



Cultura organizacional de ciberseguridad

Construyendo confianza

Noviembre 2018



Por qué invertir en cultura de ciberseguridad

El entorno evoluciona

Las amenazas están evolucionando rápidamente así como las regulaciones, además, las personas exigen más seguridad.

Esto representa riesgos operacionales, de sanciones y de reputación



GDPR

40%

de los CEO consideran a las ciberamenazas entre las más relevantes

69%

de los consumidores creen que las compañías son vulnerables a los ciberataques



Las personas no tienen porque ser el eslabón más débil




Pueden ser la más efectiva primera línea de defensa de la organización

Hay factores que inciden en nuestra conducta

Los ataques se han centrado en las personas

50%

de los peores incidentes del 2018 fueron causados por errores humanos

-  No somos racionales
-  Nuestras decisiones son influenciadas por emociones
-  No evaluamos bien el riesgo





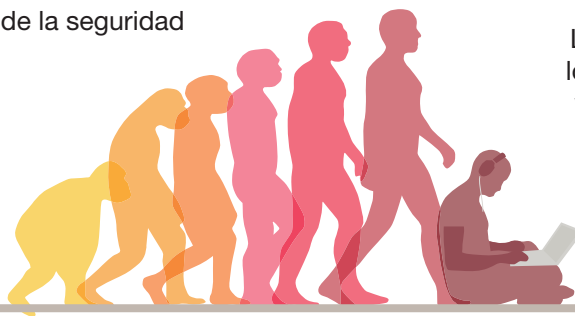
Por qué invertir en cultura de ciberseguridad

Entender la cultura, motivaciones y sesgos de la empresa es crítico

Primero cambia la cultura, luego la mentalidad

Cultura es más que conciencia

Se ve poca inversión en el factor humano de la seguridad



Desafíos

Los empleados no sienten responsabilidad por la seguridad, se sienten aparte del riesgo.

El entrenamiento de seguridad es visto como un trámite que no cambia conductas

Las personas se saltan los controles estrictos y ven las políticas como impracticables o inconvenientes

Beneficios

Las conductas seguras son incorporadas a la organización y sus rutinas

Las personas se transforman en la primera barrera de seguridad de su organización. Dejarán de ser el eslabón más débil y los incidentes por errores humanos serán reducidos

Aumentará la confianza y reputación, lo que en el mundo digital pronto se traducirá en una ventaja competitiva difícil de replicar



Hacia una potente cultura organizacional de ciberseguridad

Definir una visión

¿A qué aspira su cultura?



PwC y su organización en conjunto podremos:

1. Entenderemos sus programas y prioridades comerciales
2. Comprometeremos a los stakeholders claves
3. Identificaremos los riesgos específicos
4. Definiremos las claves de la conducta de seguridad esperada

Diagnosticar

Condición actual de su cultura de ciberseguridad



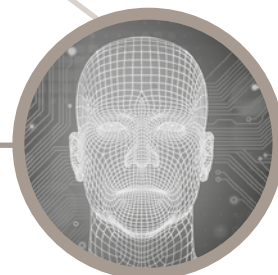
Haremos un diagnóstico de la cultura organizacional de ciberseguridad:

1. Evaluación: pruebas de ingeniería social, entrevistas, encuestas; entre otras
2. Análisis y reporte: para identificar riesgos y desalineamientos
3. Estrategia: definición de la estrategia y plan de mejoras



Transformar

Ciberseguridad como hábito



Implementación del plan de mejoras:

1. Actividades de conocimiento y compromiso:
 - Direccionamiento y liderazgo
 - Educación, entrenamiento y Coaching
 - Campaña comunicacional
 - Fomento de las conductas de seguridad



Hacia una potente cultura organizacional de ciberseguridad

Curiosidad

Básico (todos)*

Completar el entrenamiento de ciberseguridad

Seguridad física (todos)*

No dejar visitas solas
Reconocer los engaños

Seguridad lógica (todos)*

Reconocer phishing
Estar al día de las amenazas
Usar redes seguras

Especialización (según roles)*

Reconocer código sospechoso
Evaluar seguridad de proveedores

** Indica que estos son ejemplos*

Responsabilidad

Básica (todos)*

Entender los roles

Seguridad física (todos)*

Proteger recursos físicos y copias en papel
Portar identificación
Passwords seguras

Seguridad lógica (todos)*

Uso apropiado de RRSS
Clasificación de los datos
Protección de información
Encriptación adecuada

Especialización (según roles)*

Programación segura
Correspondencia con política de seguridad de datos

** Indica que estos son ejemplos*

Reportar

Básica (todos)*

Posibilidad sugerir mejoras

Seguridad física (todos)*

Reportar personas o paquetes sospechosos
Evitar aglomeraciones

Seguridad lógica (todos)*

Reportar email o programas sospechosos
Detectar uso de malas passwords

Especialización (según roles)*

Evitar proveedores con mala seguridad
Mejorar la resiliencia

** Indica que estos son ejemplos*

Métodos:

- Aprendizaje innovador
- Orientación por roles

Motivación:

- Mejorar gestión ciberseguridad
- Administración consecuente



Hacia una potente cultura organizacional de ciberseguridad



Medir efectividad

Monitorear y demostrar los progresos



Diseñar, construir e implementar
tableros de progreso, incluyendo:

1. En el diseño: utilizar métricas cuantitativas y cualitativas
2. Procesos y gobernanza: identificar a los dueños de los datos, procesos, frecuencias, taxonomías y objetivos
3. Establecer líneas de base y operacionalizar



Contacto

Para ampliar el contenido de alguno de los temas indicados y evaluar las implicancias en su empresa, no dude en contactarse con nosotros.



Federico Morello

Socio Líder de Consultoría y Asesoría Empresarial
PwC Chile
federico.morello@cl.pwc.com
(56)2 2940 0181



Héctor Gómez

Cybersecurity Senior Manager
PwC Chile
hector.gomez@cl.pwc.com
(56)2 2940 0181

A large, faint fingerprint graphic is centered in the background of the orange page.

Toma el control de tu Ciberseguridad