HABÍA UNA VEZ UN AUDITOR ...

"20 casos de no éxito de ISO 27001"



Cuentos de SGSI para auditores que no pueden dormir

CLOUD LEGION



Fracaso vs Éxito
Casos de no éxito de SGSI/ISMS
Errores Típicos
¿Como evitar o mitigar?
Conclusiones
Autores

FRACASO VS ÉXITO



PRUEBAS

ERRORES



A veces me pregunto si tanto nos gustan las historias de superación....

¿Porque ninguna empresa o consultor publica sus casos de no éxito y como lo superaron?



La cultura del éxito

(Un freno para la innovación)

Solemos reverenciar el éxito, el logro, la realización de lo que esperamos, pero qué pasaría con la humanidad si no existiera el intento, la falla, esa búsqueda permanente de ir más allá.

El éxito en realidad "frena el proceso de aprendizaje"

Aprendemos más de los fracasos que de los éxitos. Cuando algo sale como se esperaba, usamos ese proceso como una plantilla mental para futuros proyectos.

Somos usuarios de manuales y metodologías creemos que hemos establecido un patrón exitoso, incluso después de una sola instancia de éxito y esto, a su vez, tiende a transformarse en **"esta es la única forma de hacerlo".**

El verdadero aprendizaje llega a través de la crisis. Si algo sale mal, tenemos que revolver, experimentar, hackear, gritas y seguir nuestro proceso.



La cultura del éxito

(Un freno para la innovación)

"Nuestras mentes agitan las nuevas ideas, están más dispuestas a experimentar, están más abiertas a aportes externos cuando estamos en modo de crisis"



Incluso el fármaco relacionado con la famosa pastillita azul, la droga que más se vende en el mundo, no es usada con el propósito original. Comenzó originalmente para el tratamiento de angina de pecho, un problema cardíaco que afecta los vasos sanguíneos que llevan la sangre al corazón. **(¿Fallo épico o mente abierta para aprender y buscar nuevas aplicaciones?)**





En el libro de Demian Sterman nos muestra el camino del fracaso, el encanto y el aprendizaje que puede conllevar ir tras algo y no conseguirlo, la posibilidad incluso de encontrar algo más, algo distinto e inesperado. Henry Ford, Albert Einstein, Steve Jobs y hasta Walt Disney son algunos de los nombres y Historias de fracasos y fracasados que cambiaron el mundo

¿Se puede aprender del fracaso tan fácilmente?



¿Se puede aprender del fracaso tan fácilmente?

Nuestra opinión es que no se aprende de fracasar, **se aprende de superar los fracasos**. Y eso es muy difícil en organizaciones que tiene el fracaso como algo negativo en vez de pasos esenciales para conseguir una innovación exitosa.

Si quieres mejorar tras un fracaso y tienes poco tiempo porque te persigue el **"Time to Market"** podes seguir esta técnica rápida de autoevaluación mediante seis preguntas:

¿Qué puedo aprender?
¿Qué hubiera hecho diferente?
¿Qué competencias debo entrenar?
¿De quién puedo aprender?
¿Cuál es el próximo paso?
¿te esforzaste lo suficiente?



¿Se puede aprender del fracaso tan fácilmente?

1. Análisis. ¿Que puedo aprender de esto?

Responsabilízate de la parte que ha ido mal por ti. Quizá no todo ha sido culpa tuya pero quizá lo fue en parte. La gente con éxito no pone excusas ni culpa a los demás sino que se hacen cargo del asunto. Se crítico pero constructivo. Intenta analizar con objetividad. Haz una lista de las cuestiones clave de lo ocurrido y analiza la lista paso a paso para encontrar los puntos que puedan servirte de aprendizaje.

2. Alternativas. ¿Qué hubiese hecho de forma diferente?

¿Qué otras opciones tenías? ¿Qué decisiones tomaste? ¿Podrías haberlo hecho de modo diferente? Mirando con perspectiva, ¿qué pasos hubieses dado de modo diferente?



¿Se puede aprender del fracaso tan fácilmente?

3. Competencias. ¿Necesito aprender o mejorar mis habilidades?



¿El problema te ha hecho ver que no tienes las habilidades necesarias? ¿Cómo podrías mejorarlas? Quizá puedas contar con libros, algún curso o alguna persona que pueda ayudar. Prepara un plan de desarrollo para mejorar o adquirir las habilidades y experiencia que necesitas.

¿Se puede aprender del fracaso tan fácilmente?

4. Modelos. ¿De quién puedo aprender?



¿A quién podrías pedir asesoramiento? Si te ha visto algún jefe, algún colega de trabajo o algún amigo les puedes pedir feedback y orientación. Mucha gente no pide ayuda porque lo consideran un signo de debilidad más que una fortaleza. No es así, sino que muestra que estás dispuesto a aprender y cambiar. Algún buen amigo estará dispuesto a ayudar.

¿Se puede aprender del fracaso tan fácilmente?

5. Acción. ¿Cuál es el próximo paso? Elabora un plan.

¿Probarías algo nuevo o algo diferente? Revisa tus metas y objetivos. Esta inversión ha sido un revés en tu camino pero piensa que ha sido algo divertido en lugar de una interrupción. Ahora puedes centrar tu rumbo hacia el nuevo plan.



¿Se puede aprender del fracaso tan fácilmente?

6. Aceptación. ¿Te has esforzado lo suficiente y has aprendido lo necesario?

Si ambas respuestas son síes, significa que posiblemente has hecho lo que estaba en tu mano para conseguir el objetivo. Tal vez tienes que plantearte un reto más asequible, mejorar tu planificación, tus competencias y tus técnicas o darte el tiempo necesario para alcanzar esa meta.



¡Fracasar es bueno! ¡Falla rápido, falla barato!



Estas afirmaciones parecen extrañas, sobre todo en nuestra cultura: **la del éxito.** Sin embargo, equivocarse es un factor clave en varias etapas del **Design Thinking.** Podríamos decir que este método espera el fracaso, o como otros lo llaman el pre- fracaso. De los errores se aprende y en eso basa su apuesta este proceso

Fallamos rápido, fallamos a menudo y aprendemos a diario de forma continua.

¡Fracasar es bueno! ¡Falla rápido, falla barato!

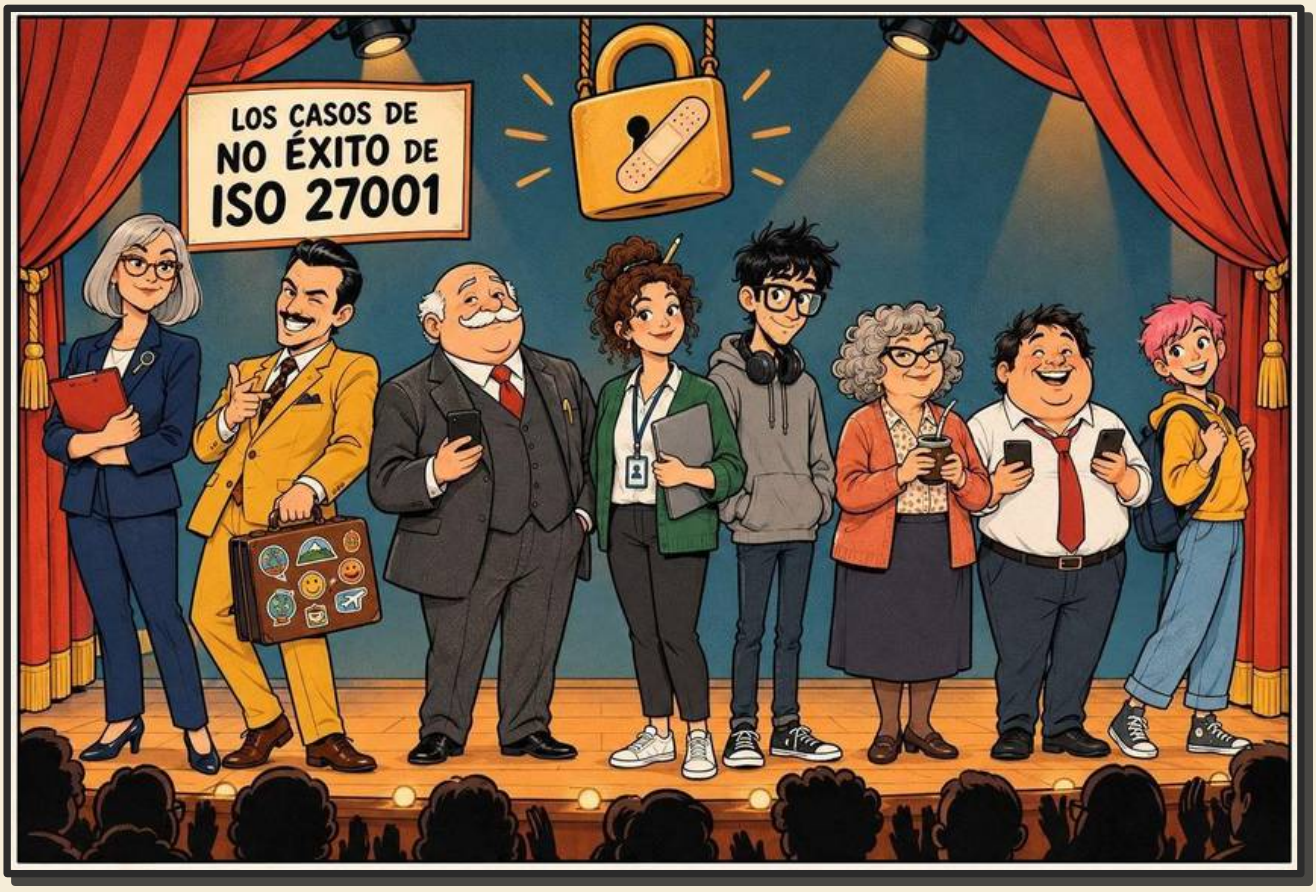
Si no fuéramos desafiados y no aprendiéramos, nuestros trabajos y nuestro trabajo serían extremadamente aburridos.

El fracaso no se debe ver como algo negativo, sino como pasos esenciales para conseguir una innovación exitosa.

Simplemente es experimentación y repetición constante. Es simple: ensayo y error, y así sucesivamente hasta dar con la solución adecuada. El tema del fracaso es una cuestión de enfoque, como lo dijo Winston Churchill **"El éxito es la capacidad de ir de fracaso en fracaso sin perder el entusiasmo".**



LOS CASOS DE NO ÉXITO DE ISO 27001



"LOS CASOS QUE VEREMOS EN EL E-BOOK SON REPRESENTATIVOS Y ESTÁN EN ALTO NIVEL, TAMBIÉN FUERON MODIFICADOS PARA NO EXPONER INFORMACIÓN SOBRE CLIENTES O CONOCIDOS"

CASO #1

EL CONSULTOR FANTASMA



UN ESPECTRO INVOCADO POR LA FRASE MÁGICA: "TENGO UN AMIGO QUE SABE DE ISO"

EL CONSULTOR FANTASMA

CASO #1

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Carlos Casper

Todo comenzó con una frase que suena inocente pero que puede costarle a una empresa miles de dólares y meses de trabajo: **"Tengo un amigo que sabe de ISO".** Así llegó Carlos a la Fintech Acelerada, una empresa con operaciones en cinco países y servicios críticos en la nube.

Sin un proceso de selección formal ni verificación de referencias, solo con la confianza de un contacto, Carlos se presentó con una promesa tan audaz como peligrosa: **"En dos meses están certificados"**.

El Inicio del Desastre

Carlos Casper, el "Consultor Fantasma", no se molestó en entender el contexto de la Fintech. Llegó con una carpeta que parecía haber sobrevivido a una inundación y un SGSI (Sistema de Gestión de Seguridad de la Información) genérico que había usado por última vez en una empresa de repuestos de maquinaria agrícola en 2007.

Su método era simple: copiar, pegar y cambiar logos.



EL CONSULTOR FANTASMA

CASO #1

La Obra Maestra del Absurdo (La Auditoría)

Cuando la auditora llegó para revisar la implementación, la farsa se desmoronó.



EL CONSULTOR FANTASMA

CASO #1

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? El caso de Carlos Gasper es un ejemplo de **"Gestión de Cumplimiento sin Gestión de Riesgos".** Las causas principales son:

- **Falta de Verificación (La Causa Raíz):** La empresa priorizó la velocidad y el bajo costo sobre la competencia, confiando en una referencia sin auditar su experiencia relevante (sectores y contextos similares).
- **Desconocimiento del Requisito de Contexto**: La empresa no entendió que la cláusula 4 de ISO 27001 (Contexto de la Organización) es fundamental. Un SGSI debe nacer de un entendimiento profundo de los activos y riesgos propios del negocio.
- **El Enfoque Checklist:** Se buscó una solución rápida para obtener el sello (el output), en lugar de una solución estratégica para ser seguro (el outcome).



EL CONSULTOR FANTASMA

CASO #1

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias Reales de la Implementación Fantasma
¨El rechazo de la certificación tuvo un efecto dominó¨:



ÁREA AFECTADA	CONSECUENCIA
Financiera	**Pérdida de Inversión:** Se malgastó dinero en consultoría y horas/hombre internas.
Operativa	**Retraso Estratégico:** Se perdieron meses. Hubo que rehacer el SGSI desde cero, duplicando el tiempo para obtener la certificación.
Recursos Humanos	**Frustración del Equipo:** El área de seguridad quedó desmotivada y se generó desconfianza hacia la iniciativa de la norma.
Negocio	**Exposición Real:** La empresa continuó operando bajo la falsa seguridad de una documentación que no protegía contra sus riesgos reales (fraude, pérdida de datos digitales).

LECCIONES APRENDIDAS

Un SGSI no se compra, se construye.
Elegí bien a tu consultor.



1 VERIFICÁ LA EXPERIENCIA RELEVANTE



No te conformes con **"ha certificado 10 empresas"**. Preguntá por tu industria, tus tecnologías y tus regulaciones.

2 PEDÍ REFERENCIAS



Llamá a **2 o 3 clientes anteriores** del consultor (en empresas parecidas) y preguntales **especificamente sobre la adaptación del SGSI.**

3 EXIGÍ PERSONALIZACIÓN DEL SGSI



El **Análisis de Riesgos debe ser una creación conjunta.** Si el consultor trae una matriz pre-llenada que no aplica a tu negocio, **encendé la alarma.**

4 INVOLUCRÁ AL NEGOCIO (NO ES UN PROYECTO DE IT)



Un buen consultor interactúa con la alta dirección y áreas clave (Legal, RR.HH., Operaciones) para definir el **Alcance y el Contexto.**

5 DESCONFIÁ DE LAS PROMESAS MILAGROSAS



La ISO 27001 **requiere un cambio** cultural y documentación adaptada. Es un proceso que toma tiempo (generalmente **6 a 12 meses**).



Si te prometen la certificación en dos semanas sin un análisis previo, te están vendiendo un sello de papel, no ssguridad real.

CASO #2

PLATAFORMAS MÁGICAS



CUANDO EL SGSI SE CONVIRTIÓ EN UN VIDEOJUEGO

PLATAFORMAS MÁGICAS

CASO #2

INTRODUCCIÓN Y DRAMATIZACIÓN:

Parecía que estaba ganando el juego de la seguridad.

Todo comenzó con una presentación deslumbrante, digna de un startup de Silicon Valley. El vendedor no hablaba de aburridos controles o normativas; hablaba de Inteligencia Artificial, Blockchain para "mayor seguridad" y dashboards futuristas con luces de colores.

Su promesa fue irresistible: "Con esta plataforma, la ISO se implementa sola. No necesitan consultores ni procesos complicados".

Seducida por la idea de **automatizar el cumplimiento con un solo clic**, la empresa pagó una fortuna, cargó sus datos y esperó el milagro.

El inicio del desastre

Lo que apareció en pantalla parecía más un videojuego que un Sistema de Gestión de Seguridad de la Información (SGSI):

Pantallas hermosas llenas de gráficos.

Alertas automáticas que parpadeaban en verde.

Pasaron los meses y nadie en la empresa volvió a hablar de seguridad.



Un "chatbot" que respondía:

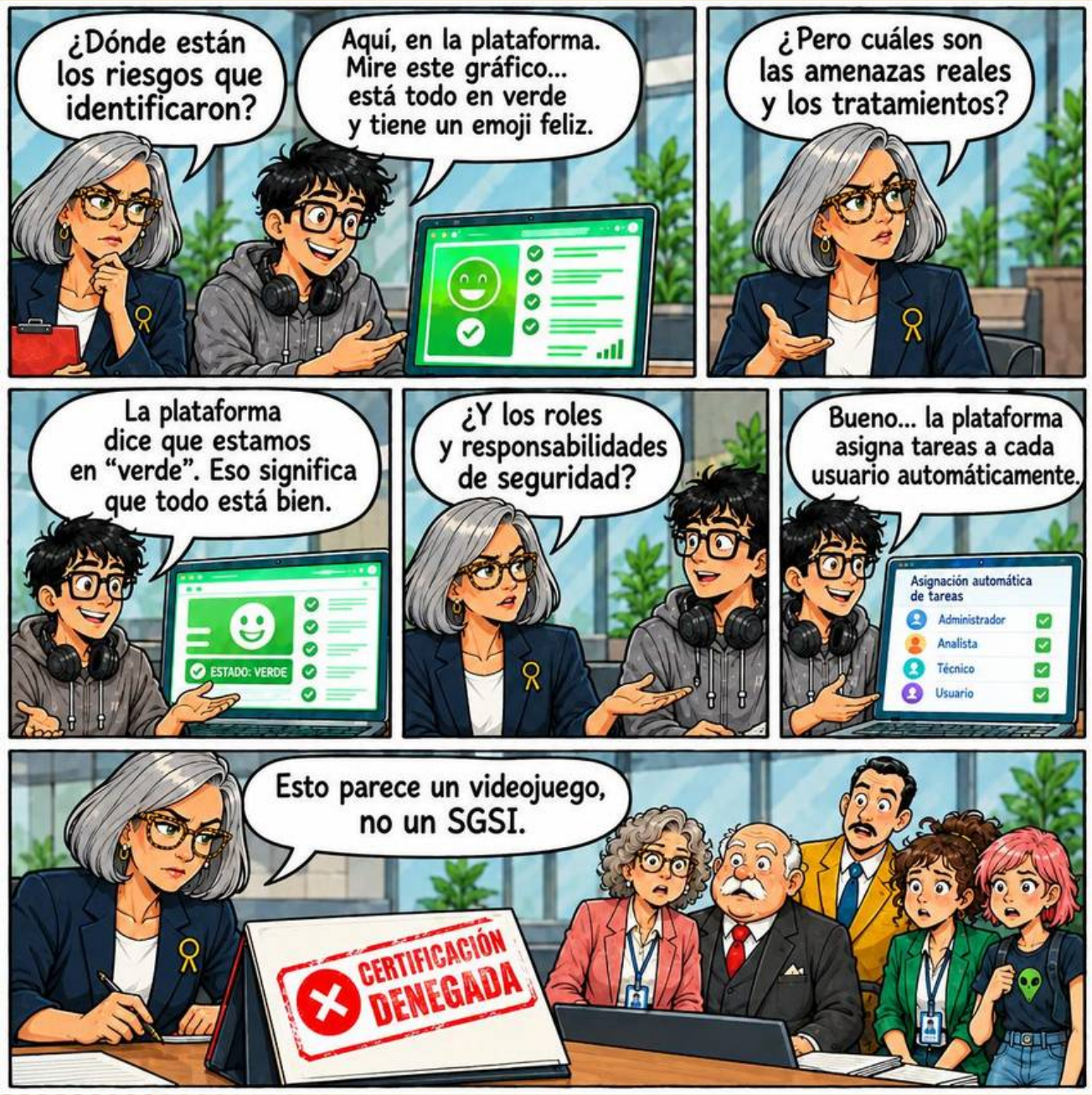
"¡Felicidades! Estás cumpliendo con ISO 27001".

PLATAFORMAS MÁGICAS

CASO #2

La plataforma enviaba correos automáticos que todos archivaban. El dashboard siempre estaba en verde, así que todos asumieron que estaban protegidos.

El problema fue que, detrás de los colores, no había sustancia. Cuando llegó el día de la auditoría, el intercambio fue surrealista:



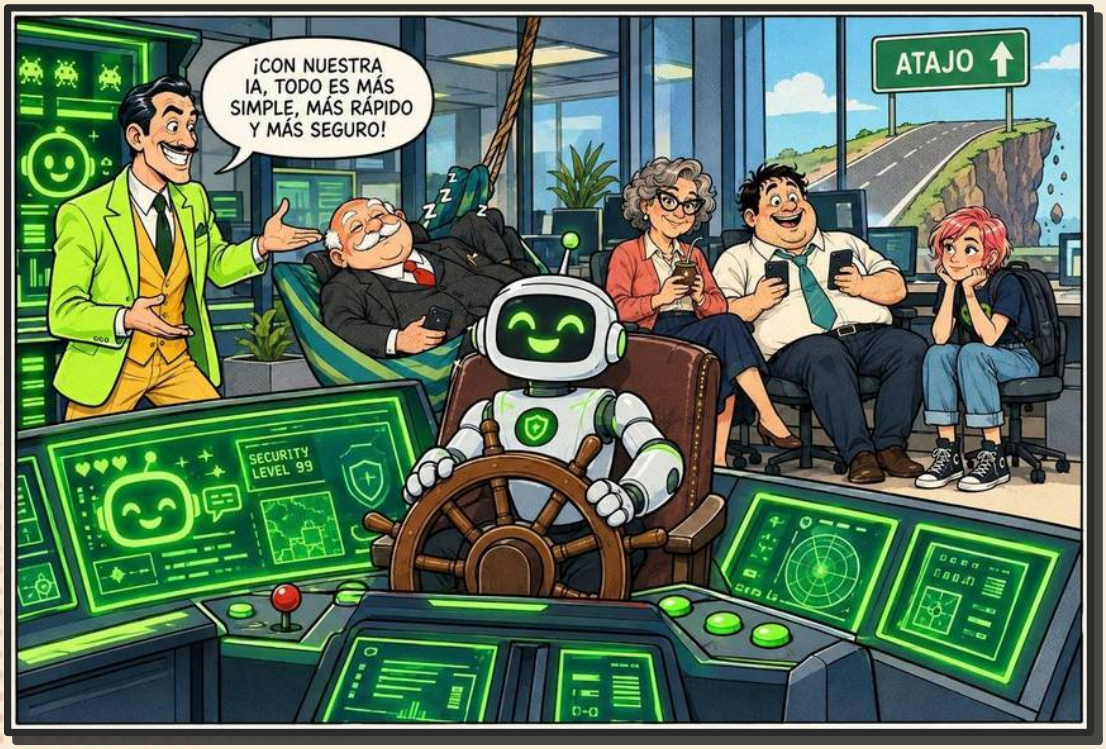
PLATAFORMAS MÁGICAS

CASO #2

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Este fallo épico ocurre por la creencia errónea de que la tecnología puede sustituir el criterio humano y la cultura organizacional. Las causas principales detectadas son:

- **Dependencia excesiva en la tecnología:** Se asume que una herramienta resolverá por sí sola la gestión de riesgos y la cultura de seguridad.
- **Falta de procesos reales:** No se definieron roles, responsabilidades ni flujos de trabajo internos; se delegó todo al algoritmo del software.
- **Ausencia de cultura organizacional:** La plataforma no capacitó al personal; solo generó documentos automáticos que nadie leía ni entendía.
- **Búsqueda de atajos:** La dirección priorizó la rapidez de una "solución enlatada" sobre la construcción de un sistema sólido.



PLATAFORMAS MÁGICAS

CASO #2

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales de la "Magia“

¨El resultado final fue un colapso absoluto de la estrategia de certificación¨:



ÁREA AFECTADA	CONSECUENCIA
Auditoría fallida:	El SGSI fue calificado como un adorno digital sin impacto real en la seguridad de la empresa.
Pérdida de credibilidad:	La reputación del área de seguridad frente a la dirección y los auditores se desplomó.
Desperdicio de recursos:	Se perdió una inversión masiva de dinero y meses de configuración en una herramienta que no sirvió para el propósito.
Frustración interna:	El equipo sintió que trabajó para alimentar un software, no para proteger la información.



LECCIONES APRENDIDAS

ISO 27001: MÁS QUE UNA HERRAMIENTA, ES UN COMPROMISO DE TODOS

1 LA TECNOLOGÍA ES SOPORTE, NO LA SOLUCIÓN

Ninguna plataforma reemplaza el análisis de riesgos humano ni la gestión del cambio cultural.



2 EVALÚA ANTES DE COMPRAR

Pregunta si la herramienta es personalizable, si cumple realmente con los requisitos de la norma y si se adapta a tu realidad, no a un modelo genérico.



3 PRIORIZA PROCESOS Y PERSONAS

La ISO 27001 se basa en cultura y compromiso. Primero define quién hace qué y cómo, luego busca software que lo facilite.



4 INTEGRA LA HERRAMIENTA EN UN SGSI SÓLIDO

Primero construye tu base (políticas, análisis de riesgos real), y recién después suma la tecnologia para optimizar y automatizar procesos ya existentes.



5 DESCONFÍA DE PROMESAS MÁGICAS

Si alguien te dice que la certificación se logra "con un clic" o sin involucrar al personal, es momento de cerrar la presentación y retirarse.



CASO
3

TIEMPOS RÉCORD



CUANDO LA ISO SE CONVIRTIÓ EN UNA CARRERA CONTRA EL RELOJ

TIEMPOS RÉCORD

CASO # 3

INTRODUCCIÓN Y DRAMATIZACIÓN:

La Maratón Imposible (Introducción y Dramatización)

Todo comenzó en una reunión de "prioridad máxima" convocada por el CEO. Con el peso de un contrato millonario en juego, la instrucción fue tajante:

"Necesitamos la certificación ISO 27001 en 30 días para cerrar con este cliente". ¿Cuánto tardamos? ¿Una semana?"

Mientras el equipo de seguridad guardaba un silencio tenso, el consultor externo, temiendo perder el negocio, aceptó el desafío sin pestañear: **"Claro, se puede".**

Lo que siguió no fue la construcción de un Sistema de Gestión de Seguridad de la Información (SGSI), sino una carrera frenética por llenar plantillas y generar documentos para "cumplir" con el papel, omitiendo cualquier validación real.
Bajo una presión asfixiante, el equipo trabajó día y noche copiando políticas de internet y redactando procedimientos sin aplicarlos a la realidad de la empresa.



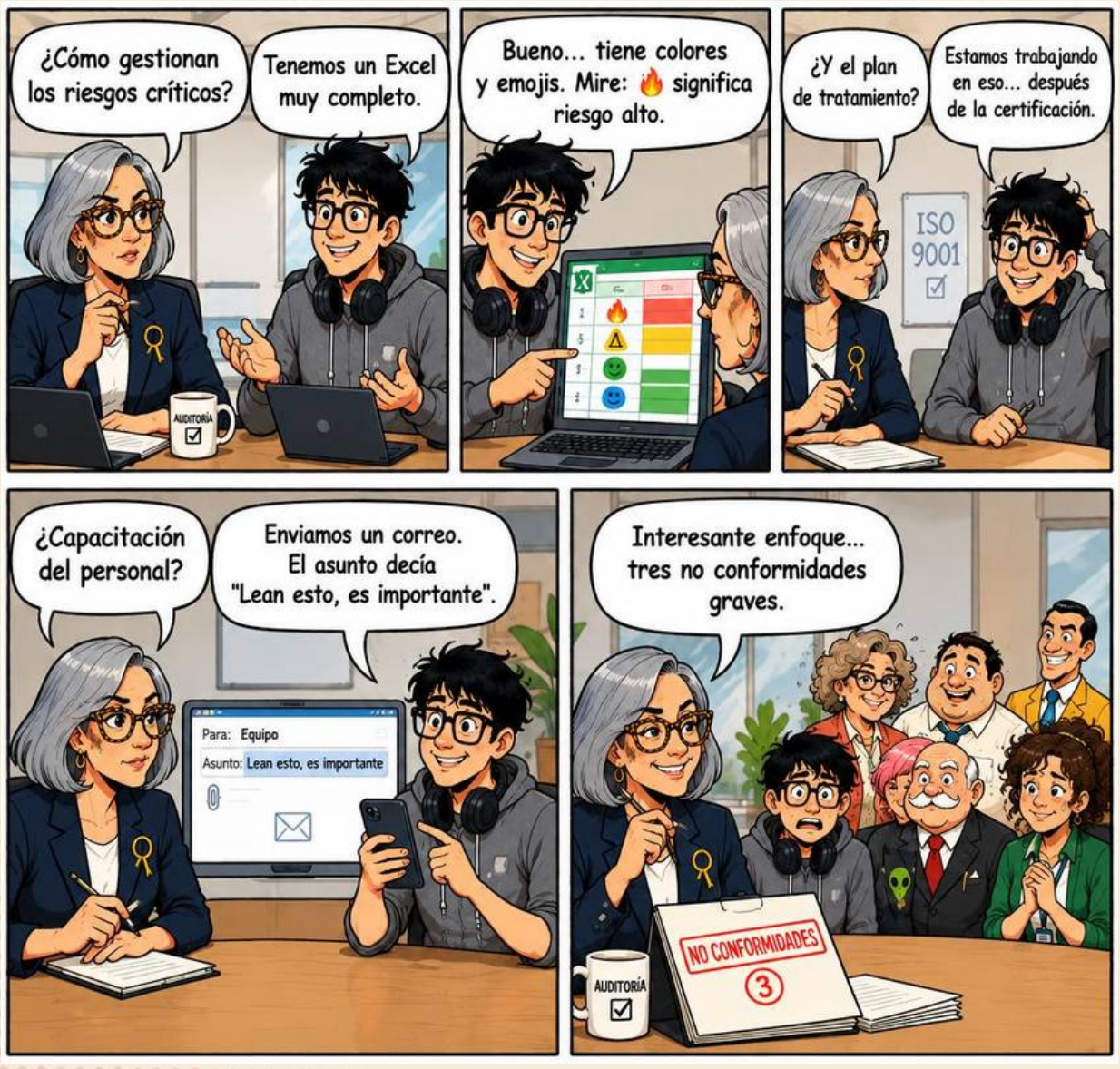
TIEMPOS RÉCORD

CASO # 3

La joya de la corona fue el análisis de riesgos: una tabla de Excel donde la severidad se medía con emojis: 🔥 para riesgos altos y 🌱 para riesgos bajos.

La capacitación obligatoria para todo el personal se despachó con un simple correo electrónico cuyo asunto era: **"Lean esto, es importante".**

El día de la verdad llegó con la auditoría.



TIEMPOS RÉCORD

CASO # 3

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Este fallo épico nace de una premisa errónea: tratar la seguridad de la información como un trámite administrativo veloz en lugar de un proceso de madurez organizacional. Las causas principales detectadas son:

- **Plazos irrealistas:** La exigencia de obtener una certificación en semanas ignora que un SGSI robusto no se puede implementar en ese tiempo.
- **Miedo al conflicto comercial:** Consultores que aceptan plazos imposibles por temor a perder el contrato o el favor de la dirección.
- **Omisión de etapas críticas:** Se sacrifican fases vitales como la formación, la concienciación del personal y la gestión del cambio en favor de la velocidad.
- **Documentación superficial:** Se prioriza el volumen de papeles sobre la aplicabilidad y el sustento real de las políticas.



TIEMPOS RÉCORD

CASO # 3

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales "El Costo de la Prisa "
¨Intentar tomar un atajo en la ISO 27001 suele terminar en un camino mucho más largo y costoso.¨:



ÁREA AFECTADA	CONSECUENCIA
Auditoría fallida:	El SGSI fue rechazado de inmediato por su falta de profundidad y coherencia.
Impacto en el negocio:	La empresa perdió el contrato que tanto ansiaba al no poder demostrar una seguridad real ante el cliente.
Pérdida de recursos:	Se malgastó tiempo valioso del personal y dinero en consultoría para obtener un producto sin valor.
Daño reputacional e interno:	El equipo de seguridad quedó desmotivado y la reputación del área ante la dirección y los empleados se desplomó.

LECCIONES APRENDIDAS

La ISO 27001 es una maratón de madurez, no una carrera de 100 metros llanos.

Para evitar este desastre, sigue estas recomendaciones:

ISO 27001

1 Planifica con tiempos realistas

Un SGSI sólido requiere meses de trabajo, planificación y adaptación, no semanas.

MESES

ANÁLISIS
RIESGOS
CONTROLES
AUDITORÍAS

SGSI

2 Educa a la alta dirección

Es fundamental explicar que la certificación no es solo un sello, sino un proceso de protección del negocio que requiere tiempo.

ISO 27001

- Protege activos
- Reduce riesgos
- Genera confianza
- Sostiene el negocio

3 Prioriza la calidad

Es preferible una implementación gradual y bien hecha que un "parche" rápido que no resistirá una auditoría seria.

PARCHE RÁPIDO

IMPLEMENTACIÓN GRADUAL Y ROBUSTA

4 Define hitos claros

Asegúrate de cumplir etapas como el análisis de contexto, riesgos, controles y auditorías internas antes de presentarte a la certificación.

HITOS DEL SGSI

1. Análisis de contexto
2. Gestión de riesgos
3. Implementación de controles
4. Auditorías internas
5. Revisión y certificación

5 Negocia el alcance

Si la presión comercial es extrema, es mejor certificar un alcance parcial de manera robusta que intentar cubrir toda la organización de forma superficial.

Primero lo esencial, con calidad.

ALCANCE

- [x] Fase 1: Crítico
- [ ] Fase 2: Departamentos
- [ ] Fase 3: Toda la organización

LA ISO 27001 NO ES UN DESTINO, ES UN CAMINO SEGURO HACIA UN NEGOCIO MÁS FUERTE.

CASO #4

DOCUMENTITIS AGUDA



CUANDO HACER DOCUMENTOS SE CONVIRTIÓ EN DEPORTE OLÍMPICO

DOCUMENTITIS AGUDA

CASO
#4



La empresa pensó que más documentos = más seguridad.

Generaron 20.000 páginas de políticas, procedimientos y anexos. Nadie los leyó.



DOCUMENTITIS AGUDA

CASO
#4

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Sofía Papeles

Todo comenzó con una intención noble: "Vamos a documentar TODO". Así arrancó Sofía en la empresa Servicios Digitales SA. Su lema era: "Si no está escrito, no existe". Y así se lanzó a redactar manuales, procedimientos, políticas, instructivos, formularios y subformularios. En seis meses había producido 187 documentos, 23 anexos y 4 manuales encuadernados con tapa dura.



El inicio del desastre: nadie en la organización había leído ninguno. Los empleados seguían trabajando como siempre, pero ahora con la sensación de que "hay un procedimiento para eso, pero no sé dónde está". Sofía estaba orgullosa de su biblioteca; nadie más entendía qué hacía.



DOCUMENTITIS AGUDA

CASO #4

La Obra Maestra del Absurdo (La Auditoría)

Cuando la auditora llegó, Sofía orgullosamente le presentó 12 carpetas con "toda la documentación SGSI". la auditora abrió la primera al azar.

El Contexto: La política de uso de contraseñas tenía 23 páginas y contradecía la política general de seguridad (también de 23 páginas). Los empleados, consultados, dijeron que usaban Excel para guardar las contraseñas. El Análisis: Cada control tenía un procedimiento, un sub-procedimiento, un manual y un formulario de evidencia. Nadie sabía qué documento aplicaba.



DOCUMENTITIS AGUDA

CASO
#4

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es un ejemplo clásico de "Cumplimiento sin Operación". Las causas principales son:

- **Confusión entre forma y fondo (La Causa Raíz):** Se interpretó que "documentar" es el objetivo del SGSI cuando en realidad es solo un medio para que las cosas se hagan de forma consistente.
- **Falta de criterio de utilidad**: Cada problema se "resolvió" con un documento nuevo en lugar de evaluar si ya existía algo aplicable o si el documento iba a ser realmente usado.
- **Burocracia defensiva:** Cuanto más papel, menos espacio para que la auditora encuentre algo, o eso pensaban. El resultado fue lo contrario: encontró mucho más.



DOCUMENTITIS AGUDA

CASO
#4

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Documentitis Aguda

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Empleados confundidos: no saben qué procedimiento aplica ni dónde encontrarlo. La documentación se vuelve inútil.
Financiera	Costo enorme de horas-persona en redactar, revisar y aprobar documentos que nadie lee. Costo de mantenimiento permanente.
Cultural	El SGSI pasa a ser sinónimo de "papelerío inútil" para el resto de la organización. Se pierde credibilidad para futuras iniciativas.
Auditoría	Hallazgos por inconsistencias entre documentos, versiones contradictorias coexistiendo y desconexión documento-realidad.

Lecciones aprendidas

No se trata de tener más documentos, sino de tener los correctos.

Menos ruido, más valor.

1 Aplicá la regla del 80/20.

El 20% de los documentos debe servir para el 80% de las situaciones.
Lo demás es ruido.



2 Hacé pruebas de uso real.

¿Un empleado nuevo encuentra y entiende el procedimiento que necesita en menos de 5 minutos?
Si no, el documento falló.



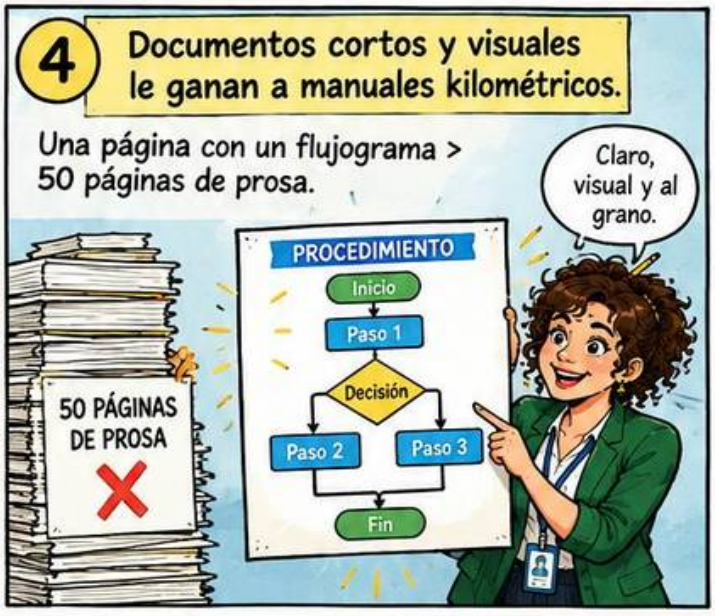
3 Establecé un proceso de revisión y poda anual.

Lo que no se usó en 12 meses, se elimina o consolida.
Sin culpa.



4 Documentos cortos y visuales le ganan a manuales kilométricos.

Una página con un flujograma > 50 páginas de prosa.



Recordá:

La ISO 27001 pide "información documentada", no "toneladas de papel".

Documentá lo que TIENE que existir para que el SGSI funcione, no lo que sería lindo tener.



CASO #5

SEGURIDAD VS. PRODUCTIVIDAD



CUANDO BLINDAR LA EMPRESA LA DEJÓ INMOVILIZADA

SEGURIDAD VS. PRODUCTIVIDAD

CASO
#5

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso CISO Murallas

Sofia llegó al puesto de CISO de TechCorp con una misión clara: "Cero incidentes". Su filosofía era simple: si bloqueamos todo, nada malo puede pasar. Procedente del mundo militar, aplicó controles con mano de hierro: USB bloqueados, sitios web filtrados, correos cifrados con tres capas, doble factor para entrar a la impresora. El inicio del desastre: a los 3 meses, los empleados habían encontrado workarounds para todo. Las ventas se hacían por WhatsApp personal, los archivos se compartían por correos personales, y el área de finanzas usaba Dropbox personal porque "el sistema corporativo no permite enviar adjuntos".

El método de trabajo: Su método era simple: ante cada riesgo identificado, agregar un control restrictivo. Si el control molesto, mejor: significa que está funcionando.



SEGURIDAD VS. PRODUCTIVIDAD

CASO #5

La Obra Maestra del Absurdo (La Auditoría)

la auditora entró a entrevistar a los empleados para validar la efectividad de los controles. La realidad superó cualquier ficción.

El Contexto: Sofía presentó una matriz con 247 controles implementados, todos en estado "verde". El Análisis: Al entrevistar a los empleados, la auditora descubrió que el 70% de la información sensible circulaba por canales no autorizados. Las restricciones técnicas eran reales, pero las personas las habían evitado completamente.



SEGURIDAD VS. PRODUCTIVIDAD

CASO
#5

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el ejemplo perfecto de "Seguridad sin Usabilidad". Las causas principales son:

- **Falta de equilibrio riesgo-impacto:** No se midió el impacto operativo de los controles. La pregunta nunca fue "¿este control vale la pena?" sino "¿este control me protege?".

- **Diseño sin involucrar a los usuarios**: Los controles se diseñaron en una sala cerrada por el equipo de seguridad, sin consultar cómo trabajan realmente las áreas de negocio.

- **Cultura de imposición:** El SGSI se vivió como castigo en lugar de habilitador. Los empleados pasaron a ver a Seguridad como "el enemigo" y no como un socio.



SEGURIDAD VS. PRODUCTIVIDAD

CASO #5

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Seguridad vs. Productividad

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Aparición masiva de Shadow IT: empleados usando sus propios sistemas y dispositivos para hacer su trabajo. Los controles oficiales se vuelven decorativos.
Productividad	Caída medible de la productividad: tareas que antes tomaban minutos ahora toman horas. Frustración crónica del equipo.
Talento	Renuncias de empleados clave que no toleran la fricción operativa. Dificultad para retener perfiles técnicos.
Seguridad real	La superficie de ataque se EXPANDIÓ: ahora la información circula por canales personales, sin monitoreo ni control corporativo.



1 Trabajá CON el negocio, no CONTRA el negocio.

Cocreá los controles con quienes los van a sufrir. La mejor matriz de riesgos surge de entrevistar a las áreas operativas.



2 Hacé pilotos antes de lanzar controles masivos.

Medí el impacto operativo real durante 30 días antes de imponerlo a toda la empresa.



3 Aplicá enfoque de riesgo real.

¿El control mitiga un riesgo concreto o solo te hace sentir más seguro? Si la respuesta es la segunda, no lo implementes.



4 Capacitá en alternatives.

Si bloqueás USBs, ofrecé al equipo una forma cifrada de compartir archivos QUE FUNCIONE.
Si no, van a usar pendrives personales.



5 Medí adopción y satisfacción.

Encuestas trimestrales al equipo sobre los controles. Si todos los odian, algo está fallando.



CASO #6

AUDITORÍA INTERNA DIY



"YO ME AUDITO SOLO, SOY MUY EFICIENTE"

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Sofia Auto auditora

Sofia era la responsable del SGSI en Consultora SA. Cuando llegó el momento de hacer la auditoría interna (requisito obligatorio de ISO 27001), la dirección le dijo: “Sofia, vos sos la que más sabe del tema, hacela vos. Total, ya conocés todo". Sofia aceptó, orgullosa. Se sentó tres tardes a revisar SUS PROPIOS DOCUMENTOS, SUS PROPIAS POLÍTICAS, SUS PROPIOS REGISTROS. El inicio del desastre: "sorprendentemente", no encontró ninguna no conformidad. El informe final tenía tres palabras: "Todo está bien".

El método de trabajo: Su método era simple: si yo diseñé el control y yo lo audito, claramente está bien. Es lógica pura.



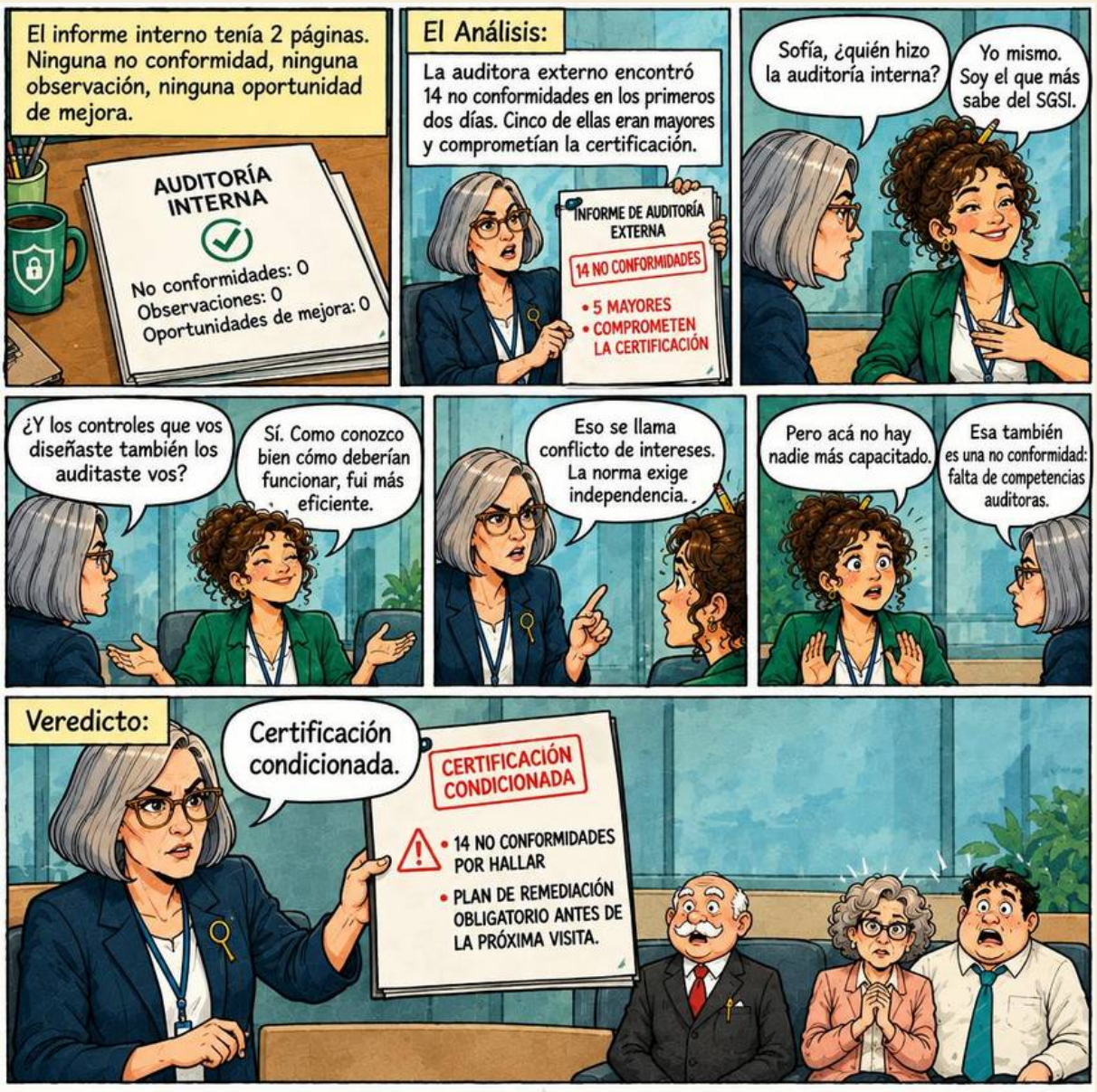
AUDITORÍA INTERNA DIY

CASO #6

La Obra Maestra del Absurdo (La Auditoría)

Cuando llegó la auditora externa de certificación, lo primero que pidió fue el informe de auditoría interna. Federico se lo entregó con orgullo.

El Contexto: El informe interno tenía 2 páginas. Ninguna no conformidad, ninguna observación, ninguna oportunidad de mejora. El Análisis: La auditora externa encontró 14 no conformidades en los primeros dos días. Cinco de ellas eran mayores y comprometían la certificación.



ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el ejemplo clásico de "Auditoría sin Independencia". Las causas principales son:

- **Falta de independencia (La Causa Raíz):** La norma exige que la auditora sea independiente del proceso auditado. Si Federico diseñó y operó los controles, no puede ser quien los evalúe objetivamente.

- **Subestimación del rol auditor**: Se confundió "conocer el SGSI" con "saber auditar". Son competencias diferentes que requieren formación específica.

- **Ahorro mal entendido:** Se prefirió no contratar auditor externo o capacitar a otro empleado, en aras de "ahorrar". El costo final fue muchísimo mayor.



AUDITORÍA INTERNA DIY

CASO #6

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Auditoría Interna DIY

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Certificación	Riesgo de pérdida o suspensión de la certificación. Las no conformidades mayores deben resolverse antes del próximo ciclo.
Operativa	Hallazgos críticos que pasaron inadvertidos hasta la auditoría externa. Acciones correctivas masivas a contrarreloj.
Credibilidad	Pérdida de confianza interna en el SGSI: "si el informe interno decía que todo está bien, ¿cómo creemos en los próximos?".
Costos	Costos de reauditoría externa, capacitación urgente de auditores internos, horas-persona en remediación. Muy superior al ahorro inicial.

Lecciones aprendidas

1 Separá auditor y auditado: si Juan diseñó el control, Pedro lo audita. Y viceversa. La norma es clara en esto.



2 Capacitá auditores con cursos certificados (IRCA, ISO 19011, AENOR). Una auditoría interna mal hecha vale menos que ninguna.



3 Si no tenés gente formada, contratá auditor externo para la auditoría interna. Es legítimo, válido para la norma y mucho más útil.



4 Cambiá auditores cada cierto tiempo: ojos nuevos encuentran cosas que los viejos ya no ven por costumbre.



5 La auditoría interna no es un trámite: es una oportunidad de detectar problemas ANTES de que lo haga el auditor externo (o peor, un incidente real).



CASO #7

SGSI FRANKENSTEIN



"BUSQUEMOS SGSI EN GOOGLE Y ARMAMOS UNO CON LO MEJOR DE CADA UNO"

SGSI FRANKENSTEIN

CASO
#7

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Sofía Plantillas

Sofia tenía que armar el SGSI de Industria Manufacturera ABC, pero el presupuesto era ajustado y el tiempo apretado. Pidió plantillas a tres colegas, descargó políticas de internet y armó un "compilado". El inicio del desastre: la política de seguridad mencionaba "estudiantes y profesores" (era de una universidad), el procedimiento de incidentes hablaba de "pasajeros y rutas" (venía de una empresa de transporte), y el plan de continuidad mencionaba "productos frescos" (era de una panadería). Sofía hizo lo posible: buscó y reemplazó las palabras obvias. Pero quedaron 137 menciones a contextos ajenos.

El método de trabajo: Su método era simple: copy-paste y replace. Total, las ISOs son todas iguales, ¿no? Solo cambian los nombres.



SGSI FRANKENSTEIN

CASO
#7

La Obra Maestra del Absurdo (La Auditoría)

la auditora abrió la documentación al azar y empezó a leer. A los 30 segundos ya tenía la primera observación. A los 5 minutos, había llenado dos páginas.

El Contexto: La política decía "los profesores deben asegurar el material académico". El procedimiento de incidentes hablaba de "reportar al jefe de ruta". La declaración de aplicabilidad mencionaba controles que no eran de una manufactura.

El Análisis: Piezas de SGSIs ajenos sin contexto. **Era un Frankenstein corporativo.**



SGSI FRANKENSTEIN

CASO #7

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es un clásico de "SGSI Copiado vs SGSI Vivido". Las causas principales son:

- **Falta de comprensión del concepto de contexto:** La cláusula 4 de ISO 27001 es taxativa: el SGSI debe nacer del entendimiento del CONTEXTO específico de la organización. No es transferible.
- **Presupuesto y tiempo mal asignados**: Se asumió que armar un SGSI es trabajo de pegar plantillas. En realidad, requiere análisis, entrevistas, comprensión del negocio.
- **Falta de validación con áreas internas:** Si Sofía hubiera leído los documentos junto con los gerentes de áreas, cualquiera habría notado las inconsistencias inmediatamente.



SGSI FRANKENSTEIN

CASO #7

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — SGSI Frankenstein

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Auditoría	Múltiples no conformidades por inadecuación al contexto. Imposibilidad de certificar hasta rehacer la base documental.
Operativa	Empleados confundidos: los procedimientos no se aplican a su realidad. Termina trabajándose "como siempre" mientras los documentos viven en otra dimensión.
Riesgos reales no identificados	El análisis de riesgos copiado de otras industrias no contempla los riesgos REALES de la organización. Lo importante queda sin tratar.
Tiempo perdido	3-6 meses de trabajo que después hay que rehacer desde cero. Más caro que haber arrancado bien.

LECCIONES APRENDIDAS

No es teoría, es experiencia. Estas son las claves para que el SGSI realmente funcione en tu organización.

Mejores procesos. Menos riesgos. Más valor.

1 LAS PLANTILLAS SON PUNTO DE PARTIDA, NO DESTINO.

Adaptalas a la realidad de TU organización, palabra por palabra.

- ✓ PROCESOS
- ✓ ROLES
- ✓ CONTEXTO
- ✓ NEGOCIO

La plantilla te guía, pero la realidad de tu organización es única.

PLANTILLA SGSI

TU VERSIÓN REAL

- ✓ PROCESOS
- ✓ ROLES
- ✓ CONTEXTO
- ✓ NEGOCIO

2 VALIDÁ CADA DOCUMENTO CON LAS ÁREAS AFECTADAS ANTES DE APROBARLO.

Si el responsable de operaciones no se reconoce en el procedimiento, hay que rehacerlo.

- ✓ PARTICIPACIÓN
- ✓ CONSENSO
- ✓ APROBACIÓN REAL

Revisemos juntos antes de aprobar.

OPERACIONES | RRHH | FINANZAS | LEGAL

3 HACÉ UN MAPA DE PROCESOS REAL PRIMERO, DESPUÉS DOCUMENTÁ SOBRE ESO. No al revés.

Primero entendemos cómo trabajamos. Después lo documentamos.

MAPA DE PROCESOS REAL

ESTRATÉGICOS

OPERATIVOS

SOPORTE

DOCUMENTACIÓN SGSI

4 SI TE TIENTA EL COPY-PASTE, PARATE Y PREGUNTATE:

"¿Esto refleja cómo trabajamos realmente?"

Si la respuesta es "no estoy seguro", consultá.

COPY-PASTE

SIN CONSULTAR = RIESGO

CONSULTAR = SOLUCIONES REALES

5 INVERTÍ EN ENTREVISTAS:

1 hora con cada gerente de área te ahorra meses de retrabajo posterior.

Y produce un SGSI que realmente funciona.

Una hora de conversación vale más que 100 correos.

- ✓ MEJOR ENTENDIMIENTO
- ✓ DOCUMENTACIÓN REAL
- ✓ MENOS RE-TRABAJO
- ✓ UN SGSI EFECTIVO

JUNTOS ES MEJOR

EL SGSI NO ES SOLO DOCUMENTACIÓN, ES UNA CONSTRUCCIÓN COLECTIVA.

¡HACÉ QUE FUNCIONE EN TU REALIDAD!

CASO #8

ALTA DIRECCIÓN AUSENTE



CUANDO EL CEO SE FUE AL RETIRO ESPIRITUAL Y NUNCA VOLVIÓ

"¿ISO QUÉ? YO SOLO FIRMO COSAS"

ALTA DIRECCIÓN AUSENTE

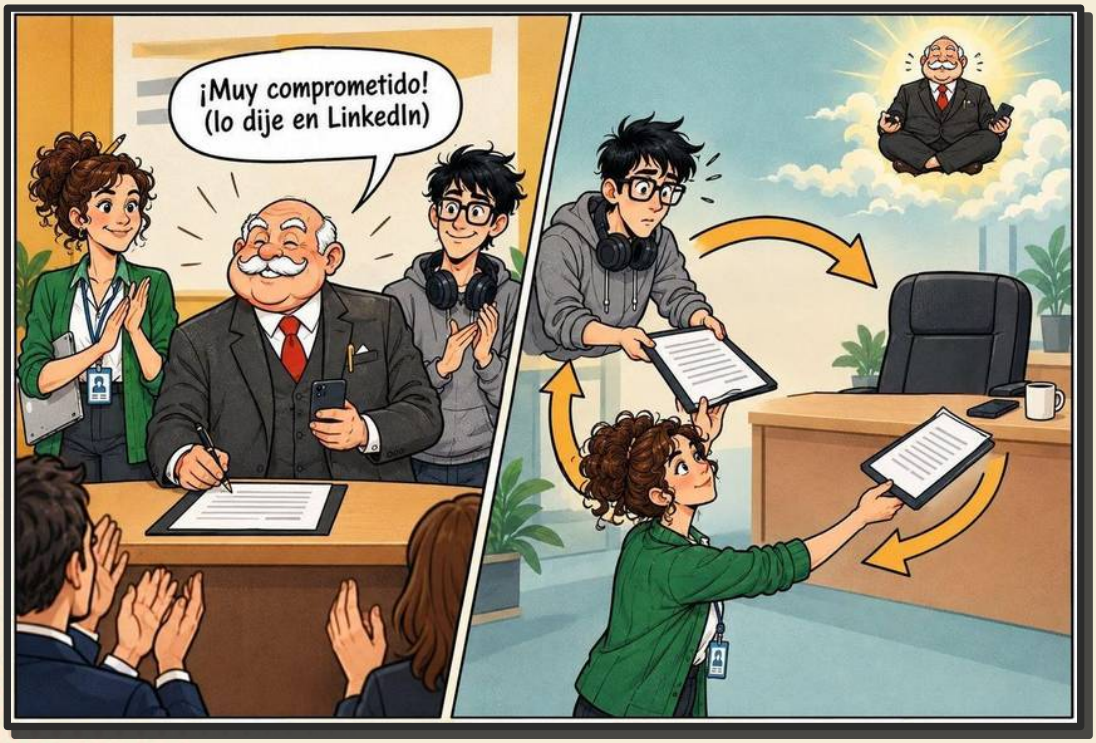
CASO
#8

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso CEO Buda

En Empresa Tradicional SA, el CEO firmó la política de seguridad con entusiasmo en el kick-off del proyecto SGSI. Sonrieron las fotos, salió en LinkedIn, hubo aplausos. Después... silencio. El inicio del desastre: el Comité de Seguridad se reunió una vez en mes 1, una vez en mes 3, y después "se reagendó indefinidamente". El CEO delegó "todo el tema técnico" en el responsable de IT, quien delegó en Nacho el responsable de seguridad, quien necesitaba aprobaciones del CEO para avanzar. Bucle infinito. Mientras tanto, el SGSI esperaba decisiones críticas: presupuesto para herramientas, autorización para política de teletrabajo, validación del plan de continuidad.

El método de trabajo: Su método era simple: confiar en que "los expertos" iban a resolver todo. La seguridad de la información es algo técnico, no estratégico.



ALTA DIRECCIÓN AUSENTE

CASO #8

La Obra Maestra del Absurdo (La Auditoría)

La auditora solicitó las actas del Comité de Seguridad y las evidencias de revisión por la dirección. Lo que recibió fue inolvidable.

El Contexto: Un acta del Comité, fechada al inicio del proyecto. Sin firmas. Una "revisión por la dirección" registrada como "reunión de pasillo de 5 minutos" entre Sofía la responsable de SGSI y el CFO. El Análisis: Liderazgo y compromiso de la dirección era prácticamente inexistente, contradiciendo el requisito explícito de la cláusula 5.1 de la norma.



ALTA DIRECCIÓN AUSENTE

CASO
#8

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el origen de la mayoría de los fracasos de SGSI. Las causas principales son:

- **Delegación mal entendida (La Causa Raíz):** La dirección entendió que "liderar" es "firmar el inicio y delegar el resto". La norma exige un liderazgo activo, visible y permanente.
- **Percepción del SGSI como tema técnico**: Mientras la dirección lo viva como "tema de IT", no le va a dedicar tiempo. El cambio requiere que se entienda como tema estratégico/empresarial.
- **Falta de visibilidad de las consecuencias:** Nadie tradujo al lenguaje del CEO qué pasa si NO se involucra: pérdida de contratos, sanciones, daño reputacional. Sin eso, la seguridad compite con todo lo demás.



ALTA DIRECCIÓN AUSENTE

CASO
#8

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Alta Dirección Ausente

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Decisiones críticas paralizadas durante meses. Recursos insuficientes para implementar y mantener controles.
Cultural	El equipo de seguridad pierde autoridad frente al resto. "Si el jefe no lo prioriza, ¿para qué lo prioriza nadie?".
Estratégica	El SGSI queda "huérfano" sin guía. Las inversiones se hacen por inercia, no por estrategia de riesgo.
Certificación	Riesgo de no obtener o perder la certificación. La auditoría externa lo detecta inmediatamente.

LECCIONES APRENDIDAS

Estas son las claves para que la dirección entienda el valor y se involucre de verdad.

Seguridad con propósito, no solo con procesos.

1 MOSTRÁ LOS RIESGOS EN SU LENGUAJE.

La dirección necesita entender qué está en juego. No hables de "controles del Anexo A". Habla de lo que realmente les importa.

Si no reforzamos la seguridad, podemos tener: dinero perdido, contratos en peligro, regulaciones aplicables y daño a la reputación.

- DINERO PERDIDO
- CONTRATOS EN PELIGRO
- REGULACIONES APLICABLES
- REPUTACIÓN

2 PEDÍ COMPROMISOS FORMALES Y MEDIBLES.

Que quede claro, por escrito, con presupuesto, agenda y KPIs. Sin ambigüedades.

COMPROMISOS

- ☑ Presupuesto anual de seguridad
- ☑ Agenda trimestral del Comité de Seguridad
- ☑ KPIs reportados a la dirección
- ☐ _____

Escrito. Medible. Con fecha.

3 LLEVÁ LA SEGURIDAD AL COMITÉ EJECUTIVO.

No es un tema aparte. Debe ser una agenda permanente del board.

La ciberseguridad y la gestión de riesgos son parte del negocio. Deben estar siempre en la agenda del Comité Eyecutivo.

COMITÉ EJECUTIVO

- ☑ Estrategia
- ☑ Riesgos
- ☑ Seguridad de la información
- ☑ Resultados del negocio

4 SI LA DIRECCIÓN NO SE INVOLUCRA DESPUÉS DE 6 MESES...

Revisá si tiene sentido seguir invirtiendo en el SGSi o si vas a generar uno de papel.

6 MESES

Si después de 6 meses no hay pedidos formales no hay involucramiento...

¿Estamos realmente construyendo seguridad o solo un documento para la foto?

SGSI DE PAPEL
= Sin impacto real

SGSI CON APOYO
= Protección, valor y resultados

5 DOCUMENTÁ LOS INTENTOS.

Guardá todo: emails enviados. actas no realizadas, pedidos de reuniones. Te protege profesionalmente y ayuda a visibilizar el problema.

La constancia también es estrategia.

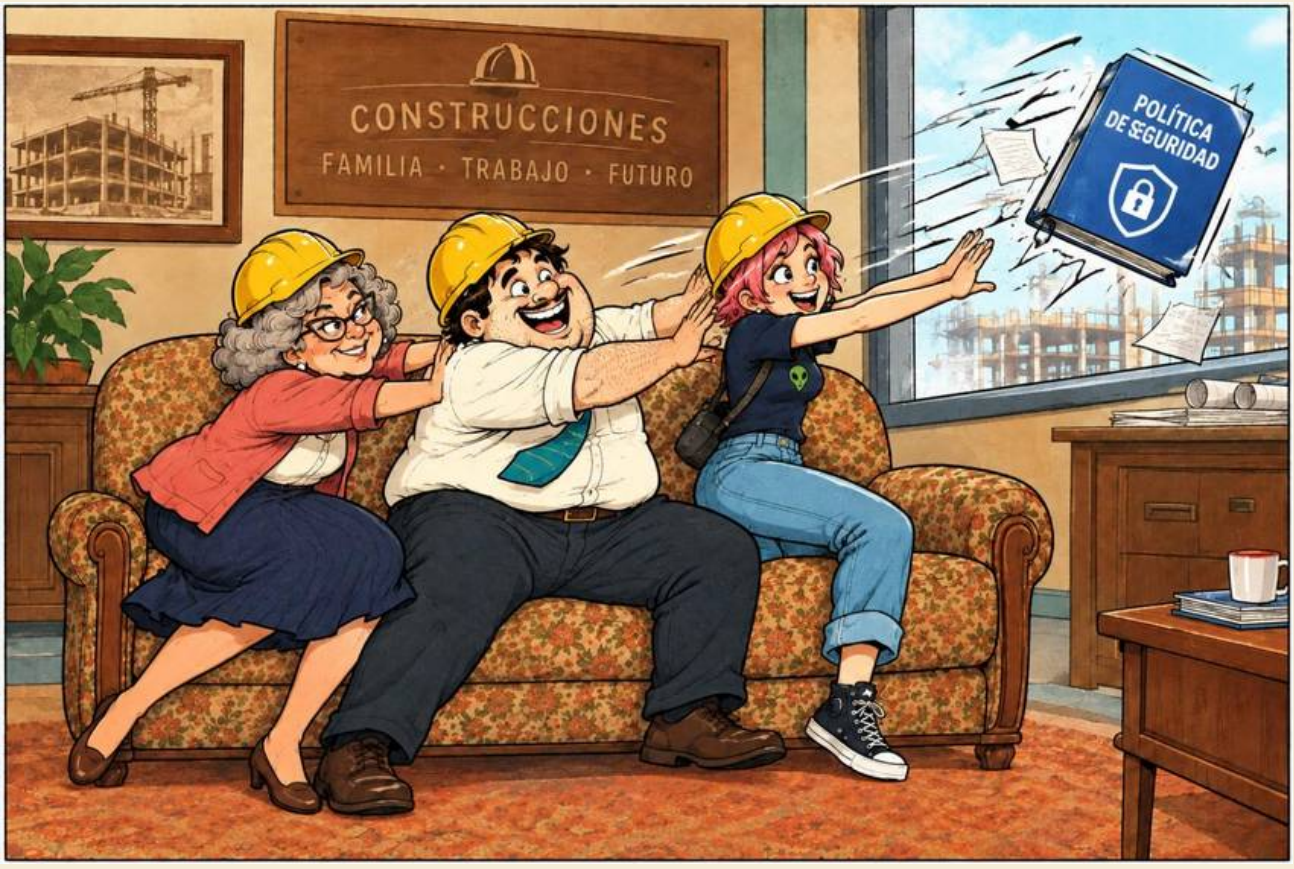
- EMAILS ENVIADOS
- ACTAS NO REALIZADAS
- PEDIDOS DE REUNIÓN

TU VOZ, TU REGISTRO, TAMBIÉN ES SEGURIDAD.

LA SEGURIDAD NO ES SOLO TECNOLOGÍA, ES TAMBIÉN GESTIÓN, COMUNICACIÓN Y LIDERAZGO.

CASO #9

CULTURA ORGANIZACIONAL



CUANDO "SIEMPRE LO HICIMOS ASÍ" VENCIÓ A LA POLÍTICA DE SEGURIDAD

CASO
#9

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Empresa Familiar Tradicional

Empresa González SRL es una constructora familiar con 40 años de historia. Cuando el hijo del fundador asumió la dirección, decidió modernizar e ir por la ISO 27001 para ganar licitaciones del estado. El inicio del desastre: 200 empleados, 30 años promedio de antigüedad. Cuando se desplegó la política de "limpieza de escritorio" (no dejar documentos sensibles a la vista), los empleados sonrieron y volvieron a dejar todo como siempre. Cuando se obligó a usar bloqueo de pantalla, escribieron la contraseña en post-its pegados al monitor. Cuando se prohibió compartir credenciales, las siguieron compartiendo "porque somos como una familia, acá nos confiamos".

El método de trabajo: Su método era simple: imponer políticas de seguridad creyendo que la gente las iba a adoptar por escrito. Como si el papel cambiara comportamientos automáticamente.



La Obra Maestra del Absurdo (La Auditoría)

la auditora decidió hacer un recorrido por las oficinas para validar la aplicación real de los controles. Lo que vio era una contradicción ambulante.

El Contexto: Las políticas estaban firmadas por todos los empleados (con firma electrónica obligatoria al ingreso). Los registros decían "100% de cumplimiento". El Análisis: La realidad operativa era radicalmente distinta. Era un SGSI documental sin tracción cultural.



ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el ejemplo clásico de "Cambio sin Cultura". Las causas principales son:

- **Subestimación de la cultura (La Causa Raíz):** Se asumió que firmar un documento equivale a cumplirlo. La cultura organizacional, especialmente en empresas con muchos años de inercia, no cambia por decreto.
- **Falta de gestión del cambio**: No hubo capacitaciones reales, ni campañas de concientización, ni reforzamientos positivos. Solo políticas firmadas y guardadas.
- **Ausencia de líderes de opinión:** Nadie identificó a los referentes internos para que adoptaran primero las nuevas prácticas. Sin líderes locales, el cambio no permea.



ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Cultura Organizacional

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Seguridad real	Brechas crónicas sin remediar: contraseñas compartidas, documentos expuestos, accesos no controlados. El riesgo real es enorme.
Compliance	Hallazgos masivos en auditoría por incumplimiento de prácticas básicas. Imposibilidad de demostrar conducta segura.
Inversión perdida	Recursos en políticas, herramientas y capacitaciones que no generan cambio efectivo. ROI cero.
Riesgo de incidente	Cuando aparezca el primer incidente serio (que aparece siempre), la organización está expuesta sin protección real.

LECCIONES APRENDIDAS

La cultura no se cambia con decretos, se construye con personas, ejemplo y acciones consistentes.

Las buenas prácticas se multiplican cuando se hacen realidad.

1 DIAGNOSTICÁ LA CULTURA ANTES DE IMPLEMENTAR

Hacé encuestas anónimas, observá comportamientos reales en el día a día. Conocé el punto de partida.

No se trata de suposiciones, sino de datos reales.

ENCUESTA ANÓNIMA
- ☑ Cultura
- ☑ Hábitos
- ☑ Percepciones
- ☑ Desafíos

Observá. Escuchá. Conocé.

2 IDENTIFICÁ LÍDERES DE OPINIÓN Y SUMALOS AL PROYECTO

Si ellos cambian, los demás siguen. Los líderes formales no siempre coinciden con los informales.

Buscá a quienes influyen, inspiran y son escuchados.

Líderes formales y también informales.

3 CAMBIOS GRADUALES Y VISIBLES

Una victoria chica por mes genera más cultura que diez políticas firmadas. Celebrá los pequeños logros.

Los avances también se celebran.

PEQUEÑAS VICTORIAS, GRANDES CAMBIOS

Mes 1 Piloto realizado ✓ → Mes 2 Más equipos sumados ✓ → Mes 3 Mejora visible ✓

Celebrá cada paso.

4 REFORZÁ POSITIVAMENTE

Reconocé públicamente a los equipos que adoptan buenas prácticas. La gente repite lo que es valorado.

El reconocimiento motiva, inspira y multiplica el cambio.

BUENAS PRÁCTICAS = GRANDES RESULTADOS

EQUIPO DESTACADO

5 CAPACITÁ CON ESCENARIOS REALES, NO CON TEORÍA

Simulacros, casos de la propia empresa, ejemplos concretos. La gente recuerda historias, no normas.

Las historias se recuerdan y se aplican.

SIMULACRO
- ☑ Caso real
- ☑ Trabajo en equipo
- ☑ Solución práctica
- ☑ Aprendizaje

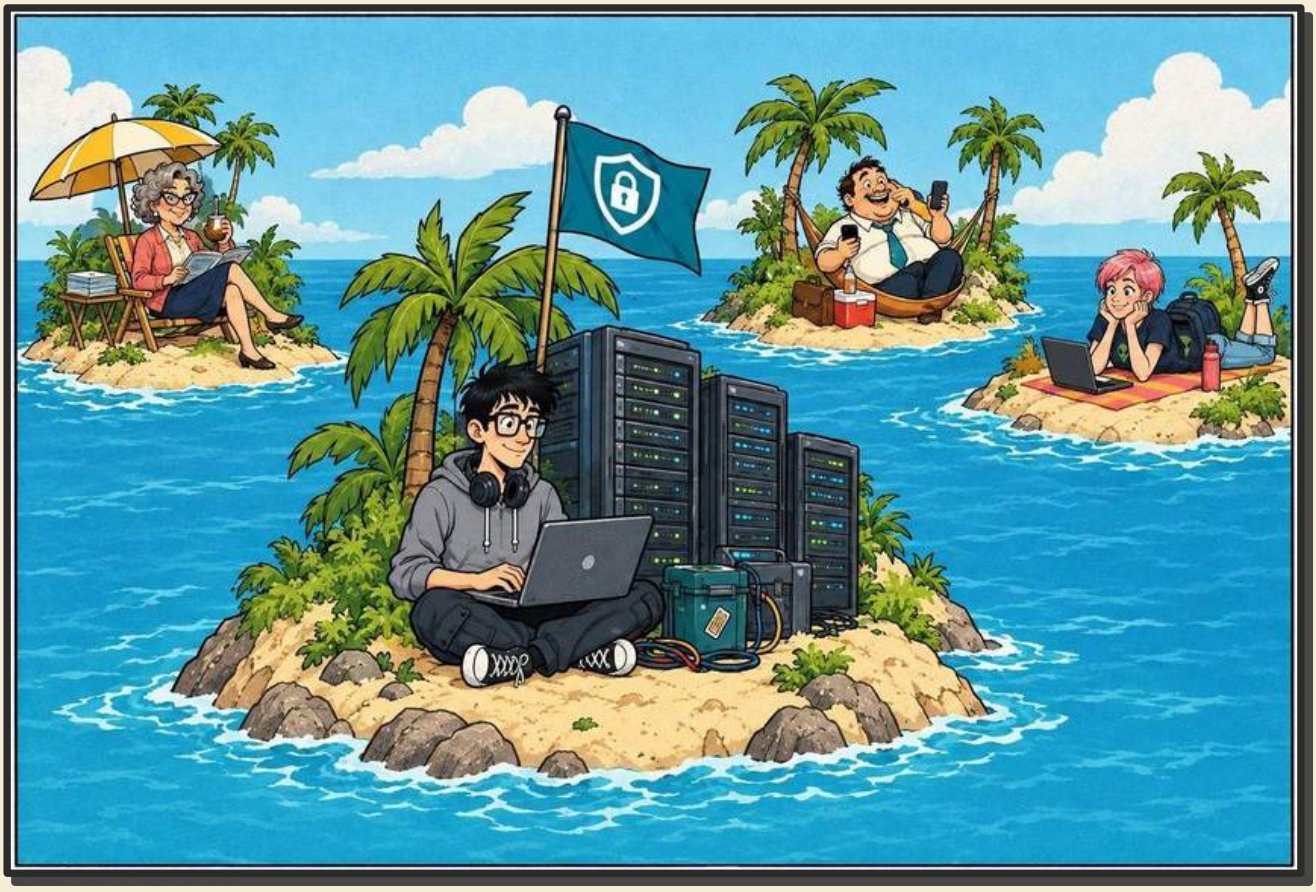
CASO REAL
- ✓ Qué pasó
- ✓ Qué aprendimos
- ✓ Qué haremos distinto

DEL PAPEL A LA PRÁCTICA.

UNA CULTURA FUERTE NO SE IMPONE, SE CONSTRUYE PASO A PASO.

CASO #10

ÁREAS CLAVE IGNORADAS



CUANDO IT ARMÓ EL SGSI SOLO Y LAS DEMÁS ÁREAS SE ENTERARON EN LA AUDITORÍA

ÁREAS CLAVE IGNORADAS

CASO
#10

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso IT Solo en la Isla

En Servicios Financieros XYZ, el director de IT propuso implementar la ISO 27001. El CEO aprobó. IT armó un equipo, contrató consultores, redactó políticas, definió procesos, hizo análisis de riesgos. Trabajaron seis meses sin parar. El inicio del desastre: nunca hablaron con RRHH, ni con Legales, ni con Compras, ni con Operaciones. "Es un tema técnico", pensaron. Cuando la auditora pidió evidencia de que RRHH hacía background check al contratar, RRHH se enteró de que eso existía en la política. Cuando preguntó por las cláusulas de seguridad en contratos con proveedores, Legales puso cara de "¿de qué me hablás?".

El método de trabajo: Su método era simple: si IT controla la tecnología y la tecnología es donde está la información, IT puede armar todo el SGSI sin necesitar a nadie más.



ÁREAS CLAVE IGNORADAS

CASO #10

La Obra Maestra del Absurdo (La Auditoría)

la auditora decidió entrevistar a las áreas "no técnicas" para validar los controles del Anexo A relacionados con personas, contratos y procesos. Lo que descubrió fue revelador.

El Contexto: La documentación SGSI mencionaba 23 controles relacionados con áreas no-IT. Todos firmados, todos aprobados. El Análisis: Al entrevistar a esas áreas, ninguna sabía que esos controles existían. Cero implementaciones reales fuera del perímetro técnico.



ÁREAS CLAVE IGNORADAS

CASO
#10

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el clásico de "SGSI técnico vs SGSI organizacional". Las causas principales son:

- **Percepción equivocada del SGSI (La Causa Raíz):** Se vio el SGSI como un proyecto de IT cuando es transversal a toda la organización. La seguridad de la información involucra a TODAS las áreas que tocan información.
- **Silos organizacionales**: Cada área en su isla. No hay tradición de colaborar en proyectos transversales. Cada uno defiende su territorio.
- **Mala comunicación inicial:** Nadie les explicó a las áreas qué rol tenían en el SGSI ni qué se esperaba de ellas. Las descubrieron de golpe en la auditoría.



ÁREAS CLAVE IGNORADAS

CASO #10

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Áreas Clave Ignoradas

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Procesos críticos sin control real: bajas de empleados que dejan accesos activos, contratos con proveedores sin cláusulas de seguridad, compras de sistemas sin evaluación.
Riesgo de información	Información sensible accesible para personas que ya no deberían tenerla. Filtraciones potenciales no detectadas.
Auditoría	Hallazgos masivos en controles "no técnicos". Imposible certificar sin involucrar a las demás áreas.
Cultural	Conflicto interno: "IT nos puso esto encima sin avisarnos". Se quema la relación entre áreas y el equipo de seguridad.

LECCIONES APRENDIDAS

EL SGSI SE CONSTRUYE EN EQUIPO



1 EMBAJADORES DEL SGSI EN CADA ÁREA

Cada área designa un embajador del SGSI: su punto de contacto y responsable local.



- ✓ Canaliza dudas y riesgos de su área.
- ✓ Acompaña la implementación de controles.
- ✓ Da seguimiento al cumplimiento.

Cercanía, responsabilidad y compromiso.

2 INTEGRACIÓN EN LOS PROCESOS EXISTENTES

No creamos flujos paralelos. La seguridad se integra en lo que ya funciona.



Por ejemplo: si RRHH ya tiene un proceso de baja, se agrega el componente de seguridad (sus accesos, datos, dispositivos). No se crea un proceso aparte.

3 CAPACITACIÓN ESPECÍFICA POR ÁREA

Cada área tiene necesidades y riesgos distintos. Por eso, la capacitación también es específica.

IT
- Gestión de accesos
- Seguridad técnica
- Respuesta a incidentes

RRHH
- Cláusulas contractuales
- Bajas seguras
- Manejo de datos personales

Legales
- Regulación y normativa
- Protección de datos
- Obligaciones y sanciones

Compras
- Evaluación de proveedores
- Riesgos de terceros
- Contratos y seguridad

Operaciones
- Seguridad en procesos
- Uso de dispositivos
- Gestión de incidentes

Finanzas
- Protección de datos financieros
- Control de accesos
- Continuidad del negocio

4 REUNIONES MENSUALES TRANSVERSALES

El SGSI no es un proyecto, es un proceso continuo. Se sostiene en el tiempo con reuniones mensuales de todas las áreas.



La seguridad se construye con constancia, coordinación y compromiso de todos.

ÁREAS DIFERENTES, UN MISMO OBJETIVO:

UN SGSI FUERTE Y SOSTENIBLE

CASO #11

RIESGOS IMAGINARIOS



CUANDO EL ANÁLISIS DE RIESGOS PARECÍA UN GUION DE CIENCIA FICCIÓN

RIESGOS IMAGINARIOS

CASO #11

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Análisis Hollywoodense: En Empresa Pyme SA, le pidieron a Nacho (programador junior) que armara el análisis de riesgos para la ISO 27001. "Mirá algunos ejemplos online", le dijeron. Nacho miró: encontró análisis de gobiernos, de bancos, de hospitales, de empresas de energía. El inicio del desastre: copió y pegó. El análisis final de la Pyme (una empresa de 30 empleados que vendía repuestos de bicicletas) identificó riesgos como: "Ataque de Estado-Nación", "Espionaje industrial chino", "Sabotaje de infraestructura crítica", "Ataque coordinado de Anonymous". Mientras tanto, los riesgos reales (un pendrive con la base de clientes que se pierde, un mail mal enviado, un empleado que se va con datos) no estaban contemplados.

El método de trabajo: Su método era simple: cuanto más asustadora suene la lista de amenazas, más profesional parece el análisis. Y total, ¿quién va a verificar si esos riesgos aplican?



RIESGOS IMAGINARIOS

CASO #11

La Obra Maestra del Absurdo (La Auditoría)

la auditora pidió revisar el análisis de riesgos y la metodología utilizada. Lo que leyó parecía sacado de una película de espías.

El Contexto: 87 riesgos identificados, todos catalogados como "críticos" o "altos". Treatment plan con controles del Anexo A aplicados masivamente. El Análisis: Cuando preguntó "¿en base a qué metodología?", la respuesta fue "copié ejemplos de internet". Ningún criterio, ninguna fuente, ningún criterio de probabilidad-impacto adaptado al negocio real.



RIESGOS IMAGINARIOS

CASO #11

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es un clásico de "Análisis sin Metodología". Las causas principales son:

- **Falta de metodología (La Causa Raíz):** No se aplicó ningún estándar reconocido (ISO 27005, NIST 800-30, OCTAVE, FAIR). Se improvisó copiando ejemplos sin entender qué aplicaba.
- **Sesgo de novedad**: Se identificaron los riesgos que están "de moda" en los medios (Estado-Nación, ransomware famosos, APT) en lugar de los riesgos reales del negocio.
- **Sin datos históricos:** No se revisaron incidentes propios pasados, ni reportes sectoriales, ni datos del propio negocio. Análisis hecho desde la especulación pura.



RIESGOS IMAGINARIOS

CASO #11

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Riesgos Imaginarios

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Recursos asignados a riesgos irrelevantes (controles para amenazas que no aplican) mientras los reales quedan sin tratar. Inversión mal dirigida.
Seguridad real	Los incidentes reales toman por sorpresa porque no estaban en el análisis. Cuando pasan, no hay procedimiento previsto.
Credibilidad	El proceso de gestión de riesgos pierde toda credibilidad interna. Nadie toma en serio futuras revisiones.
Compliance	la auditora identifica inmediatamente que el análisis es teatro. No conformidad mayor en el corazón del SGSI.



1 Usá metodologías reconocidas



2 Basate en datos reales



3 Hacé el análisis con un equipo multidisciplinario



4 Revisá el análisis al menos una vez al año o ante cambios significativos

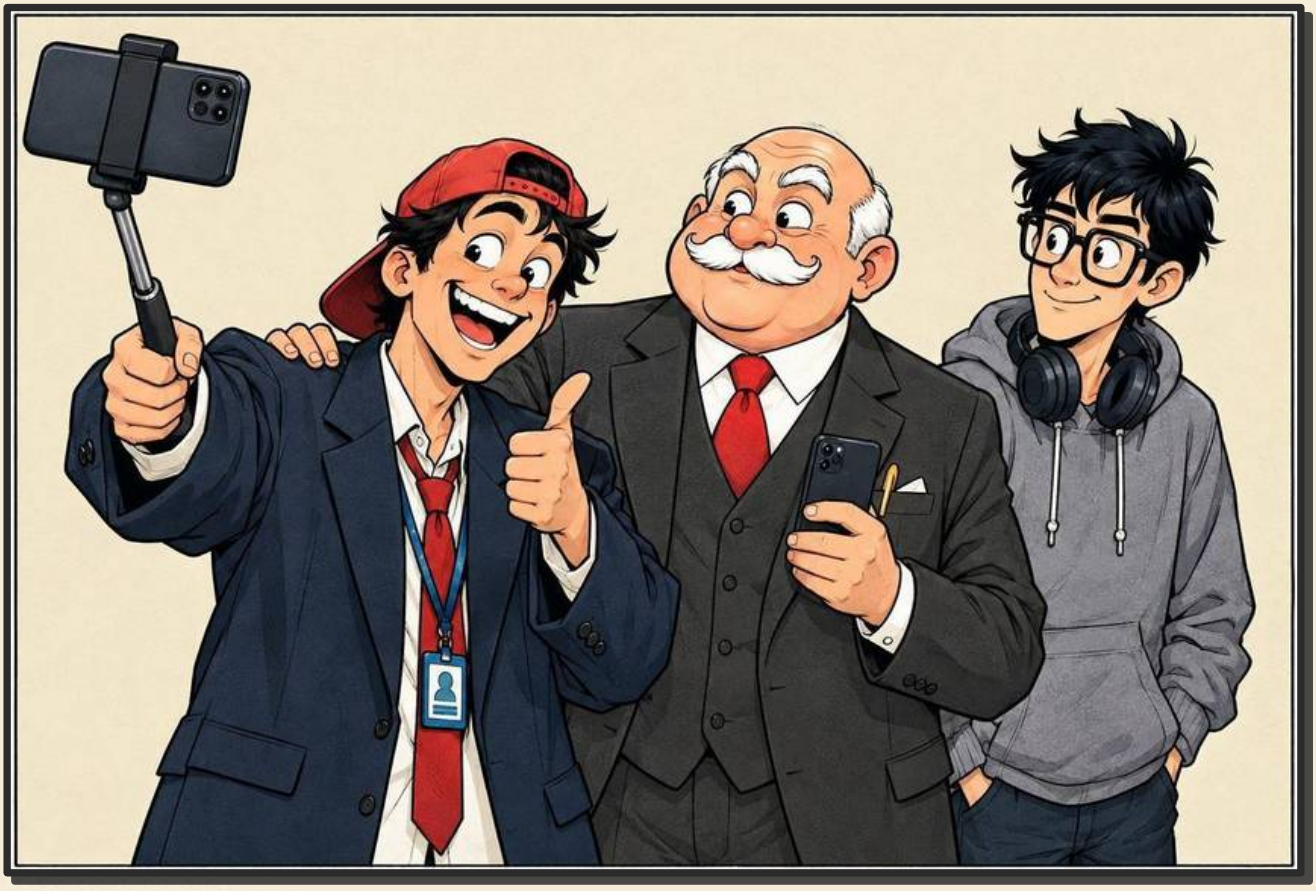


5 Si copiás ejemplos, hacelo como inspiración, no como contenido



CASO #12

AUDITORÍA INTERNA (OTRA VEZ)



CUANDO EL SOBRINO DEL GERENTE SE CONVIRTIÓ EN AUDITOR

AUDITORÍA INTERNA (OTRA VEZ)

CASO #12

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Sobrino YouTuber

En Empresa Mediana SA decidieron "ahorrar" en la auditoría interna. "El sobrino de Sofía está estudiando sistemas, que la haga él", propuso el gerente. El sobrino, Lucas, de 19 años, aceptó orgulloso. Su preparación fue mirar tres videos de YouTube: "ISO 27001 en 10 minutos", "Cómo auditar fácil" y "Trucos para auditor novato". El inicio del desastre: Lucas no entendía la mayoría de los términos de la norma. Confundió "política" con "manual". No sabía qué era una "no conformidad". Pero el informe final, que firmó con orgullo, decía: "TODO ESTÁ JOYA".

El método de trabajo: Su método era simple: leer los documentos, sonreír, dar el visto bueno. Total, si todos los documentos existen, está todo bien.



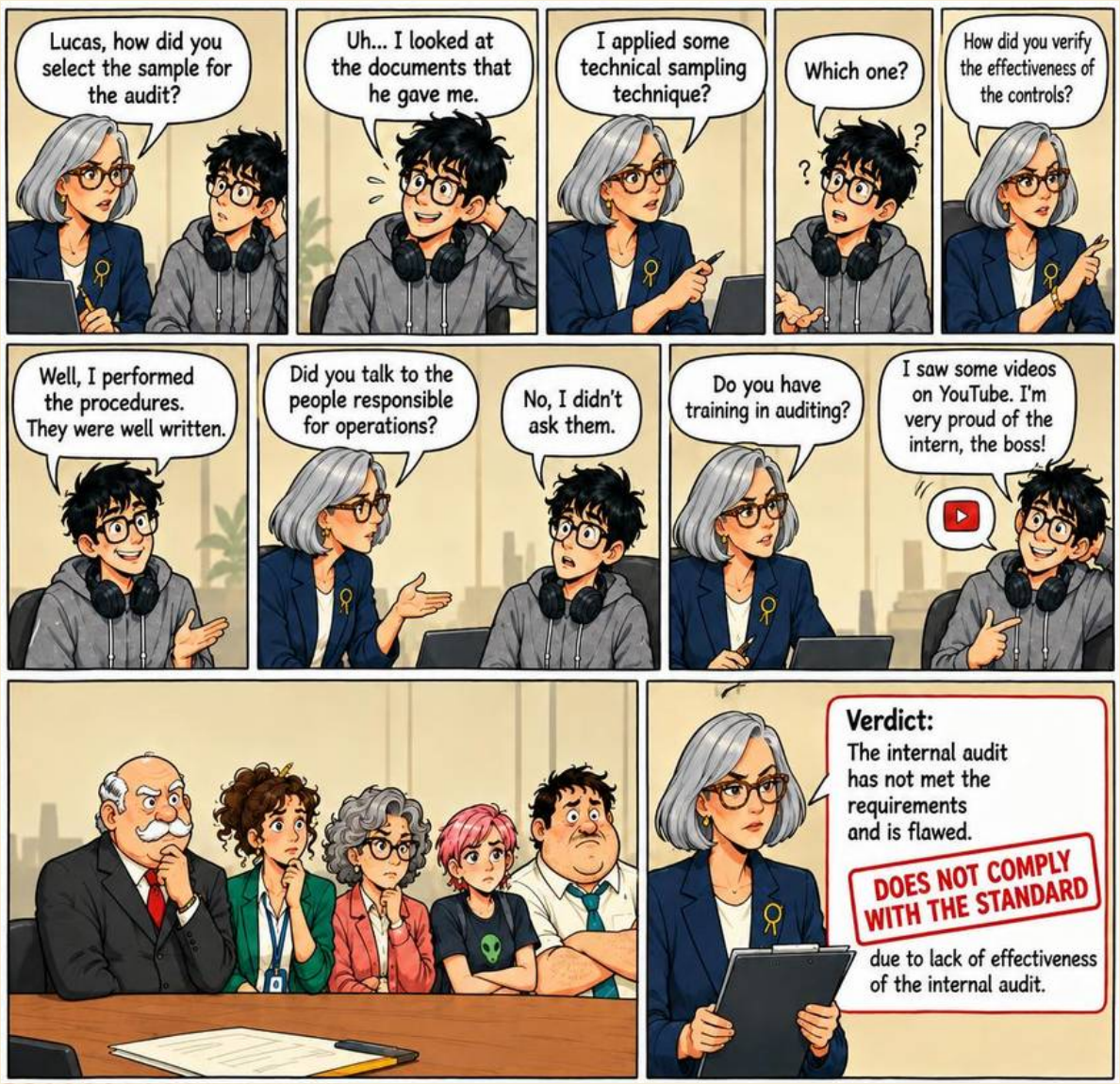
AUDITORÍA INTERNA (OTRA VEZ)

CASO #12

La Obra Maestra del Absurdo (La Auditoría)

Cuando llegó la auditora externo profesional, pidió el informe de la auditoría interna. Lucas se lo entregó con orgullo. la auditora lo leyó en 30 segundos.

El Contexto: Informe interno de 1 página, sin hallazgos, con la frase "todo está cumpliendo correctamente". Sin metodología, sin checklist, sin evidencias. El Análisis: la auditora externa encontró 23 no conformidades en los primeros días. 8 mayores. La auditoría interna había sido teatro puro.



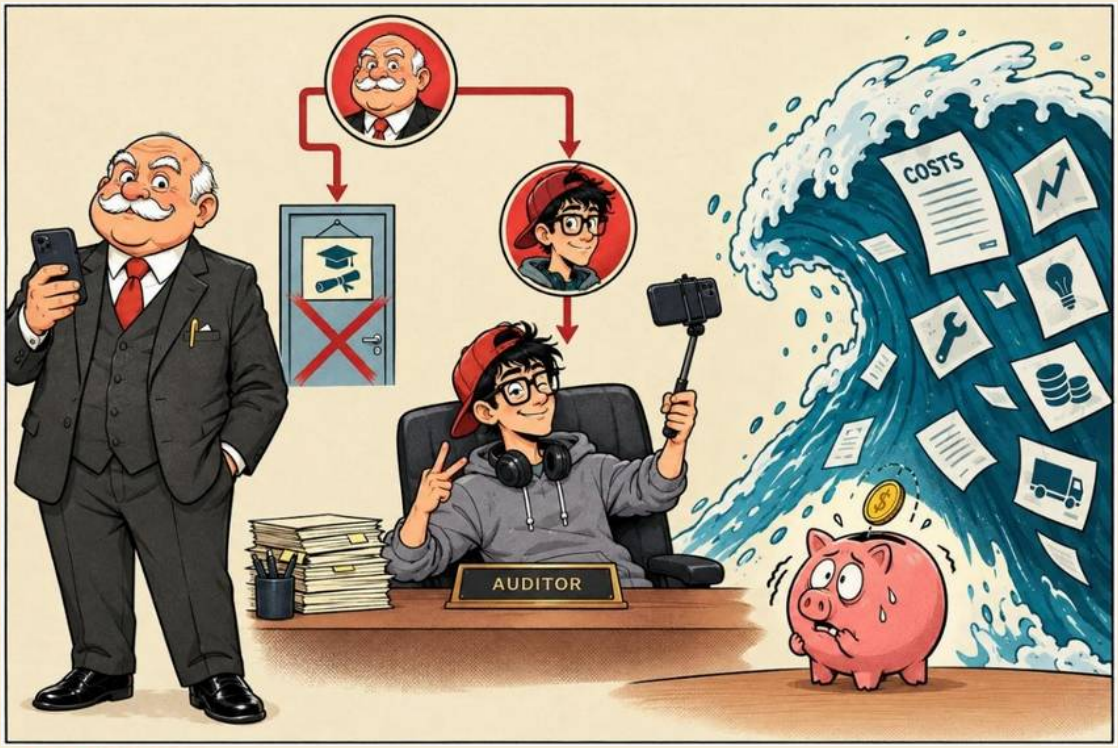
AUDITORÍA INTERNA (OTRA VEZ)

CASO #12

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es similar al caso 6 pero con un agravante adicional. Las causas principales son:

- **Subestimación del rol auditor (La Causa Raíz):** Se confundió "saber de tecnología" con "saber auditar". Son cosas distintas. Un auditor requiere formación específica, criterio profesional, técnicas de entrevista, análisis crítico.
- **Falsa economía**: Querer ahorrar el costo de un auditor formado terminó costando muchísimo más: auditoría externa con masivas no conformidades, costo de remediación, riesgo de no certificar.
- **Nepotismo y favoritismo:** Decisiones de asignación basadas en relaciones personales en lugar de competencia profesional. Receta para el desastre en cualquier proceso crítico.



AUDITORÍA INTERNA (OTRA VEZ)

CASO
#12

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Auditoría Interna (otra vez)

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Auditoría externa	Informes inútiles que dan falsa sensación de cumplimiento. La auditoría externa descubre todos los problemas y aplica no conformidades en cadena.
Calidad del SGSI	Pérdida de la principal oportunidad de mejora interna: detectar problemas antes de que los detecte el cliente, el regulador o un incidente.
Compliance	Riesgo de pérdida o no obtención de la certificación. Las no conformidades mayores deben resolverse a contrarreloj.
Credibilidad	Frustración del equipo que confió en el informe interno. Pérdida de confianza en futuros procesos internos.

LECCIONES APRENDIDAS



1 Capacitá auditores con cursos certificados (IRCA Lead Auditor, ISO 19011, certificaciones PECB).

Es una inversión, no un gasto.



2 Mantené independencia y competencia: el auditor no puede haber trabajado en lo que audita en los últimos 12 meses, Y debe tener formación demostrable.



3 Si no tenés perfil interno disponible, contratá auditor externo para la auditoría interna.

Es legítimo, válido y mucho más efectivo.



4 Auditá con criterio profesional:

el objetivo no es "pasar" sino encontrar y corregir problemas. Una auditoría sin hallazgos es probablemente una mala auditoría.



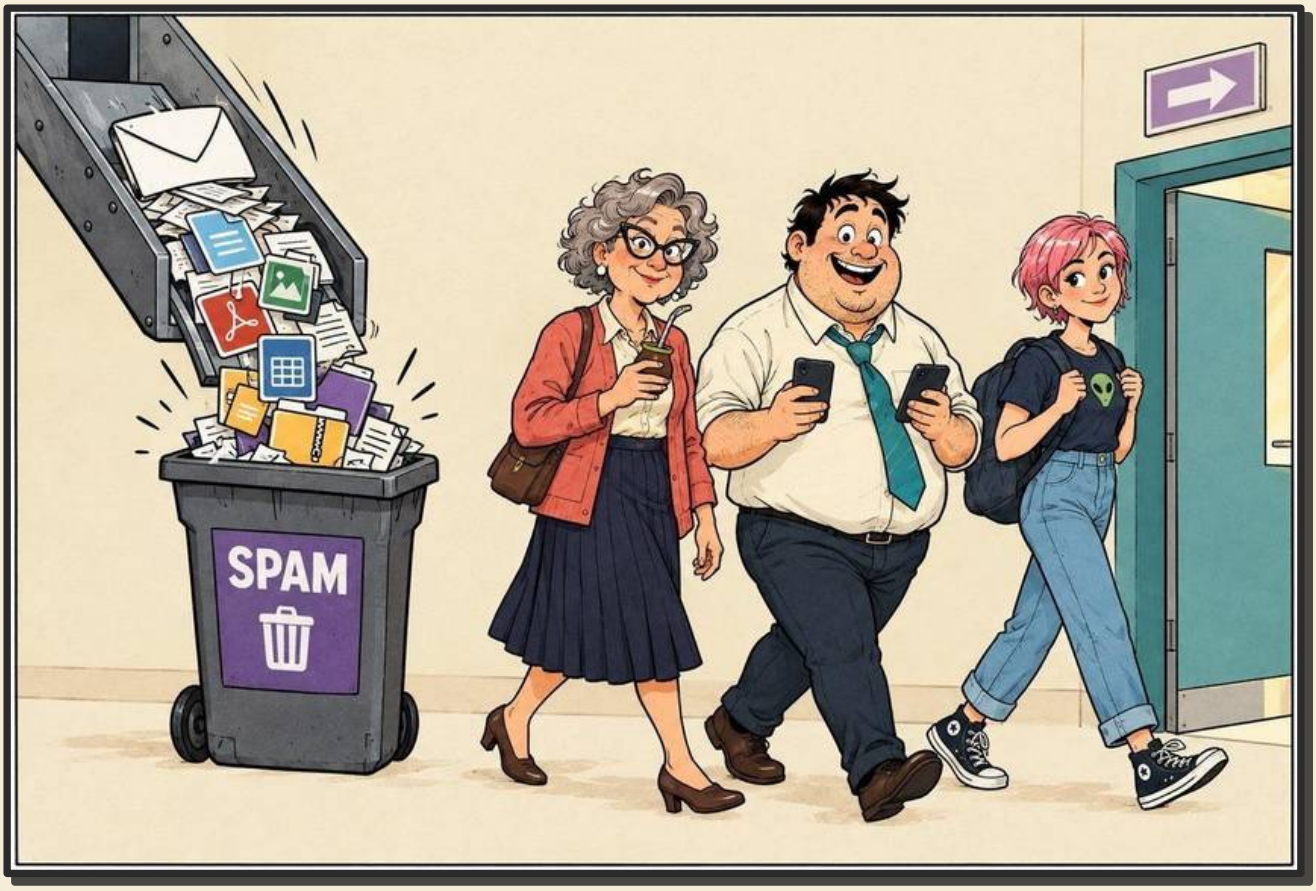
5 Documentá la competencia del auditor: CV, certificaciones, experiencia previa.

Es parte de la evidencia que pide ISO 27001 (cláusula 7.2).



CASO #13

SIN GESTIÓN DEL CAMBIO



CUANDO COMUNICARON EL SGSI POR MAIL AL SPAM DE LOS EMPLEADOS

SIN GESTIÓN DEL CAMBIO

CASO
#13

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Anuncio Olvidable

En Empresa Global SA implementaron el SGSI con consultor caro, plataforma costosa y políticas redactadas con esmero. Llegó el momento de comunicarlo. Sofía la responsable mandó un mail: "Estimados, a partir de hoy entra en vigor nuestro SGSI. Adjunto las 47 políticas. Por favor, leerlas y firmarlas. Saludos". El inicio del desastre: el mail llegó un viernes a las 18:30. La mayoría lo borró sin abrirlo. Los pocos que lo abrieron leyeron "47 archivos adjuntos" y se fueron a tomar mate. Las firmas se completaron a las 3 semanas con clics automáticos. Nadie había leído nada.

El método de trabajo: Su método era simple: si está comunicado por mail, todos lo saben. Y si lo firmaron, lo entendieron. Y si lo entendieron, lo cumplen.



SIN GESTIÓN DEL CAMBIO

CASO #13

La Obra Maestra del Absurdo (La Auditoría)

la auditora decidió entrevistar empleados al azar para validar el conocimiento real de las políticas firmadas. Los resultados fueron desoladores.

El Contexto: Política de gestión de incidentes firmada por 247 empleados. Compromiso "100% comunicado". El Análisis: De 15 empleados entrevistados, ninguno recordaba haber leído la política. 12 ni siquiera sabían que existía. 3 dijeron "creo que firmé algo, pero no me acuerdo". Cero adopciones reales.



SIN GESTIÓN DEL CAMBIO

CASO
#13

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el típico "comunicación = mail enviado". Las causas principales son:

- **Subestimación de la curva de adopción (La Causa Raíz):** Se asumió que las personas leen, entienden y aplican algo automáticamente al recibirlo. La realidad humana es radicalmente distinta.
- **Falta de inversión en gestión del cambio**: No hubo presupuesto, plan ni responsables para el componente de comunicación, capacitación y refuerzo. Se trató como "trámite final" en lugar de "piedra angular".
- **Mono-canal y mono-formato:** Solo mail con PDFs adjuntos. Sin videos, sin reuniones, sin posters, sin gamificación, sin nada que llame la atención o genere interés.



SIN GESTIÓN DEL CAMBIO

CASO #13

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Sin Gestión del Cambio

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Empleados que no saben qué cambió ni qué hacer. Procesos clave (incidentes, accesos, clasificación) ejecutados como antes o peor.
Riesgo real	Incidentes mal gestionados porque nadie conoce el procedimiento. Cuando ocurre, el reloj corre y nadie sabe a quién llamar.
Cultural	Resentimiento del personal: "otra cosa que nos imponen sin explicar". Pérdida de buena voluntad para futuras iniciativas.
Auditoría	Hallazgos inmediatos en cualquier entrevista. Imposible disimular: las preguntas básicas no se responden.

LECCIONES APRENDIDAS

La comunicación también es parte del cambio



1 PLANIFICÁ LA GESTIÓN DEL CAMBIO COMO UN PROYECTO EN SÍ MISMO

Cronograma, responsables, KPIs, presupuesto.
No es "el último paso".



2 USÁ MÚLTIPLES CANALES

Email, reuniones, videos cortos (3-5 minutos máximo), intranet con FAQs, posters, gamificación, simulacros prácticos.



3 PERSONALIZÁ EL MENSAJE POR AUDIENCIA

Lo que necesita saber un desarrollador no es lo que necesita un vendedor.
Mensajes específicos, no generalistas.



4 MEDÍ ADOPCIÓN

Encuestas trimestrales, simulacros, pruebas con escenarios reales.
Si los empleados no pueden responder preguntas básicas, comunicar más fuerte.



5 REFORZÁ CONTINUAMENTE

La primera comunicación no basta.
Recordatorios mensuales, casos reales discutidos en reuniones, integración en evaluaciones de desempeño.



RECORDATORIOS MENSUALES



CASOS REALES EN REUNIONES



INTEGRACIÓN EN EVALUACIONES

COMUNICACIÓN + COMPROMISO = CAMBIO REAL

CASO #14

CONTROLES SIN MANTENIMIENTO



CUANDO EL FIREWALL QUE PROTEGÍA TODO DEJÓ DE PROTEGERSE A SÍ MISMO

CONTROLES SIN MANTENIMIENTO

CASO
#14

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Firewall Fantasma

En Empresa Tecnológica SA, hace 5 años implementaron un firewall robusto, un IDS top de línea y un SIEM con todos los moños. Todo aprobado, todo certificado, todo en producción. Después… nada. El inicio del desastre: el técnico que instaló todo se fue dos años atrás. Nadie revisó las reglas. Nadie aplicó actualizaciones. Nadie miró los logs (que se guardaban dutifully, sin que ningún humano los abriera). Las alertas del IDS se acumularon en una bandeja de mail no leída. El SIEM tenía 11.847 alertas críticas sin atender desde 2023.

El método de trabajo: Su método era simple: instalar herramientas robustas y confiar en que la tecnología hace su trabajo sola. La tecnología es como un perro guardián: alimentas una vez y listo.



CONTROLES SIN MANTENIMIENTO

CASO #14

La Obra Maestra del Absurdo (La Auditoría)

la auditora decidió revisar la efectividad operativa de los controles técnicos. Pidió ver logs recientes, evidencias de revisión, registros de mantenimiento.

El Contexto: 23 herramientas de seguridad implementadas y "operativas". Inversión: USD 280.000. El Análisis: Cero registros de revisión de reglas en los últimos 18 meses. Cero alertas atendidas. Cero parches aplicados. Las herramientas existían físicamente, pero estaban funcionalmente abandonadas.



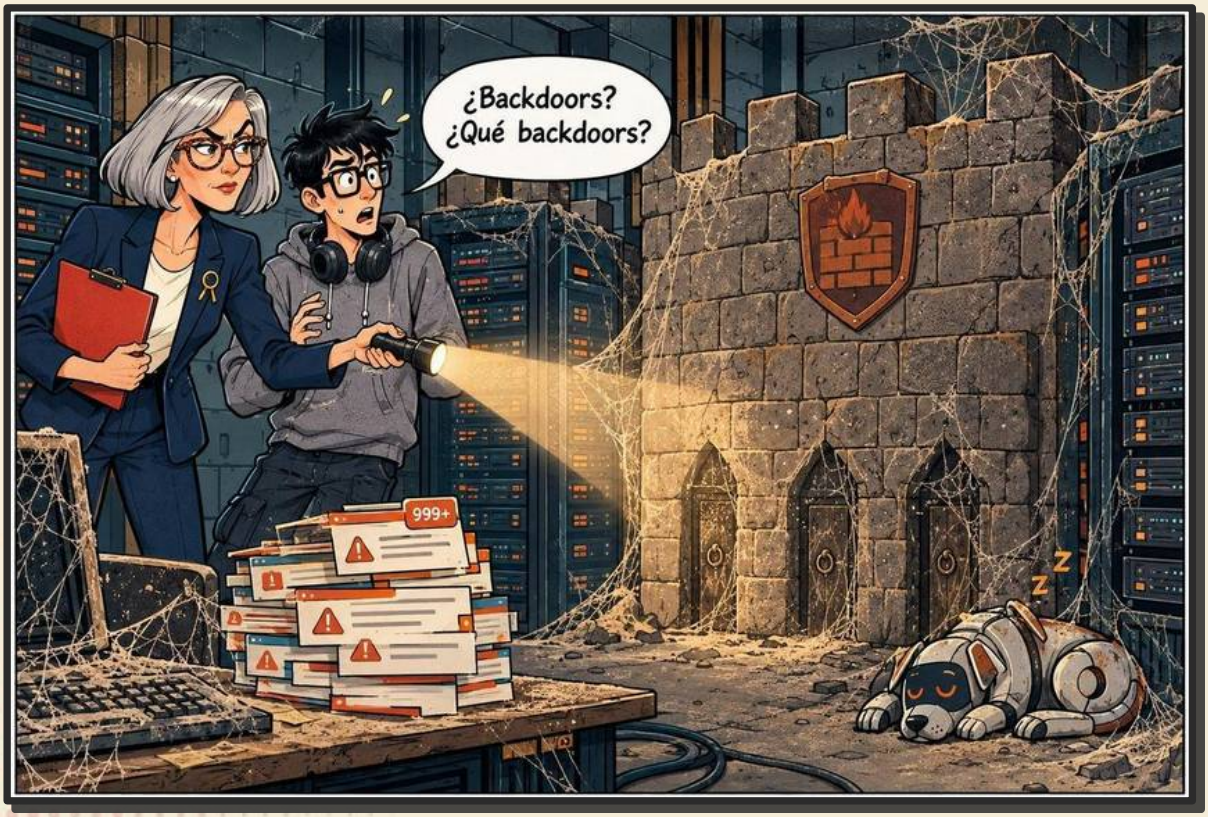
CONTROLES SIN MANTENIMIENTO

CASO
#14

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es el típico "instalar y olvidar". Las causas principales son:

- **Mentalidad de proyecto vs proceso (La Causa Raíz):** Se trató la seguridad como un proyecto con fecha de cierre ("implementemos esto y listo") en lugar de como un proceso continuo que requiere atención permanente.
- **Falta de procesos operativos**: Nadie tenía asignada la responsabilidad del mantenimiento, monitoreo y actualización. Los roles operativos no estaban definidos.
- **Rotación de personal sin transferencia:** El experto se fue y nadie heredó el conocimiento. La documentación operativa era inexistente o estaba en su cabeza.



CONTROLES SIN MANTENIMIENTO

CASO
#14

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Controles sin Mantenimiento

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Seguridad real	Controles "fantasma" que parecen funcionar, pero no protegen nada. Detección tardía de incidentes: el atacante puede llevar meses adentro sin que nadie lo note.
Operativa	Cuando finalmente se descubre el problema, los costos de remediación son altísimos: parches, reconfiguraciones, contratación de expertos, análisis forense.
Reputacional	Si un incidente público ocurre y se descubre el abandono, daño reputacional severo y posibles sanciones regulatorias.
Compliance	Hallazgos múltiples en auditoría: monitoreo, gestión de cambios, mantenimiento, registros. Todos vinculados al mismo problema raíz.

LECCIONES APRENDIDAS

1 Cada control técnico debe tener un dueño nombrado, un plan de mantenimiento documentado y una cadencia de revisión definida.



2 Monitoreá los controles, no solo los activos: si tu firewall deja de loguear, ¿alguien se entera? Si tu IDS no genera alertas en una semana, ¿es porque no hay amenazas o porque dejó de funcionar?



3 Hacé revisiones técnicas periódicas: trimestrales para controles críticos, semestrales para el resto. Documentadas, con responsable y firma.



4 Documentá el conocimiento operativo: si tu único experto se va mañana, ¿alguien puede tomar la posta sin perder semanas? Si no, hay riesgo crítico de continuidad.



5 Plan de sucesión técnica: rotar conocimiento, documentar runbooks, hacer drills regulares. La seguridad no puede depender de una sola persona.



CASO #15

CERTIFICACIÓN COMO META ÚNICA



CUANDO COLGARON EL CERTIFICADO Y SE OLVIDARON DEL SGSI PARA SIEMPRE

"Ya tenemos el sello, ahora a lo de siempre"

CERTIFICACIÓN COMO META ÚNICA

CASO #15

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Certificado Decorativo

Empresa Crecimiento SA lo logró: certificación ISO 27001. Foto en LinkedIn, comunicado al cliente, fiesta en la oficina, certificado enmarcado en la recepción. El inicio del desastre: el equipo de seguridad, una vez "terminada la misión", fue reasignado. Sofía la responsable volvió a sus tareas anteriores. El comité de seguridad dejó de reunirse "porque ya no hay nada nuevo que discutir". Los KPIs dejaron de medirse. Pasaron los meses. Pasaron los riesgos sin tratar, las políticas sin actualizar, las capacitaciones sin hacer, los nuevos empleados sin onboarding de seguridad.

El método de trabajo: Su método era simple: certificarse era la meta. Una vez alcanzada, la mochila vacía. El certificado dura 3 años, podemos relajarnos.



CERTIFICACIÓN COMO META ÚNICA

CASO #15

La Obra Maestra del Absurdo (La Auditoría)

Al año, llegó la auditoría de mantenimiento (obligatoria anual). la auditora pidió evidencias del último año de operación del SGSI. Lo que encontró fue un cementerio.

El Contexto: SGSI certificado hace 11 meses. El Análisis: Cero actas de comité en el último año. Cero capacitaciones realizadas. Cero KPIs medidos. La política vencida hace 8 meses sin actualizar. 14 nuevos empleados sin onboarding de seguridad. El SGSI estaba clínicamente muerto, pero seguían colgando el certificado.



CERTIFICACIÓN COMO META ÚNICA

CASO #15

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es probablemente el MÁS común post-certificación. Las causas principales son:

- **Enfoque de proyecto, no de proceso (La Causa Raíz):** Se cerró el "proyecto SGSI" después de la certificación. Pero la norma exige un proceso CONTINUO, no un evento. PDCA (Plan-Do-Check-Act) no se detiene.
- **Desafectación de recursos**: El equipo se disuelve, los recursos vuelven a sus tareas originales. Sin equipo dedicado (aunque sea parcial), el SGSI muere por inanición.
- **Falsa sensación de seguridad:** "Ya somos seguros, ya cumplimos". Cuando en realidad las amenazas evolucionan, los riesgos cambian, los activos se renuevan. La seguridad es móvil, no estática.



CERTIFICACIÓN COMO META ÚNICA

CASO #15

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Certificación como Meta Única

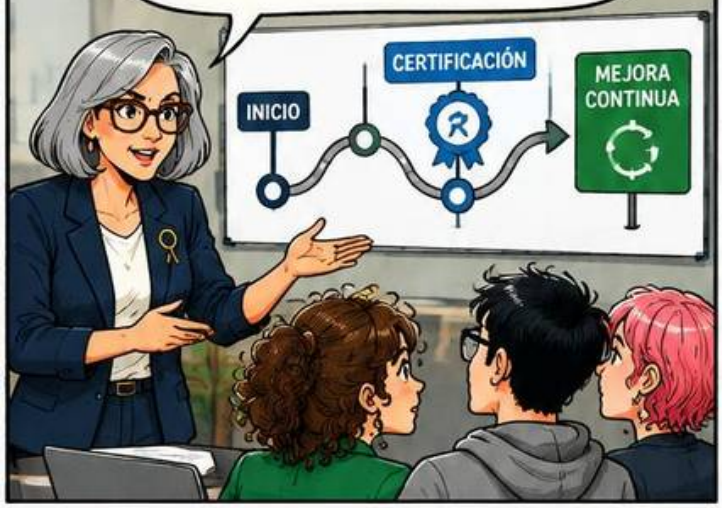
Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Compliance	Pérdida o suspensión de la certificación. Costos de reauditoría y posiblemente reimplementación parcial.
Reputacional	Si la certificación se pierde, daño reputacional ante clientes que la exigen. Posibles incumplimientos contractuales con multas.
Seguridad real	Vulnerabilidad real que crece silenciosamente. Sin monitoreo y revisión, los problemas se acumulan invisibles hasta el incidente.
Cultural	La organización aprende que "el SGSI era un trámite". Reactivarlo después es 10 veces más difícil que mantenerlo desde el inicio.

Lecciones aprendidas

1 Tratá el SGSI como un proceso continuo, no como un proyecto con fin. La certificación es un hito en el camino, no el destino.



2 Definí indicadores y revisalos mensualmente: incidentes, capacitaciones, hallazgos, acciones cerradas, riesgos nuevos. KPIs visibles, no escondidos.



3 Mantené el comité activo con agenda real, no solo cuando llega el auditor. Mínimo trimestral, idealmente bimestral.



4 Reasigná recursos permanentes al SGSI: aunque sea parcial, debe haber alguien con dedicación real, preuspuesto y autoridad para sostenerlo en el tiempo.



5 Recordá: la certificación dura 3 años, pero las auditorías de mantenimiento son anuales. Y cada vez son más estrictas que la primera.



CASO #16

EL COMITÉ FANTASMA



CUANDO LAS REUNIONES DE SEGURIDAD ERAN COMO POKÉMON: MUY POCOS LAS VEÍAN

"¿Reunión de SGSI? Uy, justo tengo otra cosa..."

EL COMITÉ FANTASMA

CASO
#16

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Reuniones Cancelables

El Comité de Seguridad de Empresa Burocrática SA estaba bien armado en el papel: CEO, CFO, CIO, CISO, RRHH, Legales. Reuniones trimestrales obligatorias. El inicio del desastre: la primera reunión se canceló "por agenda del CEO". La segunda se canceló "por viaje del CFO". La tercera se hizo, pero solo asistió el CISO, así que se canceló por falta de quórum. La cuarta directamente "se olvidaron". En 14 meses, se hicieron 2 de 5 reuniones planificadas, y en esas dos solo el CISO y dos personas más estuvieron presentes. Las decisiones críticas seguían acumulándose.

El método de trabajo: Su método era simple: agendar reuniones formales, pero darles prioridad cero. Si surgía cualquier otra cosa, se cancelaba. "Total, no es urgente".



EL COMITÉ FANTASMA

CASO #16

La Obra Maestra del Absurdo (La Auditoría)

la auditora pidió las actas de los últimos 12 meses de comité. Lo que recibió fue desconcertante.

El Contexto: 4 reuniones programadas en el año, 2 efectivamente realizadas, ninguna con quórum completo. El Análisis: Decisiones críticas pendientes: 23 (presupuesto, política de teletrabajo, incidente importante sin tratar, evaluación de proveedor crítico). El comité existía formalmente pero no operaba realmente.



EL COMITÉ FANTASMA

CASO
#16

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es la consecuencia natural de no priorizar la gobernanza. Las causas principales son:

- **Agenda saturada y falta de priorización (La Causa Raíz):** El comité de seguridad es lo primero que se cancela cuando hay cualquier otra reunión. Refleja la prioridad REAL que la dirección le da.
- **Composición equivocada**: Gente sin autoridad real para decidir. O perfiles operativos que no pueden comprometer recursos. Cuando hay quórum, no hay decisión.
- **Falta de seguimiento:** Lo que se decide no se ejecuta. Las actas (cuando existen) se archivan y se olvidan. Sin accountability, las decisiones son teatro.



EL COMITÉ FANTASMA

CASO #16

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — El Comité Fantasma

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Decisiones críticas	Demoras de meses o años en decisiones que requieren respuesta inmediata. El SGSI se paraliza esperando aprobaciones que nunca llegan.
Coordinación	Falta de coordinación entre áreas. RRHH, IT, Legales y Operaciones no tienen foro para alinear sobre temas de seguridad.
Compliance	Imposibilidad de demostrar liderazgo y compromiso (cláusula 5.1 de ISO 27001). Hallazgo seguro en auditoría.
Operativa	El SGSI queda huérfano sin guía estratégica. Las decisiones se toman ad-hoc, sin criterio común, sin trazabilidad.

LECCIONES APRENDIDAS

1 Asegurá representación con autoridad.

Que cada participante pueda decidir o se comprometa formalmente.
Sin esto, las reuniones son simbólicas.



2 Agendas concretas y compartidas con anticipación.

Temas con decisión esperada, no solo "informativos". Si todos saben qué se va a decidir, asisten más.



3 Acta breve con acciones, responsables y fechas.

En menos de 24h después de la reunión.
Y seguimiento mensual de las acciones pendientes.



4 Cadencia regular y firme.

Si se cancela una reunión, se reagenda en la misma semana, no en 3 meses.
La urgencia genera urgencia.



5 Reportá el comité al directorio.

Si el CISO informa al board sobre la efectividad del comité (incluyendo ausencias), aumenta la presión por asistir.



MEJORES REUNIONES, MÁS IMPACTO

El comité de seguridad es fuerte cuando todos participan.

CASO #17

MANUAL DEL USUARIO



CUANDO EL MANUAL DE SGSI GANÓ EL RÉCORD GUINNESS DE PÁGINAS NO LEÍDAS

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Manual Ladrillo

En Empresa Tradicional SA, la responsable del SGSI Sofía se propuso crear "el manual definitivo". Trabajó 4 meses en él. Resultado: 387 páginas, índice de 12 páginas, glosario de 47 términos, anexos por todos lados. El inicio del desastre: se imprimió en tapa dura, se distribuyó a 200 empleados con la consigna "léanlo y firmen el formulario de comprensión". El manual era exhaustivo: cubría desde políticas estratégicas hasta cómo apagar correctamente la computadora. Estaba escrito en Comic Sans ("para hacerlo más amigable"). Tenía dibujos hechos en Paint para "ilustrar conceptos".

El método de trabajo: Su método era simple: cuanto más completo, mejor. Si está en el manual, está cubierto. Y si está cubierto, está implementado.



MANUAL DEL USUARIO

CASO #17

La Obra Maestra del Absurdo (La Auditoría)

la auditora pidió ver el manual del usuario y validar que los empleados lo aplicaran. Lo encontró rápidamente: estaba sobre un escritorio… como soporte de monitor.

El Contexto: El Contexto: 387 páginas firmadas "como leídas" por 200 empleados. El Análisis: Al entrevistar empleados, nadie podía citar una sola política del manual. Pero todos confirmaron "sí, lo recibimos, está sobre la heladera del comedor". El manual se usaba como peso, posavasos y soporte improvisado.



ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es similar al de Documentitis, pero con un agravante: convirtieron al usuario en víctima.

- **Mentalidad de cumplimiento (La Causa Raíz):** Se interpretó "la norma pide manual" como "hagamos un manual lo más gordo posible". Más es mejor, porque demuestra esfuerzo.

- **Desconfianza en la capacidad del lector**: Se pensó "mejor explicar todo por las dudas" porque "los empleados no saben nada". Resultado: el manual quedó tan grande que NADIE lo lee.
- **Ausencia de diseño instruccional:** Nadie sabía cómo hacer documentación efectiva. Se confundió "completar" con "comunicar". Documentación no es lo mismo que pedagogía.



ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Manual del Usuario

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Manual ignorado: nadie lo lee, nadie lo aplica, nadie lo actualiza. El esfuerzo de redacción fue tiempo perdido.
Riesgo real	Personal sigue trabajando "como siempre" sin guía real. Cuando hay un incidente, no saben qué hacer porque no recuerdan dónde buscar.
Cultural	El SGSI queda asociado a "burocracia inútil". Daña la disposición del personal para futuras iniciativas.
Auditoría	Hallazgos por desconexión entre lo documentado y la práctica. Las entrevistas con empleados revelan inmediatamente que la documentación es teatro.

LECCIONES APRENDIDAS

Mejor documentación, mayor seguridad



1 Pensá en el lector

¿Cuándo va a buscar esto?
¿Qué necesita saber rápido?
¿En qué formato lo va a consumir (mobile, desktop, impreso)?



2 Formatos cortos y visuales

Infografías, videos de 3 minutos, checklists de 1 página, flujogramas. La gente recuerda imágenes, no párrafos.



3 Validá usabilidad

Pedile a un empleado nuevo que use el manual para una tarea real. Si tarda más de 5 minutos en encontrar lo que necesita, hay que rediseñar.



4 Versioná y revisá

Documentos vivos, no archivos congelados en 2019. Una buena documentación de SGSI se renueva cada 6-12 meses.



5 Separá por audiencia

Un manual para todos no sirve para nadie.
Mejor: guía rápida operativa (2 páginas), procedimiento detallado (10 páginas), política estratégica (1 página).

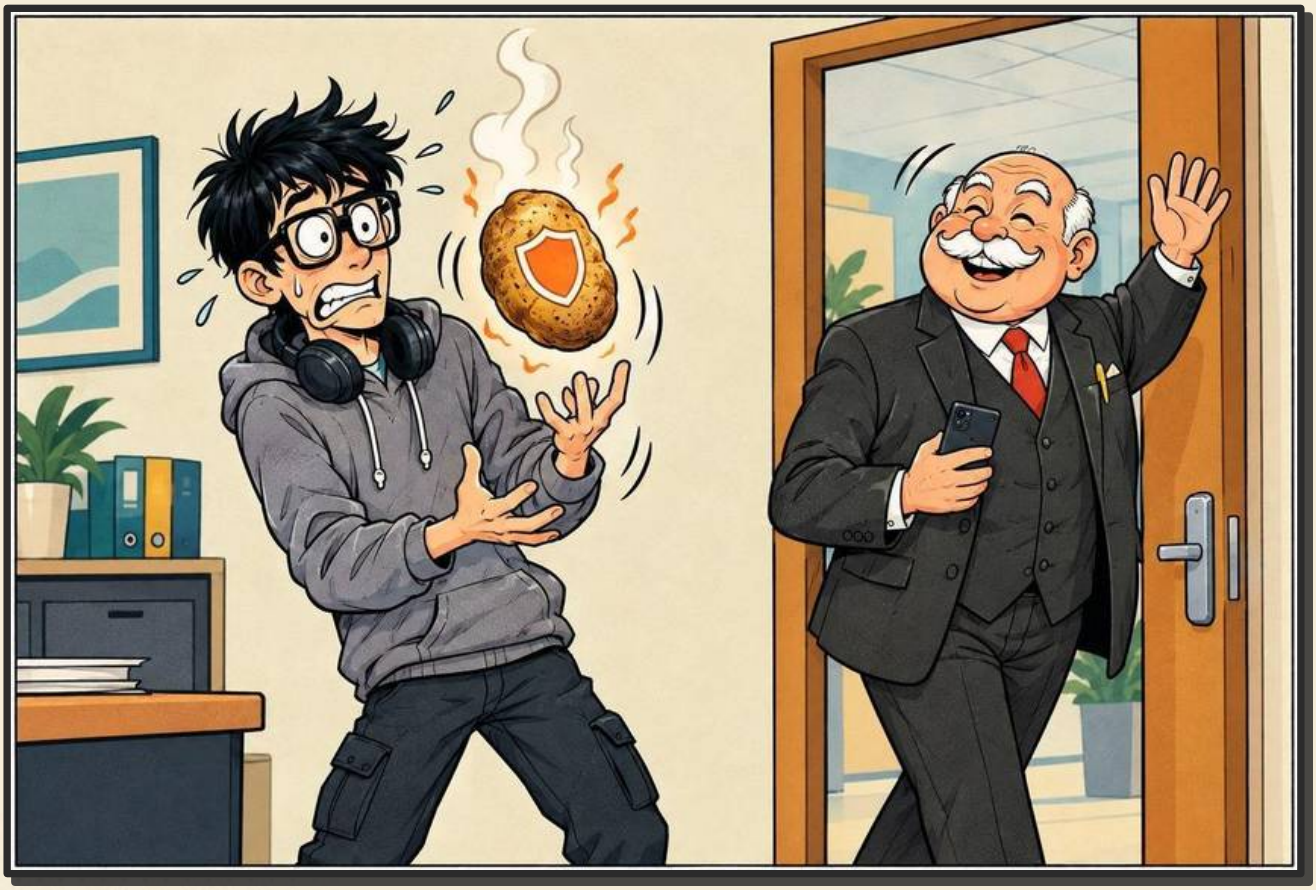
GUÍA RÁPIDA OPERATIVA	PROCEDIMIENTO DETALLADO	POLÍTICA ESTRATÉGICA
2 PÁGINAS	10 PÁGINAS	1 PÁGINA



BUENA DOCUMENTACIÓN = EQUIPOS MÁS SEGUROS = MEJORES RESULTADOS

CASO #18

RESPONSABLE DEL SGSI POR SORPRESA



CUANDO LE PASARON LA PAPA CALIENTE SIN AVISAR

"Yo no pedí esto, pero bueno..."

RESPONSABLE DEL SGSI POR SORPRESA

CASO #18

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Martín Designado

Martín era programador en Software Solutions SA. Un lunes a la mañana recibió un mail: "Felicitaciones Martín, desde hoy sos el Responsable del SGSI. Éxitos". Firmado por el CEO. Sin reunión previa, sin capacitación, sin transición. El responsable anterior se había ido el viernes. El inicio del desastre: Martín no sabía qué era un SGSI. Tuvo que googlear. "ISO 27001" le sonaba, pero no estaba seguro de qué se trataba. Recibió una carpeta con "todos los documentos" del responsable anterior: 230 archivos sin ningún orden lógico. Heredó 47 acciones pendientes, 3 auditorías por venir, 14 incidentes sin cerrar.

El método de trabajo: Su método era simple: aprender mientras hace, improvisar cuando no sabe, mantener la calma siempre que sea posible. El método del aprendiz forzoso.



RESPONSABLE DEL SGSI POR SORPRESA

CASO #18

La Obra Maestra del Absurdo (La Auditoría)

Dos meses después de la designación, llegó la auditoría de mantenimiento. Martín hizo lo que pudo. Lo que pudo no fue suficiente.

El Contexto: Responsable del SGSI con 8 semanas en el rol, sin formación previa, sin transición ordenada. El Análisis: Auditor reveló sistemáticamente las brechas: decisiones técnicas mal tomadas por desconocimiento, procesos abandonados a medio camino, métricas no medidas. No por mala intención de Martín, sino por imposibilidad fáctica.



RESPONSABLE DEL SGSI POR SORPRESA

CASO #18

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es desafortunadamente común en organizaciones que minimizan el rol. Las causas principales son:

- **Subestimación de la complejidad del rol (La Causa Raíz):** Se asumió que "alguien con perfil técnico" puede asumir el SGSI "capacitándose en el camino". Pero la curva de aprendizaje es de meses, y mientras tanto el SGSI sufre.
- **Falta de plan de sucesión**: No había perfil formado internamente, ni proceso de transición. El rol se vivió como "se va uno, designamos otro", como si fuera intercambiable.
- **Ahorro mal calculado:** Contratar un externo formado o capacitar formalmente parecía caro. El costo de las consecuencias (no conformidades, pérdida de certificación, estrés del responsable) fue muchísimo mayor.



RESPONSABLE DEL SGSI POR SORPRESA

CASO
#18

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Responsable del SGSI por Sorpresa

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	SGSI estancado o mal implementado por falta de competencia. Decisiones técnicas inadecuadas que crean problemas a largo plazo.
Personal	Estrés crónico y burnout del "responsable accidental". Sensación de estar nadando en aguas profundas sin salvavidas.
Compliance	No conformidades en auditoría por falta de competencia demostrable. Riesgo para la certificación.
Continuidad	Si el responsable accidental se va (probable por el estrés), hay que empezar de cero otra vez. Espiral descendente.



1 DEFINÍ EL PERFIL ANTES DE ASIGNAR EL ROL



2 CAPACITÁ FORMALMENTE



3 ASIGNÁ RECURSOS



4 SI NO HAY PERFIL INTERNO DISPONIBLE, CONTRATÁ EXTERNAMENTE O TERCERIZÁ TEMPORALMENTE.



5 PLAN DE TRANSICIÓN



CASO #19

PLAN DE CONTINUIDAD INVISIBLE



CUANDO EL PLAN DE CONTINUIDAD EXISTÍA... EN UN SERVIDOR QUE YA NO ESTABA

PLAN DE CONTINUIDAD INVISIBLE

CASO #19

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso BCP Encriptado

Empresa Logística Express SA tenía su Plan de Continuidad de Negocio (BCP) bien documentado: 156 páginas, aprobado por la dirección, revisado anualmente. Cumplía todos los requisitos de la norma. El inicio del desastre: un viernes a las 14:00, un ransomware afectó toda la infraestructura. Todos los archivos cifrados. Incluido el plan de continuidad, que estaba en el mismo servidor de archivos. Cuando el gerente preguntó "¿dónde está nuestro BCP?", la respuesta fue: "En el servidor X, pero está encriptado". "¿Y la copia?". "En el servidor Y, también encriptado". "¿Una copia impresa?". Silencio.

El método de trabajo: Su método era simple: documentar el plan, guardarlo en el sistema corporativo, asumir que estaría siempre disponible. Plan de continuidad para todos los escenarios menos el de no tener acceso a sistemas.



PLAN DE CONTINUIDAD INVISIBLE

CASO #19

La Obra Maestra del Absurdo (La Auditoría)

Mientras el equipo improvisaba la respuesta al ransomware, llegó (por casualidad) la auditora para una visita de mantenimiento. Lo que vio fue la auditoría más reveladora de su carrera.

El Contexto: BCP documentado, aprobado, certificado en auditoría anterior. El Análisis: BCP inaccesible al momento de necesitarlo. Cero pruebas realizadas en 14 meses. Roles asignados, pero personas que no recordaban tener ese rol. Crisis manejada por improvisación pura.



PLAN DE CONTINUIDAD INVISIBLE

CASO #19

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este caso es trágicamente común. Las causas principales son:

- **Mentalidad documental (La Causa Raíz):** Se hizo el plan, se aprobó, se guardó, se olvidó. La norma exige que el plan funcione EN LA REALIDAD, no solo que exista EN PAPEL.
- **Falta de cultura de simulacros**: "Eso es para los bomberos" o "perdemos productividad". Sin simulacros, el plan es ficción. Cuando llega la crisis real, nadie sabe qué hacer.
- **Almacenamiento único del plan:** Plan guardado solo en sistemas corporativos. Si los sistemas caen (que es justamente el escenario para el que existe el plan), el plan cae con ellos.



PLAN DE CONTINUIDAD INVISIBLE

CASO #19

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — Plan de Continuidad Invisible

Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Operativa	Crisis prolongadas que podrían haber sido contenidas en horas. En el caso, lo que pudo ser 4 horas de downtime se convirtió en 12 días de operación parcial.
Financiera	Pérdidas económicas exponencialmente mayores a lo necesario. Cliente perdido por incumplimiento de SLA. Multa de regulador.
Reputacional	Daño reputacional que tarda años en recuperarse. La historia se cuenta entre clientes potenciales que evalúan al proveedor.
Legal	Decisiones improvisadas que generan nuevos problemas: pagos a ransomware (con implicaciones legales), notificaciones tardías a reguladores, decisiones de compra apuradas.

LECCIONES APRENDIDAS

Después de la crisis, estas son las claves que aprendimos. No son solo teoría: son lo que nos mantiene a salvo.

1. DOCUMENTACIÓN ACCESIBLE INCLUSO SI TODO ESTÁ CAÍDO

Siempre tenés que poder acceder a la documentación crítica, aunque todo esté fuera de línea.

- ✓ Copias físicas en cajas de seguridad.
- ✓ Copias offline en USBs cifrados en distintas ubicaciones.
- ✓ Copias en cuentas personales de los responsables.

2. SIMULACROS AL MENOS UNA VEZ AL AÑO, CON ESCENARIOS REALISTAS

Hay que practicar escenarios reales:

- Ransomware
- Indisponibilidad de proveedor crítico
- Pérdida del data center principal
- Brecha de datos masiva

3. ROLES CLAROS EN CRISIS

¿Quién decide? ¿Quién comunica al cliente? ¿Quién a los empleados? ¿Quién al regulador? ¿Quién a los medios?

Definido y practicado, no improvisado.

DECIDE | CLIENTES | EMPLEADOS | REGULADOR | MEDIOS

4. REVISIÓN POST-INCIDENTE / SIMULACRO

Las lecciones aprendidas deben actualizar el plan en el siguiente ciclo.

Si después del simulacro no cambia nada, el simulacro fue inútil.



5. TEST DE LA "CHOCOLATERA"

¿Podés ejecutar el plan si tu responsable de IT y tu CISO están en un vuelo sin señal?

Si depende de personas específicas, hay riesgo crítico.

El plan debe ser robusto, con roles reemplazables y procesos claros.

VEREDICTO

La resiliencia no se improvisa.
Se construye con planificación, práctica, acceso a la información y personas preparadas.

CASO #20

EL MITO DEL «YA ESTAMOS CUBIERTOS»



CUANDO LA SOBERBIA DE SEGURIDAD INVITÓ AL RANSOMWARE A ENTRAR POR LA PUERTA

EL MITO DEL «YA ESTAMOS CUBIERTOS»

CASO #20

INTRODUCCIÓN Y DRAMATIZACIÓN:

El Caso Invulnerables SA

Empresa Líder SA acababa de obtener su segunda recertificación ISO 27001. Habían pasado las auditorías sin observaciones. Tenían 27 herramientas de seguridad, 4 SOC propios, certificaciones en cascada, un equipo de 47 personas dedicadas a seguridad. El CEO declaraba a la prensa: "Somos invulnerables". El inicio del desastre: un viernes a las 19:00 (cuando la mayoría se había ido), un mail de phishing dirigido a un asistente administrativo abrió la puerta. El asistente no tenía permisos elevados, pero su credencial sirvió para reconocimiento. En 72 horas, el atacante había escalado privilegios, llegado al dominio, exfiltrado 2 terabytes de datos, y desplegado ransomware en toda la red. Demanda: USD 12 millones.

El método de trabajo: Su método era simple: confiar en que la combinación de certificaciones + herramientas caras + equipo grande = inmunidad. La fórmula era inquebrantable. Hasta que se quebró.



EL MITO DEL «YA ESTAMOS CUBIERTOS»

CASO #20

La Obra Maestra del Absurdo (La Auditoría)

Después del incidente, llegaron 3 auditorías paralelas: el regulador, el seguro y la propia ISO. Lo que descubrieron juntos pintó un cuadro desolador.

El Contexto: SGSI "maduro" con dos recertificaciones, equipo grande, inversión millonaria. El Análisis: Múltiples brechas operativas detrás de la fachada certificada. Capacitación al personal era teatro. Pruebas de phishing internas: 38% de tasa de click (cuando se medía, hacía 14 meses). MFA: implementado solo en sistemas "críticos" según definición laxa. Logs: existían, pero nadie revisaba alertas en off-hours.



EL MITO DEL «YA ESTAMOS CUBIERTOS»

CASO #20

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

¿Por qué Sucedió? Este es el caso más doloroso y revelador. Las causas principales son:

- **Confianza excesiva en certificaciones (La Causa Raíz):** Se confundió "certificado" con "seguro". El certificado dice que el SGSI cumple requisitos formales en un momento. No dice que la organización sea inmune.
- **Métricas vanity vs métricas reales**: Se medían cosas que se ven bien (cantidad de controles, capacitaciones realizadas) y no las que importan (tasa real de phishing, tiempo de detección, capacidad de respuesta off-hours).
- **Cobertura operativa con huecos sistemáticos:** Buena cobertura horas hábiles, débil en off-hours. Buenos controles técnicos centrales, débiles en endpoints distribuidos. La superficie real tenía costuras invisibles para auditores.



EL MITO DEL «YA ESTAMOS CUBIERTOS»

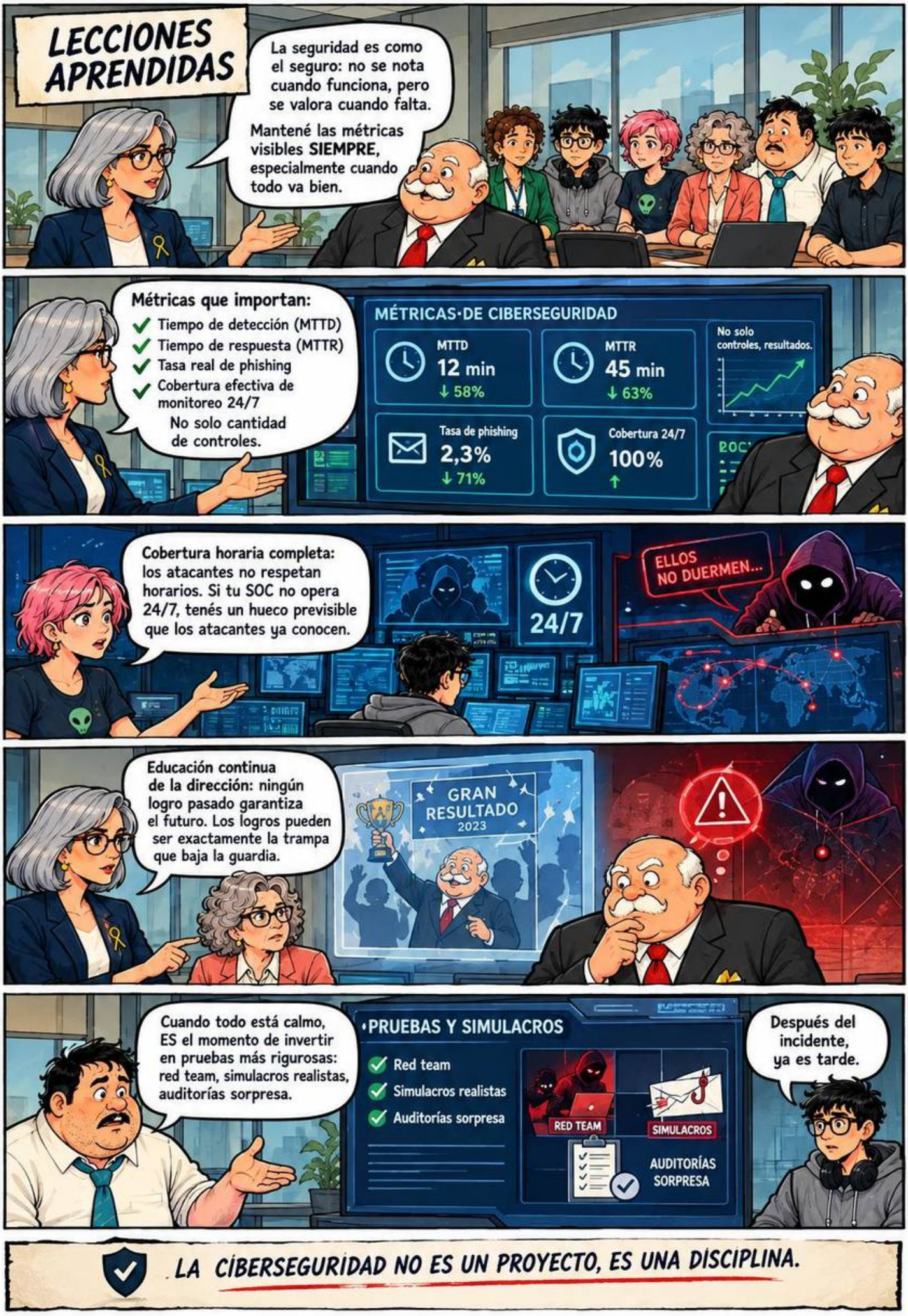
CASO #20

ANÁLISIS DE CAUSAS Y CONSECUENCIAS:

Consecuencias reales — El Mito del «Ya estamos cubiertos»
Las consecuencias se materializaron en distintas áreas:



ÁREA AFECTADA	CONSECUENCIA
Financiera	Pérdidas directas e indirectas: USD 12M de ransomware, USD 4M en consultoría forense y legal, USD 30M en pérdida de clientes, multas regulatorias.
Reputacional	Daño masivo. Clientes que cancelaron contratos. Pérdida de oportunidades comerciales por años. Recovery: 3-5 años minimum.
Operativa	Operación paralizada por semanas. Reconstrucción de infraestructura. Trauma organizacional severo.
Cultural	Reconfiguración completa de la mentalidad de seguridad. "Ya estamos cubiertos" pasó a ser frase prohibida. La paranoia constructiva se volvió obligatoria.


LECCIONES APRENDIDAS
La seguridad es como el seguro: no se nota cuando funciona, pero se valora cuando falta.
Mantené las métricas visibles SIEMPRE, especialmente cuando todo va bien.
Métricas que importan:
Tiempo de detección (MTTD)
Tiempo de respuesta (MTTR)
Tasa real de phishing
Cobertura efectiva de monitoreo 24/7
No solo cantidad de controles.
MÉTRICAS DE CIBERSEGURIDAD
MTTD
12 min
↓ 58%
MTTR
45 min
↓ 63%
Tasa de phishing
2,3%
↓ 71%
Cobertura 24/7
100%
↑
No solo controles, resultados.
Cobertura horaria completa: los atacantes no respetan horarios. Si tu SOC no opera 24/7, tenés un hueco previsible que los atacantes ya conocen.
24/7
ELLOS NO DUERMEN...
Educación continua de la dirección: ningún logro pasado garantiza el futuro. Los logros pueden ser exactamente la trampa que baja la guardia.
GRAN RESULTADO 2023
Cuando todo está calmo, ES el momento de invertir en pruebas más rigurosas: red team, simulacros realistas, auditorías sorpresa.
PRUEBAS Y SIMULACROS
Red team
Simulacros realistas
Auditorías sorpresa
RED TEAM
SIMULACROS
AUDITORÍAS SORPRESA
Después del incidente, ya es tarde.
LA CIBERSEGURIDAD NO ES UN PROYECTO, ES UNA DISCIPLINA.

CONCLUSIONES



CONCLUSIONES

¿Qué hilo conecta los 20 casos?

Si llegaste hasta acá, probablemente reconociste varios escenarios. Tal vez te enojaste, tal vez te reíste, tal vez tomaste notas. Cualquiera de las tres reacciones es válida.

Lo que une a los 20 casos no es la mala fe de nadie. Es algo más sutil: la combinación de presión, desconocimiento, urgencia y la ilusión de que la seguridad de la información es un proyecto con fecha de cierre.

Cinco verdades incómodas

1. **Un SGSI no se 'implementa', se vive.**
Si tu organización trata la seguridad como un proyecto, vas a tener que Re implementarlo cada tres años.

2. **El certificado no protege de nada.**
Protege la documentación. Las protecciones reales las ejercen los procesos vivos.

3. **La parte más difícil no es técnica, es organizacional.**
Cualquier área de IT puede aprender los controles del Anexo A.



Y DOS MÁS, IGUAL DE NECESARIAS:



4. La auditoría no es un examen, es un termómetro.

Si la pasaste con esfuerzo, no estás sano: estás disimulando. La meta es que la auditoría confirme lo que ya sabés. Cuando la confunden con un examen, se preparan para pasarla en lugar de aprovecharla para detectar problemas.

5. El SGSI no es de seguridad, es de la organización.

Si los líderes de RRHH, Compras, Legales y Operaciones no se sienten dueños, no va a funcionar. Y eso depende de cómo se les comunique desde el día uno.

Y DOS MÁS, IGUAL DE NECESARIAS:

4. La auditoría no es un examen, es un termómetro.
Si la pasaste con esfuerzo, no estás sano: estás disimulando. La meta es que la auditoría confirme lo que ya sabés. Cuando la confunden con un examen, se preparan para pasarla en lugar de aprovecharla para detectar problemas.

5. El SGSI no es de seguridad, es de la organización.
Si los líderes de RRHH, Compras, Legales y Operaciones no se sienten dueños, no va a funcionar. Y eso depende de cómo se les comunique desde el día uno.

UNA ÚLTIMA PREGUNTA

Mirá tu próxima reunión de comité de seguridad y pregúntate honestamente:
¿Si mañana esta organización sufre un incidente serio, este grupo de personas está preparado para responder?



CONCLUSIONES

La ISO no certifica empresas. Certifica decisiones.

Cada caso que leíste en este libro fue, en el fondo, una secuencia de decisiones. Algunas tomadas con buena información, otras con prisas, otras delegadas a quien no debía. Ninguna fue 'mala' por sí sola: las consecuencias aparecen cuando se acumulan.

La buena noticia es que las decisiones también se pueden revertir. Un consultor mal contratado se puede cambiar. Una documentación inflada se puede podar. Un comité dormido se puede despertar. Una cultura desinteresada se puede transformar, aunque lleve tiempo.

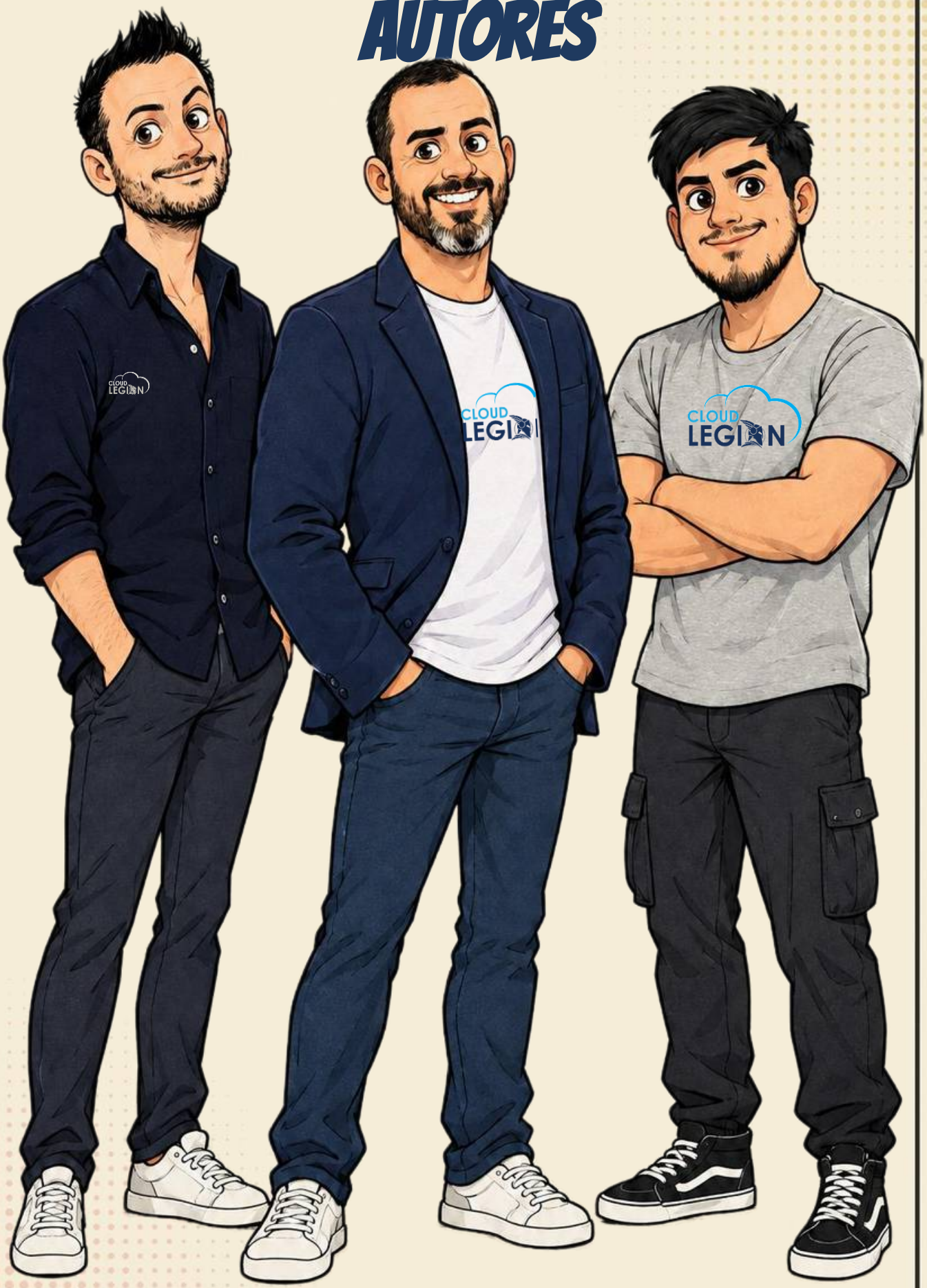
Lo que NO se puede revertir es la decisión de no decidir. La parálisis es el único error realmente irrecuperable.



Equivocarse forma parte del aprendizaje.

Pero, si se puede, mejor aprender de errores ajenos.

AUTORES



AUTORES

https://www.linkedin.com/in/lucianomoreiradacruz/

https://twitter.com/Luciano_m_cruz

LUCIANO MOREIRA



Me gusta describirme como un buscador de soluciones en todos los ámbitos laborales y personales. Creo que el conocimiento debe ser libre y que las personas deberían buscarlo todo el tiempo.

Tengo un Master en Ciberseguridad por la Universidad Camilo José Cela. DevOps Institute Ambassador, uno de los seleccionados por la gente de peerlyst como, "50 Influential DevSecOps Professionals"
Primer Auditor CSA STAR certificado en la región SOLA, Fui Elegido Cybersecurity Consultant of the Year en los premios Cybersecurity Excellence Awards 2016, 2017 y 2018, MVP - Most Valuable Professional Azure (Security, Security AI), Auditor Líder ISO 27001, 27701 27018, 27017, 20000, 22301, 42001, Tisax, WLA, CSA STAR, IATF.

Cofundador y Tribe leader de DevSecOps Latinoamérica, Presidente del capítulo argentino de la CSA Cloud Security Alliance. Embajador de Wazuh en Argentina, Miembro de ISSA, ISACA, OWASP, del comité académico de los eventos E-gisart y Cyber de ISACA y del comité científico en Ciberseguridad del evento IEEE ARGENCON, Orador e Instructor de seguridad en varios institutos.

Cuento con más de 25 años de experiencia en IT, de los cuales los últimos 20 años trabaje en una docena de proyectos en todas las capas de seguridad y infraestructura hibridas. Durante los últimos años con foco en seguridad en desarrollo y arquitectura de seguridad en entornos de computación en la nube.

Actualmente me desempeño como Chief Transformation & Strategy Office en Cloud Legion

AUTORES

www.linkedin.com/in/christian-ibiri

https://twitter.com/Christianibiri

CHRISTIAN IBIRI



Soy una persona apasionada por la tecnología y sobre todo las disruptivas o las que transforman la forma en que estamos acostumbrados de hacer las cosas, como computación en la nube, metodologías Agile, o Infraestructuras Agiles.

La verdad me encanta la época que estamos viviendo hoy por hoy donde uno puede levantar varias instancias para correr lo que se necesite sin tener que contar con un parque computacional enorme, mucho más si me acuerdo de mis principios donde teníamos que desplegar maquinas físicas, armar clústeres, "virtualización si teníamos suerte".
Uno de los seleccionados por la gente de peerlyst como, "50 Influential DevSecOps Professionals".
Auditor Líder ISO 27001, 27701, 42001, 9001

Cofundador de DevSecOps Argentina, tengo mas de 13 años de experiencia en IT, de los cuales los últimos 8 años en las áreas de Infraestructuras hibridas, cloud, DevOps y automatizacion de herramientas.
Participe en muchos proyectos de infraestructura, networking, migración e implementación en nubes publicas y privadas, automatización, comunicaciones unificadas y colaboración, acompañando a las demás partes involucradas en los mismos, desde la etapa de requerimientos hasta la implementación y pos-implementación. Creo en la interoperabilidad y que el mundo OpenSource puede tranquilamente coexistir con tecnologías propietarias sin ningún tipo de limitaciones. Entusiasta de DevOps y infraestructuras agiles.

AUTORES

https://www.linkedin.com/in/martin-ambort-08a7a8b3

https://twitter.com/mambort2014

MARTIN AMBORT



Soy una persona simple, fan de la tecnología que hacen la vida más fácil y un entusiasta del movimiento de DevOps y la Calidad del producto de software. Creo que compartir el conocimiento es una de las maneras más eficaces para construir una sociedad más justa, coherente y evolucionada, yo creo que el conocimiento debe ser libre y que todos deben tener acceso a el.

Tengo un profundo respeto por la naturaleza, Me gusta la música de calidad como, también la literatura y sobre todo películas y series.

Soy Arquitecto de Seguridad y Calidad - por la auto enseñanza y mi foco se centra en las tecnologías modernas. En los últimos años me he especializado en la automatización de la infraestructura, especialmente la automatización definida por código, la calidad del producto de software y la seguridad en todo el proceso y ciclo de vida de desarrollo.

Consultor, Auditor y instructor experto en TI con un enfoque profundo en seguridad y cumplimiento. Cuento con más de 15 años de experiencia en la gestión de redes informáticas, servidores y seguridad.

DevSecOps chapter Líder en Cloud Legion

Referente en DevSecOps en la región

DevSecOps Engenieer (DSOE)

Cybersecurity Team of the Year en los premios Cybersecurity Excellence Awards del 2019

Scrum Master

Auditor Líder ISO 27001, 27701 27018, 27017, 20000, 22301, 42001, 2500, 9001 Tisax, WLA.

Analista de Sistemas de Computación

CLOUD LEGION



NO SOMOS SOLO CONSULTORES, SOMOS LEGIONARIOS DIGITALES.

"Somos un cuerpo de élite multidisciplinario.
En un mundo de amenazas híbridas, nuestra legión
protege el activo más sagrado de las organizaciones:
su **integridad** y su capacidad de **innovar sin miedo**."

CIBERSEGURIDAD | CLOUD | TECNOLOGÍA | CONSULTORÍA | TALENTO

CLOUD LEGION

LOGROS Y RECONOCIMIENTOS

2024
GLOBEE AWARDS SILVER WINNER
CYBERSECURITY

Business Philanthropist of the Year (Cybersecurity)

2023 CHAMPION
CYBERSECURITY AWARENESS MONTH

2023 Nuevamente somos **"Cybersecurity Awareness Month champion"** by NCSA & CISA of the U.S. Department of Homeland Security.

2023
GLOBEE AWARDS BRONZE WINNER
CYBERSECURITY

Chief Technology Officer of the Year (Cybersecurity)

TOP CYBERSECURITY COMPANY
Clutch
ARGENTINA 2023

TOP CLOUD CONSULTING COMPANY
Clutch
BUENOS AIRES 2023

TÜVRheinland
CERTIFICADO
Sistema de Gestión
ISO 9001:2015
ISO/IEC 27001:2013
www.tuv.com
ID 9000006672

Certificamos **ISO 9001:2015 y ISO/IEC 27001:2013** en todos los procesos de la empresa.

2022 CHAMPION
CYBERSECURITY AWARENESS MONTH

Somos **"Cybersecurity Awareness Month champion"** by NCSA & CISA of the U.S. Department of Homeland Security.

Info Security Products Guide 2020
GLOBAL EXCELLENCE
BRONZE

Fuimos nombrados ganadores en la 16ta edición de los Premios a la excelencia **global** 2020 de Info Security PG´s **(Silicon Valley, USA)**

NETWORK PRODUCTS GUIDE
IT World Awards 2020
BRONZE

NETWORK PRODUCTS GUIDE
IT World Awards 2020
GOLD

Fuimos nombrados ganadores CTO of the Year | IT Software & Security Software en la 15th Annual IT World Awards 2020 de Network Products Guide **(Silicon Valley, USA)**

LOGROS Y RECONOCIMIENTOS

2019 to date Nuestro CDSO Chief DevSecOps strategy Officer fue reconocido como **Ambassador of DevOps Institute (Global Association)**

DEVOPS INSTITUTE Ambassador by PeopleCert

2021 GLOBEE AWARDS BRONZE WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

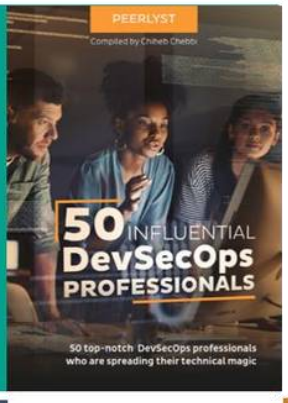
Ganamos el premio Cybersecurity Excellence Awards 2019 como **Best Cybersecurity Startup y Cybersecurity Team of the Year (Global Association)**

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Microsoft® MVP Most Valuable Professional

Nuestro CDSO - Chief DevSecOps strategy Officer otro año es seleccionado como **MVP en Microsoft Azure, Developer Technologies**

2019 Christian Ibiri & Luciano Moreira, fueron seleccionados por la gente de peerlyst, **"50 Influential DevSecOps Professionals" (Global Association)**



Fuimos finalistas del premio Cybersecurity Excellence Awards 2017 en la categoría Best Cybersecurity Startup

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

Ganamos el premio Cybersecurity Excellence Awards 2018 en la categoría Best Cybersecurity Startup

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

Cloud Legion es la primer consultora en Latinoamérica en lograr ser **CSA Global Consultancy de Cloud Security Alliance (American continent)**

CLOUD SECURITY ALLIANCE Trusted Cloud Consultant CSA

CYBERSECURITY Excellence Awards Cybersecurity Consultant of the Year WINNER 2016

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

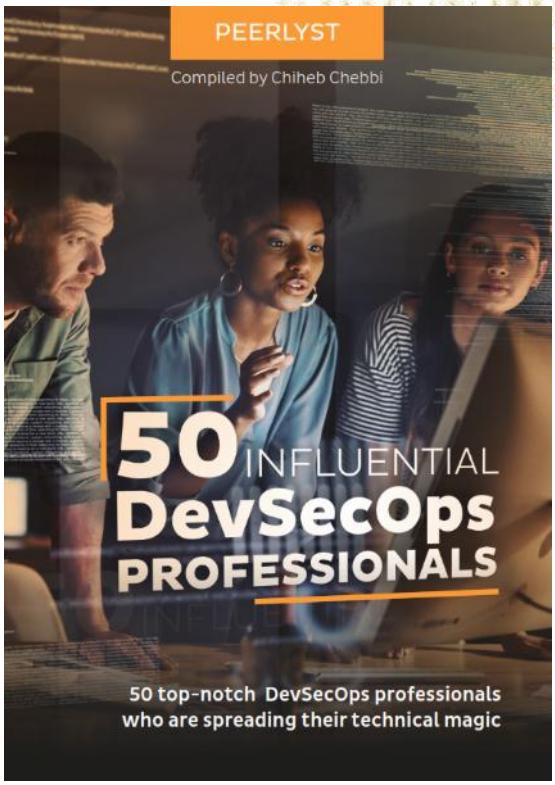
Nuestro CDSO - Chief DevSecOps strategy Officer fue elegido Cybersecurity Consultant of the Year en los premios Cybersecurity Excellence Awards 2016, 2017 y 2018.

SOMOS REFERENTES EN DEVOPS Y DEVSECOPS

DEVSECOPS Argentina by Cloud Legion

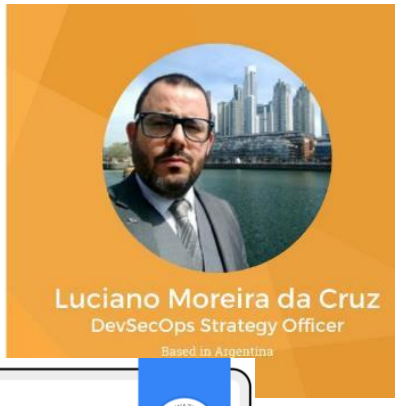
DEVSECOPS Latinoamérica

Somos fundadores de la iniciativa y organización de la comunidad **DevSecOps Argentina y Latam**



Christian Ibiri & Luciano Moreira, fueron seleccionados por la comunidad peerlyst, **"50 Influential DevSecOps Professionals"**

AMBASSADOR DevOps INSTITUTE Human of DevOps





Nuestro CDSO Chief DevSecOps strategy Officer fue reconocido como **Ambassador del DevOps Institute y de WAZUH**

SOMOS REFERENTES EN SEGURIDAD Y GESTIÓN DE LA NUBE

Somos la primera consultora en la región en calificar como **CSA Global Consultant** y contar con un **Certified CSA STAR Auditor**

El Programa de consultoría global de CSA (CSA GCP) es un marco que permite a los clientes de la nube trabajar con una red de profesionales y organizaciones de seguridad de confianza que ofrecen servicios profesionales cualificados basados en las mejores prácticas de CSA. Estos proveedores tienen un amplio conocimiento de los retos a los que se enfrentan las organizaciones al pasar a la nube.

https://cloudsecurityalliance.org/global-consultancy/registry/

Nuestro CDSO - Chief DevSecOps strategy Officer es **MVP en Microsoft Azure, Developer Technologies, Cloud Security, Security AI**

SOMOS REFERENTES EN CUMPLIMIENTO NORMATIVO

Contamos con profesionales, certificado y acreditados por diferentes entidades en las principales normas de la industria. Expertos en Sistemas de Gestión, Cumplimiento Normativo ISO y Cumplimiento Legal

Nos respaldan el 100% de empresas certificadas a la primera, y un 95% clientes que repiten



CQI | IRCA

TISAX®









CSA STAR LEAD AUDITOR

ISO 27017 CERTIFIED Cloud Security

ISO 27018 CERTIFIED Privacy Protection

onetrust Privacy PROFESSIONAL

GENERAL LAW FOUNDATION CertiProf DATA PROTECTION LGPDF™

bsi.

WORLD COMPLIANCE ASSOCIATION MIEMBRO ASOCIADO

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY — Certified to ISO/IEC 27001:2022 — TÜVRheinland Precisely Right.

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY — Certified to ISO/IEC 27701:2019 — TÜVRheinland Precisely Right.

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY — Certified to ISO/IEC 42001:2023 — TÜVRheinland Precisely Right.

SOMOS REFERENTES EN IA

Somos la primer consultora de Latinoamérica en hacer parte del Compromiso de Confianza en IA de la CSA, afirmado nuestro compromiso a los principios fundamentales de seguridad, transparencia, responsabilidad ética y privacidad en los sistemas de IA.

Contamos con el equipo mas preparado de la región, con auditores/ implementadores certificados y acreditados en la ISO 42001.

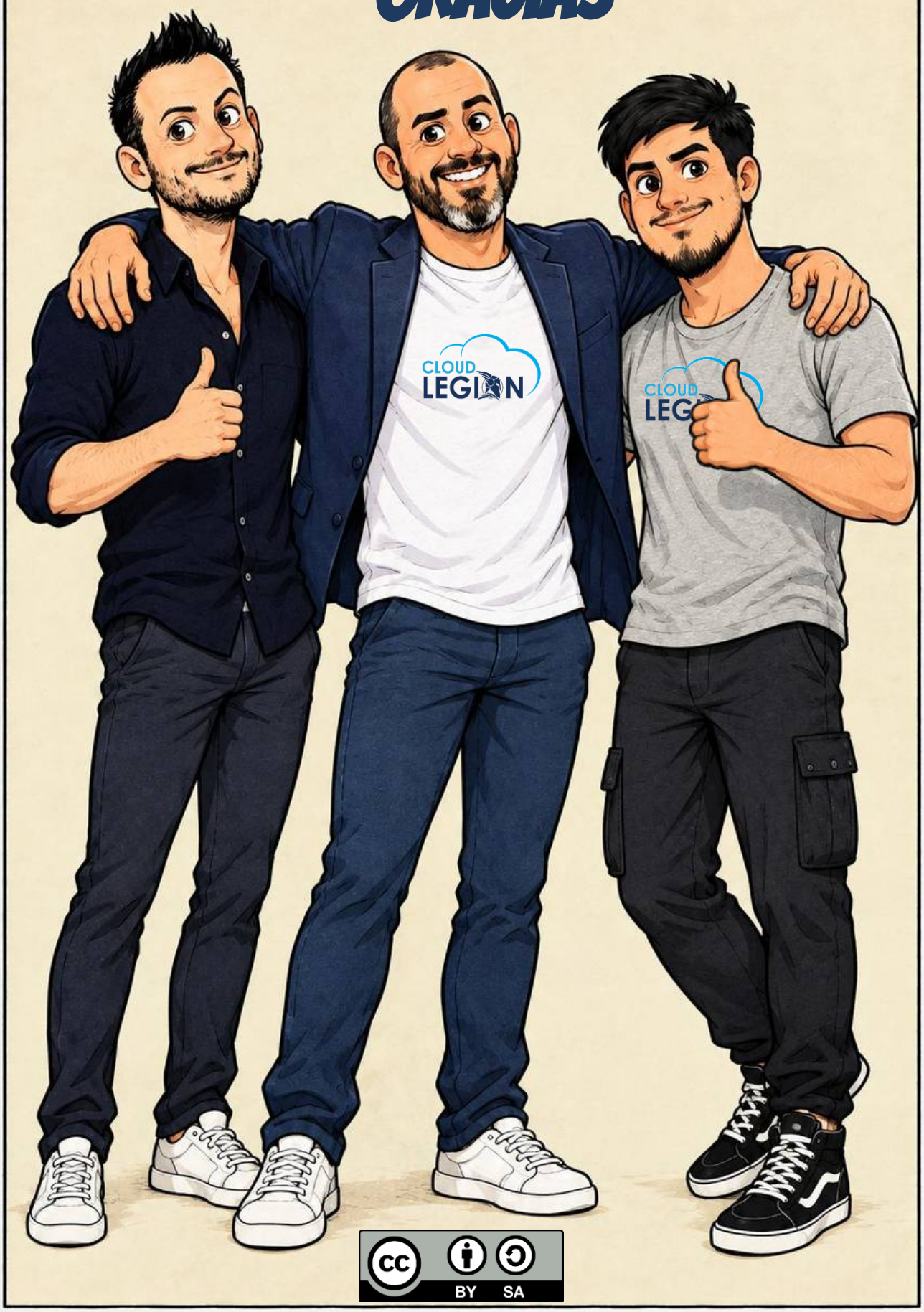
Somos la primera empresa en Argentina y la primer consultora en Latam en lograr la certificación ISO 42001.

Contamos con el primer caso de éxito de adecuación y certificación ISO 42001 de la región Latam.



Nuestro Chief Transformation & Strategy Officer otro año es seleccionado como MVP de Microsoft y paso a formar parte de la comunidad de MVP de Microsoft Security Copilot: un grupo selecto de expertos de confianza, reconocidos por su experiencia, liderazgo y pasión. Juntos, impulsamos el futuro de la inteligencia artificial aplicada a la seguridad.

GRACIAS



CC BY SA