cybertrust
INSPIRANDO CONFIANZA

Cultura en Ciberseguridad

El Mejor Retorno de la Inversión

José Lagos

Socio Principal

jose.lagos@cybertrust.cl

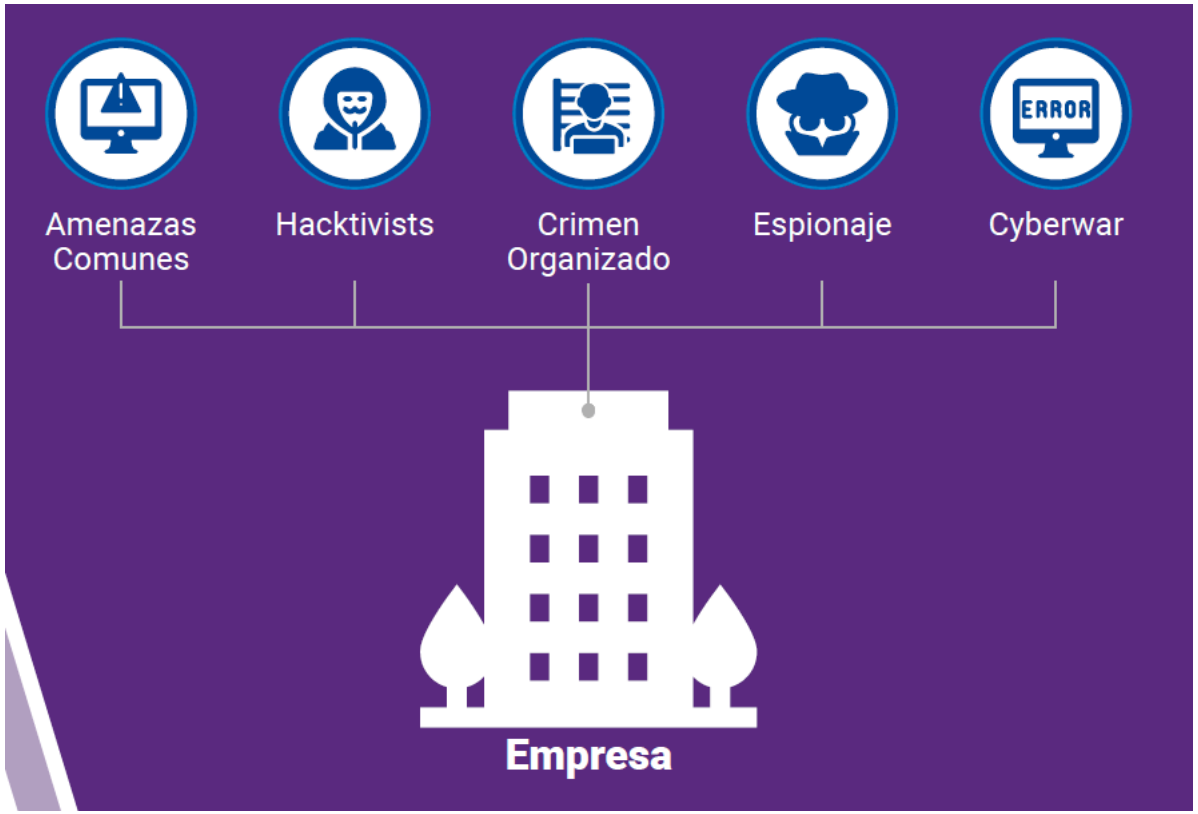
Cybertrust

- Magnitud del Problema
- Vectores de Ataque y Amenazas
- Minimizando los Riesgos
- Cultura en Ciberseguridad
- Estudio de Ciberseguridad
- Resultados del Estudio
- Fundamentos Estadísticos

MAGNITUD DEL PROBLEMA


Política

VECTORES DE ATAQUE Y AMENAZAS



VECTORES DE ATAQUE

cybertrust
INSPIRANDO CONFIANZA

AMENAZAS

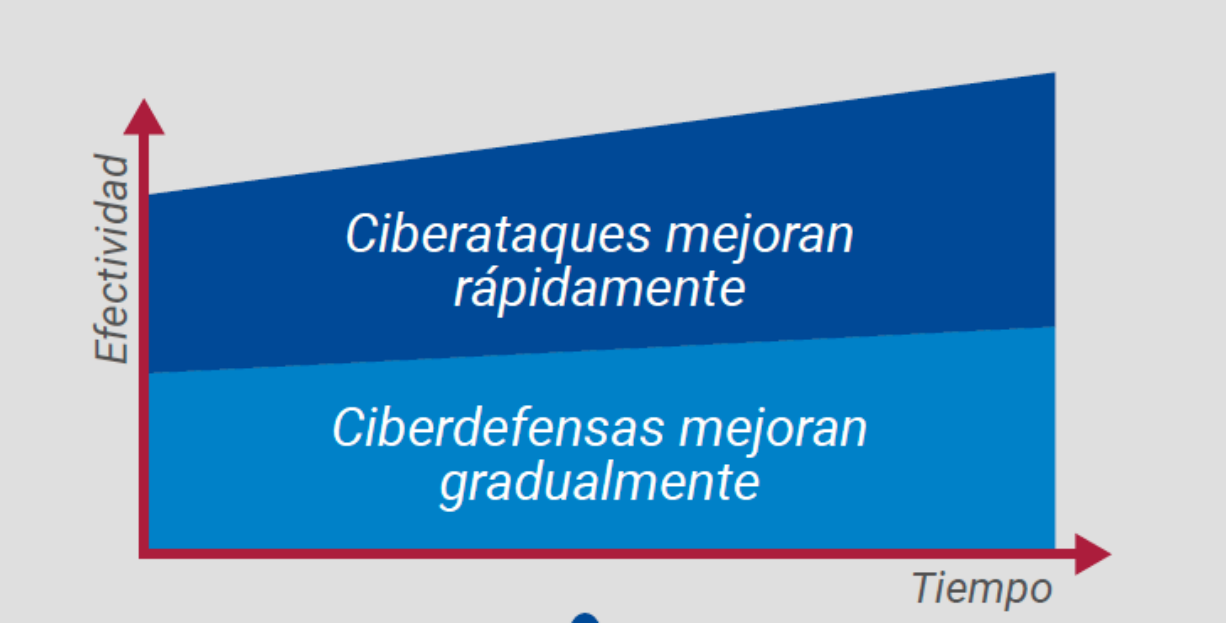
- Tecnología No Autorizada
- Errores Humanos
- Error de Procesos
- Defacement del Sitio Website
- Acceso Físico no Autorizado
- Entrenamiento Inadecuado
- Ingeniería Social
- Phishing
- Ransomware
- Amenaza Persistente Avanzada (APT)
- Denegación de Servicio

cybertrust
INSPIRANDO CONFIANZA

ACTIVOS

- Email Corporativo
- Dispositivo Móvil
- Aplicación Móvil (APPS)
- Registros de Clientes
- Respaldos
- Dispositivos de Red
- Información Electrónica Privada
- Información de Tarjeta de Crédito
- Laptop Endpoint
- Endpoint Wokstations
- Endpoint Server
- Infraestructura Crítica
- Redes de Terceros (Proveedores)
- Network Firewall

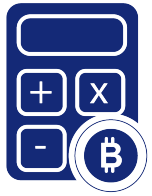
MINIMIZANDO LOS RIESGOS



¿Cuál es el Problema ?

cybertrust
INSPIRANDO CONFIANZA

MEDIDAS DE MITIGACION



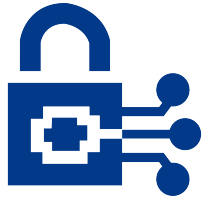
Estrategia

Gobernabilidad

Cultura en Ciberseguridad

Framework

Monitoreo End Point - SIEM



Ciber Crisis

Ciber Forense

Ciber Insurance

Ciber Law

CULTURA EN CIBERSEGURIDAD

Cultura en Ciberseguridad es pensar acerca de los valores compartidos de una organización que son importantes

Incluye la creencia de los empleados acerca de que cosas trabajan en la organización

Implica como los valores y creencias interactúan e impactan sobre los sistemas organizacionales **produciendo normas de comportamiento**

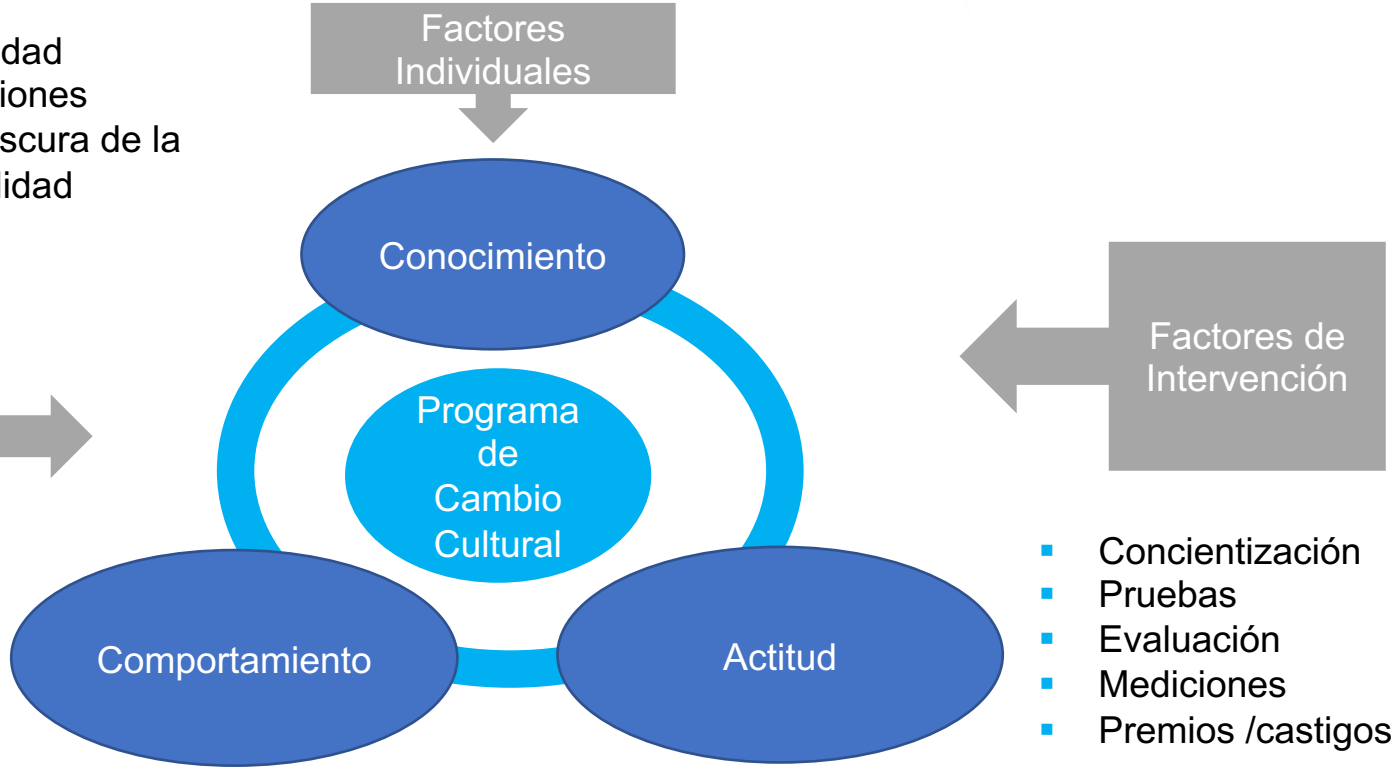
Las normas impactan el comportamiento de las personas, acerca de aquello **que queremos asegurar** de manera apropiada en la organización, **asegurando que esté bien protegido**


Políticas y Procedimientos de ciberseguridad ampliamente aceptadas por la organización
Claridad acerca de cómo los colaboradores debieran desarrollar sus roles en relación a los riesgos de ciberseguridad
Buena comunicación y conciencia de los riesgos
Cultura Ciberseguridad
Uso de incentivos para reforzar el comportamiento de los colaboradores
Ownership de los colaboradores
Sponsor de la administración superior o Top Management Team


Mayor probabilidad de tener brechas de seguridad no intencionales
Menos inclinación a informar comportamientos relacionados a brechas en general
DÉBIL CULTURA EN CIBERSEGURIDAD
Empleados fácilmente manipulables o vulnerables a temas de ingeniería social
Terroristas o Cibercriminales tienen menos probabilidad de ser detectados
Bajo nivel de Cumplimiento

Visión del Modelo

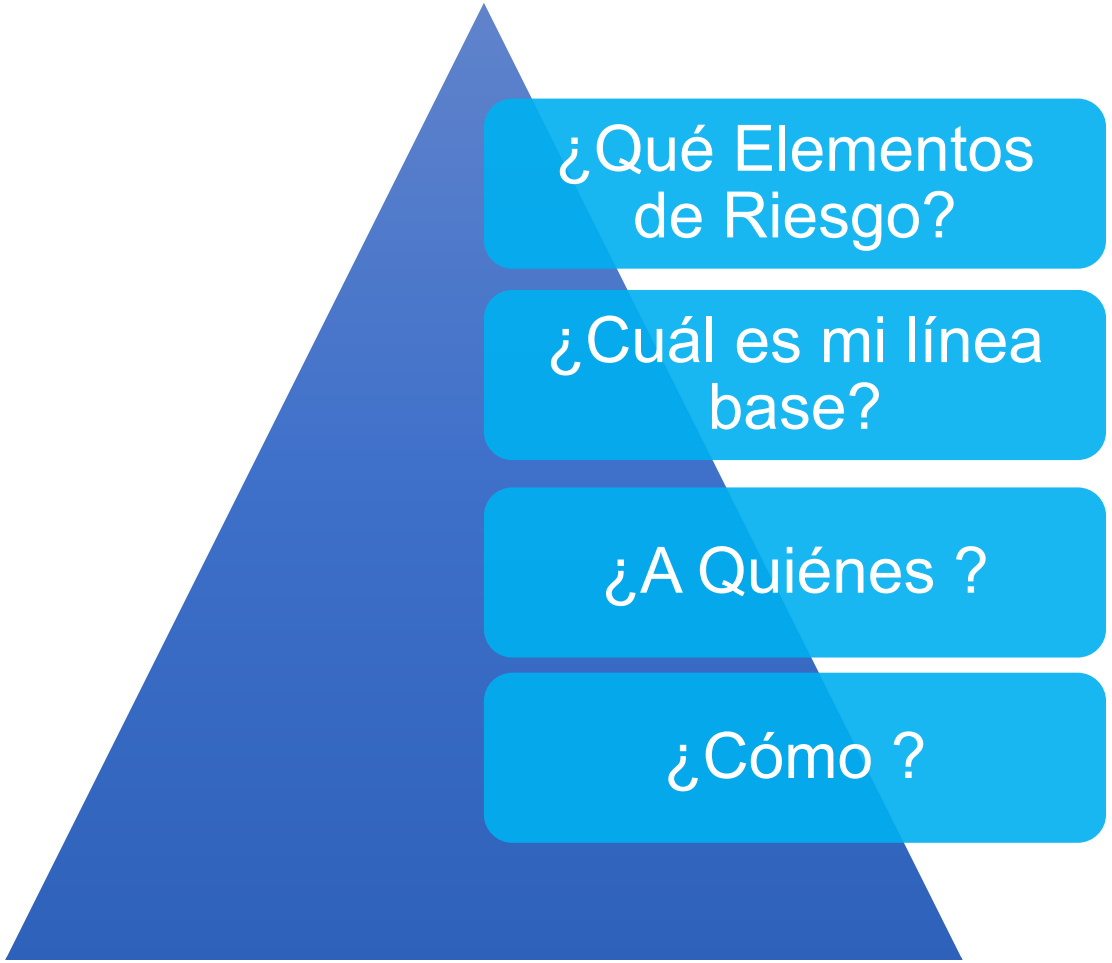
- Impulsividad
- Generaciones
- Triada Oscura de la Personalidad



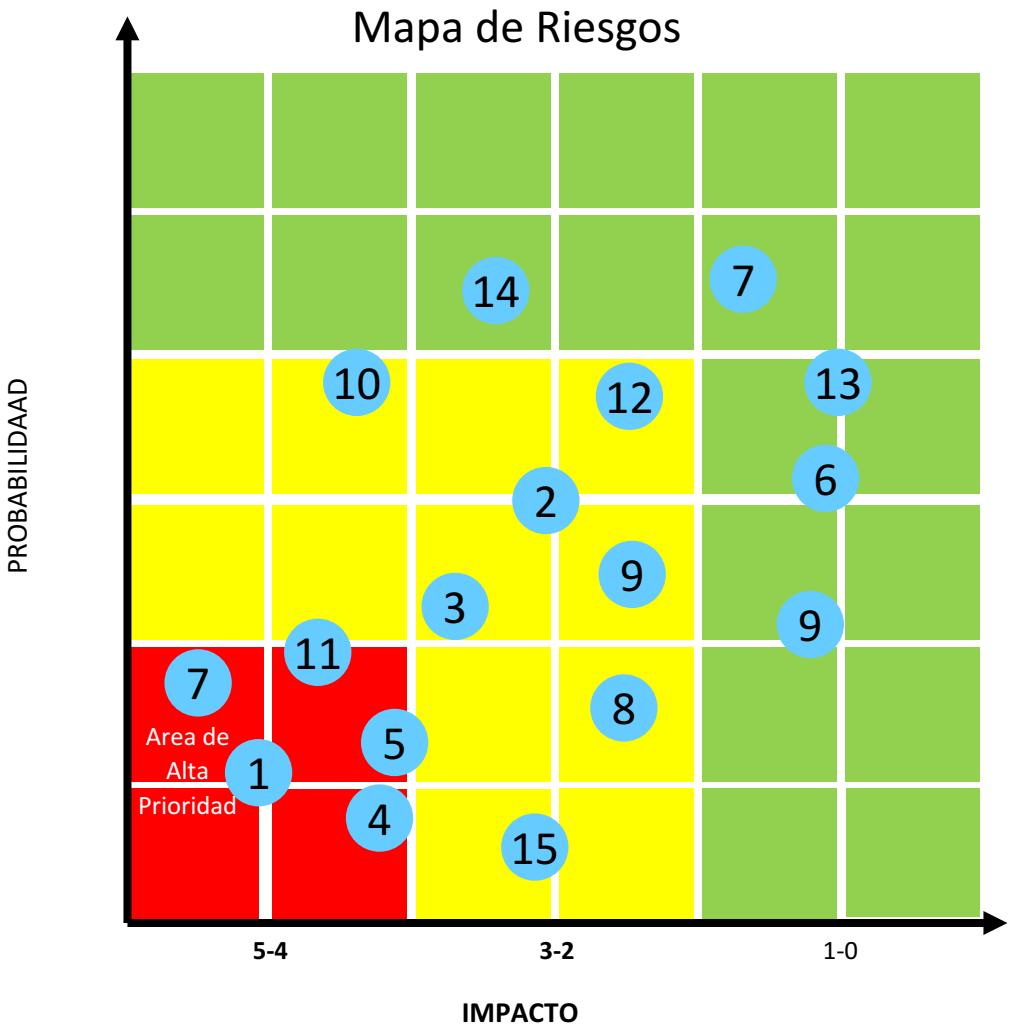
- Cultura Organizacional
- Industria
- Cultura País

- Concientización
- Pruebas
- Evaluación
- Mediciones
- Premios /castigos

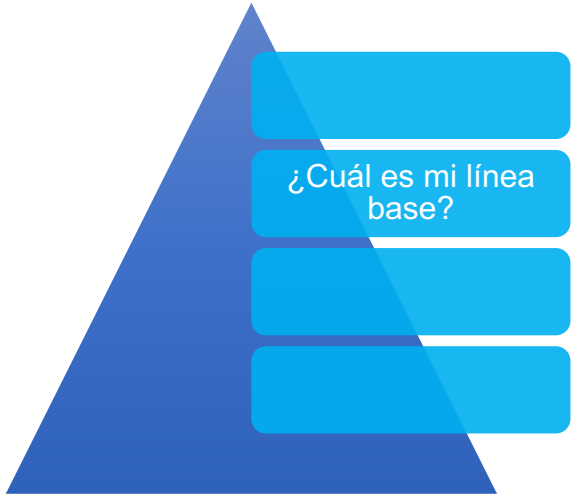
Preguntas esenciales para iniciar el viaje hacia una Cultura en Ciberseguridad



¿Qué Elementos de Riesgo?



1. Ransomware
2. Phishing
3. Password Seguras
4. Navegación Segura en Internet
5. Seguridad de las Conexiones WIFI Públicas
6. Uso seguro de Dispositivos Móviles
7. Uso seguro de redes sociales
8. Protección de Datos
9. Uso de Pendrives
10. Ingeniería Social
11. Insider Threat
12. Malware
13. Trabajo Remoto
14. Seguridad Física
15. Viajes Internacionales



Conocimiento

El proceso de sensibilización debe mejorar o aumentar el nivel de conocimiento sobre temas de Ciberseguridad

Actitud

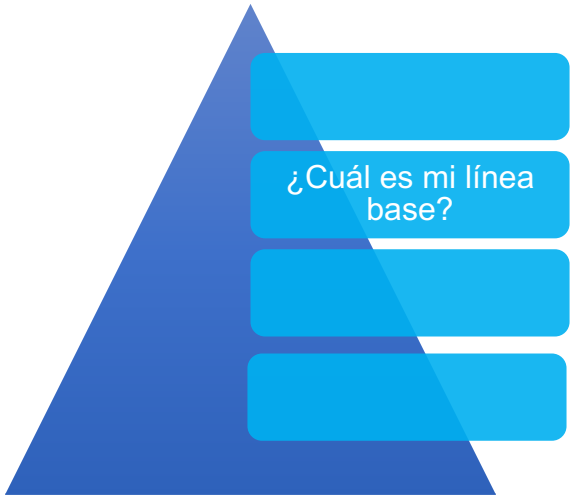
El proceso de conocimiento debe crear un cambio de actitud en las personas

Comportamiento

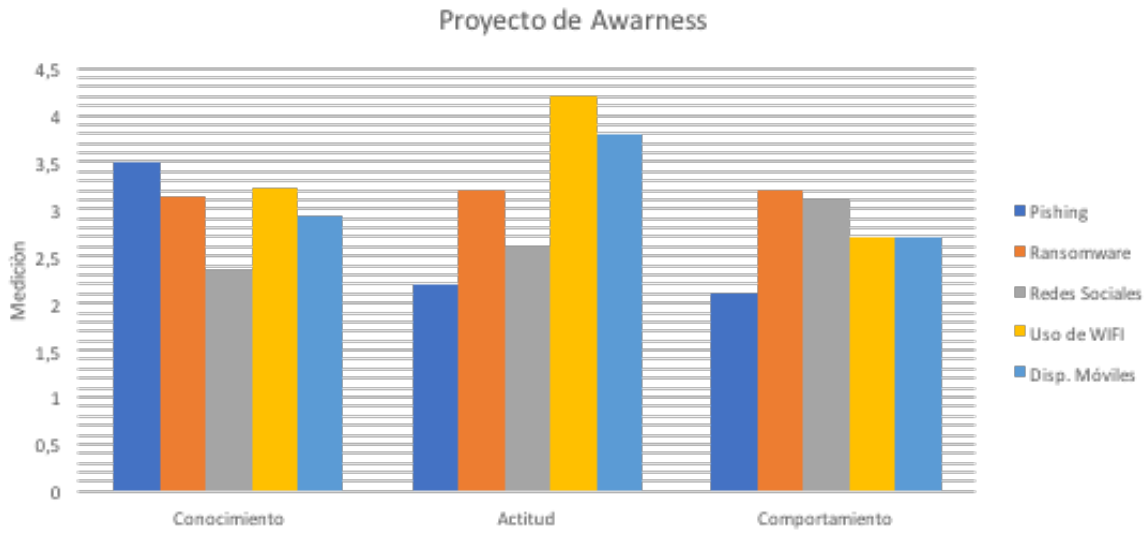
El cambio de actitud debe crear un cambio de comportamiento online

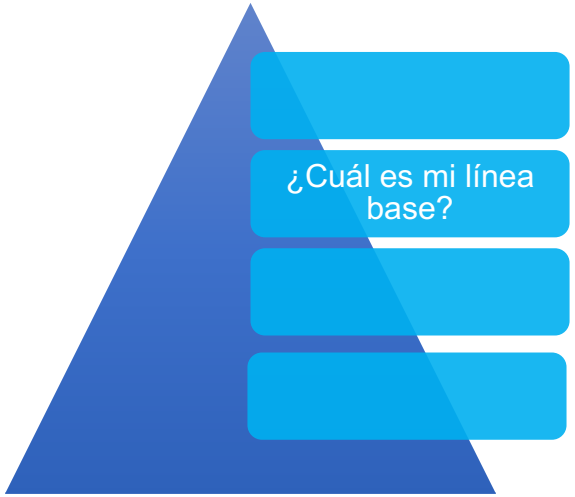
- Uso de Pendrives
- Navegación Segura
- Uso Seguro de Disp. Móv.
- Administración Password
- Phishing
- Ransomware

¿Cuál es mi línea Base ?



Elemento de Riesgo	Conocimiento	Actitud	Comportamiento
Administración de Password			
Utilización de la misma password	Es aceptable usar mi password en mis redes sociales en la cuenta de mi trabajo	Es seguro usar la misma contraseña en mis redes sociales y cuentas de mi trabajo.	Yo uso una password diferente para mis redes sociales y otras password en las cuentas de mi trabajo.
Compartir password	Yo me permito compartir mis password con mis colegas de trabajo	Es una buen idea compartir las password de mi trabajo, incluso si un colega me pregunta por ella	Yo comparto mis passwords del trabajo con mis colegas
Uso de una password fuerte	Es necesario para las password de las cuentas del trabajo una mezcla de letras, números y símbolos especiales.	Es seguro tener una password de la cuenta del trabajo con solo letras	Yo utilizo una combinación de símbolos especiales, números y letras en las password de mi trabajo



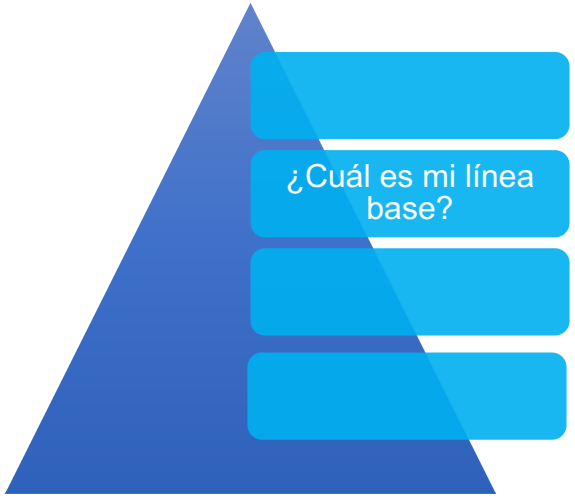


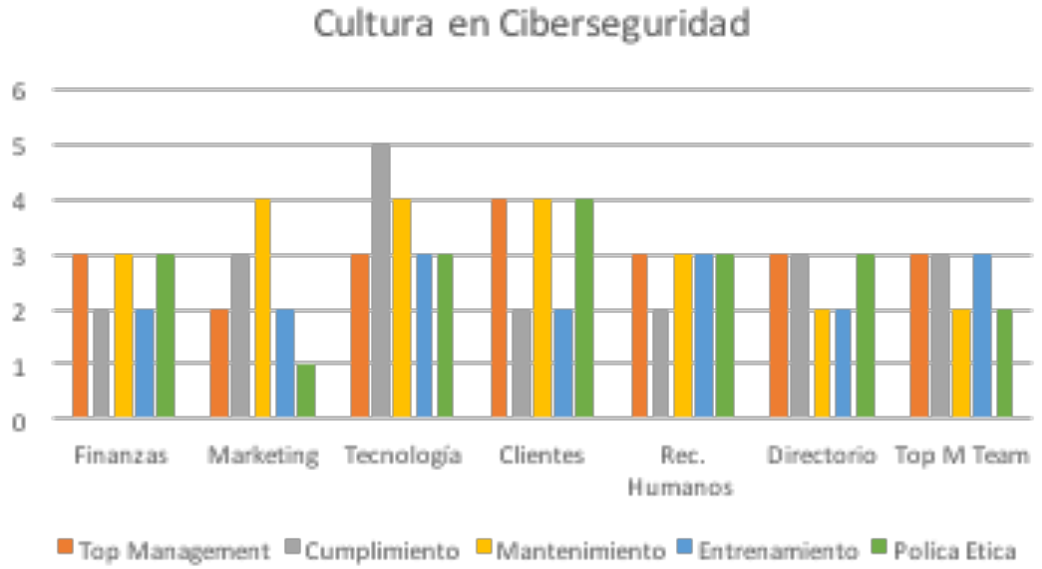
¿Cuál es mi línea Base ?

- Soporte de Top Management Team
- Cumplimiento de Políticas
- Mantención de las Políticas
- Capacitación en Ciberseguridad
- Políticas de Conducta Ética

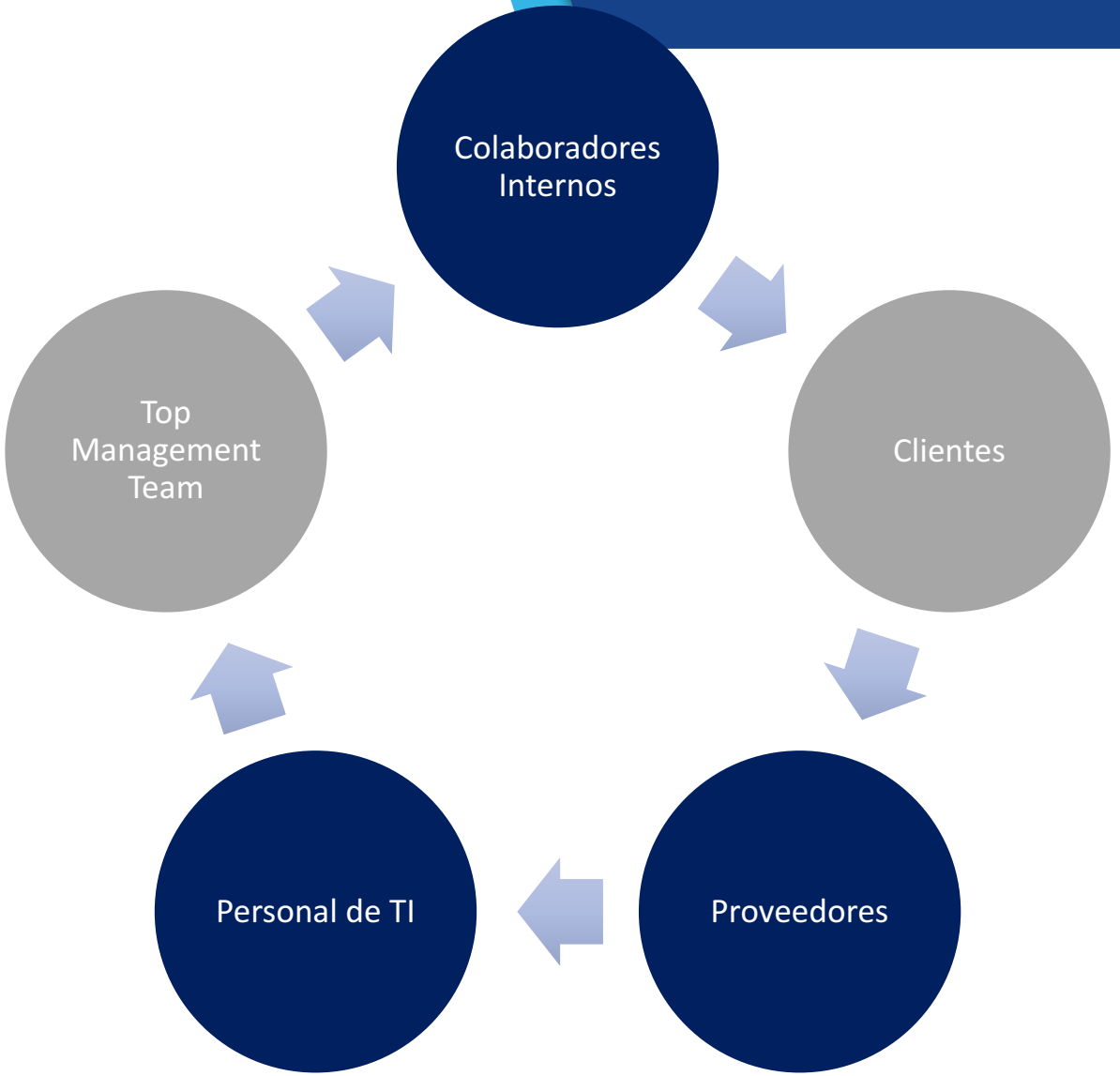
Cultura en Ciberseguridad

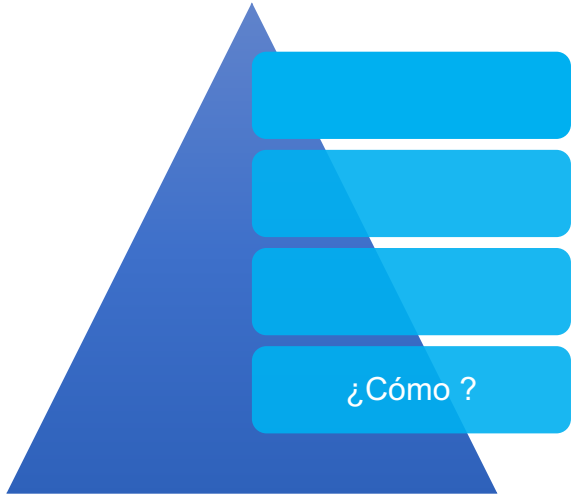
- Awareness en Ciberseguridad
- Cumplimiento en Ciberseguridad
- Ownership en Ciberseguridad






Quiénes?


Colaboradores Internos
Clientes
Proveedores
Personal de TI
Top Management Team



- Posters /Afiches / Wallpapers
- Newsletter, Blog
- Talleres/Seminarios/ Workshops
- Campañas E-mail
- Plataforma On-line
- Métodos basados en Juego de Roles
- Videos, Otros

	Marzo	Abril	Mayo	Junio	Julio	Agosto
RIESGO	Ingeniería Social	Reporte Incidentes	Redes WIFI	Ransomware	Navegación Segura	
MEDIOS DE DIFUSION	Webinar Videos E-Learning Infografía	Webinar Videos E-Learning Infografía	Webinar Videos E-Learning Infografía	Webinar Videos E-Learning Infografía	Webinar Videos E-Learning Infografía	
Pruebas		Campaña Ing. Social	Campaña Reporte Incidentes	Campaña Redes WIFI	Campaña Ransomware	Campaña Navegación Segura
ENCUESTA		Ing. Social	Reporte de Incidentes	Redes WIFI	Ransomware	Navegación Segura
Encuesta Cultura						Encuesta Cultura

Métricas

Métricas Estratégicas

Orientadas a Medir la efectividad del Programa de Cambio Cultural

- Nivel de Conocimiento, Actitud y Comportamiento
- Nivel de Cultura en Ciberseguridad

Implementación y medición de 2 tipos de Métricas, ***aquellas de nivel estratégico y aquellas métricas operacionales***

Métricas Operacionales

Orientadas a Medir la efectividad de las actividades del programa, en este aspecto se consideran a modo de ejemplo las siguientes métricas:

- % de personas victimas de Phishing
- % de personas victimas de WIFI falsas
- % de personas que participaron en e-learmning
- % de Personas que visualizan poster digitales
- Otras

Métrica	Tipo	¿Qué mide?	¿Cómo se mide?	Cuando se mide	Objetivo	¿Quién mide?
Participación TMT	Organizacional – Efectividad del Plan	Participación del TMT	Encuesta	Anual – terminada la implementación	Obtener a lo menos un índice de 4.0	Equipo de Seguridad / Proveedor Externo
Cumplimiento de Políticas	Organizacional – Efectividad del Plan	Cumplimiento de las Políticas	Encuesta	Anual – terminada la implementación	Obtener a lo menos un índice de 4.0	Equipo de Seguridad / Proveedor Externo
Mantención de la Política	Organizacional – Efectividad del plan	Mantenimiento de las Políticas	Encuesta	Anual – terminada la implementación	Obtener a lo menos un índice de 4.0	Equipo de Seguridad /proveedores Externo
Capacitación	Organizacional – Efectividad del plan	Capacitación en Ciberseguridad	Encuesta	Anual – terminada la implementación	Obtener a lo menos un índice de 4.0	Equipo de Seguridad /proveedores Externo
Política de Conducta Ética	Organizacional – Efectividad del plan	Políticas de ética y conflicto de interés	Encuesta	Anual – terminada la implementación	Obtener a lo menos un índice de 4.0	Equipo de Seguridad /proveedores Externo

Métrica	Tipo	¿Qué mide?	¿Cómo se mide?	Cuando se mide	Objetivo	¿Quién mide?
Ingeniería Social E-learning	Operacional - Actividad	Nº de personas que tomaron el curso	Ejecución Campaña de E-learning	Mensual – mes siguiente lanzada la campaña	Más del 70% de los colaboradores	Equipo de Seguridad / Proveedor Externo
Ingeniería Social - Examen	Operacional - Actividad	Nº de personas con aprobación del curso superior al 80%	Ejecución Campaña de exámenes	Mensual - mismo mes de la campaña de e-learning	Mínimo 80 puntos de aprobación del curso	Equipo de Seguridad / Proveedor Externo
Ingeniería Social- Campaña	Operacional - Actividad	Nº de personas que pueden identificar, parar y reportar un ataque de ingeniería social	Realización de ejercicio de ingeniería social y llamadas telefónicas	Mensual – después de realizada la campaña de examen	Menos del 20% de los colaboradores	Equipo de Seguridad /proveedores Externo
Ingeniería Social - CAC	Organizacional - Efectividad	Nivel de Conocimiento, actitud y comportamiento	Encuesta	Mensual – Mes siguiente de realizada la búsqueda de datos online	Obtener puntación igual o mayor a 4 en los 3 ámbitos	Equipo de Seguridad /proveedores Externo

Modelo de Incentivos

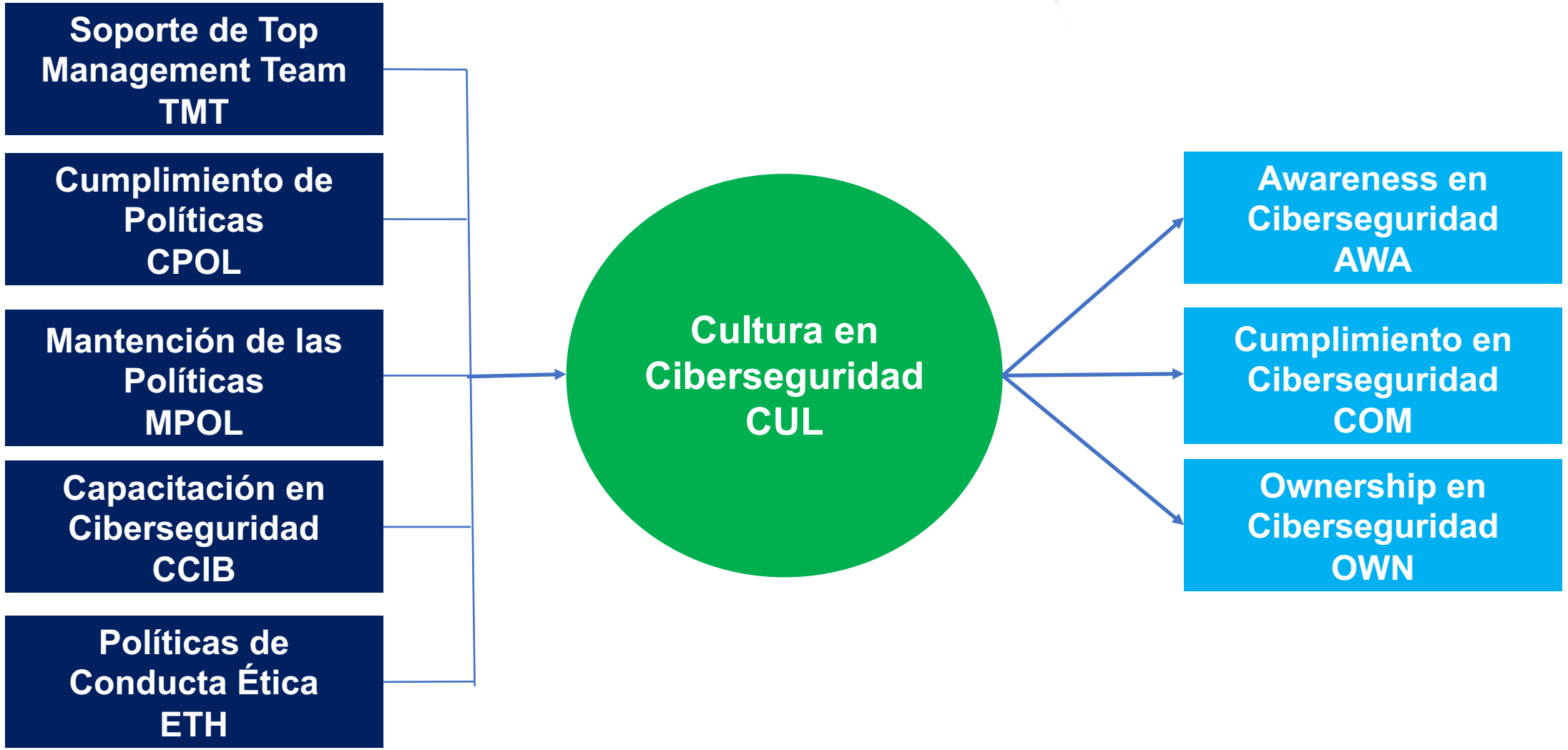
Los diferentes colaboradores obtendrán puntos por los resultados de las encuestas, la participación en las distintas campañas a efectuar y se les descontará puntos, por no participación en las actividades y cuando sean víctimas de las campañas a realizar

Aprendiz	Sensibilización Básica	100 Ptos
Padawan	En proceso de sensibilización	200 Ptos
Caballero	Buen Conocimiento y Actitud	300 Ptos
Master	Cambio de Comportamiento	400 Ptos
Gran Master	Posee una Cultura en Ciberseguridad	500 Ptos
		600 Ptos

Aplicación Encuesta de Cultura en Ciberseguridad

El objetivo de la investigación fue evaluar el nivel de cultura en Ciberseguridad existente en variados **países de la región, entre ellos Argentina, Perú, Colombia, México, Venezuela, España y Chile.**

La investigación para lograr medir la Cultura en Ciberseguridad, se basó en identificar los principales factores que son la causa para mejorar la cultura en ciberseguridad y aquellos elementos que son constitutivos.


Soporte de Top Management Team TMT
Cumplimiento de Políticas CPOL
Mantención de las Políticas MPOL
Capacitación en Ciberseguridad CCIB
Políticas de Conducta Ética ETH
Cultura en Ciberseguridad CUL
Awareness en Ciberseguridad AWA
Cumplimiento en Ciberseguridad COM
Ownership en Ciberseguridad OWN

Soporte del Top Management Team

La alta gerencia debe apoyar y participar en la seguridad de información y ciberseguridad.

Su compromiso y participación en la seguridad y ciberseguridad se considera uno de los factores más importantes para mejorar o crear una cultura de seguridad y un entorno que respalde la seguridad

Cumplimiento de las Políticas

Se refiere a la capacidad de la organización de hacer cumplir las políticas, las actitudes y comportamientos de los colaboradores.

Una forma común de hacer esto es auditar y monitorear la política de Ciberseguridad, las prácticas y los procedimientos.

El uso de auditoría interna o externa independiente es particularmente valioso para ayudar a lograr el cumplimiento de las políticas.

Mantenimiento de Políticas

Revisar, actualizar y mejorar continuamente las políticas de seguridad de la información y ciberseguridad, los procedimientos y el programa de seguridad tendrán como beneficio mejorar la cultura en Ciberseguridad. Esto se puede llevar a cabo por medio de una continua evaluación de riesgos y una gestión del cambio.

Comprender los riesgos y mejorar las políticas focalizado en la reducción de riesgos es un factor crítico para el mejoramiento de la cultura en seguridad de la información y ciberseguridad en el tiempo.

Capacitación y Concientización

La capacitación y la concientización es el camino fundamental para comunicar las políticas de seguridad de la información y ciberseguridad a la organización, así como los factores asociados al elemento humano, lo anterior influirá en el conocimiento, actitud y comportamiento de los colaboradores y creará una mejor cultura en ciberseguridad

Políticas de Conducta Ética

Las políticas de conducta ética (por ejemplo, código de conducta, conflicto de intereses) ayudan a los colaboradores a comprender y ser conscientes de sus responsabilidades de seguridad y ayudan a reducir el riesgo asociado con su comportamiento de seguridad

Security Awareness

Los empleados deben conocer las políticas de seguridad para crear un entorno que promueva la creación de una cultura de seguridad, se debe establecer una conciencia de seguridad que sea sustentable en el tiempo.

La falta de conciencia de seguridad en sí misma ha sido considerada repetidamente como un problema importante para garantizar la seguridad de las organizaciones.

La conciencia de seguridad puede mejorar el comportamiento de los empleados directamente al influir en ellos para que contribuyan al establecimiento y mantenimiento de una cultura de seguridad.

Security Compliance

Se puede crear una cultura de seguridad si se cumple con la política de seguridad. Al cumplir con una política de seguridad, las organizaciones pueden reducir la cantidad de violaciones de seguridad que resultan del comportamiento de los empleados.

El mal comportamiento de los empleados también podría influir en las prácticas de seguridad de la información que podrían causar daños y pérdidas a los activos de la organización.

Ownership en Seguridad

Es importante que el personal de cualquier organización entienda y comprenda sus funciones y responsabilidades de seguridad, con el fin de mejorar su propio rendimiento de seguridad y, por tanto, el rendimiento de seguridad de la organización.

Al comprender sus responsabilidades y la importancia de proteger la seguridad de la información, el personal puede comprender qué riesgos de seguridad están asociados con sus acciones. Esto aumentará sus niveles de conciencia de seguridad, lo que aumentará el cumplimiento de la política de seguridad de la organización. Por esta razón, la responsabilidad de los empleados y la propiedad de la necesidad de proteger la seguridad de la información es un aspecto importante de la creación de una cultura de seguridad.

Al ser responsable y tener un sentido de propiedad, el comportamiento del personal cambiará con respecto a la protección de los activos de la organización, lo que llevará a la creación de una cultura en Ciberseguridad.

- La cantidad de personas que participaron en el estudio fue de 939, incluyendo países como Argentina, Perú, Colombia, México, Venezuela, España y Chile.

- La cantidad de personas que participaron en el estudio, que trabajan actualmente en chile fue de 521.

- Las personas que participaron en el estudio son profesionales que se desempeñan en distintas posiciones dentro de las organizaciones

- El grupo objetivo de la muestra fueron hombres y mujeres, con título profesional de cualquier universidad o instituto, que actualmente se encuentren trabajando en algún país de los antes mencionados.

- La encuesta aplicada consideró 47 preguntas, las cuales estaban orientadas o medir los diversos constructos

- La encuesta fue respondida según una escala de 1 a 5, donde 1 es muy en desacuerdo y 5 que es muy de acuerdo

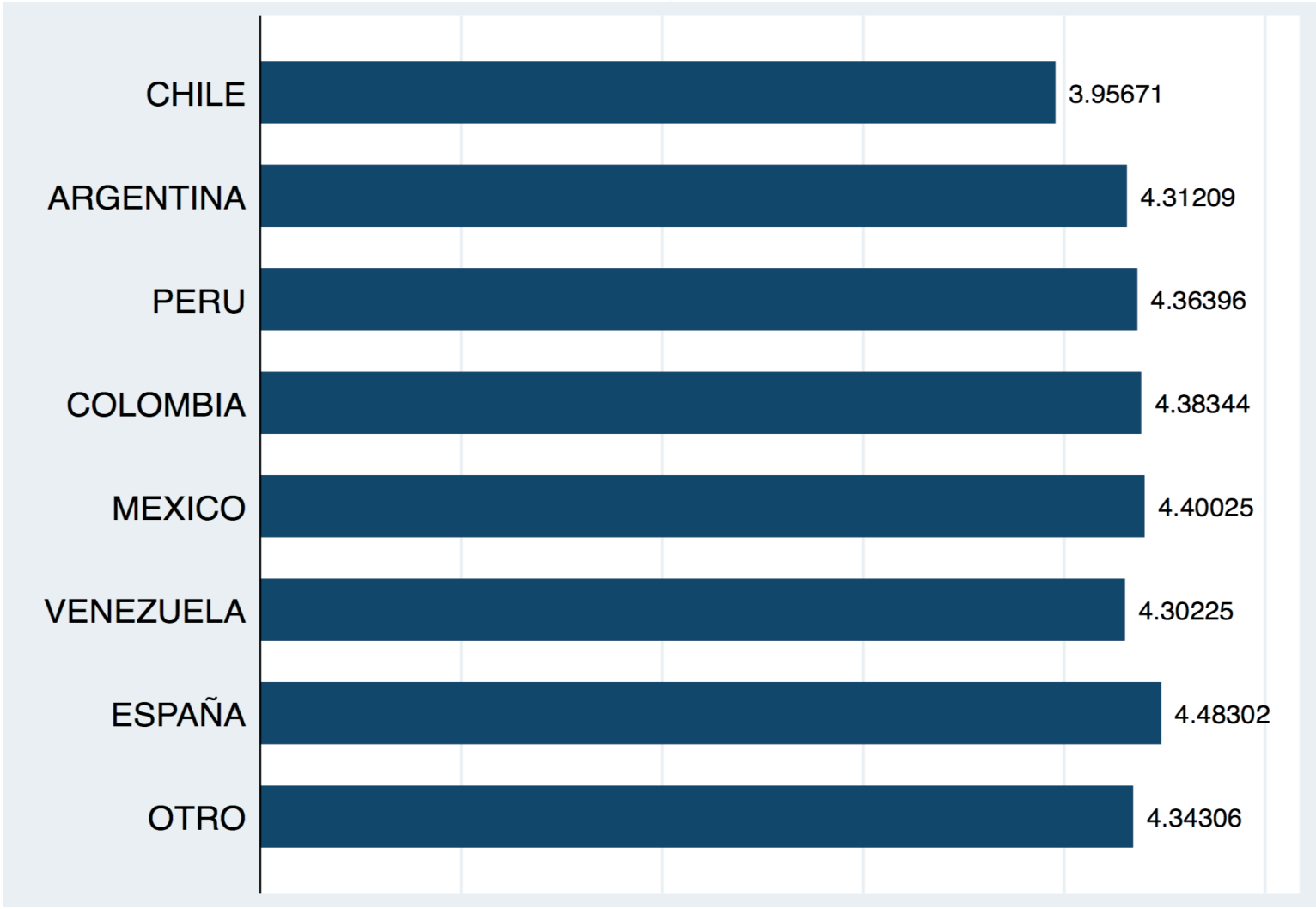
- Dentro de los factores demográficos aplicados, se encuentra el país, tipo de organización, número de empleados, industria, edad de la organización y edad de la persona que contesta, como también su nivel educacional

- La aplicación de la encuesta fue vía web, utilizando el software Qualtrics.

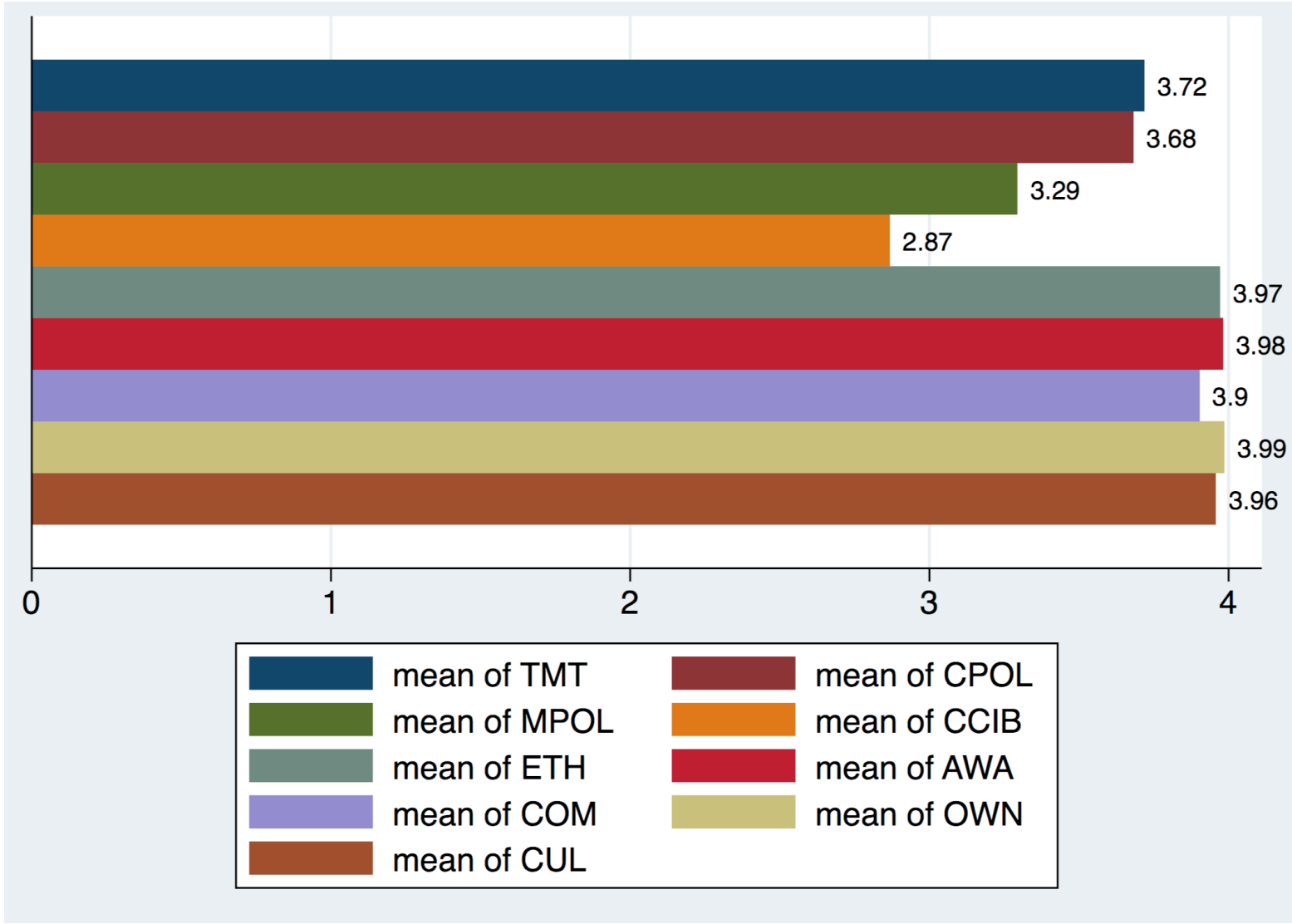
- La fecha de aplicación del estudio fue entre Octubre y Diciembre del año 2018

RESULTADOS

Si comparamos el nivel de Cultura en Ciberseguridad de Chile, con otros países de la región, como Argentina, Perú, Colombia, México, Venezuela, y España, nuestro estudio evidencia que Chile tiene la Cultura más baja en Ciberseguridad, siendo ésta de 3,95 en una escala de 1 a 5.

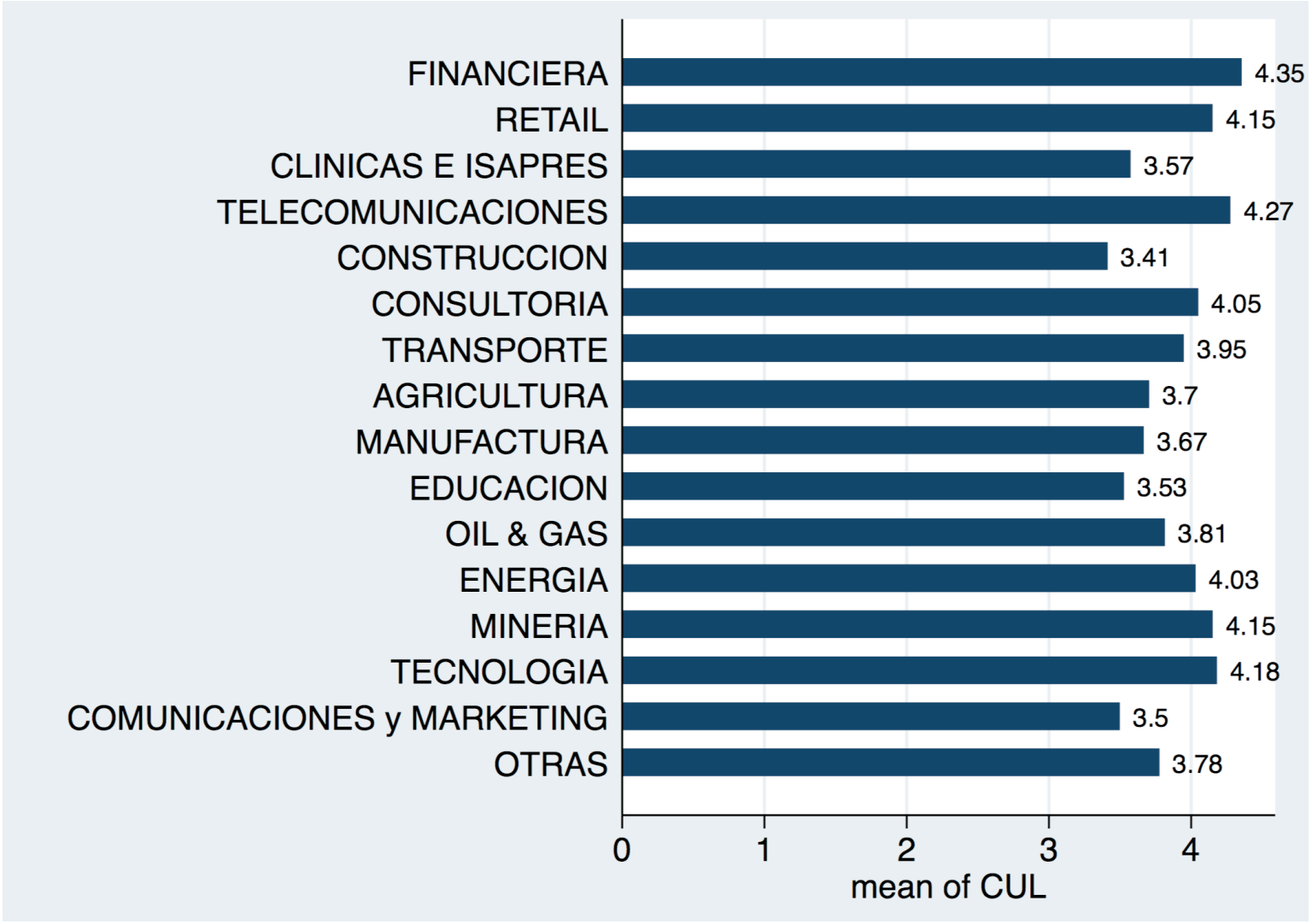


El factor peor evaluado se refiere a la capacitación de Ciberseguridad

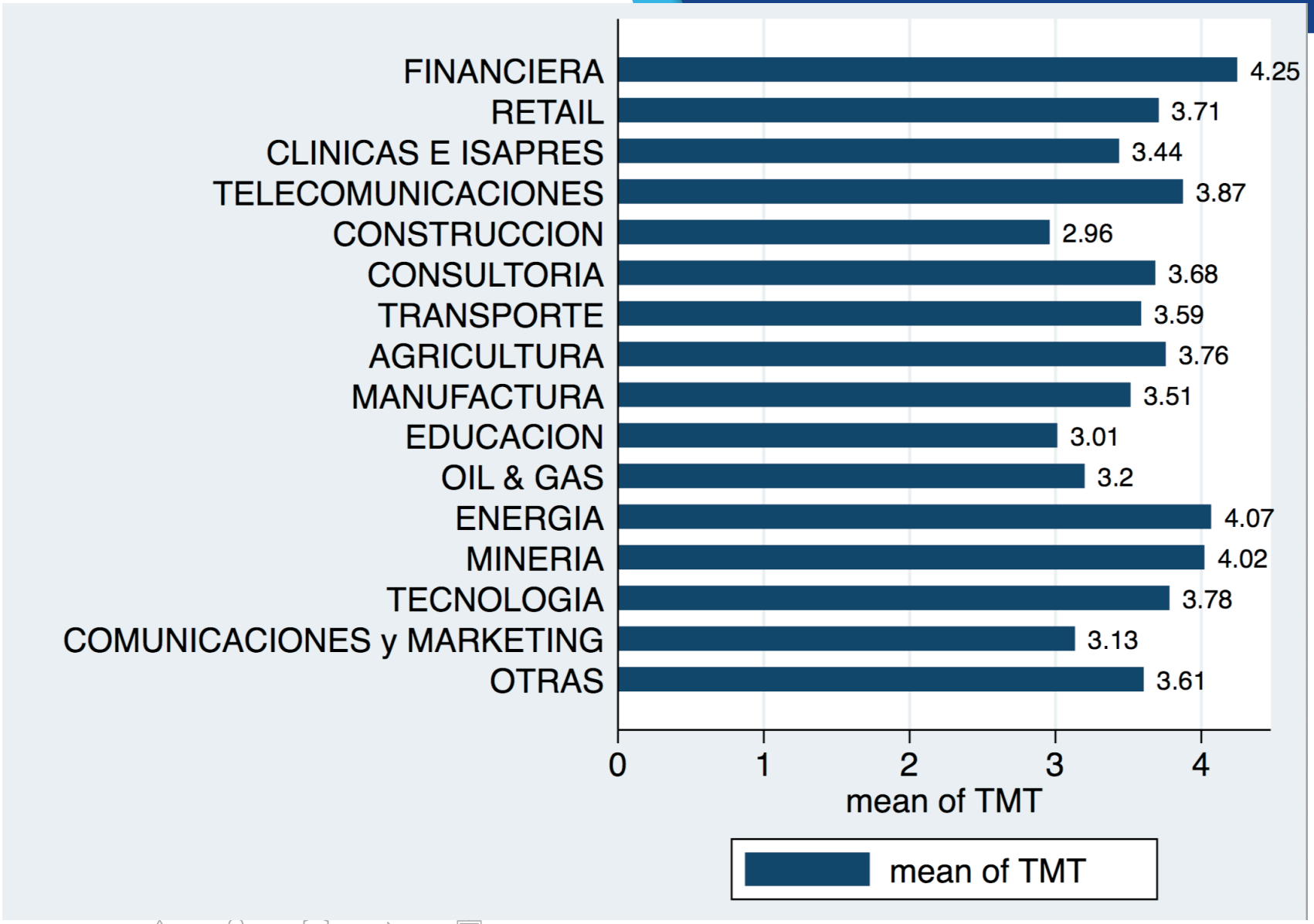


Un análisis por las diversas industrias del mercado chileno, nos indica que la industria mejor evaluada es la industria financiera, con un indicador de 4.35, seguida por la industria de tecnología con un 3.98 y en tercer lugar la industria de telecomunicaciones con un 4.27.

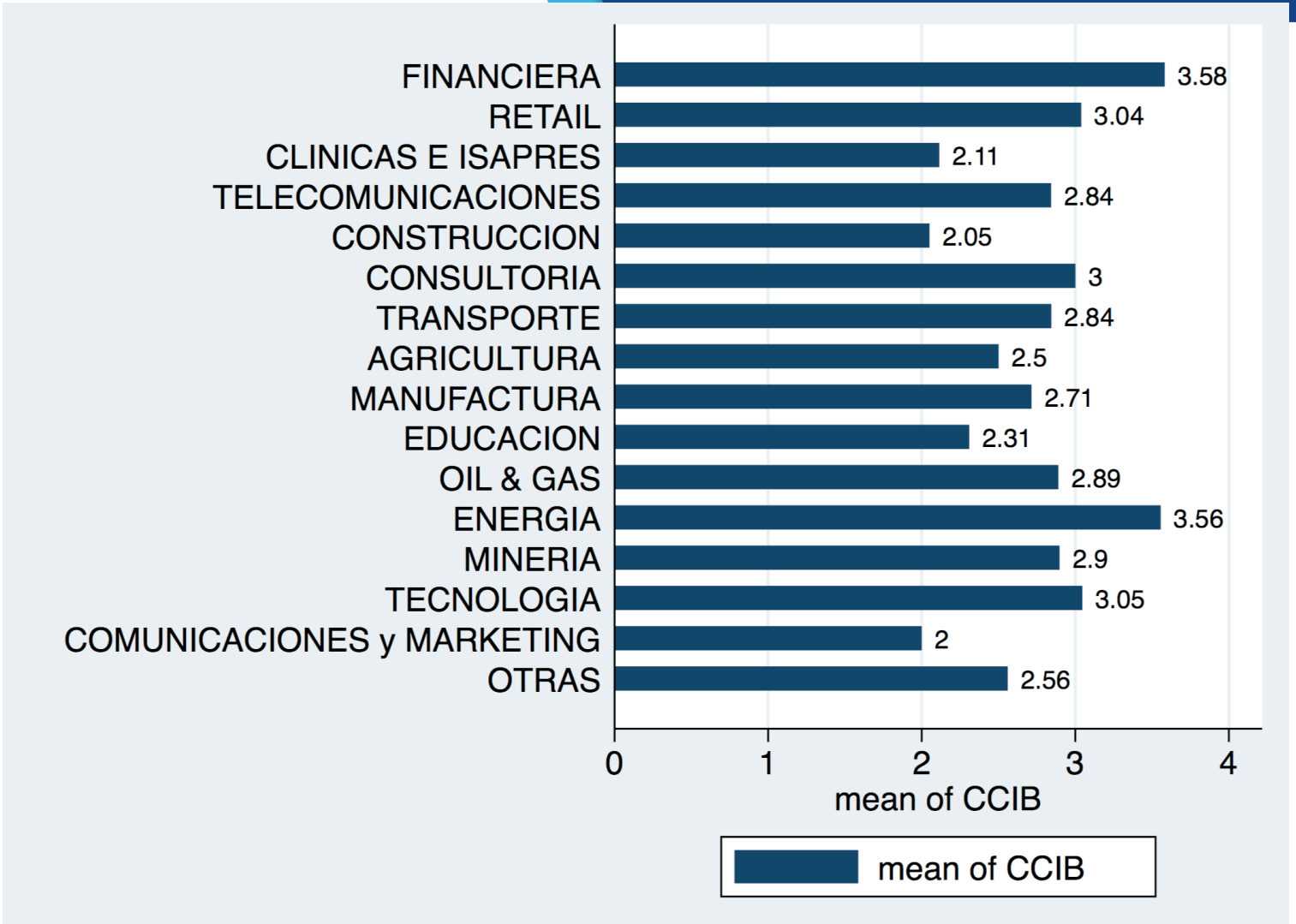
Dentro de las peores industrias se encuentran Construcción, Comunicaciones y marketing, Educación y Clínicas e Isapres



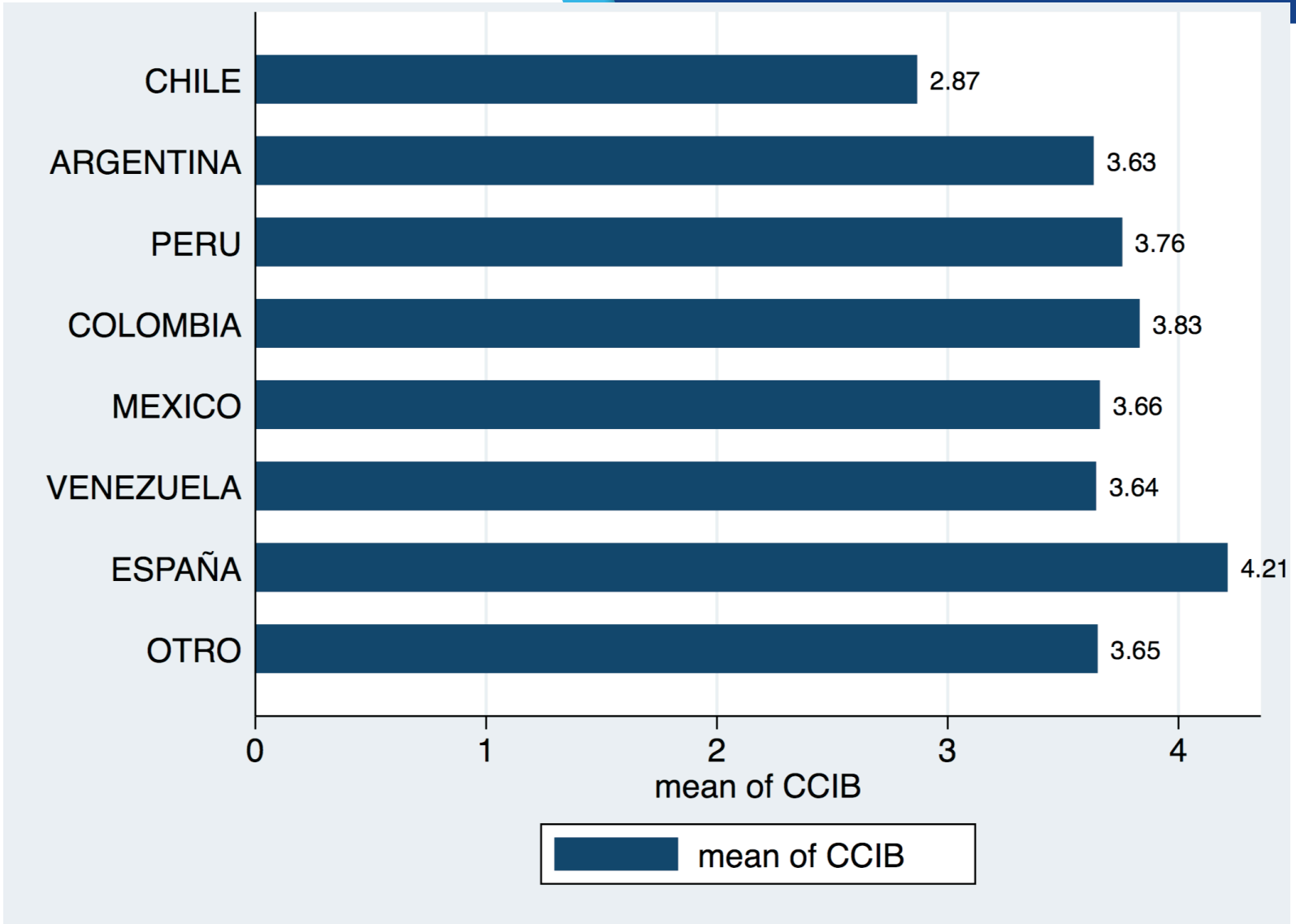
El nivel de involucramiento del TMT se da principalmente en la industria Financiera, Energía y Minería.



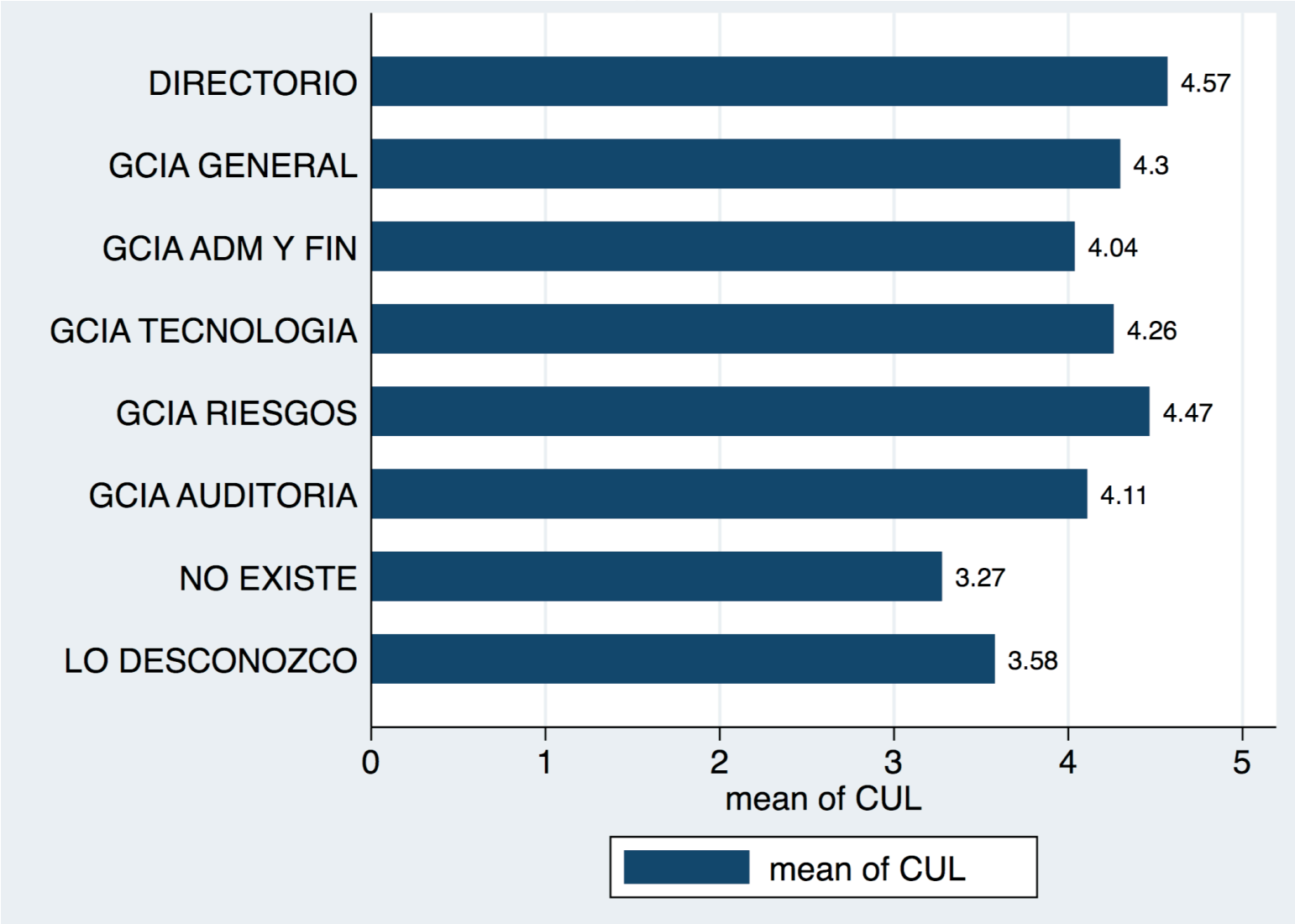
La Capacitación en Ciberseguridad, es el nivel más bajo del modelo, siendo la Industria Financiera, Energía y Tecnología los mejor evaluados.



Chile continua siendo el país pero evaluado en temas de Capacitación en Ciberseguridad.



La Dependencia del CISO es fundamental para mejorar la Cultura en Ciberseguridad de las organizaciones.



FUNDAMENTOS ESTADISTICOS

Test scale = mean(unstandardized items)

Average interitem covariance: .711297
Number of items in the scale: 9
Scale reliability coefficient 0.9242

```
. reg CUL TMT CPOL MPOL CCIB ETH
```

Source	SS	df	MS		
Model	430.800112	5	86.1600224	Number of obs	= 939
Residual	285.650544	933	.306163499	F(5, 933)	= 281.42
				Prob > F	= 0.0000
				R-squared	= 0.6015
				Adj R-squared	= 0.5992
Total	716.450657	938	.76380667	Root MSE	= .55332

CUL	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TMT	.1473876	.027 3065	5.40	0.000	.0937983	.2009768
CPOL	.1077079	.022 8214	4.72	0.000	.0629207	.152495
MPOL	.0817511	.027 2195	3.00	0.003	.0283325	.1351697
CCIB	.2051776	.018 4395	11.13	0.000	.16899	.2413653
ETH	.1439084	.020 4782	7.03	0.000	.1037198	.1840971
_cons	1.604228	.085 0401	18.86	0.000	1.437336	1.77112

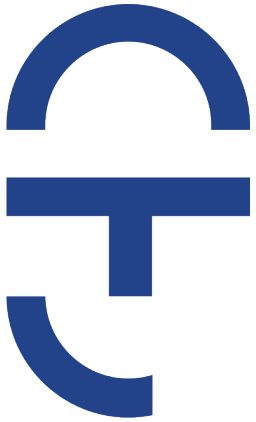
```
. vif
```

Variable	VIF	1/VIF
MPOL	3.58	0.279324
TMT	2.68	0.373329
CPOL	2.23	0.447607
CCIB	2.12	0.472242
ETH	1.41	0.709706
Mean VIF	2.40	

```
. hettest

Breusch-Pagan / Cook-Weisberg test for heteroskedasticity
         Ho: Constant variance
         Variables: fitted values of CUL

         chi2(1)      =  301.17
         Prob > chi2  =    0.0000
```



cybertrust

INSPIRANDO CONFIANZA