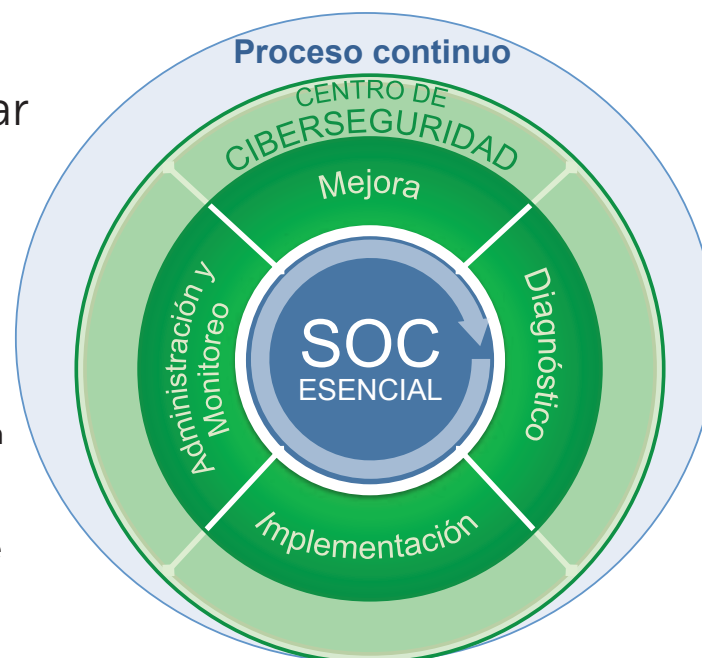




Recomendación a considerar

- » Definir los roles y responsabilidades relacionados con la seguridad de la información
- » Conocer y gestionar los riesgos en materia de seguridad de la información.
- » Aplicar los controles de seguridad, con un enfoque basado en el costo beneficio
- » Establecer mediciones de eficiencia de los controles que permitan establecer acciones de mejora continua



Estrategia por prioridad

Meta anual	Tarea / Actividad	Plazos	Recursos necesarios

MEDICIÓN Y EVALUACIÓN DE RESULTADO

¿cómo lo mediremos?

--



Para más información comuníquese al 9150.7400 ext. 1731 y 1815 o envíenos un correo a ventas@scitum.com.mx



/scitum.sadecv



@Scitum_MX



scitum

TU SOCIO DE NEGOCIO EN CIBERSEGURIDAD

WWW.TELMEX.COM/IT



GUÍA PLANIFICACIÓN ESTRATÉGICA DE SEGURIDAD DE LA INFORMACIÓN

Premisa de seguridad IT:

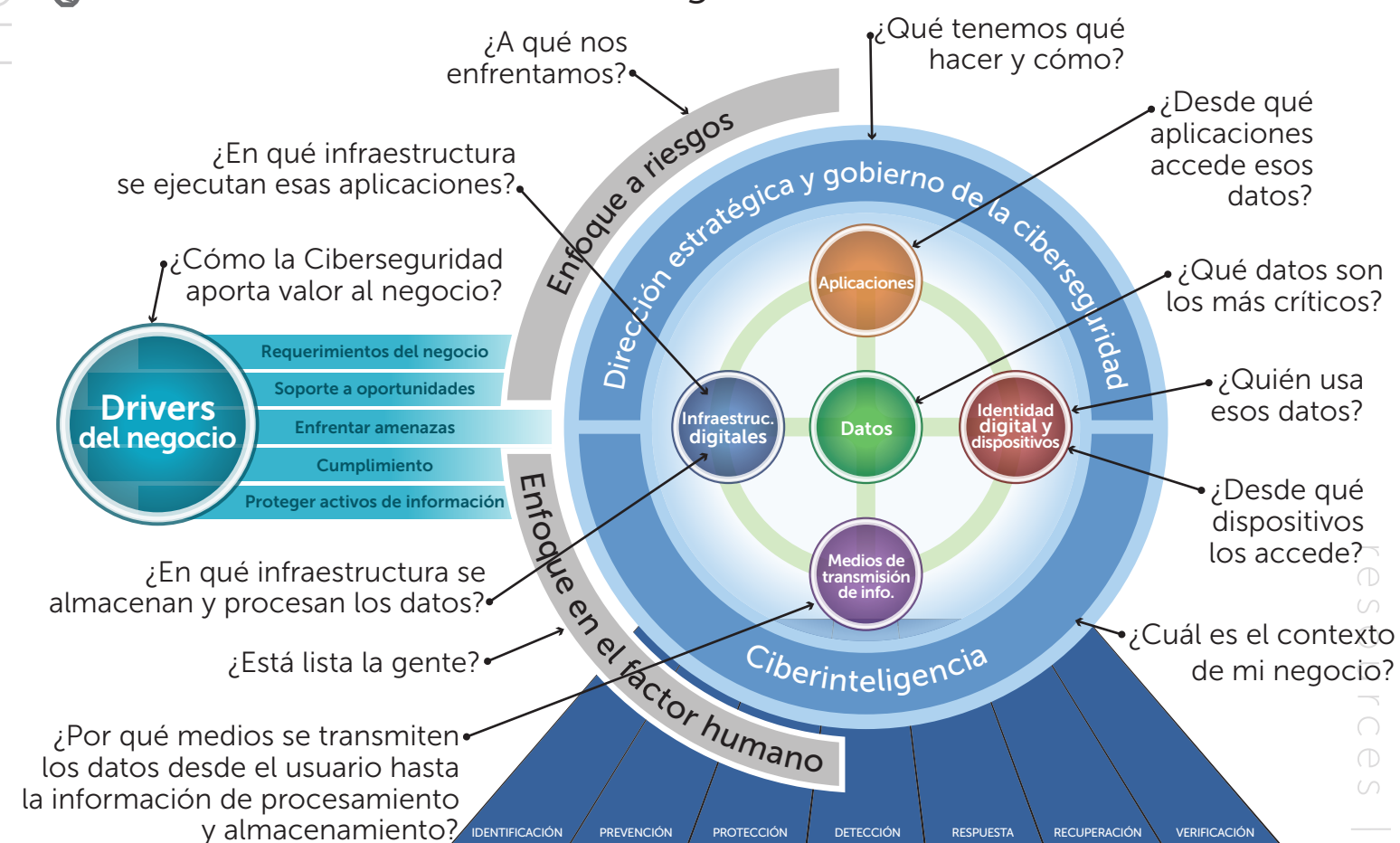
HOY NO SE TRATA DE SABER SI TE VAN A ATACAR, SINO CUÁNDO...

Hay una nueva realidad:

- » Las cosas ya cambiaron. Los ataques son más intensos y sofisticados, los atacantes tienen mayores recursos, tenemos más elementos que cubrir y nuestra superficie de exposición ha crecido.
- » Debemos entrar con otra mentalidad. No podemos pensar en defender como la estrategia básica. Hay que proteger pero también detectar y actuar.
- » Buscar nuevas tecnologías no debiera ser el primer paso. Hay que considerar al personal que diseñará, implementará y administrará la seguridad (incluyendo el monitoreo, la detección y manejo de incidentes), así como los procesos y procedimientos necesarios.



Visión Holística de la Ciberseguridad



1. ¿Cuál es el objetivo de tu organización en seguridad de la información a corto plazo?

2. ¿Cuál es tu situación actual en seguridad y ciberseguridad?

¿A qué nos enfrentamos?

PUNTOS FUERTES

¿Dónde estamos?

¿Dónde hay que aplicar los controles?

PUNTOS DÉBILES

OPORTUNIDADES

DESAFÍOS

Check list de seguridad:

Evalua y reflexiona que afronta tu organización actualmente.

	Incidentes de seguridad repetitivos que no han sido manejados adecuadamente en tiempo y forma
	Información sin clasificar de acuerdo a su criticidad.
	Ausencia de procesos y políticas formales sobre la seguridad de la información.
	Desconocimiento del personal sobre las actividades que debe realizar para el manejo seguro de la información.
	Sanciones por parte de organizaciones gubernamentales o del sector debido al mal manejo o pérdida de información de clientes o proveedores
	Escándalos o noticias que han sido de dominio público en los que la institución se ha visto involucrada debido a la pérdida de información confidencial o a la mala administración de la misma

3. ¿Qué controla tu organización y cómo responde actualmente?

4. ¿A dónde quiere llegar tu organización en seguridad y ciberseguridad?

¿Dónde hay que aplicar los controles?

Enumerar 5 metas que tu organización desea lograr a largo plazo

1.-

2.-

3.-

4.-

5.-

5. ¿Cuál es la visión en seguridad TI para tu organización, desde tu área o perspectiva?



¿Cómo puedes llegar?

Tip: Establecer prioridades estrategicas, que ayuden a mejorar la seguridad informática de las organizaciones para alcanzar la visión, teniendo en cuenta:

- » Aspectos fuertes, débiles
- » Oportunidades y desafíos
- » Tus metas en seguridad y ciberseguridad
- » La opinión de expertos en seguridad (temas de la reunión)
- » Plazo a un año para lograrlo