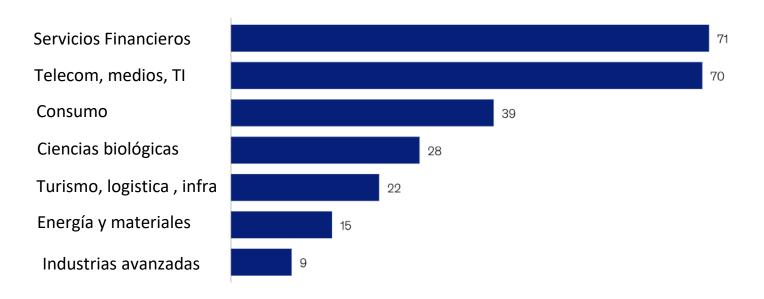


Transformación de negocio y tecnologia



% del impacto de cambios en negocio, dependientes de tecnologías de la información

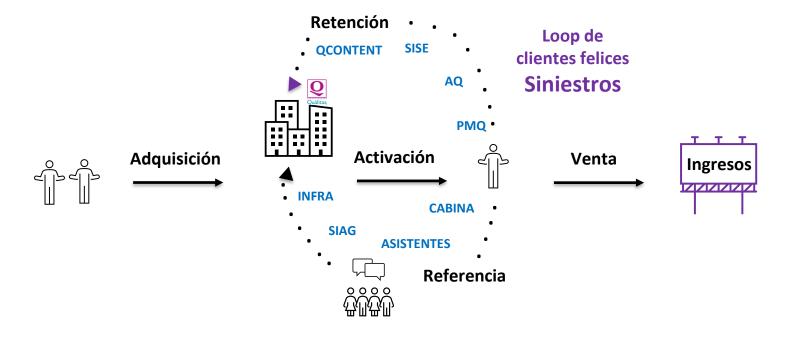


Fuente : McKinsey Analysis

Gestión de siniestros – servicio al cliente



Protección de plataformas existentes, en adición a innovación continua



Gestión de siniestros – servicio al cliente



Riegos de continuidad de negocios y ciberseguridad

01

Continuidad de negocios

02

Ciberseguridad

Continuidad de negocios

Adiciones en 2023

* Actualizaciones requeridas



Qcontent *

Portal de valuación *

Plataformas criticas emisión y siniestros SISE - 41% Web services – 36% Portal de Agentes – 14% **OPL - 4% *** Comerciales Página Pública Link de pago * Infaestructura Generales Correo electrónico estrategica Cabina AQ **SIAG PMQ Siniestros** Telefonía Internet **Asistentes virtuales Quali** Alcance 2022

Continuidad de negocios

Reto afinación permanente, cambios altos que hacen difícil planear



	Transacciones	2021	2022	2023 A la fecha	* Tendencia 2023	% var 21 vs 23
SISE	Siniestros	1.3 M	1.6 M	0.75 M	1.8 M	14%
SAC	Reportes	1.5 M	1.7 M	0.79 M	1.9 M	14%
AQ	Tableta	0.90 M	1 M	0.46 M	1.1 M	10%
SIAG	AV	0.38 M	0.46 M	0.22 M	0.52 M	26%
Cabina	Llamadas	2.86 M	2.9 M	1.02 M	2.95 M	3%
ASISTENTES	Reportes	0.23 M	0.19 M	0.17 M	0.4 M	95%
QCONTENT	Documentos	26.66 M	26.66 M	12.5 M	30 M	14%
A Express	Siniestros	9.5%	12.5%	15.3%	25%	

"No puedes entrar al mismo rio dos veces, porque el rio ha cambiado y tú también"

[↑] Transacciones, concurrencia procesos, modificaciones requeridas, nuevos proyectos, regulaciones, ciberseguridad

Estrategia de sistemas alternos

- Amplia alternos DRP + Alta disponibilidad
- 2 Adiciona más sistemas críticos
- **3** Aumenta número de procesos cubiertos



Proceso continuo

Inició: Cotización, emisión, consulta

Cada año: Más sistemas y procesos

Fortalecer redundancia varios niveles

Existente en 2021

√ Nuevo o aumento

* Migraciones



√ + procesos No existe No existe No existe No existe No existe Migración * **√** + procesos No existe No existe **√** + procesos **v** + procesos No existe **√** + procesos No existe No existe No existe No existe Migración * Actualizar * No existe No existe **v** replica No existe Prueba real No existe Prueba real No existe Prueba real

2022

Plan 23

2021

Datos de la CFE, bajo ciberataques "ransomware"

En los últimos años la Comisión Federal de Electricidad (CFE) recibió 368 mil 883 ciberataques, sin embargo, casi una quinta parte de ellos (17.54 por ciento) fueron 'ransomware' o secuestro de datos mediante los cuales intentaron tomar el control de sus sistemas informáticos; es el mismo tipo de virus que paralizó durante días una red de oleoductos en EEUU en mayo pasado

Las agresiones informáticas contra la empresa productiva del Estado mexicano vienen desde diferentes países del planeta, de acuerdo con un informe interno de la propia Comisión



Hackers secuestran datos de Lotería Nacional; dan 240 horas para negociar rescate

CIBERSEGURIDAD

Hackers cumplen amenaza y liberan información supuestamente robada a Lotería Nacional

El 28 de mayo, el grupo de ciberdelincuentes amenazó a Pronósticos Deportivos de la Lotería Nacional y dio un plazo 10 días para pagar un "rescate"

Sedena Hackeada



¿ Que es Ciberseguridad?



- Ciberseguridad es una combinación de personas, politicas, procesos y tecnologias usadas en una empresa para proteger sus activos digitales.
- Sub conjuntos incluyen seguridad de IT, seguridad de IoT, seguridad de la information y seguridad operativa.



3 cosas que liderazgo necesitas saber



El ciber riesgo impacta nuestra estrategía, operaciones, reputación y resultados.

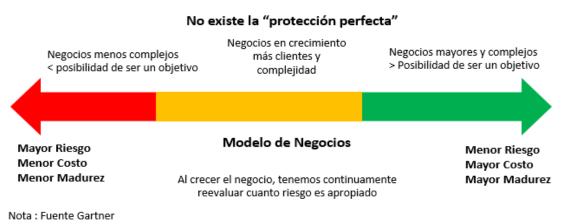
Todos somos un blanco.

Necesitamos un plan que balancee crecimiento con riesgo.

¿ Cuál es el nivel apropiado de riesgo?



Espectro de Administracion del riesgo



El objetivo es construir un programa sustentable que balancee la necesidad de proteger versus las necesidad de correr nuestro negocio





















Vulnerabilidades y amenazas



	Endpoints	Redes	AD	Servers	O365	Atención de Incidentes
Ransornware	✓	1	1		1	✓
Acceso a ser ridores		1	1	✓		✓
Robo de datos	✓	1	1	1	1	✓
Cosecha de credenciales	✓	1	1		1	✓
Compromiso de correo			1		1	✓
Spear phishing					1	✓
Fuga de información			1	✓		✓
Amenaza interna			1		1	✓
Tro yanos bancarios	✓					✓

¿ Liderazgo que necesitas hacer?



Hacer lo básico bien

Muchas companies fallan aqui!







Cultura organizacional de la ciberseguridad





Responsabilidad directiva



Grupo de alto riesgo – ¿ QUIEN YO?

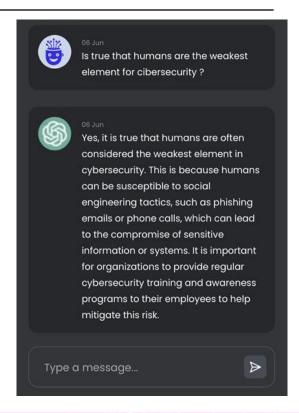


Los directivos son alvos de ataques 12x más que otros empleados.

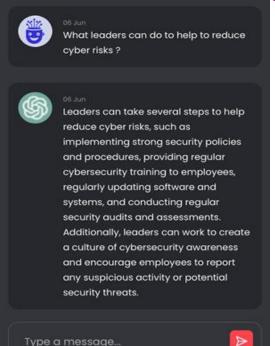
"La mayoría de las encuestas de riesgo, muestran que los directivos son los menos propensos a adherirse a las políticas que esperan que sigan todos los demás. En parte, esto se debe a que son el grupo más dispuesto a sacrificar la seguridad por conveniencia y tienen la influencia corporativa para exigirla"

Preguntando a IA - ChatGPT











Impulsar cultura, conciencia y entrenamiento de ciberseguridad con sus equipos



Cuando caes en una trampa de ciberseguridad, las consecuencias pueden ser mayores



"Maniobrar con un ejército es ventajoso. Maniobrar con una multitud indisciplinada, es peligroso"

Sun-Tzu



Quiz



2 ¿Servicios críticos a clientes como la gestión de siniestros, pueden verse afectados por riesgos de continuidad de negocios y de ciberseguridad?

VERDADERO

¿Un plan de recuperación en caso de desastres DRP, debe estar en la misma localidad en donde se encuentre la infraestructura principal?

FALSO

¿ El ramsomeware es una de las mayores amenazas cibernéticas en la actualidad ?

VERDADERO

¿Tecnología, procesos y personas son necesarios en un programa sólido de seguridad de información ?

VERDADERO

Preguntas





