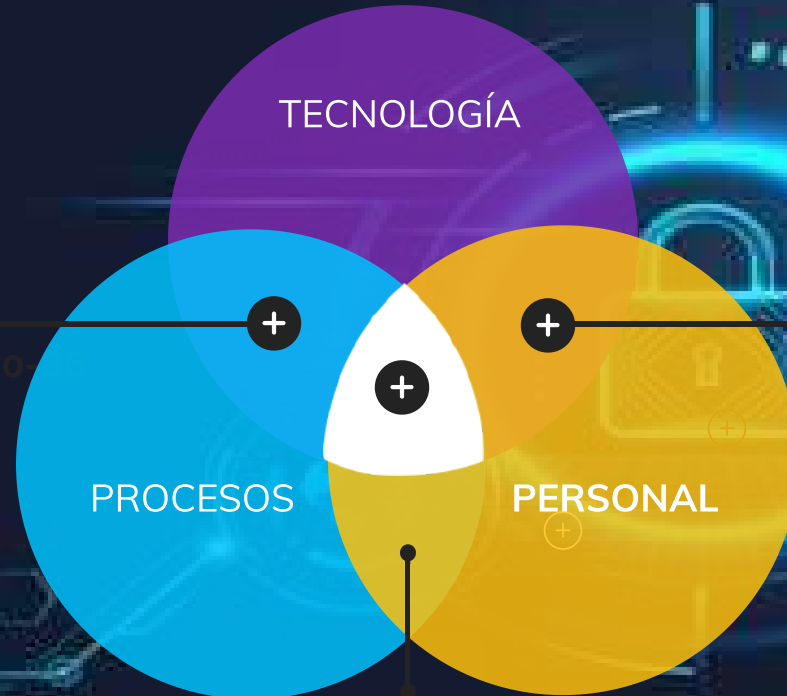
Recomendamos campañas
automatizadas de concientización y
medición de la participación y
evolución en la identificación de
riesgos por parte del personal.



NIST (National Institute of Standards and Technology)



- Identificación de los activos de cada negocio.
- Creación de una matriz de vulnerabilidades, riesgos y planes de mitigación.
- Establecimiento de sistemas de gestión de seguridad de la información.
- Capacitación y campañas de concientización.
- Optimización de los presupuestos de TI para gestión de la ciberseguridad
- Auditorías, análisis de brechas y seguimiento a la implementación de recomendaciones.
- Análisis forense en el Marco NIST-86 de equipos



- Entrevistas directas con los usuarios involucrados directa o indirectamente en el Incidente.
- Entrevistas con CIO, Administradores de Infraestructura y Equipo de Procesos
- Aplicación de técnicas de ingeniería social

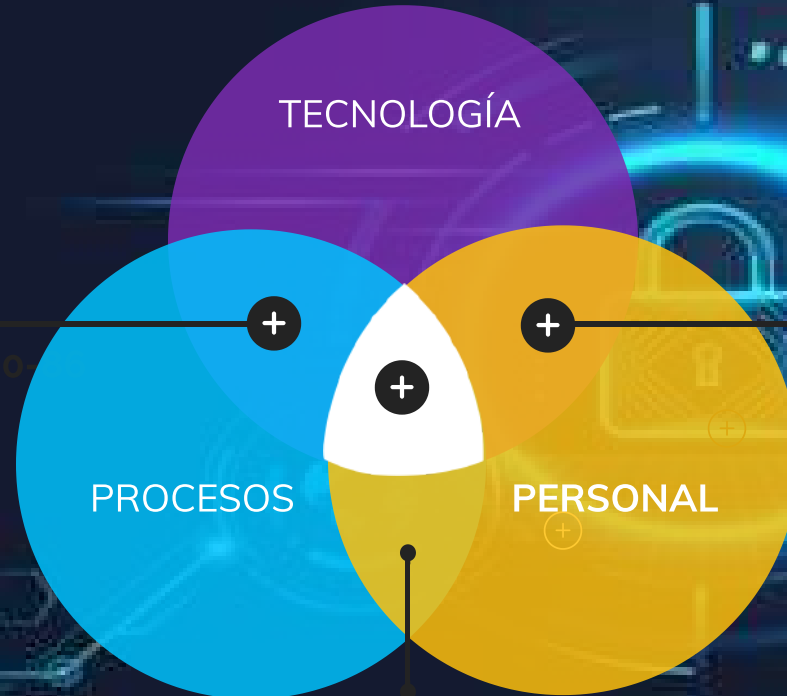
- Análisis forenses
- Cacería de amenazas
- Monitoreo proactivo y herramientas de correlación de eventos de ciberseguridad
- Consultoría para elaboración de políticas y procedimientos para protección de datos y propiedad intelectual



NIST (National Institute of Standards and Technology)



- Identificación de los activos de cada negocio.
- Creación de una matriz de vulnerabilidades, riesgos y planes de mitigación.
- Establecimiento de sistemas de gestión de seguridad de la información.
- Capacitación y campañas de concientización.
- Optimización de los presupuestos de TI para gestión de la ciberseguridad
- Auditorías , análisis de brechas y seguimiento a la implementación de recomendaciones.
- Análisis forense en el Marco NIST-86 de equipos



- Entrevistas directas con los usuarios involucrados directa o indirectamente en el Incidente.
- Entrevistas con CIO, Administradores de Infraestructura y Equipo de Procesos
- Aplicación de técnicas de ingeniería social

- Análisis forenses
- Cacería de amenazas
- Monitoreo proactivo y herramientas de correlación de eventos de ciberseguridad
- Consultoría para elaboración de políticas y procedimientos para protección de datos y propiedad intelectual





CIO- CIBERSEGURIDAD

¿CUÁLES SON LOS INCIDENTES MÁS FRECUENTES?

MÉXICO 2021-2022

ATAQUES CIBERNÉTICOS DEL 2021



GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702

01

IDENTIFICAR INFORMACIÓN Y ACTIVOS

RANSOMWARE:
consiste en el robo de información o infraestructura para pedir un rescate.

EJEMPLO:
COLONIAL PIPELINE (oleoductos estadounidenses pagaron 5 millones de dólares)

+ INFO

02

PROTEGER POLÍTICAS Y TECNOLOGÍA

ROBO DE CREDENCIALES.
Como parte de una cadena de ataque cuyo objetivo puede ser extorsión, denegación de servicios, obtención de información.

03

DETECTAR POLÍTICAS, PERSONAL

PHISHING
Consiste en un engaño a través del correo electrónico para robar credenciales o explotar alguna vulnerabilidad de un sistema o infraestructura.

04

RESPONDER POLÍTICA, PERSONAL

MALWARE
Son archivos maliciosos que pueden provocar comportamientos inusuales en los equipos de cómputo, abrir puertos para comunicarse con servidores externos.

05

RECUPERAR POLÍTICA, TECNOLOGÍA

SUPLANTACIÓN DE IDENTIDAD
Fingir o aparentar ser una persona. Ocurre en redes sociales, a través de llamadas telefónicas, en correo electrónico. Su objetivo es la extorsión o el robo.

+

+

+

+

+

ATAQUES CIBERNÉTICOS DEL 2021



GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702

06

IDENTIFICAR INFORMACIÓN Y ACTIVOS

VULNERABILIDADES
DE DÍA CERO

Son armas que utilizan los ciberatacantes para ejecutar código malicioso y permitir tomar el control de sistemas vulnerables (LOG4SHELL)

07

PROTEGER POLÍTICAS Y TECNOLOGÍA

VULNERABILIDAD EN
LOS SERVICIOS DE
IMPRESIÓN

PrintNightmare
Es un código malicioso con la posibilidad de escalar privilegios en una red a partir de una vulnerabilidad en sistemas windows

08

DETECTAR POLÍTICAS, PERSONAL

DDoS
(Denegación de Servicio)
Es un ataque en el que múltiples fuentes se dirigen a un servidor web u otro dispositivo de red con el objetivo de bloquearlo y que los datos no estén disponibles para los usuarios.

09

RESPONDER POLÍTICA, PERSONAL

Ataque del hombre en el Medio (MitM)

Consiste en la intercepción de una transacción entre dos partes.

10

RECUPERAR POLÍTICA, TECNOLOGÍA

Rootkits en dispositivos IoT

Es código malicioso en dispositivos como cámaras de cctv, electrodomésticos, vehículos entre otros.

+ INFO



CIO- CIBERSEGURIDAD

TÉCNICAS PARA EL ANÁLISIS

NIST - CSF (Ciber Security Framework)

CADENA DEL CIBERATAQUE



RECONOCIMIENTO

LOS ATACANTES
BUSCAN UNA
DEBILIDAD



EL ATACANTE ENVÍA UN
MALWARE POR LO
REGULAR MEDIANTE EL
CORREO

INSTALACIÓN

INSTALAR EL
MALWARE EN EL
OBJETIVO

ENTREGA



ARMAMENTO

LOS ATACANTES CONSTRUYEN
LA CARGA EXPLOSIVA PARA
EXPLOTAR LA VULNERABILIDAD

EXPLOTACIÓN

SE EJECUTA EL
CÓDIGO EN EL
EQUIPO DE LA
VÍCTIMA



CONTROL Y COMANDO

EL ATACANTE CREA UN
CANAL PARA
CONTROLAR
REMOTAMENTE

ACCIONES



CIO- CIBERSEGURIDAD

PLAN DE RUTA (CTI-> EMPRESA)

ANÁLISIS DE VULNERABILIDADES AUTOMATIZADO

El panorama de amenazas se está complicando



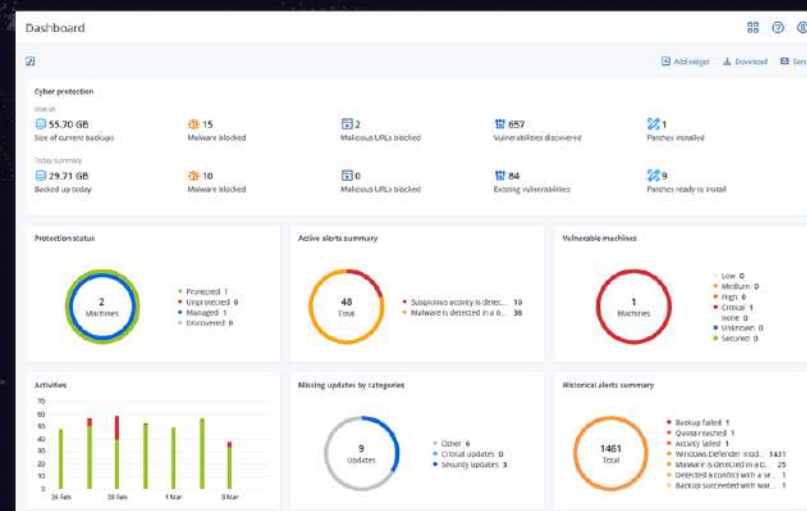
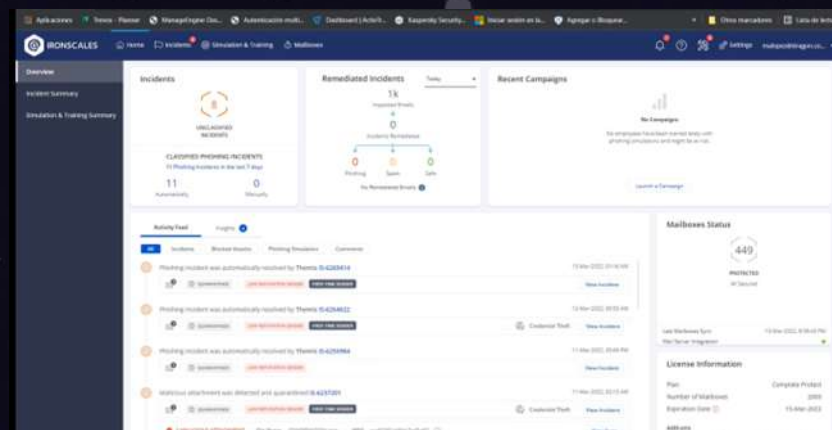
300 %
aumento de la
ciberdelincuencia
durante la pandemia de
COVID-19



57 %
ciberataques no
detectados por las
soluciones antivirus
tradicionales



69 %
más tiempo dedicado a
gestionar las herramientas
que a defenderse
de las amenazas



GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702

01

ANÁLISIS

HERRAMIENTAS
AUTOMÁTICAS

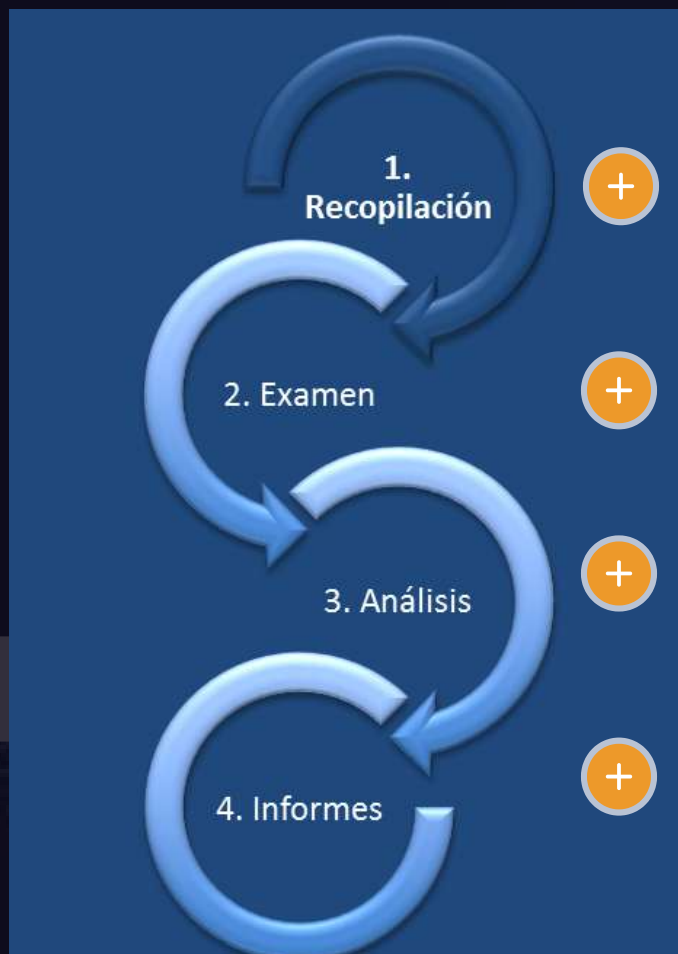
ANÁLISIS DE VULNERABILIDADES

. Mediante la instalación de 3 tipos de agente dependiendo el caso:

a) Empresas con servicio de correo ON-CLOUD
(IDENTIFICAR QUIENES SON LOS USUARIOS MÁS
ATACADOS)

b) Empresas con alguna o ninguna seguridad
tecnológica.

(MEDIANTE UN DIAGNÓSTICO AUTOMÁTICO
IDENTIFICAR LAS VULNERABILIDADES)



02

2. ELABORACIÓN DE REPORTE

03

3. Alternativas de solución



CIO- CIBERSEGURIDAD

RIESGOS

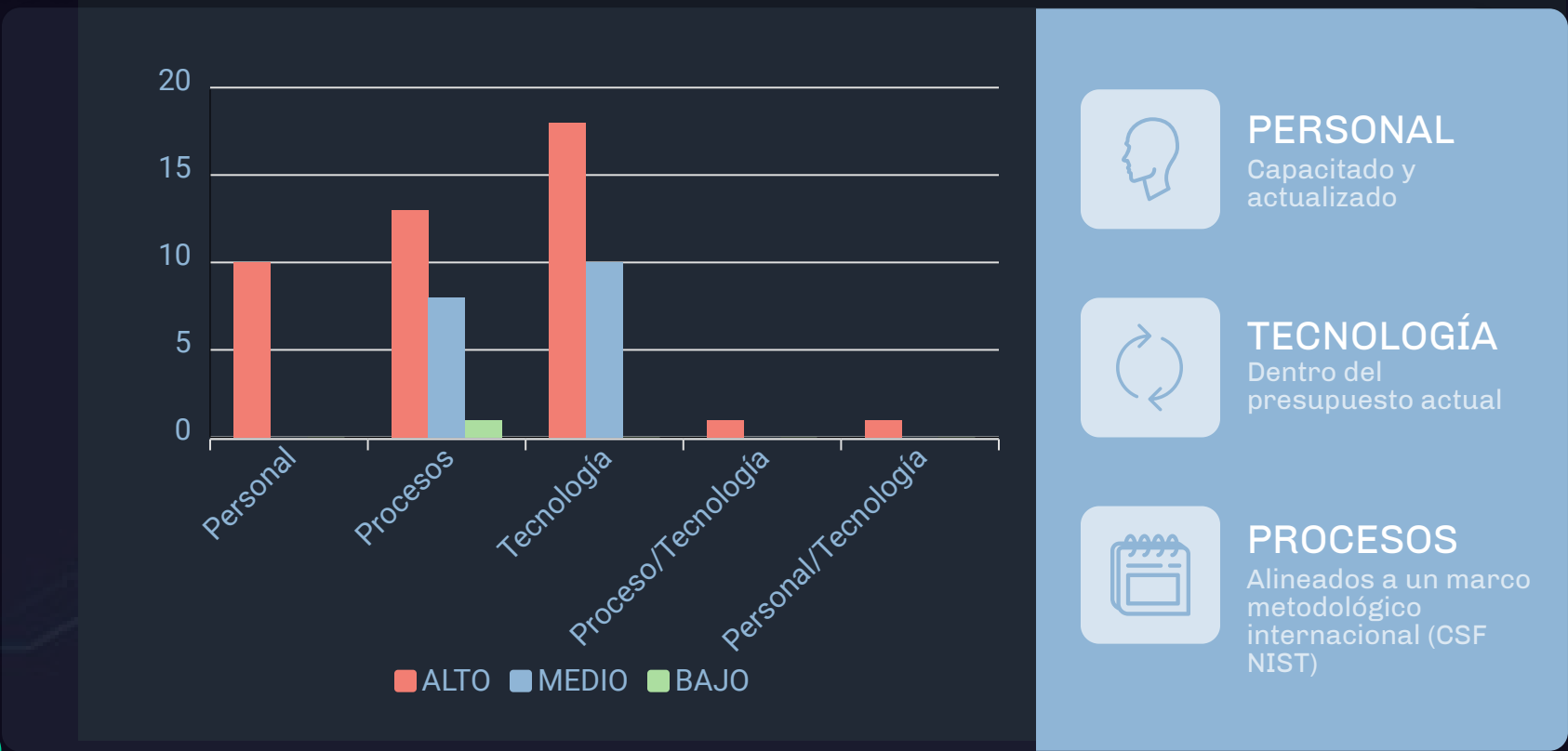
costo vs. beneficio

05

GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702

RECOMENDACIONES

CIBERSECURITY FRAMEWORK (RESULTANTE)



+ INFO





CIO- CIBERSEGURIDAD

PREGUNTAS

06

GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702

¡GRACIAS!



GRUPO CTI
HERMOSILLO
+52 662 105 8370

lgruiz@consultores-cti.com.mx
carias@consultores-cti.com.mx
ehuerta@consultores-cti.com.mx

+52 811 588 03 05

GRUPO CTI TECHIN POS, S.A. DE C.V. Tel. 662.105.83702