# DOCUMENTACIÓN ESCENARIOS CYBEROPS

## Escenario 1: Eficiencia energética.

El primer escenario de optimización definido en este proyecto es un escenario de ineficiencia energética. Se trata de un escenario neutral, sin la utilización de la técnica del miedo ni de ninguna de las nombradas en el Entregable 13 (E13), en el que el director de operaciones, con la información que se le muestra, puede optar o no por la aplicación de alguna de las medidas propuestas.

La finalidad de este escenario es mostrar la predisposición de la persona a la toma de decisiones, a través de un dashboard con información neutral acerca del centro de operaciones y el estado del arte, sin dejar perfectamente clara la mejor opción a tomar.

Concretamente, la información proporcionada por el dashboard corresponde a un nivel PUE (Power Usage Effectiveness) mayor que el resto de centros de datos y el estado del arte. Las medidas propuestas están enfocadas a reducir el valor de este indicador de tres formas distintas.

Posteriormente, los resultados de este escenario serán utilizados para compararlos con aquéllos del segundo escenario de eficiencia energética (escenario 3) en el que se mostrará, esta vez sí, información no neutral, estableciendo a través del dashboard correspondiente las acciones disponibles y su coste-beneficio.



**Figura 1.-** Dashboard 1, correspondiente al escenario número 1 de eficiencia energética.

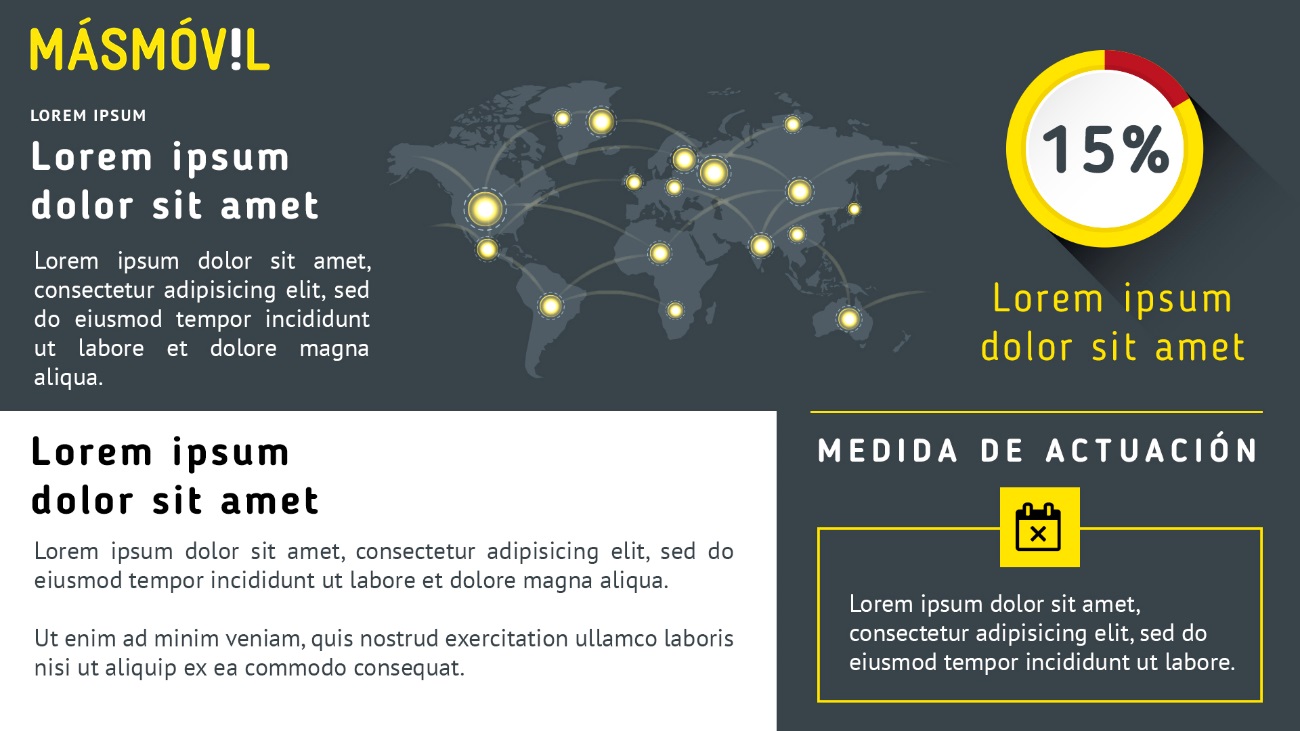
## Escenario 2: Seguridad.

En el caso del escenario número dos se plantea una situación puntual del centro de datos, el cual está siendo objeto de un ataque DDoS. Se hace uso de un mapa de peticiones y degradación de servicio, utilizando la culpabilidad para inducir la toma de decisiones.

En este caso, se plantean opciones a corto y largo plazo, mostrando los riesgos de no actuar como se recomienda.

Para ello, se hace uso de un mapa con los ataques que están siendo recibidos y el porcentaje de degradación del servicio sufrido como consecuencia de estos ataques. Así pues, se presenta información acerca del escenario al que están haciendo frente, lo que ocurriría si no se actúa y, por último, la solución recomendada.

De esta manera se pretende forzar al encuestado a la toma de decisión mediante la culpabilidad de la no acción, mostrando las consecuencias de su pasividad ante el problema.



**Figura 2.-** Dashboard 2, correspondiente al escenario número 2 de seguridad.

## Escenario 3: Eficiencia energética.

En este escenario se plantea una situación de sobredimensionamiento del sistema de refrigeración del centro de datos. Para ello se muestra, a través de un mapa térmico, los puntos calientes de la sala.

A través de la estrategia del miedo, enfocada al sobrecoste de esta situación para la empresa y el impacto medioambiental, se plantean tres posibles soluciones entre las cuales, el director de operaciones deberá elegir (analizando el coste y el beneficio de la acción) la solución más acertada.

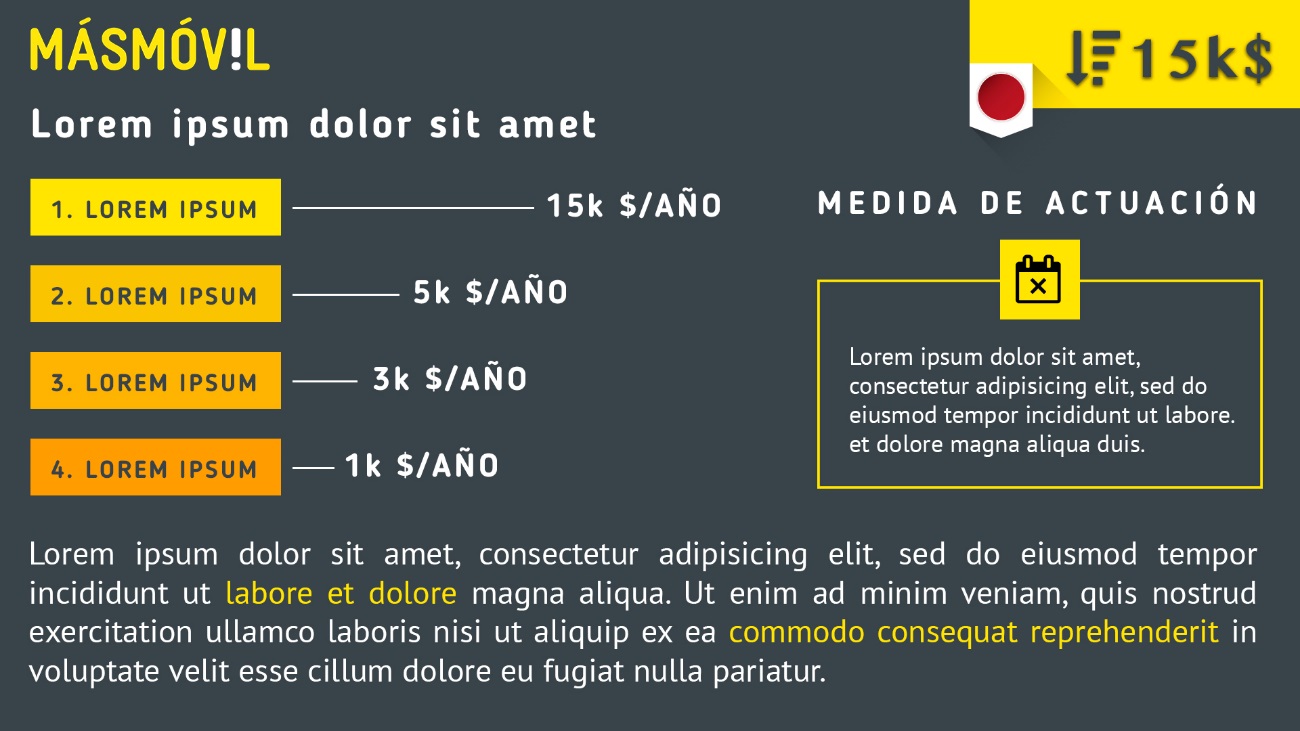


**Figura 3.-** Dashboard 3, correspondiente al escenario número 3 de eficiencia energética.

## Escenario 4: Eficiencia energética.

Se trata de un escenario de eficiencia media, enfocado a la influencia de la presión de grupo en la toma de decisiones.

Para ello se presenta el dashboard número cuatro, con acciones de eficiencia energética desarrolladas por otros centros de datos de la competencia junto con el beneficio que han obtenido por su realización. El objetivo es crear cierta presión de grupo para incentivar las acciones de mejora recomendadas.



**Figura 4.-** Dashboard 4, correspondiente al escenario número 4 de eficiencia energética.

## Escenario 5: Seguridad (reactiva tradicional).

Este escenario va dirigido al responsable de seguridad del centro de datos. El objetivo es convencerle de que utilice un sistema de detección de anomalías con Inteligencia Artificial mediante un símil que le transmita vergüenza.

El símil en concreto hace referencia a que la no utilización de un sistema de detección de anomalías es igual que dejar la puerta de una vivienda abierta, esperando a que entre algún intruso y haga lo que quiera con ella.

Con el objetivo de crear esta sensación de vulnerabilidad y vergüenza, la imagen principal del dashboard es un candado abierto y a punto de caerse, el cual induce a la predisposición de querer hacer algo para evitarlo.

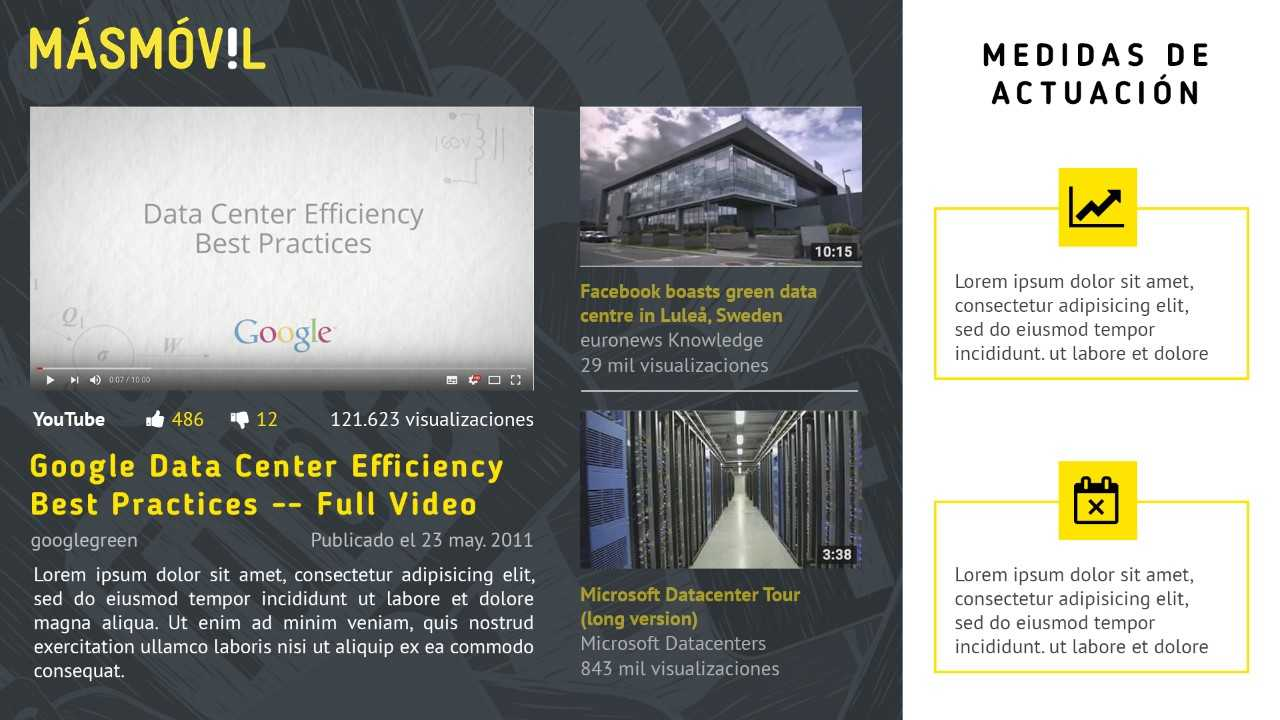
El dashboard se estructura en dos partes, una parte de texto (izquierda), donde se detalla la vulneración de seguridad sufrida y las posibles medidas de actuación para corregirla, y otra parte de imagen (derecha) donde se establece la comparación o símil.



**Figura 5.-** Dashboard 5, correspondiente al escenario número 5 de seguridad.

## Escenario 6: Eficiencia energética.

En este escenario se hará uso de la integración de redes sociales para incentivar acciones de mejora de eficiencia energética por presión de grupo, ejercida por los centros de datos de referencia.

En el dashboard número seis se publican una serie de vídeos y noticias de centros de datos de referencia (con su acción y mejora) y se pretende que el director de operaciones tome alguna medida para su centro de datos (aunque podría elegir no hacer nada), midiendo la efectividad de la presión de grupo en la toma de decisiones. En conctreto, los centros de datos seleccionados fueron aquéllos de Google, Facebook y Microsoft.

**Figura 6.-** Dashboard 6, correspondiente al escenario número 6 de eficiencia energética.

## Escenario 7: Seguridad.

El objetivo de este escenario y su dashboard correspondiente, consiste en crear sensaciones de paz, relajación y descanso (a través de la armonía de colores, formas, sonidos…) para incentivar decisiones de cambios para la mejora de la seguridad en el centro de datos.

De esta manera se pretende comprobar la eficacia de la asociación de sensaciones en la toma de decisiones.

Para ello se ha elaborado un dashboard con colores claros y neutros (como el azul y el blanco) que, junto con la figura relajada del trabajador, transmiten la sensación de paz y tranquilidad buscadas.



**Figura 7.-** Dashboard 7, correspondiente al escenario número 7 de seguridad.