PULSE | GRUPO SCANDA

Reforzar la resiliencia de negocio
a través de capacidades digitales
De la intuición a la decisión

Guía ejecutiva para construir casos de negocio en ciberseguridad

Cómo ayudar a la alta dirección a tomar mejores decisiones de riesgo digital

1. UNA CONVERSACIÓN INCÓMODA EN LA SALA DE JUNTAS

El director de TI entró a la sala con una solicitud aparentemente sencilla: fortalecer la protección del correo electrónico. Los incidentes de phishing se habían incrementado y el riesgo era evidente.

La respuesta fue inmediata y tajante: “¿Para qué? Ya tenemos EDR.”

Nadie actuó de mala fe. Sin embargo, en esa frase se concentró uno de los errores más comunes en ciberseguridad: ***creer que la seguridad es una herramienta y no un sistema de gestión de riesgos.***

Este documento parte de esa conversación, porque se repite todos los días en empresas medianas de México y América Latina.

El verdadero problema: no es presupuesto, es percepción del riesgo. La alta dirección rara vez rechaza una iniciativa de ciberseguridad por indiferencia. La rechaza porque no logra ver con claridad qué riesgo se está mitigando.

Cuando la conversación se presenta en términos técnicos —productos, marcas o funcionalidades— el comité pierde el marco de decisión.

Los consejos no deciden sobre tecnología. Deciden sobre continuidad operativa, impacto financiero, reputación y responsabilidad legal.

Si el riesgo no se hace visible, el presupuesto difícilmente llegará.

2. POR QUÉ HABLAR DE ROI EN CIBERSEGURIDAD SUELE FRACASAR

Durante años, las organizaciones han intentado justificar la ciberseguridad utilizando modelos financieros cada vez más sofisticados: ROI (Return on Investment), ROSI (Return on Security Investment), ALE (Annual Lost Expectancy), ARO (Annual Rate of Occurrence), análisis actuariales, y escenarios probabilísticos.

En el papel, estos modelos son correctos. En la práctica, rara vez funcionan en la sala de juntas, y no porque estén mal diseñados, el problema no es el modelo; el problema es el contexto en el que se pretende usar.

El error de fondo: tratar todas las decisiones como si fueran iguales.

Uno de los errores más frecuentes en ciberseguridad es asumir que toda inversión debe justificarse con el mismo nivel de análisis financiero, independientemente de su naturaleza.

Esto genera una paradoja peligrosa:

A controles básicos se les exige un ROI que nunca podrán demostrar.
A riesgos críticos se les analiza tarde, cuando el incidente ya ocurrió.
Y la toma de decisiones se vuelve lenta, defensiva y reactiva.

Exigir un ROI sofisticado para controles fundamentales es conceptualmente incorrecto. Es equivalente a pedir un retorno financiero detallado por: instalar cerraduras en un edificio, o colocar cámaras en un estacionamiento, o contratar seguros obligatorios.

No se hace porque generen ingresos. Se hace porque permiten operar con un nivel de riesgo aceptable.

En muchas organizaciones, el discurso del ROI termina teniendo el efecto contrario al deseado. En lugar de ayudar a decidir mejor, se convierte en una barrera que: ***retrasa inversiones necesarias, castiga iniciativas preventivas, y favorece decisiones reactivas, tomadas bajo presión.***
Paradójicamente, los controles que más valor generan —los que evitan incidentes— son los más difíciles de justificar con métricas tradicionales, porque su éxito se mide en eventos que no suceden.

Cuando no hay incidentes, el control parece innecesario.
Cuando ocurre un incidente, la pregunta cambia a:
"¿Por qué no invertimos antes?"

El verdadero dilema: prevención invisible vs impacto visible es una de las tensiones centrales de la ciberseguridad porque la prevención es silenciosa, invisible y poco agradecida y el impacto de un incidente es inmediato, visible y costoso.

Los modelos financieros tradicionales funcionan mejor cuando el beneficio es tangible y directo.

La ciberseguridad, en cambio, opera principalmente en el terreno de la reducción de probabilidad y de impacto, no en la generación directa de ingresos.

Intentar justificar todas las decisiones con el mismo lente financiero genera frustración tanto en TI como en la alta dirección.

Las preguntas que cambian la conversación deben ser:

- ***¿Qué tipo de decisión estamos tomando?***
- ***¿Es una decisión de higiene básica?***
- ***¿Es una obligación para operar y cumplir?***
- ***¿O es una inversión estratégica para reducir un riesgo específico?***

En lugar de preguntar:
"¿Cuál es el ROI de esta herramienta?"

Responder las preguntas sugeridas antes de hablar de números cambia por completo el enfoque.

No se trata de abandonar el análisis financiero. Se trata de usarlo donde realmente aporta valor.

Al reconocer que no todas las decisiones son iguales, no todos los controles cumplen la misma función, y no todos los riesgos requieren la misma profundidad de análisis, se abre la puerta a una conversación más honesta, más ágil y efectiva con comité y consejo.

Este razonamiento nos lleva directamente a una idea clave: ordenar las decisiones antes de intentar cuantificarlas. Y es precisamente eso lo que nos da la pauta a hablar de la Pirámide de ROI en Ciberseguridad.

3. LA PIRÁMIDE DE ROI EN CIBERSEGURIDAD Y SU RELACIÓN CON NIST CSF

¿Y si el problema no fuera cuánto medir, sino cuándo y qué medir?

La Pirámide de ROI en Ciberseguridad parte de una premisa simple pero poderosa: no todas las decisiones de ciberseguridad son iguales, y por lo tanto no deben justificarse de la misma manera.

Pretender que cada control, cada herramienta y cada iniciativa pase por el mismo filtro financiero es uno de los errores más comunes —y más costosos— en la toma de decisiones de seguridad.
La pirámide no elimina el análisis financiero. Lo pone en el lugar correcto.

La lógica detrás de la pirámide es que la pirámide organiza las decisiones de ciberseguridad en tres capas, de abajo hacia arriba:

1. **Higiene digital básica**
2. **Cumplimiento y continuidad**
3. **Riesgo específico y estratégico**

Cada capa responde a una pregunta distinta de la alta dirección:

- ¿Podemos operar?
- ¿Podemos operar sin exponernos?
- ¿Qué riesgos críticos estamos dispuestos a aceptar?

Entender esto cambia radicalmente la conversación en comité.

CAPA 1 - HIGIENE DIGITAL

En esta capa se encuentran los costos mínimos para participar de manera segura en la economía digital. Es la base de la pirámide, y está compuesta por los controles fundamentales que permiten a una organización operar en un entorno digital inherentemente hostil.

Aquí no estamos hablando de sofisticación. Estamos hablando de **supervivencia operativa.**

Desde la perspectiva de **NIST CSF**, esta capa se alinea principalmente con los dominios de:

- **Identify**
- **Protect**

Y la razón es que antes de defenderse, una organización debe:

- Saber qué activos tiene
- Qué información es crítica
- Quién tiene acceso
- Cuáles son los controles preventivos mínimos

Sin Identify, no hay visibilidad de quién hace qué cosas, y sin Protect, no hay barrera de entrada.

Algunos ejemplos típicos de esta capa son herramientas y procesos para:

- Inventario de activos
- Gestión básica de identidades y accesos
- Controles de acceso
- Protección del correo electrónico
- Configuraciones seguras en endpoints

Estas decisiones **no requieren un ROI sofisticado**. Se justifican igual que cerraduras, controles de acceso físicos, o sistemas básicos de seguridad.

No invertir aquí no es una estrategia financiera agresiva.

Es **aceptar un riesgo innecesario y evitable.**

CAPA 2 - CUMPLIMIENTO Y CONTINUIDAD

La idea una vez cubierta la higiene básica, la organización se enfrenta a una segunda realidad que es: Operar sin exponerse legal, contractual ni reputacionalmente en donde no todo es opcional.

En esta capa, la ciberseguridad deja de ser solo protección técnica y se convierte en **habilitador de operación y confianza.**

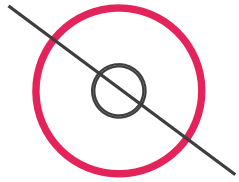
Desde el framework de NIST CSF, esta capa se apoya principalmente en los dominios:

- **Protect**
- **Detect**

Y las preguntas a responder aquí son:
¿Tenemos controles?
¿Podemos demostrar que los tenemos y detectar fallas a tiempo?

Esta capa existe y es necesaria porque:

- Los clientes lo exigen cada vez más
- Los socios en la empresa lo esperan
- Los contratos lo requieren
- El mercado castiga a quien falla



Aquí viven decisiones relacionadas con servicios y herramientas para:

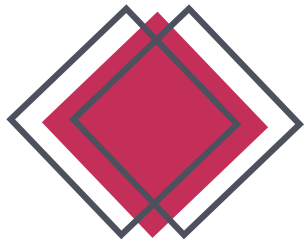
- Monitoreo
- Registro de eventos
- Detección temprana
- Evidencia de cumplimiento
- Respaldos de información

El ROI en esta capa **no se mide en ingresos**, sino en:

- Evitar sanciones
- Evitar pérdida de clientes
- Evitar interrupciones operativas prolongadas
- Preservar la confianza.

No invertir aquí no genera ahorro. Genera fragilidad operativa.

CAPA 3 - RIESGO ESPECÍFICO Y ESTRATÉGICO



En la cima de la pirámide están las decisiones más maduras, complejas y estratégicas. Aquí la organización ya acepta una verdad fundamental:
Los incidentes van a ocurrir. La diferencia está en cómo se responde y cuánto duele.

Desde NIST CSF, esta capa se alinea principalmente con los dominios:

- **Detect**
- **Respond**
- **Recover**

Y la conversación en esta capa gira en torno a:

- Escenarios reales de impacto
- Tiempos de recuperación
- Resiliencia del negocio
- Continuidad frente a eventos críticos.

Aquí sí tiene sentido:

- Hablar de escenarios
- Estimar impactos
- Priorizar riesgos
- Aplicar modelos como ALE o ROSI

Pero solo porque la base ya existe, la operación es estable, y las decisiones son marginales, no fundamentales.

En esta capa, la ciberseguridad deja de ser reactiva y se convierte en gobierno del riesgo digital. El verdadero poder de este modelo no está en memorizar capas o dominios. Está en cambiar la pregunta correcta en el momento correcto.

La conversación deja de ser:
¿Por qué necesitamos otra herramienta?
Y se convierte en:
¿En qué capa estamos tomando esta decisión y qué riesgo estamos dejando descubierto?

Esa sola pregunta debería ayudar al negocio a reducir fricción, eliminar comparaciones, y elevar la responsabilidad ejecutiva.

Esta estructura que nos parece más clara, hace mas evidente por qué comparaciones como Antispam vs EDR no solo son incorrectas, sino peligrosas. Y no porque una herramienta sea mala, sino porque viven en capas distintas de la pirámide y cubren dominios distintos del riesgo.

Ese es precisamente el ejemplo que exploraremos en el siguiente capítulo.

4. LAS TRES CAPAS DE DECISIÓN EXPLICADAS PARA COMITÉ Y CONSEJO

La idea es evitar discusiones técnicas y elevar la responsabilidad ejecutiva.
Una vez presentada la Pirámide de ROI en Ciberseguridad, ocurre algo interesante en la conversación con la alta dirección: **por primera vez, todos están hablando del mismo problema**, aunque aún no lo sepan.

La pirámide no es un modelo técnico. **Es un modelo de toma de decisiones.** Su verdadero valor no está en clasificar controles, sino en **ordenar conversaciones.**

El problema que viven muchos comités sin saberlo es que en la práctica, la mayoría de los comités toman decisiones de ciberseguridad sin distinguir entre:

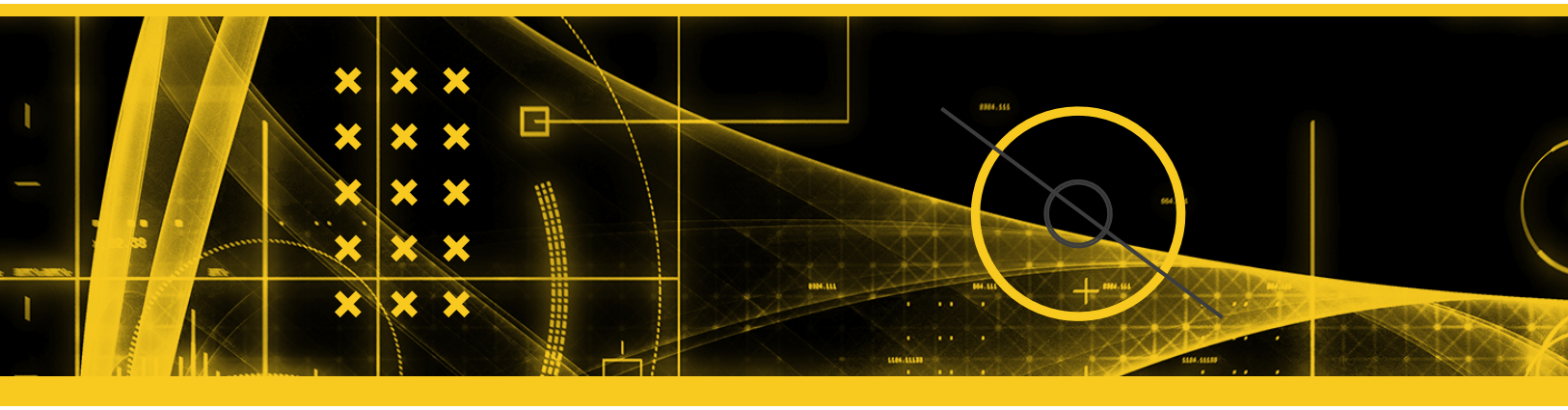
- Decisiones básicas
- Decisiones obligatorias
- Decisiones estratégicas

Todo se discute en el mismo plano y el resultado suele ser predecible:

- Comparaciones incorrectas entre herramientas
- Solicitudes de ROI inaplicables
- Frustración en TI
- Una sensación constante de que “la seguridad siempre pide más”

No es un problema de personas, es un problema de **marco mental**.

La Pirámide de ROI permite que el comité entienda algo fundamental:
No todas las decisiones de ciberseguridad son equivalentes, y no todas deben pasar por el mismo tipo de justificación.



Cada capa responde a una pregunta distinta de liderazgo.

En la **Capa 1 donde las decisiones deben enfocarse en la higiene digital** la pregunta a responder debe ser: **“¿Podemos operar sin exponernos innecesariamente?”**

Cuando una decisión pertenece a la base de la pirámide, el comité debería entender que:

- No se está debatiendo sofisticación
- No se está buscando ventaja competitiva
- Se está asegurando la operación mínima

Y estas decisiones no deberían buscar optimizar, deberían **buscar no fallar**.

Aquí, pedir un ROI detallado no solo es innecesario, sino contraproducente porque retrasa decisiones que deberían ser automáticas.

Para el comité, esta capa implica aceptar una verdad sencilla: **hay controles que no se evalúan por retorno, sino por responsabilidad.**

En la **Capa 2 las decisiones deben ser orientadas al cumplimiento y la continuidad** y la pregunta a responder debería ser: **“¿Podemos operar sin exponernos legal, contractual o reputacionalmente?”**

En esta capa, la conversación cambia de tono. Ya no se trata solo de proteger activos, sino de:

- Cumplir expectativas
- Mantener la confianza
- Y sostener la operación frente a auditorías, clientes y socios

Las decisiones aquí no son opcionales, son habilitadores de negocio.

Para el comité, esta capa implica entender que: no invertir no genera ahorro, genera restricciones, pérdida de oportunidades, o exposición legal.

Aquí, la pregunta correcta no es:
“¿Cuánto retorno genera?”
Sino:
“¿Qué costo tendría no hacerlo?”

Y finalmente en la **Capa 3 las decisiones deben ser orientadas a riesgos específicos y estratégicos,** luego entonces la pregunta a responder debe ser: **“¿Qué riesgos críticos estamos dispuestos a aceptar como líderes?”**

Esta es la capa donde la ciberseguridad se convierte en un tema de liderazgo y gobierno corporativo.

Aquí el comité ya no discute controles genéricos. Discute escenarios reales:

- ¿Qué pasaría si este sistema cae?
- ¿Cuánto tiempo podemos estar fuera?
- ¿Qué impacto tendría en clientes, ingresos o reputación?
- ¿Qué tan preparados estamos para responder?

Es en esta capa donde el análisis financiero sí agrega valor, los escenarios se vuelven concretos, y la conversación se eleva al nivel estratégico.

Aquí no decidir también es una decisión, y generalmente, es una decisión riesgosa.

Cuando el comité adopta este modelo, aparece una pregunta más de manera natural: **“¿En qué capa de la pirámide estamos tomando esta decisión?”**. Esa pregunta elimina discusiones técnicas innecesarias, evita comparaciones absurdas, y obliga a todos a hablar de riesgo, no de herramientas.

A partir de ahí, el diálogo cambia: TI deja de justificar tecnología, el comité asume su rol de gobierno del riesgo, y las decisiones se vuelven más claras y más rápidas.

5. EL CORREO ELECTRÓNICO: EL VECTOR QUE NADIE QUIERE VER

Hay una verdad incómoda en ciberseguridad que se repite año tras año, en todos los sectores y tamaños de empresa: **la mayoría de los incidentes graves empiezan con un correo electrónico.** Esto no es nuevo, no es sofisticado, y precisamente por eso, suele subestimarse.

En muchas organizaciones, el correo electrónico se percibe como: un servicio maduro, estable, **"ya resuelto"**, lo cual puede ser percepción es peligrosa.

El correo electrónico es uno de los activos digitales más críticos de la organización porque, no solo, conecta a empleados, clientes y proveedores, si no que, habilita procesos operativos y comerciales, y es la puerta de entrada a identidades, aplicaciones y datos. Y, al mismo tiempo, es uno de los servicios más normalizados.

Funciona todos los días, no "falla" de forma visible, no genera ingresos directos, lo cual provoca que sea el candidato perfecto para quedar fuera de las prioridades estratégicas hasta que algo sale mal.

Uno de los errores conceptuales más comunes es tratar el correo como un **servicio de TI**, cuando en realidad debería verse como un **vector de riesgo**.

Desde la perspectiva de un ataque, el correo electrónico es ideal porque:

- Llega directamente al usuario
- Explota confianza y urgencia
- Elude muchos controles perimetrales
- Y convierte a las personas en parte del vector

Phishing, fraude, ransomware y robo de credenciales no comienzan con exploits complejos, comienzan con un mensaje bien redactado.

Desde la **Pirámide de ROI en Ciberseguridad**, la protección del correo pertenece claramente a la **Capa 1 – Higiene digital**. No porque sea simple, sino porque **su ausencia eleva drásticamente la probabilidad de incidentes.**

En términos de NIST CSF, el correo se alinea principalmente con dos dominios:

- **Identify porque hay que:**
  - entender que el correo es un activo crítico,
  - reconocerlo como vector principal de ataque.
- **Protect porque hay que:**
  - implementar controles preventivos que reduzcan la exposición del usuario.

Ojo, y aquí no estamos hablando aún de detección avanzada ni respuesta sofisticada, estamos hablando de **reducir el ruido, el volumen y la probabilidad**.

Cuando el correo se percibe como “ya cubierto”, suele ocurrir lo siguiente:

- Se asume que el proveedor de correo “ya incluye seguridad”.
- Se confía excesivamente en la capacitación del usuario.
- Se delega el riesgo al endpoint o a la respuesta posterior.

Sin decirlo explícitamente, el comité está tomando esta decisión: **Aceptamos que los ataques lleguen al usuario y apostamos a detectarlos después.**

Eso no es irresponsable por definición, pero sí **es una decisión de riesgo**, y debería tratarse como tal. El problema es que rara vez se discute en esos términos.

La protección del correo sufre de un problema estructural porque cuando funciona bien, no pasa nada, no hay incidentes, no hay alertas, no hay crisis, y eso hace que su valor sea difícil de percibir.

Pero cuando falla: se robran las credenciales, el ransomware entra, el fraude ocurre, y la pregunta inevitable aparece demasiado tarde: “¿cómo fue que esto empezó?”

Por eso, el correo electrónico es el ejemplo perfecto para entender la Pirámide de ROI:

- Es claramente higiene básica.
- Reduce probabilidad, no impacto.
- No compite con controles avanzados.
- Los complementa.

Y, sobre todo, permite hacer visible algo fundamental para la alta dirección: **No todos los controles existen para “detectar mejor”.**

Algunos existen para que el problema no llegue.

6. CASO PRÁCTICO: ANTISPAM vs EDR

Volvamos a la sala de juntas. El director de TI presenta una solicitud concreta: fortalecer la protección del correo electrónico mediante una solución de antispam más robusta.

Los intentos de phishing han aumentado y el riesgo es evidente. La respuesta del comité es inmediata: "¿Para qué? Ya tenemos EDR."

Nuevamente, no hay mala intención, no hay negligencia, hay algo más peligroso: **una decisión tomada con un marco mental incorrecto.**

Desde la perspectiva de la alta dirección, la lógica parece razonable:
- Ya se invirtió en ciberseguridad
- El EDR es una herramienta "avanzada"
- Comprar algo adicional suena redundante

El problema no es la herramienta existente, el problema es **confundir controles que viven en capas distintas de la pirámide.**

Antispam y EDR no compiten: cumplen funciones distintas. Para entender el error, no hay que hablar de tecnología.
Hay que hablar de **riesgo**.

El **antispam actúa antes** de que el ataque llegue al usuario, su función es: filtrar intentos de phishing, bloquear enlaces y adjuntos maliciosos, reducir el volumen de amenazas que alcanzan al empleado.

Desde la Pirámide de ROI, el antispam pertenece claramente a la:
Capa 1 – Higiene digital, y desde el marco de NIST CSF, se alinea principalmente con:
- **Identify** (reconocer el correo como vector crítico)
- **Protect** (controles preventivos)

Su valor está en algo que no se ve: los incidentes que no ocurren.

Por otro lado, el **EDR actúa cuando el ataque ya llegó al endpoint**, su función es: detectar comportamientos anómalos, contener la amenaza, apoyar la respuesta al incidente.

Desde la Pirámide de ROI, el EDR vive entre la **Capa 2 – Cumplimiento y continuidad, y la Capa 3 – Riesgo específico**. Y desde NIST CSF, se alinea con:

- **Detect**
- **Respond**

El EDR parte de una premisa distinta: **algunos ataques van a pasar**. Su valor está en **limitar el daño**, no en evitar la entrada.

Cuando el comité responde "ya tenemos EDR", en realidad está tomando esta decisión implícita: **Aceptamos que los ataques lleguen por correo y apostamos a detectarlos después.**
Eso no es incorrecto por definición, es una decisión de riesgo.
El problema es que no se expresa como tal, no se dimensiona su impacto, y no se compara con alternativas preventivas.

Luego entonces, la organización no decidió conscientemente aumentar la probabilidad de incidentes. Simplemente **no vio esa consecuencia.**

Aquí está el núcleo del problema: **El antispam reduce probabilidad**, y el EDR reduce impacto. Ambos son necesarios, ninguno sustituye al otro.

Compararlos como si fueran equivalentes es como decidir **no poner cerraduras porque ya tenemos un seguro contra robos**.

Este ejemplo me parece interesante, no requiere conocimiento técnico, y refleja una situación real, que evidencia cómo una decisión de riesgo suele pasar desapercibida, y además, muestra claramente cómo una inversión preventiva puede parecer innecesaria, mientras una inversión reactiva se percibe como suficiente. Hasta que ocurre el incidente.

La conversación correcta, en este ejemplo, no era: "¿Tenemos EDR?", sino **"¿Qué riesgo reduce esta inversión y qué riesgo estamos dejando intacto?"**

Cuando el comité adopta esta pregunta, la dinámica cambia: desaparecen las comparaciones incorrectas, TI deja de "defender herramientas", y la decisión se toma desde el riesgo, no desde la intuición.

Antispam vs EDR no es un caso aislado. Es un patrón. El mismo error ocurre cuando se comparan: alternativas de solución para prevención vs respuesta, alternativas de solución para higiene vs sofisticación, y alternativas relacionadas con controles básicos vs herramientas "avanzadas".

7. CÓMO CONSTRUIR UN MINI BUSINESS CASE SIN SER EXPERTO EN FINANZAS

Llegados a este punto, muchos directores de TI se hacen la misma pregunta: "Todo esto tiene sentido... pero ***¿cómo lo llevo a comité sin entrar en fórmulas, modelos financieros o discusiones técnicas?"***

La buena noticia es que no necesitas ser financiero para construir un business case sólido en ciberseguridad. Necesitas hacer visible el riesgo de forma clara y estructurada.

La mayoría de los casos fracasan por una razón sencilla: **empiezan por la solución.**

- "Necesitamos una herramienta"
- "Esta tecnología es líder"
- "Tiene mejores capacidades"

Para un comité, eso no es un business case. Es una solicitud de gasto.

Un buen business case **no empieza por la herramienta,** empieza por el riesgo. Éste puede construirse **respondiendo cinco preguntas de negocio clave**, en este orden:

1. ¿Cuál es el activo crítico?
Todo riesgo existe porque hay algo valioso que proteger, luego entonces el primer paso es identificarlo claramente: ¿es el correo electrónico?, ¿es la operación?, ¿los datos de los clientes?, ¿los ingresos de la compañía?, ¿la reputación de la empresa?

Si el activo no está claro, la discusión se diluye.

Ejemplo: "El correo electrónico es crítico porque es el principal medio de interacción interna y externa y está ligado directamente a identidades y accesos."

2. ¿Cuál es el principal vector de ataque?
Aquí se nombra la forma más probable en que ese activo puede verse comprometido, no se listan todos los riesgos posibles; la idea es solo identificar el dominante.

Ejemplo: "El principal vector de ataque es el phishing dirigido a usuarios internos."

Esto enfocará la conversación y evitará dispersiones.

3. ¿Qué pasa si el ataque tiene éxito?
Esta es la pregunta más importante, y la más evitada. Aquí la idea es traducir el incidente a **impacto de negocio**: interrupción operativa, y/o pérdida financiera, y/o daño reputacional, y/o impacto en clientes, y/o responsabilidad legal.

No se necesitan cifras exactas, pero sí se necesita claridad en las consecuencias.

Ejemplo: "Un incidente exitoso puede derivar en robo de credenciales, fraude financiero o ransomware, con impacto directo en la operación y la reputación."

4. ¿Qué control reduce la probabilidad?
Aquí aparece la prevención. No se habla de marcas ni de funcionalidades detalladas, se habla del tipo de control.

Ejemplo: "Un control de protección del correo reduce significativamente la probabilidad de que el ataque llegue al usuario."

5. ¿Qué control reduce el impacto?
Finalmente, se aborda la contención y respuesta.

Ejemplo: "Controles de detección y respuesta permiten limitar el daño cuando un ataque logra pasar los controles preventivos."

Aquí entran herramientas como EDR, respuesta a incidentes y respaldos.

Este enfoque funciona mejor porque: no requiere métricas complejas, no exige modelos financieros avanzados, y permite al comité ver el riesgo completo, no solo una parte.

Además, evita discusiones innecesarias como: "¿cuál herramienta es mejor?", o "¿por qué necesitamos dos controles?"

Cómo presentar este mini business case en comité

Un error común es llevar este modelo como documento técnico. Es recomendable presentarlo como una narrativa y no como un reporte, funciona mejor.

El objetivo no es convencer, es habilitar una decisión informada.

Cuando este modelo se utiliza de forma consistente: las conversaciones se acortan, las decisiones se aceleran, y la responsabilidad se vuelve compartida.

TI deja de ser visto como el que viene a "pedir presupuesto", y el comité decide conscientemente qué riesgo acepta y cuál mitiga.

8. LAS PREGUNTAS QUE UN COMITÉ RESPONSABLE DEBERÍA HACERSE

En muchas organizaciones, el comité ejecutivo cree que su rol en ciberseguridad es aprobar o rechazar presupuestos.

En realidad, su responsabilidad es mucho mayor.

El comité no gobierna herramientas, gobierna riesgos.

La diferencia entre una organización reactiva y una madura no está en cuántos controles tiene, sino en las preguntas que su liderazgo se atreve a hacer.

Cada vez que un comité no formula una pregunta clave sobre ciberseguridad, está tomando una decisión implícita.

No decidir no elimina el riesgo, simplemente lo acepta sin conciencia.

Este capítulo propone un conjunto de preguntas que ayudan a: hacer visible ese riesgo, elevar la conversación, y asumir la responsabilidad que corresponde al liderazgo.

Pregunta 1: ¿Qué riesgos estamos aceptando sin saberlo?
Esta es la pregunta más incómoda y la más importante. No se trata de los riesgos conocidos, se trata de los que **no se discuten**. Ejemplos típicos: dependencia excesiva del usuario, ausencia de controles preventivos básicos, confianza implícita en que “no nos va a pasar”.

Cuando esta pregunta no se hace, la organización opera bajo **supuestos no validados**.

Pregunta 2: ¿Qué controles son básicos y cuáles son estratégicos?
No todos los controles cumplen el mismo propósito. Algunos existen para: permitir operar, reducir exposición básica, cumplir expectativas mínimas.

Otros existen para: diferenciarse, reducir riesgos críticos, mejorar resiliencia.

Confundirlos lleva a errores como: exigir ROI a controles básicos, o subestimar controles estratégicos.

Un comité responsable entiende esta diferencia.

Pregunta 3: ¿Dónde estamos apostando a que "nada pase"?
Toda organización apuesta en algún punto. La pregunta no es si existe esa apuesta. La pregunta es dónde y con qué conciencia. Apostar puede ser válido, pero hacerlo sin saberlo es irresponsable.

Esta pregunta obliga a identificar: dependencias ocultas, controles inexistentes, supuestos culturales ("la gente sabe qué no abrir").

Pregunta 4: ¿Qué pasaría si mañana somos noticia?
Esta pregunta cambia el eje emocional de la conversación. No se trata de inducir el miedo, se trata de ser realista. Plantearla obliga a pensar en: respuesta pública, impacto en clientes, continuidad operativa, y reputación, no para dramatizar, sino para prepararse.

Pregunta 5: ¿Quién es responsable del riesgo digital?
Cuando ocurre un incidente, muchas organizaciones buscan culpables. Las organizaciones maduras buscan responsables claros antes.

Esta pregunta ayuda mucho a definir: roles, expectativas, y líneas de decisión.
El riesgo digital no pertenece solo a TI, pertenece a la organización.

Cuando un comité adopta este tipo de cuestionamiento: las conversaciones se vuelven más cortas y más claras, la fricción disminuye, las decisiones se documentan, y el riesgo se gobierna, no se reacciona.

Por lo tanto la ciberseguridad deja de ser un tema técnico, y se convierte en **disciplina de liderazgo**.

9. DE APAGAR FUEGOS A GOBERNAR EL RIESGO DIGITAL

Este es el verdadero salto de madurez en ciberseguridad. Durante años, muchas organizaciones han vivido la ciberseguridad como una sucesión de incidentes, urgencias y correcciones tardías.

Un correo malicioso, un equipo comprometido, una auditoría inesperada, una vulnerabilidad crítica. Cada evento se atiende. Cada crisis se resuelve. Y, sin embargo, el patrón se repite.

Este enfoque tiene un nombre: gestión reactiva, y funciona... hasta que deja de hacerlo.

En un modelo reactivo, la ciberseguridad se vive así: algo ocurre, se responde bajo presión, se corrige el síntoma, y se vuelve a la normalidad, hasta el siguiente incidente.

El tema es que este ciclo genera: fatiga en los equipos de TI, frustración en la alta dirección, decisiones apresuradas, y una falsa sensación de control. No porque falten herramientas, sino porque no existe gobierno del riesgo.

Apagar fuegos es operativo, gobernar riesgos es estratégico.

La diferencia no está en la tecnología, sino en la intencionalidad. Cuando una organización gobierna su riesgo digital: identifica de antemano sus exposiciones más relevantes, decide conscientemente qué riesgos acepta, invierte de forma proporcional, y prepara respuestas antes de necesitarlas. Por lo tanto el incidente deja de ser una sorpresa, y se convierte en un escenario previsto.

La Pirámide de ROI es una herramienta de gobierno que permite al liderazgo: distinguir entre lo básico y lo estratégico, priorizar sin urgencia, y asignar recursos con criterio. No sirve para justificar herramientas, sirve para ordenar decisiones, y cuando las decisiones están ordenadas, la organización deja de reaccionar y empieza a dirigir.

Pasar de apagar fuegos a gobernar el riesgo implica un cambio profundo, aunque silencioso, en un escenario como este: TI deja de ser el “dueño del problema”, el comité asume su rol de decisor, y la ciberseguridad se integra a la conversación de negocio.

Este cambio no ocurre con una herramienta nueva, ocurre cuando cambian las preguntas. Y esas preguntas ya las vimos en el capítulo anterior.

Las organizaciones que dan este paso empiezan a notar diferencias claras porque: las decisiones se toman antes del incidente, los presupuestos se discuten con menos fricción, los equipos trabajan con mayor claridad, y la respuesta ante eventos es más serena y efectiva.

No porque el riesgo desaparezca, sino porque se entiende y se gestiona.

10. REFLEXIÓN FINAL: LA SEGURIDAD COMO DECISIÓN DE LIDERAZGO

A lo largo de este documento hemos hablado de riesgos, decisiones, ejemplos reales y marcos conceptuales. Pero el mensaje central es mucho más simple:

La ciberseguridad no es un problema tecnológico. Es un problema de liderazgo.

Las organizaciones no fallan porque carezcan de herramientas, fallan porque toman decisiones incompletas, tardías o basadas en intuición.

Tomar decisiones “de buena fe” ya no es suficiente. En un entorno digital hostil, **la intuición no es una estrategia**. Cada vez que una organización: posterga una decisión, confunde controles básicos con controles estratégicos, o evita conversaciones incómodas, está ejerciendo liderazgo... pero de forma implícita, y el riesgo implícito siempre es más peligroso que el riesgo consciente.

Este documento no busca: vender herramientas, imponer modelos financieros, ni crear miedo, busca algo más fundamental: ayudar a los líderes a tomar mejores decisiones de riesgo digital.

A través de: una estructura clara (la Pirámide de ROI), un lenguaje común (riesgo, probabilidad, impacto), y ejemplos reales (como Antispam vs EDR), el objetivo propone cambiar la conversación.

Una organización madura no es la que nunca tiene incidentes, es la que puede responder con claridad a estas preguntas:

- ¿Qué riesgos estamos aceptando?
- ¿Por qué los aceptamos?
- ¿Qué controles los mitigan?
- ¿Quién es responsable de esas decisiones?

Cuando esas respuestas existen, el incidente deja de ser una sorpresa. Se convierte en un escenario previsto.

La ciberseguridad puede ejecutarse en TI, pero no puede decidirse solo ahí. Aceptar, mitigar o transferir riesgos digitales es una decisión de liderazgo, al mismo nivel que: inversiones estratégicas, expansión de mercado, o gestión de crisis.

Delegar la decisión no elimina la responsabilidad.

El paso más importante que una organización puede dar ***no requiere una nueva herramienta, requiere: mejores preguntas, conversaciones más honestas, y decisiones conscientes.*** Y cuando eso ocurre: el presupuesto encuentra sentido, las inversiones se priorizan mejor, y la seguridad deja de competir contra el negocio, y se vuelve parte de él.

Si este documento logra que: un Director de TI y/o de Ciberseguridad cambie la forma en que presenta un riesgo, un comité haga una pregunta que antes no hacía, o un líder reconozca un riesgo que estaba asumiendo sin saberlo, entonces cumplió su propósito.

Porque el mayor riesgo digital no es el ataque externo, es no saber qué decisiones estamos tomando como líderes.

La ciberseguridad no empieza con tecnología, empieza con una decisión, y las decisiones que realmente importan siempre son decisiones de liderazgo.

Si este whitepaper te dejó una idea clara, es esta: la ciberseguridad no se gana con "otra herramienta", se gana con decisiones conscientes (y sí: eso es liderazgo, no intuición). En Pulse by Scanda podemos ayudarte a aterrizar esa conversación para comité y consejo: identificar el riesgo que de verdad importa, ordenar decisiones (higiene, continuidad y estrategia), armar un mini business case que se entienda sin diccionario técnico, y convertirlo en un plan accionable.

FUENTES Y REFERENCIAS

El contenido y los enfoques presentados en este whitepaper se desarrollan a partir de una combinación de marcos conceptuales reconocidos, investigación académica aplicada, y práctica profesional en ciberseguridad y gestión de riesgos. Las principales referencias incluyen:

Antwerp Management School – Blog de investigación en management y tecnología
https://www.antwerpmanagementschool.be

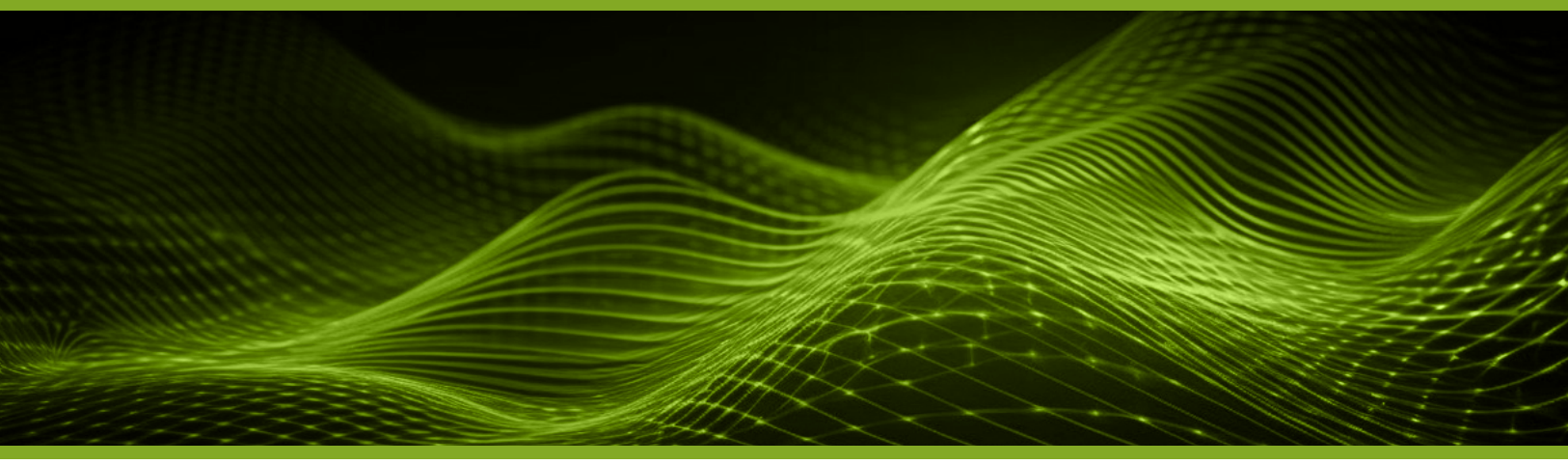
National Institute of Standards and Technology – Cybersecurity Framework
https://www.nist.gov/cyberframework

Modelos clásicos de análisis de riesgo en ciberseguridad
Conceptos como ROI, ROSI, ALE y ARO se mencionan como referencia a modelos tradicionales de análisis financiero y de riesgo, ampliamente utilizados en seguridad de la información y gestión de riesgos empresariales.

Buenas prácticas de gobierno corporativo y gestión de riesgos alineados con lineamientos de organismos como:

- World Economic Forum (WEF)
- ISACA
- OECD (gobernanza y riesgo)

Experiencia práctica y casos reales



- scanda.com.mx
- Pulse by Scanda
- Grupo Scanda
- GrupoScanda_
- Grupo Scanda
- grupo_scanda