Una iniciativa de:

isms forum CSC CYBER SECURITY CENTRE

En colaboración:

cisco

CyberIndicatorsFramework: el CISO y la Alta Dirección

CyberIndicatorsFramework:

El CISO y la Alta Dirección

Cisco, a través de su programa de inversiones CDA "Country Digital Acceleration", llamado DIGITALIZA en España, está comprometido en acelerar la digitalización de nuestro país en los distintos ámbitos de nuestra economía y sociedad. En particular, el desarrollo del conocimiento y concienciación de la práctica de ciberseguridad en las organizaciones españolas es un punto clave. En este caso ahondamos en el uso de métricas de ciberseguridad relevantes para los Comités de Dirección, y/o Consejos de Administración que permitan comprender el impacto de estos indicadores en la operación de las organizaciones y en los riesgos empresariales a que se enfrentan, para ayudar en la toma de decisiones.

AUTORES

Coordinadores:

Sergio Padilla

Toni García

Nuria Jordi

Participantes

Alberto Bernáldez

Amelia Maria Torres

Angel Ortiz

Carlos Martinez

José Manuel Rivera

Iago Crespo

Javier Pinillos

Josep Bardallo

Manuel Sánchez

Mariano J. Benito

Mario Encinas

Martín de Riquer

Oscar Sánchez

Revisores:

Sergio Padilla

Oscar Sánchez

Gestión de proyecto

Beatriz García

Diseño y Maquetación

Marta Barroso

Beatriz García

CONTENIDO

1.

Introducción y contexto

1.1. Propósito del documento

Existe una gran variedad de organizaciones, con diferentes tamaños, objetivos, misiones y visiones, entre otros aspectos que definen sus modelos de gobierno. Pero en todas ellas existe una persona o comité que tiene la responsabilidad última de tomar las decisiones finales en varios aspectos, uno de ellos es sin duda la seguridad de la información. En este documento nos referiremos a todas ellas, independientemente de sus características, como "organizaciones" y a esas personas o comités como "Alta Dirección".

Asimismo, en las organizaciones existe un rol encargado de gestionar la seguridad de la información. Al igual que en el caso de la Alta Dirección, este rol puede variar considerablemente según la organización. Puede ser una función exclusiva o compartida con otras responsabilidades, y su ubicación dentro de la estructura organizativa puede depender del área tecnológica, de riesgo o de cumplimiento, entre otras. En cualquier caso, este rol debe existir y debe reportar directamente a la Alta Dirección. En este documento nos referiremos a este perfil como "Chief Information Security Officer" o "CISO"; su traducción al español suele ser "Responsable de Seguridad de la Información" o "RSI".

Es importante aclarar que la responsabilidad de la Alta Dirección y la del CISO son complementarias pero distintas: la Alta Dirección tiene la responsabilidad última de la ciberseguridad de la compañía. Debe garantizar que la estrategia de ciberseguridad queda integrada, convenientemente, en la estrategia corporativa, así como supervisar y controlar la implementación de las medidas de gestión de riesgos de ciberseguridad, tomar decisiones y garantizar que los recursos necesarios estén disponibles, entre otras responsabilidades. El CISO deberá definir e implementar la estrategia de ciberseguridad, definir políticas, gestionar los riesgos de seguridad de la información en el día a día, y proporcionar a la Alta Dirección la información necesaria para la toma de decisiones, entre otras muchas actividades. Esta separación de responsabilidades es clave para garantizar una gobernanza efectiva de la seguridad de la información.

El propósito de esta guía es ofrecer al CISO unas pautas que le permitan reportar a la Alta Dirección la información del estado de madurez en cuanto a la seguridad de la información, en forma de un marco de indicadores de riesgo a los que nos referiremos en adelante como KRI, e indicadores de rendimiento a los que nos referiremos como KPI.

Sin embargo, siempre con el foco en que reportar no es un aspecto meramente técnico ni de indicadores, sino que estos son un medio para que el CISO reporte de forma efectiva y, así, la Alta Dirección pueda también cumplir con sus responsabilidades. Las habilidades habitualmente conocidas como "blandas" juegan, pues, un factor determinante.

Sin perjuicio de lo anterior, en este documento ofrecemos también al CISO una serie de buenas prácticas y ejemplos de tipos de indicadores, cómo elegir los mejores indicadores para sus organizaciones, cómo estructurarlos, cómo medirlos y, no menos importante, cómo comunicarlos correctamente a la Alta Dirección. Tener buenas métricas no implica que sepamos comunicarlas correctamente y tener buenos indicadores nos habilita para transformar esta información técnica obtenida de las métricas en datos de valor que permitan a la Alta Dirección tomar decisiones informadas.

También en este documento el CISO encontrará información muy valiosa acerca de los diferentes modelos de reporte, cómo adaptarlos a los diferentes tipos de organizaciones independientemente de su tamaño o composición, cómo personalizar ese reporte a su Alta Dirección y qué habilidades debe tener el CISO para comunicarlas de forma adecuada. Explicaremos en este documento

también actividades más orientadas a la gestión, cómo obtener la información de las diferentes herramientas y fuentes, y cómo transformarla en métricas que nos permitan medir los indicadores correctamente en los cuadros de mando.

1.2. Importancia del reporte a la Alta Dirección y el rol del CISO. Contexto normativo.

Los objetivos principales de la Alta Dirección en cuanto a la seguridad de la información, sin ánimo de ser exhaustivos ni exactos, son: **comprender, guiar y apoyar** la estrategia general de riesgo de la información de la organización y la postura de seguridad actual. Además, tienen la responsabilidad última de asegurar que la organización adopte una postura adecuada frente al riesgo, lo que incluye aprobar la estrategia de ciberseguridad, asignar los recursos necesarios para su ejecución y garantizar el cumplimiento normativo y regulatorio que le aplica. Esta rendición de cuentas no puede ser delegada, aunque sí apoyada y complementada por el trabajo técnico del CISO y su equipo.

Se aseguran de que se establezcan controles, capacidades y medidas adecuadas para proporcionar protecciones razonables, y mantienen la rendición de cuentas al tiempo que fomentan el progreso continuo. No se espera que participen en las operaciones habituales de las actividades de seguridad y riesgo de la información de una organización, ni tampoco que las comprendan profundamente, para eso está el CISO y los equipos que gestionan la seguridad de la información y sus riesgos. Por lo general, forman sus opiniones, análisis y orientación sobre la base de la información que el CISO y otros actores relevantes de su organización les proporciona en un momento dado y ese momento es el del reporte a la Alta Dirección. En ese momento la Alta Dirección utilizará la información recibida y el conocimiento y comprensión de esos indicadores para la toma de decisiones informadas.

Es importante que la Alta Dirección entienda cómo el riesgo de ciberseguridad puede afectar a los objetivos de negocio de la organización, sus actividades y lo vital que es dedicar recursos a reducir ese riesgo y desarrollar la madurez cibernética de su organización.

La Alta Dirección debe tener presente que una gestión deficiente de la ciberseguridad puede derivar en consecuencias legales, operativas y reputacionales graves, y que en muchos marcos regulatorios como la Directiva NIS2 se establece

explícitamente que los órganos de gobierno tienen una responsabilidad directa sobre los riesgos de ciberseguridad y deben implicarse activamente en su supervisión. No es suficiente con delegar: deben estar informados y demostrar diligencia en la toma de decisiones relacionadas con la seguridad.

La Directiva NIS2, en su artículo 20, refuerza esta idea al establecer que los órganos de dirección de las entidades esenciales e importantes deben aprobar las medidas de gestión de riesgos de ciberseguridad, supervisar su aplicación y rendir cuentas de su cumplimiento. Además, exige que los miembros de la Alta Dirección reciban formación periódica en ciberseguridad para garantizar que disponen de los conocimientos necesarios para comprender los riesgos y tomar decisiones informadas. Estas obligaciones legales subrayan que la ciberseguridad no es solo un asunto técnico, sino una responsabilidad estratégica que afecta directamente a la gobernanza corporativa.

Las presentaciones a la Alta Dirección pueden ser estresantes para muchos CISO. Normalmente, sobre todo al principio, el CISO duda de si la información que proporciona será útil y comprensible para la Alta Dirección y, en caso negativo, teme que pierdan el interés en sucesivas reuniones. De ahí la importancia capital, para el CISO y para la compañía, de un buen reporte a la Alta Dirección.

Sin duda alguna, las habilidades blandas o *soft skills* del CISO juegan un papel fundamental. El CISO debe manejar estas habilidades tan bien como las llamadas *hard skills*, más relacionadas con los aspectos técnicos de la ciberseguridad.

El CISO debe enfocar sus reportes en ofrecer información clara, útil y relevante para la toma de decisiones de la Alta Dirección. Esto implica comprender qué aspectos son prioritarios para los líderes estratégicos y estructurar su comunicación para responder directamente a esas necesidades.

Los reportes deben ser concisos, completos e informativos, facilitando decisiones alineadas con los objetivos de negocio y con una adecuada gestión del riesgo. No obstante, hay aspectos que, aunque suelen estar en las prioridades de cualquier organización, debe incluir el reporte del CISO a la Alta Dirección, uno de los más relevantes es el cumplimiento normativo. Es función del CISO comprender el marco regulatorio que le aplica a su organización e informar a la Alta Dirección del estado de ese cumplimiento. Hay normativas y regulaciones que aplican a casi todas las organizaciones y otras que aplican a determinados sectores, el reporte del CISO debe informar en qué grado de

cumplimiento se encuentra la organización y en sucesivos reportes, informar sobre los avances en el nivel de madurez de dicho cumplimiento.

> ***Los reportes deben ser concisos, completos e informativos, facilitando decisiones alineadas con los objetivos de negocio y con una adecuada gestión del riesgo.***

1.3. Importancia de los indicadores en ciberseguridad y un marco estandarizado

Como acabamos de explicar, el reporte de indicadores a la Alta Dirección es un elemento fundamental de las funciones del CISO en el momento de aportar valor a los objetivos de sus organizaciones, pero para que eso ocurra efectivamente y la Alta Dirección no pierda el interés en estos reportes, los indicadores del cuadro de mando deben ser relevantes para la Alta Dirección. Por ello, el éxito del reporte a la Alta Dirección se basa en tener unos buenos indicadores, basados en datos objetivos y no en opiniones del CISO, que sean medibles y comparables con periodos anteriores, que sean accionables y le permita a la Alta Dirección tomar decisiones informadas y sobre todo que sean comprensibles en cuanto al propósito del indicador. Presentar que el 70 % de los empleados ha completado la formación y concienciación en ciberseguridad es un dato relevante, pero insuficiente por sí solo. La Alta Dirección debe comprender qué nivel de riesgo y exposición implica ese porcentaje actual, así como los posibles beneficios de invertir recursos para elevarlo al 80 % o 90 %.

Esta información permite evaluar el retorno en términos de reducción de incidentes, mejora de la resiliencia organizativa, a la vez que el cumplimiento normativo.

Este tipo de información más allá del dato concreto de la métrica es el valor que deben aportar los indicadores que propone el CISO.

Un **marco estandarizado** es la herramienta que permite al CISO gestionar la información que va a componer el reporte a la Alta Dirección, este documento tiene la ambición de proponer un marco estandarizado que permita al CISO de cualquier organización construir su propio cuadro de mando, identificar los indicadores más apropiados para ello, establecer las mejores prácticas en la gestión de estos y cómo presentarlos a la Alta Dirección de la forma más adecuada.

Es evidente y como hemos mencionado al principio del documento, que cada organización es diferente y este marco estandarizado es una base que puede ser adoptada en cada organización, adaptándolo a las particularidades y objetivos de cada una de ellas, pero sin duda es un buen punto de partida y pretende ser una buena ayuda para el CISO en su importante función del reporte a la Alta Dirección.

Estos indicadores no son un fin, sino una herramienta para que el CISO y la Alta Dirección comprendan mejor la ciberseguridad y tomen decisiones informadas.

2.

Marco Estándar de indicadores en Ciberseguridad

2.1. ¿Qué es un indicador?

Un indicador es cualquier medida diseñada para seguir el progreso, facilitar la toma de decisiones o supervisar el rendimiento respecto a un objetivo establecido.

Los indicadores de seguridad de la información sirven para informar de forma objetiva del estado de la seguridad y permitir tomar decisiones a nivel táctico, operacional o estratégico. El objetivo es medir y monitorizar el rendimiento de las actividades de seguridad: *cómo se está ejecutando el programa de seguridad, cuál es el nivel de madurez de la función de ciberseguridad y cuál es el grado de alineación con la estrategia de la organización.*

Se pueden plantear desde diferentes niveles de la organización:

- A nivel de sistemas

Número de vulnerabilidades por sistema, número de puertos abiertos.

- A nivel de programa

Número de incidentes de seguridad, coste por incidente.

- A nivel de organización

Cumplimientos de los objetivos vinculados con la estrategia, Nivel de Riesgos.

De esta forma los CISO podrán demostrar el valor de su área explicando la reducción de los riesgos y también demostrando cómo los planes de seguridad están alineados con la organización utilizando indicadores adecuados. Además, una buena comunicación puede aumentar la colaboración entre áreas y el presupuesto de seguridad.

Un indicador debería tener las siguientes características:

- Exacto

Recopilando los datos adecuados dentro del alcance establecido.

- Preciso

Siempre que sea posible numérico, y en el caso de que sea cualitativo, hay que establecer criterios objetivos para la calificación relativa.

- Correcto

Deben de estar alineados a estándares y metodologías conocidas.

- Consistente

Permitiendo obtener el mismo resultado independientemente de quién y cómo se mida.

- **Basado en el tiempo**
  Permitiendo así establecer un punto fijo de referencia y su evolución temporal.
- **Replicable**
  Bajo las mismas condiciones y desde diferentes puntos de medición.

2.2. Criterios para la selección de indicadores

Existen gran número de indicadores con diferentes objetivos. Permiten entender las propiedades y el comportamiento de los procesos a través de mediciones definidas, repetibles y fáciles de obtener.

Presentamos diferentes criterios:

Por la finalidad que persiguen

- **Métrica**
  Parámetro que puede ser medido directamente y seguido en el tiempo para determinar tendencias.
- **KPI (Key Performance Indicator)**
  Parámetro especializado, generalmente obtenido a partir de varias métricas y que sirve para tomar decisiones de rendimiento de un proceso o negocio.
- **Métrica cuantificable**
  Permite medir el progreso y o variación en el tiempo de un objetivo previamente establecido.
- **KRI (Key Risk Indicator)**
  Métrica que permite identificar, monitorizar y prever la anticipación de un riesgo.
- **OKR (Objectives and Key Results)**
  A partir de un objetivo definido se establecen unas métricas que indican el progreso hacia la consecución del mismo.

Por los aspectos que miden

- **Rendimiento**
  Cantidad de recursos utilizados.
- **Fiabilidad**
  Capacidad de ejecutar funciones específicas bajo ciertas condiciones en cierto intervalo de tiempo.

- **Mantenibilidad**

Habilidad para mantener un proceso eficaz y efectivamente mientras se evoluciona o repara.

- **Usabilidad**

Valora si el servicio es fácil de aprender y operar.

- **Adecuación funcional**

Si las funciones cumplen las necesidades explícitas e implícitas requeridas.

- **Seguridad**

Capacidad para proteger los activos de información.

  - Confidencialidad
  - Integridad
  - Autenticidad
  - Privacidad
  - Rendición de cuentas

- **Grado Implementación**

Muestra el grado de progreso de controles específicos.

- **Eficacia**

Indica como los procesos y controles implementados consiguen el resultado establecido.

- **Eficiencia**

Mide el tiempo, la cobertura y el coste para implementar y ejecutar los controles.

- **Impacto**

Comprueba el impacto del programa de seguridad en relación con la estrategia y objetivos de la organización midiendo aspectos como costos ahorrados e incurridos, nivel de cumplimiento, nivel de riesgo, etc.

Por el nivel al que reportan

- Estratégico.
- Sobre incidentes y el nivel de Riesgos.
- Sobre eficiencia operacional y madurez.
- Respecto a Cumplimiento y no conformidades de Auditoria.
- A nivel de programas y proyectos.
- A nivel de Costes.
- A nivel de objetivos.

Por el espacio temporal en el que se desarrollan

- **Indicadores de progreso (*leading indicators*)**
  Actúan de forma proactiva y predictiva proporcionando información sobre el seguimiento de un proceso o actividad permitiendo predecir o anticipar resultados futuros del funcionamiento previsto de un sistema, favoreciendo así la toma de decisiones antes de que se materialicen los hechos medidos. Son complejos de definir y seguir.
- **Indicadores retrospectivos (*lagging indicators*)**
  Muestran el funcionamiento actual de los sistemas partiendo de datos ya conocidos. Son más sencillos de identificar y monitorizar.

2.2.1. Relevancia estratégica

Es fundamental que los programas de ciberseguridad estén alineados con la estrategia global de la organización y con sus objetivos de negocio. Esta alineación estratégica permite que la ciberseguridad deje de percibirse como una función meramente técnica para convertirse en un habilitador del crecimiento sostenible, la resiliencia y la competitividad. En este contexto, los indicadores son herramientas clave para construir un programa de ciberseguridad eficaz.

Medir la eficiencia operacional, los costes y los beneficios permite confirmar si estamos alineados con los objetivos de la organización. Para ello se debe poner foco en las siguientes cuestiones:

- ¿Cuáles son las principales áreas de riesgos para la compañía y cuál es el plan para mitigarlas?
- ¿Cuáles son los principales riesgos sobre los activos de la información?
- ¿Somos lo suficientemente seguros?
- ¿Cómo estamos en comparación con otras organizaciones?
- ¿Cómo estamos de seguros hoy en comparación con cómo estábamos antes?
- ¿Tenemos una estrategia de seguridad?
- ¿Cuáles son las principales iniciativas de seguridad y como soportan la misión global de la organización?
- ¿Como de efectiva es nuestra respuesta a incidentes y como la testeamos?
- ¿Es el programa de ciberseguridad sostenible financieramente?

Es importante conocer la audiencia a la que se dirige la información y tener muy en cuenta:

- Cuáles son las necesidades de la audiencia:
  - Identificar Riesgos.
  - Valorar costes.
  - Cuál es su visión general de la función de seguridad.
- Qué mensajes clave quiero compartir.
- Cuál es el objetivo de la comunicación:
  - Informar.
  - Persuadir.
  - Crear un foro de discusión o debate.
  - Poner en valor el programa.

2.2.2. Medición y comparabilidad

Los indicadores se deben abordar desde dos perspectivas complementarias:

TOP DOWN

A partir de los objetivos de seguridad establecidos se identifican las métricas que ayuden a determinar si se alcanzan.

BOTTOM UP

Se identifican qué procesos de operaciones de seguridad están implementados para identificar qué métricas útiles se pueden obtener.

Deben ayudar a saber si estamos haciendo lo correcto y si lo estamos haciendo de la forma correcta.

La magnitud es toda propiedad que se pueda medir, esta puede ser directa o relativa.

Los principales son:

La comparabilidad se refiere a cómo los conjuntos de datos se pueden comparar y es clave para interpretar los datos con precisión garantizando los resultados derivados de diferentes orígenes. Estos pueden ser internos o externos. El interno tratar de establecer la coherencia de las mediciones en la organización desde diferentes herramientas y puntos de vista.

El externo supone comparar diferentes conjuntos de datos para que puedan producir información y conclusiones significativas.

Los factores claves que afectan a la comparabilidad son los métodos de medición, cómo definimos las variables y las técnicas de recopilación de los datos.

2.2.3. Escalabilidad y adaptabilidad

La **escalabilidad** se refiere a la capacidad de un sistema para manejar una cantidad creciente de componentes de manera eficiente sin que el aumento de demanda comprometa su rendimiento y funcionalidad.

Para poder gestionarla es conveniente:

- Normalizar el proceso de medición.
- Identificar posibles cuellos de botella.
- Automatizar en la medida de lo posible.
- Tener procesos flexibles ante el crecimiento.
- Revisar periódicamente el proceso de medición para confirmar que cumple con su objetivo.

La **adaptabilidad** es la capacidad de un sistema para ajustarse y responder a los cambios manteniendo o mejorando su funcionalidad eficacia o eficiencia.

Este concepto se puede considerar desde dos puntos de vista:

Como los indicadores se adaptan a cambios en los elementos que miden. Deben aceptar cambios de contexto sin que se distorsione o pervierta el objetivo de la medición.

La capacidad de adaptación de los sistemas a cambios en términos como funcionalidad, eficiencia, eficacia, robustez, fiabilidad o flexibilidad.

2.3. Tipos de indicadores

Los tipos de indicadores referidos en es pueden categorizarse principalmente en dos grandes tipos:

Los KPIs son métricas cuantificables que reflejan el rendimiento de una organización, área, proceso, etc. en relación con los objetivos establecidos.

Los KPIs son herramientas esenciales para medir el éxito y la eficiencia de las acciones emprendidas, permitiendo a las organizaciones tomar decisiones informadas y ajustar sus estrategias según sea necesario.

Su correcta definición y seguimiento permite a las organizaciones tomar decisiones informadas y mejorar continuamente sus procesos y resultados.

Características clave de los KPIs:

- **Específicos:**
  Un KPI debe estar claramente definido y alineado con un objetivo concreto, basándose en datos objetivos y verificables.
- **Medibles:**
  Es esencial que los KPIs sean cuantificables. Esto implica que deben ser expresados en cifras o porcentajes que permitan comparar el rendimiento a lo largo del tiempo.
- **Integrados:**
  Los KPIs deben estar alineados con los objetivos estratégicos de la organización.
- **Alcanzables:**
  Los KPIs deben ser realistas y basarse en la capacidad operativa de la organización con el fin de asegurar que los objetivos sean alcanzables con un esfuerzo razonable.
- **Temporales:**
  Es importante establecer un determinado marco de tiempo para evaluar el desempeño.
- **Comparables:**

Los KPIs deben permitir la comparación a lo largo del tiempo para identificar tendencias y evaluar el progreso.

El objetivo principal de los KPIs es proporcionar información que permita tomar decisiones y realizar acciones concretas.

Los KRIs permiten a las organizaciones identificar y medir los riesgos potenciales que podrían afectar a la consecución de los objetivos de la organización.

Este tipo de indicadores se focalizan en predecir riesgos futuros:

- Detección temprana de riesgos, mediante la identificación de vulnerabilidades que permiten anticiparse a la materialización de aquellos.
- Toma de decisiones, mediante la adaptación de los controles internos de forma proactiva, mejorando la eficiencia y capacidad de respuesta
- Monitorizar continuamente tendencias que permitan identificar la acumulación de riesgos no detectados por otros medios, así como evaluar la efectividad de las medidas de mitigación tomadas.

Características clave de este tipo de indicadores:

- **Medibles:**
  Los KRIs son cuantificables por porcentajes, números, etc. siendo fundamental que puedan ser medidos de manera objetiva.
- **Predictivos:**
  Los KRIs se pueden usar como un sistema de alerta temprana, permitiendo a las organizaciones anticipar problemas antes de que se materialicen.
- **Integrados:**
  Los KRIs se utilizan para moldear la toma de decisiones, debiendo estar integrados en los sistemas de control interno de las organizaciones, alineados con los objetivos de éstas
- **Comparables:**
  Los KRIs se deben poder comparar internamente y con los estándares de la industria.

2.4. Estructura de un indicador

Cada KPI o KRI debe seguir una estructura, la cual debe seguir una serie de pasos para considerar ciertos elementos clave:

- **Definición del objetivo:**
  Establecer claramente el propósito del indicador, alineado con los objetivos estratégicos de la organización.
- **Identificación de riesgos (para KRI) /Identificación de áreas de desempeño (para KPI):**
  Determinar los riesgos/áreas específicas que se desean monitorizar.
- **Aspectos que medir:**
  Definir qué se va a medir, incluyendo la unidad de medida, la periodicidad y los factores internos y externos relevantes.
- **Cuantificación:**
  Asegurarse de que los indicadores sean medibles y expresados en cifras o porcentajes para facilitar la comparación y el análisis.
- **Relevancia:**
  Alinear los indicadores con los objetivos críticos de la organización para asegurar que proporcionen información útil y accionable.
- **Predictividad:**
  Los indicadores deben ser capaces de anticipar posibles problemas antes de que ocurran, permitiendo tomar medidas preventivas.
- **Comparabilidad:**
  Los indicadores deben permitir la comparación a lo largo del tiempo para identificar tendencias y evaluar el progreso.
- **Accionabilidad:**
  Los indicadores deben proporcionar información que permita tomar decisiones informadas y realizar acciones correctivas.
- **Temporalidad:**
  Establecer un marco de tiempo para la evaluación del indicador.
- **Basados en datos:**
  Utilizar datos objetivos y verificables para la construcción de los indicadores.
- **Comunicación clara:**
  Definir y comunicar los indicadores de manera clara y comprensible a todos los miembros de la organización.

- **Monitorización continua:**
  Implementar un sistema de monitorización constante para evaluar el desempeño de los indicadores y ajustar estrategias según sea necesario.
- **Documentación:**
  Mantener una documentación detallada de los indicadores, incluyendo su definición, metodología de cálculo y resultados históricos.
- **Revisión y actualización:**
  Revisar y actualizar periódicamente los indicadores para asegurar que sigan siendo relevantes y efectivos.

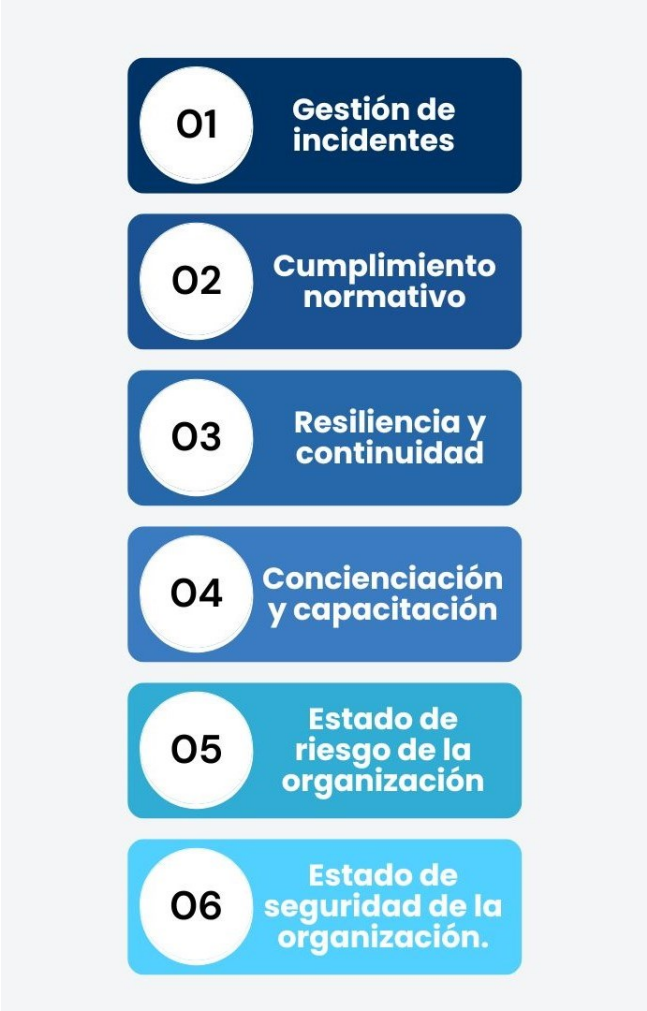
2.5. Categorías de indicadores

Existen diferentes enfoques para definir las categorías que deben incluirse en un cuadro de mando integral que refleje el nivel de salud y madurez de la seguridad de la información de la organización.

Una forma básica de hacerlo consiste en dividir los indicadores según los pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad, sin embargo, una categorización más avanzada podría dividir los indicadores en función de los dominios del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a las normas internacionales de la Organización Internacional de Normalización (ISO), de la certificación ISO 27001, o bien en función del estándar del Instituto Nacional de Estándares y Tecnología (NIST).

Como se ha mencionado previamente, es importante adaptar los indicadores al nivel de madurez de la organización y que estos permitan evolucionar en el cuadro de mandos y ampliar de manera escalable su funcionalidad. No es relevante tener muchos indicadores, sino que estos aporten valor a la hora de informar a la Alta Dirección y que permitan reflejar una evolución constante en la madurez de la organización.

A modo de referencia, se sugiere agrupar los indicadores en seis subcategorías diferentes:



2.5.1. Gestión de incidentes

Las mejores prácticas en SGSI y en gestión de incidentes implican siempre la mejora continua, conforme al ciclo de Deming[1].

Dentro de la categoría de gestión de incidentes se incluyen indicadores sobre el número de incidentes en un periodo de tiempo (último trimestre, año, lustro, etc.), así como indicadores sobre los tiempos de detección del incidente, tiempos medios de reconocimiento, tiempos de respuesta, tiempos de resolución, tiempos de implementación de las lecciones aprendidas durante el incidente, esfuerzo económico, tiempo y recursos dedicados a la resolución de incidentes, incidentes recategorizados, tasa de reincidencia, etc.

2.5.2. Cumplimiento normativo

En un entorno cada vez más regulado, los indicadores de cumplimiento normativo son cada vez más importantes para las organizaciones.

Más allá de si la organización ha certificado su SGSI conforme a la ISO 27001 (o cualquier otra norma ISO relativa a la seguridad de la información), o al estándar NIST, dependiendo del sector de la organización y de su tamaño, podrían aplicarse normativas tales como la Directiva sobre «*Network and Information Systems*» (NIS2), el *Reglamento Digital Operacional de Resiliencia* (DORA), la *Ley de Ciberresiliencia de la Unión Europea (EU Cyber Resilience Act*), *la Ley de Transferibilidad y Responsabilidad del Seguro de Salud (Health Insurance Portability and Accountability Act*, *HIPAA*) y el *Reglamento de la Industria de Tarjetas de Pago* (*Payment Card Industry*, PCI), por nombrar solo algunas.

Estas normas y estándares internacionales o europeos tienen continuidad en España con normativas como el *Esquema Nacional de Seguridad* (ENS) o la *Ley de Infraestructuras Críticas*.

[1] *El* ***ciclo PHVA****, el* ***ciclo de Shewhart*** *y el* ***ciclo de Deming*** *son diseños iterativos y métodos de gestión desarrollados para iniciar procesos de mejora continua en diferentes empresas de producción de bienes y servicios.*

Asimismo, es posible que desde el ámbito de la seguridad de la información se requiera o se considere relevante implementar indicadores referentes al *Reglamento General de Protección de Datos* (RGPD), que, si bien quedarían bajo el ámbito de la figura de delegado de protección de datos personales, requieren controles técnicos para su implementación.

No es objeto de la presente guía detallar los indicadores correspondientes a cada una de estas regulaciones, dada su diversidad y ámbito, sino ofrecer una idea de los indicadores que sería necesario implementar en cada organización, dependiendo de las regulaciones sectoriales o generalistas que le puedan afectar.

2.5.3. Resiliencia y continuidad

Los indicadores de resiliencia y continuidad muestran a la Alta Dirección la capacidad de recuperación y reducción del tiempo de inactividad de la organización en caso de ataque. También incluyen información sobre las pruebas y simulacros realizados para preparar a la organización ante un posible incidente.

Relacionada con el punto anterior, de cumplimiento normativo, es posible, también, incluir los controles relacionados con la norma ISO 22301, Sistema de Gestión de la Continuidad de Negocio, para gestionar los riesgos generales a los que esté expuesta la continuidad del negocio de una organización.

Los indicadores deben estar adaptados al tiempo objetivo para la recuperación (RTO, por sus siglas en inglés) y al punto objetivo de recuperación (RPO), definidos por la Alta Dirección, y mostrar no solo las capacidades de redundancia de la organización (porcentaje de equipos con copias de seguridad, tanto de equipos de usuario como de servidores de información y almacenamiento total, tiempos de restauración, etc.), sino también la eficiencia de estas conforme a criterios de coste o de sostenibilidad (por ejemplo, conforme al pacto de la ciberseguridad sostenible «*Cyber Green Proof*[2]» de ISMS Forum).

2.5.4. Concienciación y capacitación

Esta categoría incluye todo tipo de formaciones destinadas a los empleados de la organización para mostrar a la Alta Dirección que se ha instruido a los empleados de manera continuada.

[2] https://master.ismsforum.es/pacto/

Los indicadores deben mostrar tanto los cursos realizados por los empleados como las tasas de éxito, el porcentaje de empleados que no han terminado la formación y la media de las calificaciones obtenidas. Muchas herramientas de concienciación y capacitación ofrecen también indicadores por departamento o por país, e incluso por sector.

Si la organización realiza pruebas para medir la propensión de sus empleados a caer en un engaño que permita a un atacante usarles como vector de entrada (por ejemplo, enviar correos electrónicos simulando phishing, usar códigos QR, hacer llamadas de devolución, etc.), también deberán incluirse en esta categoría.

Los indicadores de concienciación y capacitación deberán garantizar siempre el anonimato y el respeto por los empleados mediante la utilización de datos agregados.

2.5.5. Estado de riesgo de la organización

Los indicadores clave del riesgo (Key Risk Indicator o KRI, por sus siglas en inglés) muestran el nivel de riesgo que posee una organización ante una amenaza o evento determinado que pueda afectarle y suelen estar asociados a un indicador clave de rendimiento (Key Performance Indicator o KPI). Los indicadores clave del riesgo deben basarse en un análisis de riesgos y en el mapa de riesgos de la organización, y estar alineados con el apetito de riesgo definido por esta. El objetivo final de los KRI es monitorizar los riesgos de manera proactiva y constante para ayudar a prevenir que el riesgo se materialice.

Algunos ejemplos de KRIs pueden ser el riesgo de que se materialice una brecha de datos debido a una fuga en un proveedor, el riesgo de que se materialice un riesgo de cumplimiento, el riesgo de que se materialice un error humano o el riesgo de que se materialice un fallo en la copia de seguridad de una base de datos.

2.5.6. Estado de seguridad de la organización

Una de las preguntas más habituales que la Alta Dirección le hace al CISO es: «¿Estamos seguros?». O cuando ven en la prensa una noticia sobre un gran organismo que ha sido atacado: «¿Esto nos puede ocurrir a nosotros?».

Más allá de que estas preguntas tengan difícil contestación, el estado de seguridad de la organización muestra los indicadores que, a alto nivel, indican el nivel de salud y madurez de la organización en general.

Dichos indicadores deben mostrar, además, la mejora constante de los niveles de madurez de la organización con el paso del tiempo.

2.6. Ejemplos de indicadores

En la ciberseguridad los indicadores se pueden agrupar en dos grandes bloques. Aquí se incluyen algunos ejemplos relevantes y representativos:

1.Indicadores Técnicos:

A. Amenazas externas:

- Numero de infecciones por dispositivo.
- Numero de vulnerabilidades conocidas no resueltas.
- Numero de certificados no configurados correctamente.

B. Amenazas Internas:

- Número se usuarios con accesos privilegiados.
- Número de días entre notificación de una baja de usuario y eliminación de accesos.

C. Concienciación:

- Porcentaje de empleados que han realizado entrenamiento en ciberseguridad.
- Porcentaje de campañas de simulación de phishing.

D. Gestión de Incidentes:

- tiempo medio de resolución de un incidente.
- Número de análisis realizados.
- Número de incidentes reportados
- Etc.

E. Operación:

- Número y tiempo de componentes disponibles.

- Gestión de alertas.
- Tiempo medio de resolución de vulnerabilidades.
- Porcentaje de sistemas parcheados.
- Etc.

F. Auditoria y Cumplimiento:

- Tiempo medio de resolución de no conformidades.
- Numero de cumplimientos por proyecto.

G. Cadena de Suministro:

- Porcentaje de software de terceros escaneado antes de su despliegue.
- Frecuencia con que se verifican controles de terceros.
- Etc.

2.Indicadores de Gobierno de la Seguridad

A. Nivel de Adopción del Programa de ciberseguridad:

- %De proyectos de seguridad planificados vs implementados,
- % De servicios y activos cubiertos.

B. Nivel de Gobierno:

- % de funciones IT cubiertas.
- % de Excepciones es vs gestión de Riesgos.
- KRIS vinculados a seguridad.
- % Progreso cumplimiento objetivos de seguridad.

C. Eficiencia Operacional:

- % de incidentes reportados.
- tiempo medio de resolución.

D. Mitigación de Riesgos:

- % de cumplimiento de las políticas de seguridad.
- % desviación línea base de seguridad.
- Severidad de las excepciones.

E. Alineación con el valor de negocio:

- Número de clientes y proveedores impactados por los incidentes.
- % de servicios afectados.
- % de Proveedores incluidos en el programa de seguridad.

F. Costes:

- % de IT asignado a seguridad.
- % de presupuesto reservado vs consumido.
- Etc.

3.

Modelos de reporting y cuadros de mando

En entornos corporativos cada vez más complejos, inciertos y orientados al dato, los modelos de reportes a la Alta Dirección se han convertido en una herramienta estratégica para la toma de decisiones informadas. Un reporte efectivo no solo presenta información, sino que traduce datos en conocimiento accionable. Esto es particularmente relevante en el caso de funciones críticas como la ciberseguridad, donde el CISO desempeña un rol clave no solo técnico, sino estratégico.

Los principios fundamentales de un reporte efectivo como la relevancia estratégica, la claridad, el enfoque en KPIs y la visualización efectiva son esenciales para garantizar que la Alta Dirección pueda interpretar rápidamente el estado del negocio y anticipar riesgos. En este contexto, los cuadros de mando se convierten en instrumentos vitales que deben ser diseñados con precisión, narrativa visual y enfoque en el valor, más que en el volumen de datos.

El CISO, tradicionalmente percibido como un rol técnico, ha evolucionado hacia una figura que puede llegar a estar plenamente integrada en la Alta Dirección. Debe ser considerado como una parte más del negocio, cuyo propósito no es únicamente proteger, sino **habilitar el negocio** a través de una gestión del riesgo cibernético alineada con los objetivos estratégicos de la organización. Esto implica que el CISO debe ser capaz de comunicar claramente a través de reportes ejecutivos y dashboards el estado de la ciberseguridad, las amenazas emergentes, el nivel de exposición y, sobre todo, el impacto potencial sobre la continuidad operativa, la reputación y la rentabilidad.

En muchas organizaciones, el CISO ya no reporta únicamente al CIO, si es que ese era el caso (era bastante habitual), sino que participa directamente en comités de dirección, reportando a otros *C-Level*, al CEO o incluso al consejo. Esta cercanía con la Alta Dirección exige que su comunicación sea clara, directa y orientada a negocio. El CISO debe facilitar una **toma de decisiones informada sobre riesgos tecnológicos y de seguridad**, permitiendo a la organización asumir riesgos de forma consciente y controlada, en lugar de evitarlos por desconocimiento.

En resumen, la claridad y concisión en el reporte a la Alta Dirección no es solo una cuestión de forma, sino de fondo. Es la base para una conversación estratégica en la que la ciberseguridad deja de ser un tema aislado para convertirse en un **habilitador clave del crecimiento, la innovación y la resiliencia empresarial**.

3.1. Principios para un reporte efectivo a la Alta Dirección

La efectividad de un modelo de reporte dirigido a la Alta Dirección no se mide solo por la cantidad de información que presenta, sino por su capacidad para facilitar decisiones estratégicas de forma ágil y fundamentada. A continuación, se desarrollan los principios esenciales que deben guiar la construcción y presentación de estos reportes:

1. Relevancia estratégica

La Alta Dirección necesita información alineada con las prioridades estratégicas de la organización. Esto implica que el contenido del reporte debe responder a las preguntas clave del negocio: ¿Estamos avanzando hacia nuestros objetivos? ¿Dónde están los principales cuellos de botella o riesgos? ¿Qué áreas requieren intervención inmediata?

Deben evitarse incluir métricas operativas o detalles que no agregan valor a la visión estratégica es esencial. En cambio, se debe privilegiar aquella información que permita evaluar el cumplimiento de los pilares estratégicos, como crecimiento, eficiencia, innovación, sostenibilidad, experiencia del cliente o transformación digital.

2. Claridad y concisión

El tiempo de la Alta Dirección es limitado, lo que conlleva tiempos limitados para la exposición y reporte del estado de la ciberseguridad y riesgos, que podría verse limitado, también, por problemas de agenda. Por eso, un buen reporte ejecutivo debe eliminar lo superfluo y priorizar una comunicación clara y sintética. Esto se traduce en:

- Uso de lenguaje ejecutivo, evitando jerga técnica innecesaria.
- Titulares o *insights* al inicio de cada bloque o gráfico.
- Informes de una extensión manejable (por ejemplo, máximo 10-15 páginas o una pantalla si es digital).
- Resúmenes ejecutivos que permitan captar el estado general en pocos minutos.

Menos, es más: la capacidad de síntesis no implica pérdida de profundidad, sino inteligencia en la selección de lo relevante para la Alta Dirección.

3. Enfoque en indicadores clave (KPIs)

Los indicadores clave de desempeño (KPIs) son la columna vertebral del reporte ejecutivo. No basta con incluir métricas, sino que deben seleccionarse aquellos KPIs que realmente representen los resultados críticos de la organización.

Cada KPI debe contar con:

- Un valor actual y su comparación con el objetivo o *benchmark*.
- Su tendencia en el tiempo.
- Umbrales predefinidos que indiquen si está en zona de control, alerta o crítica.
- Un análisis contextual que explique posibles desviaciones y medidas correctivas.

El uso de KPIs debería permitir transformar datos en información y esta, en decisiones relevantes e informadas por parte de tu audiencia.

4. Visibilidad de riesgos y oportunidades

Un reporte efectivo no debe limitarse a mostrar el estado actual, sino que debe mostrar una visión, proyectando escenarios futuros. Esto implica:

- Identificar riesgos emergentes (operativos, financieros, regulatorios, reputacionales, etc.) y su impacto potencial.
- Visibilizar oportunidades estratégicas: nuevas líneas de negocio, mejoras de eficiencia, sinergias, alianzas, etc.
- Ofrecer una visión de impacto cruzado: cómo un riesgo en un área puede afectar otras dimensiones del negocio.

Incorporar esta dimensión proactiva permite a la Alta Dirección anticiparse y no solo reaccionar. Esta será una palanca clave para defender estrategias y planes de ciberseguridad que permitan la asignación de recursos a un área tan crítica como la ciberseguridad.

5. Integridad y trazabilidad de los datos

La confianza en la información presentada es crítica. Para garantizarla, el reporte debe sustentarse en datos precisos, completos y provenientes de fuentes confiables. Además, debe ser posible:

- Ver la fuente de cada dato o métrica, ya sea a través de una leyenda o metadatos accesibles.
- Rastrear la transformación del dato hasta el indicador final.
- Hay que asegurar que los datos han sido validados y auditados previamente a su publicación.

Una sola inconsistencia puede poner en duda todo el reporte y comprometer decisiones estratégicas. En este sentido, un dato matizable o no del todo claro podría generar un debate alrededor del mismo y en ese momento se perdería el foco del reporte.

6. Periodicidad y consistencia

Un buen modelo de *reporting* requiere una cadencia definida que responda a las necesidades de control y decisión: semanal para seguimiento de operaciones críticas, mensual para desempeño general, trimestral para revisión estratégica, por ejemplo.

Además, la consistencia en el formato, estructura y visualización de los reportes facilita la lectura rápida, la comparación temporal y la identificación de patrones. Cambios frecuentes en el diseño o los indicadores dificultan la lectura y reducen la eficacia del reporte.

7. Adaptabilidad al perfil del lector

No todos los ejecutivos requieren la misma profundidad ni visualización de la información. Un CFO puede estar más enfocado en aspectos financieros, mientras que un CEO busca una visión global y transversal del negocio.

3.2. Elementos clave de un cuadro de mandos

El cuadro de mando es una herramienta esencial para facilitar el seguimiento estratégico, operativo y financiero de una organización. Su valor reside en su capacidad para sintetizar grandes volúmenes de información en visualizaciones claras que permiten evaluar el estado general del negocio y tomar decisiones informadas. Para cumplir este propósito, debe construirse sobre una arquitectura sólida compuesta por los siguientes elementos clave:

1. Objetivos estratégicos vinculados

Todo cuadro de mando debe partir de una clara vinculación con los objetivos estratégicos de la organización. Cada métrica o visualización que se presenta debe responder a una pregunta estratégica concreta: ¿Cómo vamos en la ejecución de nuestra estrategia? ¿Qué indicadores nos alertan de posibles desvíos?

Esta alineación garantiza que el dashboard no se convierta en una acumulación de datos, sino en una herramienta de gestión efectiva.

2. Indicadores clave de desempeño (KPIs)

Los KPIs son el núcleo del cuadro de mando. Deben ser seleccionados con criterios claros de relevancia, representatividad y capacidad de acción. Algunos aspectos esenciales incluyen:

- Definición clara: qué mide, cómo se calcula y por qué es importante.
- Periodicidad de actualización: diaria, semanal, mensual, etc.
- Unidad de medida y metas asociadas: establecer rangos aceptables, objetivos y alertas.
- Visualización adecuada: uso de gráficos, tablas, semáforos o velocímetros para facilitar la lectura rápida.

La selección de KPIs debe limitarse a los más significativos, evitando la "infoxicación".

3. Dimensiones de análisis

Un cuadro de mando efectivo permite ver los indicadores desde distintas perspectivas, conocidas como dimensiones: por unidad de negocio, por región, por canal, por segmento de cliente, por producto, entre otras.

Estas dimensiones permiten detectar patrones, causas raíz y oportunidades de mejora que no serían visibles en una vista agregada. También favorecen una gestión más granular y focalizada.

4. Línea base y evolución temporal

Para interpretar correctamente cualquier indicador, es necesario conocer su evolución en el tiempo. El cuadro de mando debe incluir comparativas:

- Versus el período anterior (mensual, trimestral, anual).
- Versus el objetivo o presupuesto.
- Versus benchmarking del sector (si aplica).

Este enfoque temporal permite identificar tendencias, estacionalidades o desviaciones estructurales que requieren atención.

5. Alertas y semáforos de desempeño

Aunque en algunos contextos ha surgido debate sobre el riesgo de "simplificar en exceso" los informes a la Alta Dirección, los sistemas visuales de alerta siguen siendo una opción recomendable. Semáforos en sus diferentes variantes, íconos de alerta o etiquetas de prioridad ayudan a identificar rápidamente situaciones críticas o áreas bajo control, aunque su uso depende del estilo del CISO y de las preferencias de la audiencia.

Estas alertas pueden configurarse en función de umbrales definidos previamente, siempre alineados con la tolerancia al riesgo y los objetivos del negocio, y adaptarse al nivel de detalle y formalidad que demande la Alta Dirección.

6. Narrativa y contexto

Detrás de cada indicador debe haber una breve explicación que contextualice su evolución: ¿qué lo está afectando? ¿qué acciones se han tomado? ¿cuáles son las perspectivas futuras?

Incluir breves anotaciones, insights o análisis integrados dentro del dashboards (por ejemplo, mediante "tooltips" o campos de texto) enriquece su valor informativo y evita malinterpretaciones.

3.3. Diseño visual y presentación de Información

El diseño visual no es un aspecto estético accesorio, sino un componente esencial de la eficacia del reporte a la Alta Dirección. Una visualización bien diseñada mejora la comprensión, reduce el tiempo de análisis y permite focalizar la atención en los elementos más relevantes. En cambio, un diseño pobre puede llevar a interpretaciones erróneas, fatiga visual o incluso a la desestimación del informe.

A continuación, se detallan los principios fundamentales para un diseño visual efectivo:

1. Claridad, ante todo

La función principal del diseño visual es facilitar la comprensión. Esto implica:

- Evitar el exceso de colores, formas o efectos visuales innecesarios.
- Utilizar tipografías legibles y de tamaño adecuado.
- Presentar la información de manera jerárquica, destacando lo más importante.
- Usar espacios en blanco estratégicamente para evitar saturación visual.

Cada elemento gráfico debe tener una razón de ser y contribuir al objetivo informativo.

2. Elección adecuada de gráficos

Cada tipo de dato requiere un tipo de gráfico específico que facilite su interpretación:

- Gráficos de barras/columnas: ideales para comparar valores entre categorías.
- Gráficos de líneas: útiles para mostrar tendencias a lo largo del tiempo.
- Gráficos de pastel: solo recomendables para proporciones simples (y con pocos elementos).
- Indicadores tipo velocímetro o termómetro: eficaces para mostrar KPIs con umbrales.
- Mapas de calor o matrices: útiles para mostrar niveles de intensidad o correlaciones.

Evitar gráficos 3D, innecesariamente complejos o decorativos, que dificultan la lectura o distorsionan la percepción de los datos.

3. Codificación visual coherente

El uso de colores, íconos y formas debe ser consistente en todo el reporte. Algunas recomendaciones clave:

- Utilizar colores asociados a significados claros (verde = positivo, rojo = negativo, amarillo = alerta).
- No abusar de la paleta cromática: 3 a 5 colores principales suelen ser suficientes.

- Usar íconos o etiquetas estándar que sean reconocibles (por ejemplo, triángulo de alerta, check de cumplimiento).
- Evitar colores similares para indicadores con significados distintos, especialmente en públicos con dificultades visuales o daltónicos (considerar accesibilidad).

La coherencia visual ayuda a crear patrones cognitivos que aceleran la interpretación.

4. Enfoque en la narrativa visual

Un buen diseño no solo presenta datos, sino que cuenta una historia. El orden de los elementos, su agrupación y énfasis deben guiar al lector hacia las conclusiones clave.

- Incluir títulos claros con mensajes interpretativos ("Ventas crecen 15% respecto al trimestre anterior") en lugar de títulos genéricos ("Evolución de ventas").
- Organizar los elementos de izquierda a derecha y de arriba hacia abajo, como lectura natural.
- Agrupar indicadores relacionados para facilitar la lectura por bloques temáticos (finanzas, clientes, operaciones).

Esta narrativa visual convierte al dashboards en una herramienta de comunicación estratégica.

5. Minimización de la carga cognitiva

El diseño debe facilitar la toma de decisiones, no exigir un esfuerzo mental excesivo para interpretar los datos. Algunas prácticas recomendadas:

- Evitar "dashboards sobrecargados" con demasiados KPIs o gráficos en una sola vista.
- Usar agrupaciones lógicas y separadores visuales para organizar la información.
- Priorizar los datos más relevantes y dejar los detalles para una segunda capa o vista expandida.

Un diseño limpio, intuitivo y centrado en el usuario ejecutivo maximiza el impacto del reporte.

3.4. Personalización según el público objetivo (CEO, CFO, CIO, Comité de dirección, Consejo de administración, etc.)

Es importante identificar la audiencia a la que van dirigidos los indicadores de seguridad: cuáles son sus intereses, sus necesidades, sus preocupaciones y el conocimiento que disponen sobre esta área.

El CEO y su equipo de dirección necesita tener en cuenta el progreso y la madurez del programa de ciberseguridad de la organización, así como su efectividad y su alineamiento con la estrategia general, incluyendo el apetito al riesgo y aportando una metodología adecuada de la gestión de los mismos. Esto dará confianza, por ejemplo, al CEO para reportar al Consejo de Administración una visión precisa de la situación y de las acciones necesarias a desplegar en caso de crisis o indicadores desfavorables.

El consejo de administración como órgano máximo que controla la estrategia de la organización y supervisa la actuación de la dirección en la consecución de la misma desempeña un rol clave en la gestión de los riesgos de ciberseguridad.

Para ello deben de entenderlo como un riesgo estratégico:

- Conocer las principales regulaciones y cumplimientos normativos relacionados.
- Conocer cuál es la cultura de ciberseguridad en la organización.
- Asegurar que se disponen de los recursos adecuados.
- Conocer y evaluar los riesgos. Conocer los planes de respuesta y los principales incidentes.

Cada área corporativa tendrá un interés más relacionado con la función que desempeñan desde 2 puntos de vista:

A. Desde los procesos de negocio de los que la propia área es responsable y cómo los activos de información involucrados son cubiertos por el programa de ciberseguridad.

B. Desde la rendición de cuentas que desde el área de ciberseguridad se debe dar al área específica. Los principales casos serán:

a. CIO. Quien necesitará una visión más operativa del programa, incluyendo los componentes tecnológicos empleados y las funciones de seguridad directas o complementarias que se deben de realizar desde el área de tecnología.

b. CFO. Necesitará una visión financiera del programa, progreso del presupuesto, desviaciones y posibles ahorros.

c. Recursos Humanos. interés en el despliegue del plan de formación y concienciación de los empleados de la organización.

d. Legal y Cumplimiento. Foco en cómo se implementan las diferentes regulaciones y estándares necesarios,

Para una mejor adaptación al público objetivo el CISO necesitará conocer las metas estratégicas de la organización, los procesos clave, las tecnologías empleadas, así como los principales escenarios de riesgos y su exposición a los mismos.

3.5. Integración con herramientas de gestión y monitorización

DASHBOARD. Un cuadro de mando de seguridad muestra la visualización de información que permite al CISO obtener conclusiones basadas en datos para ser usadas en toma de decisiones basadas en datos. Según su finalidad puede consolidar y centralizar datos tanto de amenazas, cumplimiento, rendimiento como otros datos de seguridad. Para ello se emplearán gráficos, tablas y recursos visuales que hagan más fácil la comprensión de los datos. Los tipos de dashboards se pueden clasificar en:

1. Estratégico: muestra los indicadores clave sobre la salud organizacional y ayuda a la dirección a identificar oportunidades y amenazas.

2. Analítico: Ofrecen análisis detallados de tendencias, midiendo datos que varían con el tiempo.

3. Operacional: Centrados en indicadores clave de rendimientos: KPIs.

4. Táctico: empleados en los niveles medio de gestión profundizando en áreas clave de la organización.

Al apoyarse en la visualización de datos deberán de lograr maximizar la representación visual y optimizando su contenido. A las recomendaciones indicadas anteriormente se podrían añadir:

- Usar jerarquías visuales.
- Usar bien los espacios.
- Escoger bien los colores.
- Aplicar la regla de los cinco segundos: el usuario en ese tiempo debe ser capaz de identificar la información relevante.
- Ser minimalista: menos, es más. No superar un número razonable de elementos visuales (por ejemplo, diez).

La información puede ser recogida en tiempo real, o recogida previamente de diferentes fuentes de datos. Crear un dashboard manual requiere consolidar datos de diferentes orígenes y después mostrarla en una plataforma que muestre los datos de forma integrada. Opciones validas pueden ir desde utilizar una hoja de cálculo consolidada diseñando una colección de gráficos y elementos visuales, o cuando el volumen se complica yendo a herramientas como PowerBI o Tableu alimentadas por diferentes hojas de cálculo en las que posteriormente se agregue toda la información en un cuadro de mando adaptado a las necesidades.

La alternativa más sofisticada sería integrar de forma directa las diferentes plataformas origen consiguiendo una visión en tiempo real. Aquí el reto es integrar las diferentes herramientas de monitorización de gestión de logs, de vulnerabilidades, de end points, de gestión de riesgos, de gestión de identidades, de gestión de brechas en una sola plataforma que permita integrarlos, personalizarlos y obtener diferentes vistas en función de cada audiencia.

Existen soluciones que conectan directamente mediante APIs a diferentes herramientas de monitorización de ciberseguridad permitiendo consolidar la información obtenida en tiempo real en diferentes tipos de Dashboards según el interés.

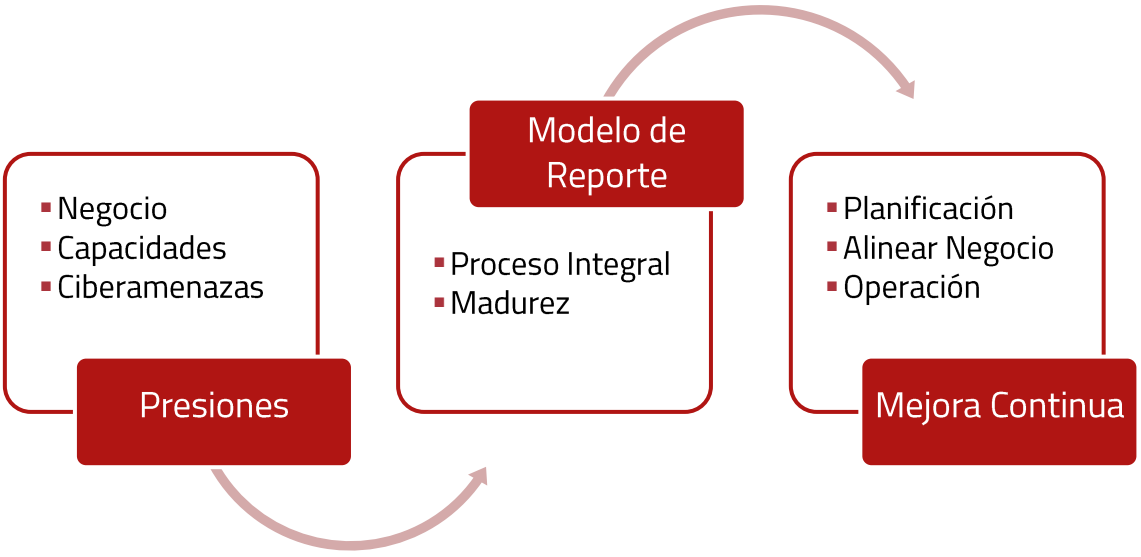
4.

Implementación y mejores prácticas

La implementación de un sistema de indicadores en ciberseguridad es proceso de adaptación continua de la función de ciberseguridad a las necesidades de la organización en la que opera, tanto por la evolución de sus **actividades de negocio**, las necesidades de sus accionistas y *stakeholders*, o las **capacidades y recursos internos y externos** de que dispone, como por la constante evolución del **escenario de ciberseguridad** y las amenazas y actores a los que está expuesta la organización.

Por ello, el proceso de reporte no debe responder a un modelo estático, que pueda ser diseñado e implementado en una fase inicial para luego mantenerlo en el tiempo. Por el contrario, debe ser entendido e implementado como un proceso organizativo integral que requiere de mejora continua en su planificación estratégica, la alineación con las necesidades de la organización y en la implementación operativa del propio modelo.

En este capítulo se detallan las mejores prácticas para adoptar el modelo propuesto, incluyendo los pasos fundamentales para su puesta en marcha, el papel de la automatización e inteligencia artificial y los desafíos comunes que surgen durante su implementación, junto con las soluciones más eficaces.



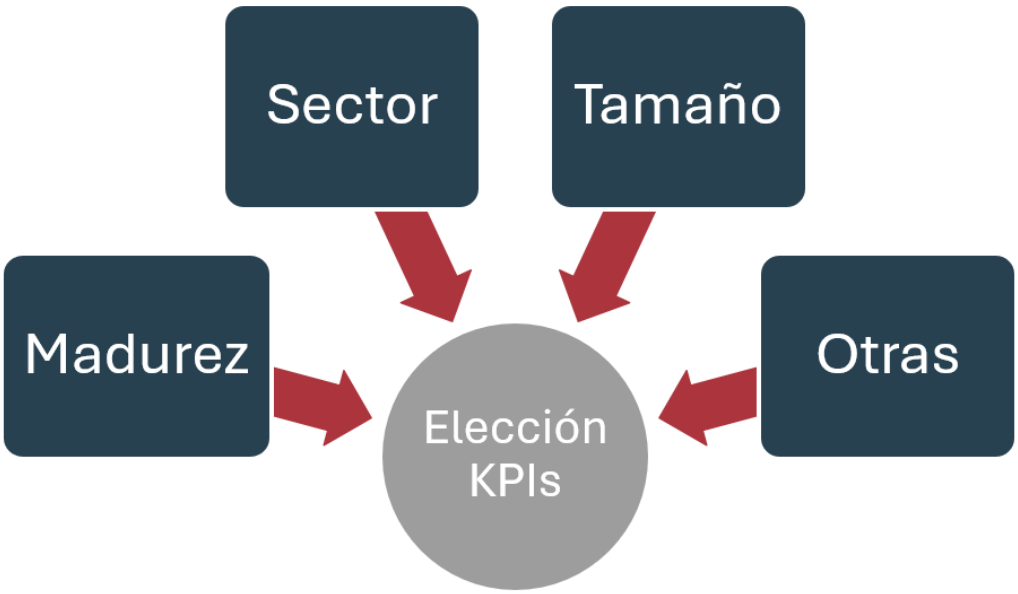
4.1. Cómo adoptar el modelo en diferentes tipos de organizaciones

El capítulo 3 de este documento ha abordado los requisitos que deben satisfacer los indicadores que se seleccionen para realizar el reporte a la dirección, tanto los KPI de la organización como aquellos otros indicadores que pueden soportar y complementar a estos KPIs, o aquellos que pueden aportar información relevante en circunstancias o momentos concretos.

Por lo tanto, la diferencias entre la implantación de un modelo en las distintas organizaciones se pueden resumir, principalmente, en cuatro tipos:

- Madurez en ciberseguridad de la organización y de sus directivos, así como dónde está encuadrado, orgánicamente, el CISO.
- Necesidades de negocio y regulatorias propias de los sectores en los que tiene presencia y que son similares a los de sus competidores, así como presencia internacional y configuración y complejidad de la organización
- Tamaño y/o recursos disponibles para el proceso de ciberseguridad y su reporte.
- Necesidades concretas puntuales de reporte, incluyendo información sobre nuevas amenazas o lecciones aprendidas de incidentes previos, así como todo d tipo de circunstancias que pueda influir en estos reportes.

La combinación de estos factores debe permitir que la CISO y la Dirección de la organización identifiquen los KPIs que deben ser recogidos en el modelo de reporte a la dirección que implante. Y también debe guiarle en la evolución del modelo en el tiempo.



De todos los elementos anteriores, la **madurez de la organización** condiciona de forma más decisiva la adopción del modelo. No todas parten del mismo punto en su gestión de la ciberseguridad ni están preparadas para entender el valor e información que contienen algunos indicadores más avanzados. Por ello, el responsable de seguridad debe comenzar con una autoevaluación realista de la madurez de la organización. Esto incluye la existencia y madurez del Sistema de Gestión de Seguridad de la Información (SGSI), la asignación de roles de ciberseguridad y la capacitación de las personas que los desempeñan, existencia de políticas, controles aplicados, recursos asignados a ciberseguridad o nivel de automatización. Y también debe valorar la cultura de la organización respecto del reporte a la dirección en otras áreas y la receptividad de la dirección a esta información.

En este sentido, una organización con bajo nivel de madurez en ciberseguridad o en reporte a la dirección deberá optar inicialmente por un conjunto reducido de indicadores básicos sobre actividades de ciberseguridad intuitivas y básicas: por ejemplo, la gestión de incidentes o el cumplimiento normativo. En cambio, una organización más madura y consolidada podrá adoptar un enfoque más avanzado, incorporando KPIs de carácter predictivo, indicadores de eficiencia, benchmarking sectorial, e integración completa con herramientas tecnológicas. El responsable de seguridad debe ser capaz de identificar el nivel correcto de madurez y conducir a la organización a estadios más avanzados y maduros en el reporte de ciberseguridad, optimizando a la vez los recursos dedicados a esta actividad.

El segundo factor más relevante es el **sector de actividad** en el que opera la organización. Existen sectores sujetos a una fuerte presión normativa (como el financiero, sanitario, energía o el sector público) donde los indicadores deben estar alineados con estándares y marcos regulatorios específicos. Por ejemplo, las entidades financieras deberán incorporar indicadores relacionados con DORA, NIS2, EBA Guidelines y el NIST CSF[3], mientras que una entidad sanitaria deberá prestar especial atención a la protección de datos personales sensibles conforme a GDPR y normativa sanitaria específica.

Por otra parte, es posible que haya organizaciones en el sector que tengan una madurez en ciberseguridad superior a la propia y que ya hayan avanzado en la identificación de KPIs relevantes y apropiados a las necesidades de negocio sectoriales. La disponibilidad de esta información permite al responsable de ciberseguridad acelerar la selección de KPIs relevantes. También puede permitir el

[3] ***NIST CSF (NIST Cybersecurity Framework)*** *es un marco desarrollado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) que proporciona directrices voluntarias para gestionar y reducir los riesgos de ciberseguridad.*

intercambio de información comparable entre organizaciones del sector para realizar *benchmarking*, tanto por las propias organizaciones como por otras entidades externas: reguladores, asociaciones sectoriales, estudios de mercado u otras. La implementación sectorial debe implicar a áreas especializadas, como cumplimiento normativo, legal o regulatorio, para asegurar que los indicadores cumplen con los requisitos y expectativas de los entes supervisores y auditores.

El tercer factor es el **tamaño y disponibilidad de recursos** de la organización. En este caso, es un factor limitante. Debe disponerse de recursos suficientes para la obtención de todos los KPIs relevantes. En caso contrario, deben descartarse KPIs e informar a la dirección de su indisponibilidad por falta de recursos suficientes. El responsable de seguridad no debe ocultar esta información a la dirección ya que generará un debate sobre aspectos muy relevantes para la CISO de la organización: la relevancia o no del KPI para la dirección; sus preferencias entre los distintos KPI; el aumento de madurez de la dirección sobre ciberseguridad; la dotación de presupuesto adicional; etc.

En el extremo opuesto, la CISO debe limitar severamente el uso de recursos para KPIs que han sido descartados por la dirección, para optimizar su presupuesto. Ello no quiere decir que no se deban calcular, porque pueden ser de utilidad para otras áreas. Pero el esfuerzo en cálculo y cómputo de KPIs debe estar alineado con el valor que proporcione. Por ello, solo deben considerarse aquellos KPIs que aporten valor suficiente a la organización, identificando (y cuantificando) ese valor. Sin descartar que el KPI que ahora no se considera sea de utilidad en escenarios futuros, cuando la organización haya madurado o crecido suficientemente.

Por último, el CISO debe ser consciente del coste de cálculo de KPIs. Las técnicas de automatización presentadas en el capítulo 4.4 son de gran utilidad en esta tarea. Por ello, en ocasiones, el CISO debe priorizar KPIs que se puedan obtener con menor coste, en base a la disponibilidad y calidad de los datos y la facilidad de cálculo del indicador. En muchas ocasiones, resulta más conveniente obtener un indicador rápido con información suficiente que un indicador excelente pero costoso de calcular.

El cuarto y último factor responde a **necesidades puntuales** de la organización y a sus circunstancias concretas. En este epígrafe, el CISO debe identificar otras necesidades de reporte que tiene la dirección, por cualquier otra razón. Algunos casos habituales son la postura de seguridad de la organización ante amenazas concretas conocidas o novedosas, grados de avance de mejoras u objetivos o el grado de avance de planes de corrección tras incidentes o auditorias. Pero también puede corresponder con intereses incluso espurios o puntuales de personas concretas. el CISO debe saber entender estas necesidades y darles respuestas.

Con todos estos factores, el CISO diseña los KPIs que puede obtener con los recursos disponibles y estructura las relaciones entre ellos, para satisfacer sus necesidades sectoriales de la forma más eficiente y acorde a la madurez de la organización, a su negocio y al estilo de reporte a la dirección de otras áreas de la organización.

El objetivo siempre debe ser que la Dirección disponga de una imagen fidedigna de su estado de ciberseguridad y riesgos después de cada reporte, que satisfaga sus necesidades de conocimiento y que le permita cumplir con sus responsabilidades.

Finalmente, y partiendo de estos KPIs iniciales, el CISO pilota la evolución del reporte mediante la inclusión o exclusión de nuevos KPIs que consigan satisfacer la necesidad de información de una forma más eficiente o completa.

4.2. Pasos para la implementación de indicadores

Aparentemente, la implementación de KPIs sigue un proceso lineal, pero en realidad, existen múltiples puntos de realimentación dentro del proceso que son necesarios para asegurar su correcta implantación y permitir su posterior mejora.

El primer paso es la identificación de un conjunto mínimo viable de KPIs. Se trata de un número reducido de indicadores de alto nivel (al menos 6, idealmente 10-15, se puede optar por un número mayor según necesidades), de muy alto valor y facilidad de cálculo, pero de precisión limitada, que permite generar resultados medibles a corto plazo, facilitar el aprendizaje organizacional y establecer una base sólida para la evolución futura de los KPIs.

Estos primeros KPIs se pueden obtener de diversas fuentes. En caso de estar disponibles, pueden replicar KPIs utilizados por otras organizaciones del sector, o basarse en ellos. También pueden identificarse en base al análisis de los objetivos estratégicos de la organización, de sus procesos críticos de negocio o de controles de ciberseguridad generales (formación, incidencias, continuidad, vulnerabilidades, parcheo, …). Por último, también pueden identificarse las métricas ya se recogen actualmente de forma natural en los controles de ciberseguridad existentes (SIEM, SOAR, ticketing, GRC, otros cuadros de mando, portales de formación o de reporte, etc). En todo caso, es perfectamente viable estructurar los KPIs en niveles, siempre que (como se señaló al hablar de cuadros de mandos) el número de indicadores en el nivel más alto sea reducido y se establezcan relaciones entre indicadores de los distintos niveles.

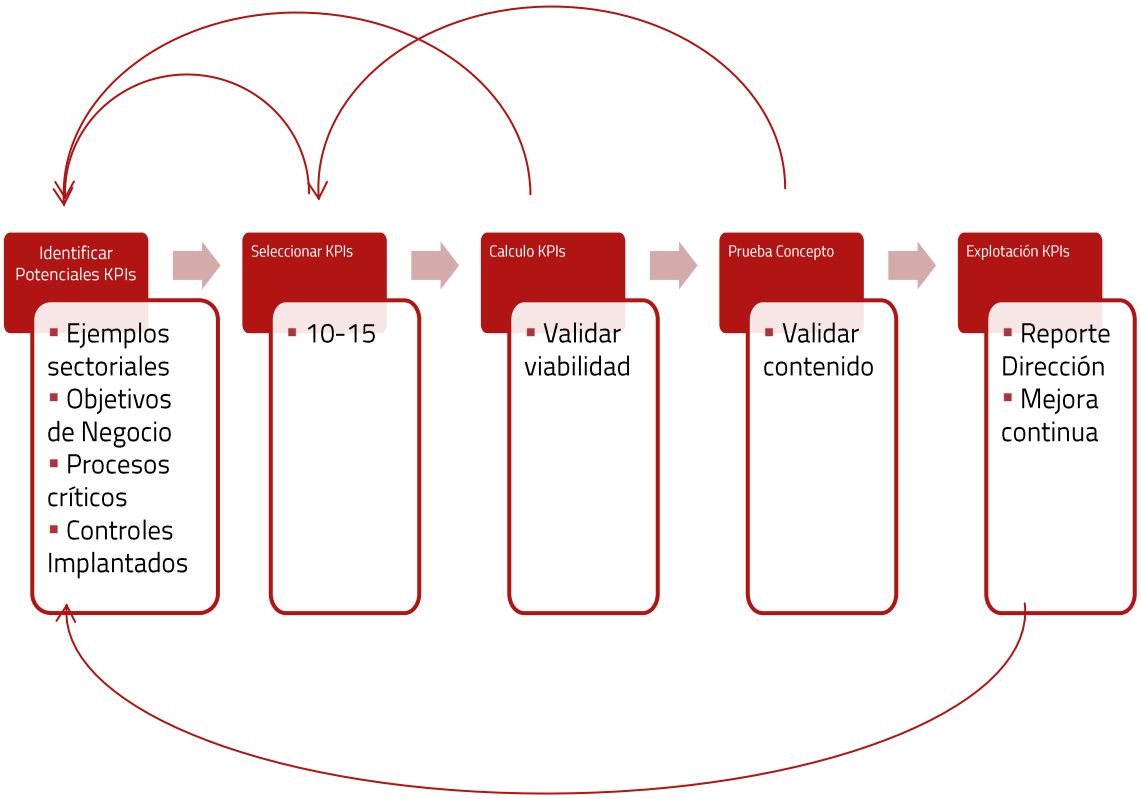
El segundo paso es el cálculo y obtención efectiva de indicadores. En ocasiones, los indicadores diseñados no resultan ser adecuados. Bien porque su cálculo resulta muy complejo, lento o directamente no es viable; Bien porque sus resultados no son

representativos; Bien porque no proporcionan información de interés para la dirección; o bien por otras razones. En cualquiera de estos casos, el CISO debería reconsiderar la viabilidad del KPI, seleccionando en su caso otros KPI alternativos que sí respondan a los objetivos deseados. En realidad, este proceso de testeo y descarte de potenciales KPIs va a realizarse de forma continua durante cualquier momento de

El tercer paso es la prueba de concepto de los KPIs que han superado la fase anterior. Esta prueba somete los KPIs seleccionados al escrutinio de una sección representativa de la dirección, para validar que aportan la información relevante que esperaba, tanto en formato, como en forma, como en la información que transmiten y en la capacidad de la dirección de toma de decisiones en materia de ciberseguridad en función de estos KPIs. Idealmente, esta muestra debería incluir al máximo directivo de la organización. En caso de que algún indicador no sea juzgado como suficientemente informativo, el CISO debería modificarlo o sustituirlo por otro indicador que sí sea relevante a criterio de la dirección. Este paso permite también asegurar que el trabajo previo realizado por el área de seguridad para el conocimiento de las necesidades de la organización ha sido correcto: Si se ha realizado correctamente, todos o casi todos los KPIs propuestos superarán esta fase.

El cuarto, pero no último paso es el uso de los KPIs seleccionados para realizar el reporte a la dirección. De nuevo, estos KPIs deberían ser considerados como útiles, pero es posible que alguno de ellos requiera de mejora y/o sustitución.

El último paso es la mejora continua del modelo de indicadores de reporte a la dirección, incluyendo nuevos indicadores, eliminando indicadores obsoletos, y optimizando su proceso de cálculo. Algunos autores proponen que esta optimización puede realizarse en fases anteriores, y es posible que en algunas organizaciones o para ciertos indicadores, esta sea la opción más.



4.3. Uso de automatización e Inteligencia Artificial en la gestión de indicadores

La automatización de los procesos de cómputo de los KPI permite reducir o controlar el esfuerzo de la organización en el reporte a la dirección, favoreciendo que sea sostenible en el tiempo. La recopilación manual de datos conlleva riesgos de error, falta de consistencia, demoras en la actualización y una elevada carga y costes operativos, mientras que la automatización permite garantizar la eficiencia, exactitud y asegura la periodicidad en el cálculo de KPIs para el reporte.

Como se ha señalado anteriormente, la capacidad de automatización y el coste de su cómputo es un factor que el CISO debe considerar para seleccionar sus KPIs mínimos o deseables. Esta automatización debe incluir desde la recopilación de datos (acceso a datos mediante APIs o repositorios, cuadros de mando automatizados, notificaciones push, o consumo de indicadores previamente generados por otras áreas), hasta su cálculo, presentación (cuadros de mando, informes periódicos, envío automatizado de informes) y generación de históricos. También son aceptables el uso de flujos de trabajo programados, bases de datos centralizadas, plataformas de Business Intelligence, o uso de algoritmos de Inteligencia Artificial. Una vez configurados, estos sistemas permiten mantener la información actualizada en

tiempo real o con la frecuencia definida (diaria, semanal, mensual), mejorando el control y la toma de decisiones.

La automatización también debe contemplar la gestión de alertas y semáforos de indicadores, para que los responsables puedan actuar rápidamente ante situaciones críticas, sin necesidad de esperar un ciclo completo de reporte.

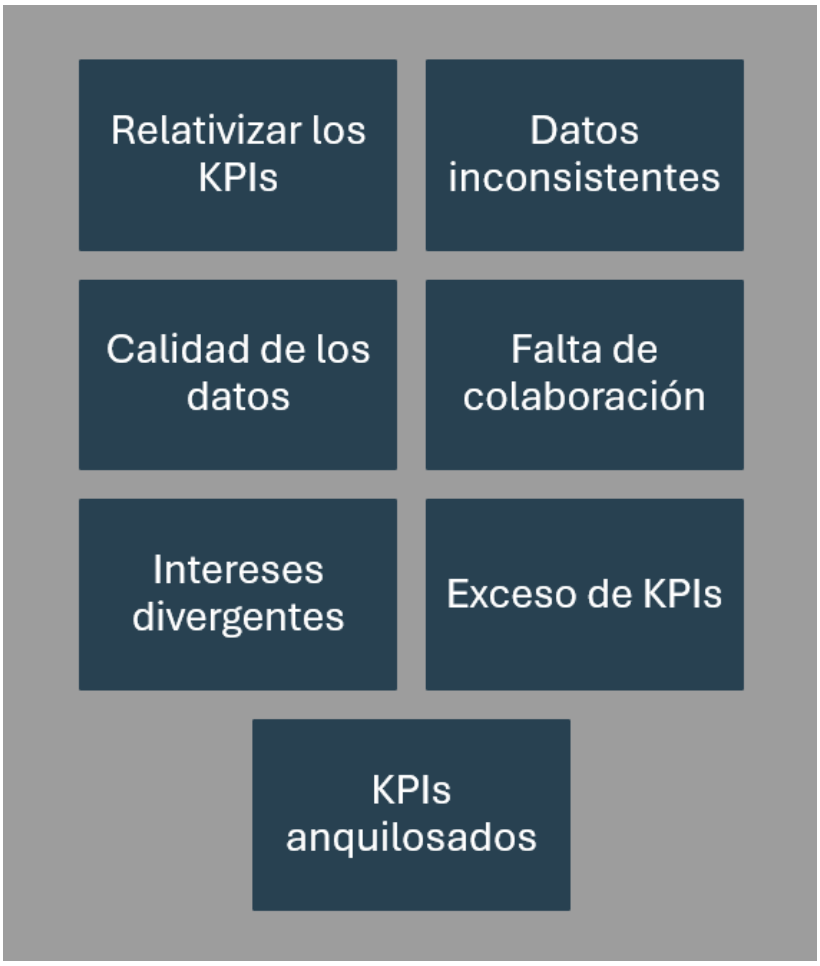
Además de estos esquemas de automatización básica, la Inteligencia Artificial habilita la gestión predictiva y proactiva de la ciberseguridad. La IA puede detectar patrones ocultos, correlaciones no evidentes y anticipar desviaciones antes de que estas se materialicen en un incidente. Para ello, se puede utilizar la IA para realizar:

- Análisis de tendencias: Evaluación de la evolución de ciertos indicadores para identificar ciclos (tanto de corto como de largo plazo), estacionalidades o cambios inesperados en las tendencias (tanto puntuales como de largo plazo).
- Detección de anomalías: Identificación de comportamientos fuera de lo habitual en los KPIs seleccionados. En particular, con cambios a corto plazo.
- Clasificación automática de riesgos, propuesta de acciones y/o reacción automática: A partir de variables históricas y contexto operativo, los algoritmos pueden establecer respuestas automáticas ante anomalías, formular propuestas de mejora ante los cambios en los KPI, o producir información analítica sobre los riesgos de la organización.

Todas estas capacidades deben estar basadas en algoritmos explicables, trazables, no sesgados y que se apoyen en datos fiables y de calidad, especialmente cuando el reporte se presenta a la Alta Dirección o se utiliza en entornos regulados. La organización conserva la responsabilidad sobre sus decisiones, por lo que la supervisión humana de la IA, o la toma de decisiones humana asistida por IA aparecen como los escenarios más aconsejables. El objetivo debe ser ampliar la capacidad analítica del CISO y apoyar la toma de decisiones con mayor anticipación y fundamento.

4.4. Desafíos y soluciones en la implementación

La implantación del modelo de KPIs presenta numerosos desafíos. Se han seleccionado 7 aspectos que son particularmente relevantes, aunque es probable que el lector pueda, en su experiencia, identificar o tener que afrontar otros también relevantes.



Una dificultad muy relevante es que el cálculo de KPIs suele ser una actividad poco glamourosa entre el total de actividades de un CISO, o que la dirección no aprecie en su justo valor el esfuerzo que precisa. Además, puede verse afectada por incidentes y necesidades concretas de corto plazo que exijan la aplicación de recursos dedicados al cálculo de indicadores y, en particular, cuando el proceso no está totalmente automatizado. Además, los KPIs pueden resultar muy dinámicos y plantear dudas sobre si la automatización en el cálculo resulta rentable si no se prevé que el indicador sea usado durante un tiempo suficiente. El resultado final puede derivar en que el proceso de cálculo y análisis de KPI pueda ser ejecutado tarde, y sin una dedicación de suficientes, y con una motivación escasa por parte del responsable de seguridad, **generando que los resultados se presenten burocráticamente y sin aprovechar su comunicación para impulsar la ciberseguridad.**

La calidad de datos disponible para el proceso de reporte es también fuente de dificultades. Desde preocupaciones básicas sobre la **calidad de los datos** recopilados y su aplicabilidad al cálculo de los KPIs deseados por ausencia de fuentes más adecuadas, hasta inconsistencias entre los datos registrados en distintos sistemas sea en su formato, valores o tipos de datos. La definición y aplicación en todos los sistemas y controles de una taxonomía de datos común permite normalizar los datos

desde la fuente para mejorar la fiabilidad y veracidad de los datos. La continua identificación de fuentes de datos disponibles con información relevante y aplicable permite mejorar y contrastar la información recibida, discriminando las fuentes de datos de baja calidad o aplicabilidad.

Por otra parte, cuando ciberseguridad no comparte objetivos o lenguaje común con otras áreas (IT, legal, operaciones, negocio u otras), los KPI de ciberseguridad pueden carecer de utilidad práctica. El CISO deber establecer una gobernanza transversal, validando los indicadores con representantes de cada área y asegurando que todos comprendan su impacto y utilidad. Para ello, debe utilizar un lenguaje común, comprensible por todos, o debe dirigirse a cada área con su terminología propia.

Este modelo también permite reducir posibles problemas de falta de colaboración de las áreas que operan los procesos de negocio, los servicios y los controles en la generación y comunicación de indicadores. También reduce problemas derivados de la definición insuficiente de los KPIs, sus procesos de obtención y sus fuentes de datos aplicables, que pueden incorporar el know-how de estas personas. En particular, esta posible desidia o falta de colaboración tiene mayor impacto en los KPIs que aún no están completamente automatizados. Sin esta colaboración que permite generar la información de base para el cálculo de indicadores, o que establece dudas sobre la calidad de los datos utilizados, la credibilidad y utilidad del modelo de indicadores queda en entredicho.

Algunas organizaciones aplican un principio de sobreabundancia en sus KPIs. “Mejor que sobre que no que falte”. El resultado final es un cuadro de mando saturado, con demasiados indicadores poco relevantes, con visualizaciones complejas, y con dificultad para encontrar la información que sí es relevante. Un cuadro de mandos que confunde y oculta información, en vez de mostrarla. Y que tiene una utilidad cuando menos discutible para la Dirección. En este caso, se debe retornar al inicio del diseño original de KPIs y seleccionar los indicadores que más información aporta a la dirección.

Por último, el CISO debe evitar que los KPIs se perpetúen en el modelo de reporte, sin analizar periódicamente su necesidad. Ciertamente, el cambio de un indicador o la modificación de fórmulas de cálculo o fuentes es un proceso costoso, y delicado: puede perderse la serie histórica de datos calculados o su trazabilidad. No obstante, al cabo de varios años, muchos de los indicadores han perdido su vigencia durante este periodo y siguen calculándose por inercia, quien que aporten valor a nadie. El CISO debe asegurarse de que los KPI se eliminan o se pasan a niveles menos relevantes cuando ya no son de utilidad.

5.

Evaluación y mejora continua

La implementación de un sistema de indicadores y reporting en ciberseguridad representa el inicio de un esfuerzo constante. El entorno de riesgos, las prioridades del negocio y la tecnología experimentan cambios continuos, al igual que las normativas. Por ello, es fundamental disponer de un proceso activo para la evaluación y mejora, asegurando así que las métricas y la forma de comunicarlas conserven su relevancia y aporten valor estratégico a la organización.

Esta sección detalla el enfoque para realizar dicha evaluación y mejora de forma sistemática.

5.1. Validación y ajuste de indicadores en el tiempo

Los indicadores definidos inicialmente requieren una revisión constante para confirmar su vigencia y alineación con los objetivos estratégicos y los riesgos actuales de la organización.

- Proceso de Revisión Periódica: Se establece una rutina definida (por ejemplo, trimestral o semestral) para revisar el conjunto de indicadores. En estas sesiones participa personal del área de ciberseguridad junto con representantes de otras áreas clave (como Riesgos, Legal, Tecnología u Operaciones), aportando una visión integral.
- Criterios de Validación: Durante la revisión, cada indicador se evalúa según criterios como:
  - ¿Conserva su alineación con los objetivos de negocio y los riesgos principales?
  - ¿La información que proporciona es precisa y fiable? ¿Refleja adecuadamente la operativa?
  - ¿Facilita la toma de decisiones y la identificación de áreas de mejora?
  - ¿El esfuerzo para obtenerlo es proporcional al valor que genera?
- Proceso de Ajuste: Con base en la evaluación, se decide si un indicador:
  - Se mantiene sin cambios.
  - Requiere modificaciones (en su definición, cálculo, umbrales o fuente de datos) para aumentar su precisión o utilidad.
  - Se retira por haber perdido relevancia, ser redundante o tener un coste de mantenimiento desproporcionado.
  - Si es preciso incorporar nuevos indicadores para cubrir aspectos emergentes (nuevas tecnologías, cambios regulatorios, etc.).
- Documentación: Todo cambio en el conjunto de indicadores queda debidamente registrado y se comunica a las partes interesadas, actualizando la documentación de referencia del sistema.

5.2. Indicadores de éxito y medición del impacto

Además de medir aspectos concretos de la ciberseguridad, resulta esencial evaluar la efectividad del propio sistema de indicadores y reporting. Es preciso determinar si este sistema cumple su objetivo de mejorar la toma de decisiones y optimizar la asignación de recursos para fortalecer la postura de ciberseguridad.

- Definición de Indicadores de Éxito del Sistema: Se pueden emplear métricas específicas para evaluar el propio sistema, tales como:
  - El grado de satisfacción de la Alta Dirección respecto a la claridad y utilidad de los informes.
  - La mejora observable en los tiempos de respuesta a incidentes críticos, relacionada con la visibilidad proporcionada.
  - La reducción demostrable en la recurrencia de ciertos tipos de incidentes tras aplicar acciones basadas en los indicadores.
  - La optimización de la inversión en ciberseguridad, por ejemplo, calculando el retorno de la inversión (ROI) de iniciativas priorizadas mediante indicadores clave de riesgo (KRIs – definidos en la sección 2 o Glosario).
  - La mejora en puntuaciones de auditorías relacionadas con la gobernanza y el reporting.
- Medición del Impacto en el Negocio: El objetivo final es conectar la gestión de la ciberseguridad con los resultados del negocio. Se busca cuantificar, en la medida de lo posible, cómo la mejora en los indicadores se traduce en beneficios tangibles:
  - Reducción de pérdidas financieras derivadas de incidentes.
  - Mejora de la confianza del cliente y la reputación.
  - Cumplimiento normativo eficiente.
  - Habilitación segura de nuevas iniciativas de negocio.
- Comunicación del Valor: Comunicar estos resultados de impacto a la Alta Dirección es fundamental para mostrar el valor que aporta la inversión y el esfuerzo en ciberseguridad.

5.3. Retroalimentación y actualización del marco de indicadores

Un componente clave de la mejora continua es la consideración de la opinión de quienes utilizan y reciben la información generada.

- Canales de Retroalimentación: Se habilitan canales formales e informales para recoger esta información:
  - Sesiones específicas de revisión con la Alta Dirección y otros comités relevantes.
  - Encuestas periódicas dirigidas a los distintos públicos de los informes.
  - La aportación directa del equipo de ciberseguridad sobre la viabilidad y utilidad operativa de los indicadores.
- Análisis de la Retroalimentación: La información recogida se analiza sistemáticamente para identificar patrones, áreas de mejora y sugerencias aplicables.
- Ciclo de Actualización: Esta retroalimentación, junto con los resultados de la validación de indicadores (5.1) y la medición del impacto (5.2), alimenta un proceso formal para actualizar el marco general de indicadores y reporting (descrito en secciones 2 y 3).
- Gobernanza del Marco: Se aplica un control sobre estos cambios para asegurar que las actualizaciones se implementan de manera ordenada, documentada y comunicada, manteniendo la coherencia del sistema.

En resumen, esta dinámica de evaluación y mejora asegura que el sistema de indicadores y reporting de ciberseguridad se mantenga como una herramienta estratégica útil y adaptada a la evolución de la organización y su entorno.

6.

Conclusiones y recomendaciones

6.1. Beneficios clave del uso de indicadores en ciberseguridad

"No se trata solo de medir, sino de comunicar de forma efectiva y estratégica". Bajo esta premisa nace esta guía. Siendo plenamente conscientes de las múltiples realidades en las diferentes organizaciones, tanto públicas como privadas, es realmente complicado tratar de amalgamar "qué hacer" y mucho más, si cabe, "cómo hacerlo" en lo relativo al uso de indicadores en ciberseguridad y reporte a la Alta Dirección.

Sin embargo, contar con capacidades efectivas tanto en el uso de indicadores en ciberseguridad, así como con unas capacidades de comunicación efectiva a la hora de hacerlo permitirá a los CISO ir aumentando en el dominio de su influencia en la organización, que, finalmente, debería traducirse en una mejora de la postura de ciberseguridad de la misma.

A tenor de lo expuesto en esta guía, los beneficios clave del uso de indicadores de ciberseguridad podrían resumirse, principalmente, en:

- Manejar información relevante y clave sobre el estado de la ciberseguridad y prever tendencias que nos permitan anticiparnos a problemas
- Contar con elementos visuales y fácilmente comprensibles para la Alta Dirección
- Dotar al CISO de una herramienta potente tanto a nivel operativo, como táctico y estratégico, que pueda compartir con facilidad con personas tanto técnicas como no técnicas
- Concienciar y poner en valor la necesidad de la ciberseguridad a todos los empleados, incluyendo la Alta Dirección
- Tener una herramienta relevante para poder romper cualquier barrera con la Alta Dirección, acompañado de una comunicación efectiva

6.2. Impacto en la gobernanza y cumplimiento normativo

El gobierno de la ciberseguridad ha ido ganando momentum en los últimos años. De este modo, la gobernanza era un ámbito menos explorado, habitualmente, en las organizaciones, que centraban su estrategia de ciberseguridad y/o planes de acción en despliegues tecnológicos, en la adquisición y gestión de su talento y, finalmente, en el desarrollo de procesos en torno a dicha ciberseguridad. Sin embargo, el propio CSF de NIST, en su última actualización pasó de sus clásicos cinco dominios a seis, incluyendo el del gobierno.

Esta guía pretende alinearse con esta importancia de la gobernanza, para lo que la aplicación de los principios aquí expuestos debería de tener un reflejo en que el CISO sea considerado como un elemento clave en la organización.

En numerosas organizaciones, dependiendo del sector, tamaño y madurez, el CISO puede ocupar puestos relevantes e, incluso, estar ya situado en la Alta Dirección, mientras que, en la mayoría de los casos, está más o menos cercano a dicha Alta Dirección. Este posicionamiento es relevante a la hora de continuar en el proceso de mejora continua de la ciberseguridad, que siempre debe ir evolucionando conforme, entre otros, a cómo va evolucionando el panorama de amenazas. Dicho gobierno y posicionamiento permite a las organizaciones tener una gestión efectiva de los riesgos y de su ciberseguridad.

Este gobierno evolucionado y posicionamiento relevante también conlleva fuertes responsabilidades para cualquier CISO, que debe comprender que no es un mero rol técnico, sino un habilitador de negocio e, incluso, deseablemente, una persona que participe de la estrategia de la organización, acompañando a esta, dándole servicio y permitiendo no sólo que se vea satisfecha de forma segura, sino anticipándose y proponiendo soluciones y capacidades que aporten el mayor valor posible a la organización.

Conviene recordar, también, que las nuevas regulaciones, tanto sectoriales como más generales, en materia de seguridad de la información/ciberseguridad ya dejan, con mayor énfasis que

nunca, patente el rol clave del CISO, pero también el de la Alta Dirección en estas materias. La Alta Dirección no puede permanecer ajena a sus responsabilidades ni el rol debe dejar de poner el acento en ello, advirtiendo de ello a la Alta Dirección y acompañándola y guiándola en dicha responsabilidad.

Además de lo anterior, las nuevas regulaciones cada vez son más exigentes en dichas materias, demandando ya no a "algunas organizaciones" más o menos críticas y/o esenciales, sino cada vez teniendo a un número mucho mayor de organizaciones públicas y privadas bajo su radar. Estas nuevas exigencias incluyen ya no sólo estar correctamente protegidos y tener capacidades de identificación y prevención adecuadas, sino también gobernanzas adecuadas, así como profundas capacidades de respuesta y recuperación ante ciber incidentes.

Esta guía, sin duda, será un facilitador para que los CISO puedan garantizar el cumplimento normativo en ese sentido, dado que controlar y manejar de forma efectiva sus indicadores, así como una comunicación efectiva a la Alta Dirección no hará sino tener un mejor conocimiento constante y "online" de la realidad de la ciberseguridad corporativa, sino también prever tendencias negativas, anticiparse a potenciales problemas futuros y, por supuesto, manejar los riesgos con datos fidedignos que permitan al CISO así como a la Alta Dirección tomar las mejores decisiones informadas.

6.3. Próximos pasos para la evolución del modelo

Este modelo desarrollado en esta guía es la primera aproximación que se realiza de una forma tan exhaustiva, por parte de una comunidad extensa de CISO y C-Level, que comprende principios fundamentales cuya actualización es conveniente.

Los indicadores y métricas deben ser recogidos, tratados y gestionados de la forma más eficiente posible, si no, pierden su sentido, convirtiéndose en una actividad tediosa y altamente consumidora de recursos que no aportará los beneficios que se pretenden.

Como se ha ido diciendo a lo largo de esta guía, no hay un modelo único ni una forma única de hacer las cosas, dado que hay un número

alto de variables que hacen que eso sea prácticamente imposible, por ello, cada organización debería de adoptar su "mejor versión" del modelo y este ir evolucionando según sus necesidades; por ejemplo, se dejarán de tomar datos que se vea que no aportan valor a una organización en concreto, así como descartar indicadores que no indiquen tendencias útiles o cuya evolución apenas varíe y se conviertan en meros "números" de poco valor. Y el CISO no debe preocuparse, dado que esto ocurre en todas las organizaciones.

Sumado a lo anterior, la tecnología e cambiante, muchas organizaciones están inmersas en procesos más o menos profundos de transformación y las tendencias actuales, así como la aparición de "nuevos paradigmas" que podrían tener un efecto disruptivo alto (por ejemplo, la instauración masiva de la Inteligencia Artificial).

Es por todo ello que conviene ir actualizando el modelo en cada organización, así como actualizar lo aquí contenido, de forma conveniente, dado que la ciberseguridad debe estar preparada para dar respuesta a las necesidades de negocio con la mayor celeridad posible, lo que hará necesario "medir" más cosas y de forma diferente y en profundidad en conceptos hasta ahora no medidos o que no han sido tan relevantes.

6.4. Llamada a la acción para los CISOs y la Alta Dirección

Los profesionales de la ciberseguridad que han participado en la elaboración de esta guía, así como las consultas realizadas a otros tantos y que ha aportado tanto valor han dejado patente la importancia de lo expuesto en esta guía, así como de que no es suficiente con escribir y describir en este documento las pautas clave para el reporte del CISO a la Alta Dirección, sino que estas pautas deben ir acompañadas de acciones, allá donde sea necesario, tanto por parte de los CISO como de la Alta Dirección.

En lo relativo a los CISO, conviene seguir ahondando en el concepto de que debe, si no ha ocurrido ya, dar el paso de convertirse en un facilitador y comprender su rol en la organización, no limitándose a ser el mayor exponente del conocimiento técnico de ciberseguridad, a nivel global, de la organización, sino incorporando o mejorando

siempre sus capacidades como C-Level, es decir, como una persona con una responsabilidad elevada que debe ser quien permita que la organización evolucione hacia la ciberseguridad que dicha organización necesita, con visión, con sentido crítico, con capacidad de comunicación a la Alta Dirección y que sea quien haga que esta comprenda su responsabilidad y que esta pueda gestionar los riesgos de ciberseguridad a los que la organización está expuesta, dotándoles de los mejores datos para la mejor toma de decisiones, que es la convenientemente informada. Muchos CISO ya dieron ese paso adelante hace muchos años, otros están en ello y otros deben hacerlo. En cualquier caso, la mejora continua del propio CISO y su actualización y evolución son fundamentales, tanto a nivel técnico como de gobierno en la organización.

En lo relativo a la Alta Dirección, es fundamental que comprenda su responsabilidad en lo que a la ciberseguridad concierne. Debe comprender, igualmente, que el CISO es la persona mejor preparada para permitirles gestionar la ciberseguridad de la organización y los riesgos asociados de la forma más eficiente y, especialmente, de forma comprensible para ellos. Por eso, es muy relevante que demanden al CISO una comunicación efectiva de estos indicadores y de cualquier circunstancia relevante en torno a la ciberseguridad, así como a los riesgos asociados. Es importante, además, que la Alta Dirección mantenga una actitud de interés en la ciberseguridad que no debe limitarse sólo a dotar presupuestariamente al CISO, sino a permitir, orgánicamente, que este sea un habilitador real del negocio, permitiendo su participación y proximidad a la estrategia de la organización, no manteniéndole al margen o en una posición que no permita que el CISO pueda desarrollar su trabajo de forma efectiva.

Desde esta guía se invita a una reflexión conjunta entre CISO y Alta Dirección sobre la necesidad de establecer puentes que permitan la mayor comprensión de aspectos a veces complejos relacionados con la ciberseguridad y sus riesgos y que permitan a las organizaciones tomar las mejores decisiones, de la forma más informada posible.

7.

Referencias

- Aufait UX. (s.f.). *Cybersecurity dashboard UI/UX design: 5 things to consider for an engaging dashboard*. Aufait UX. https://www.aufaitux.com/blog/cybersecurity-dashboard-ui-ux-design/
- ColorBrewer 2.0.

  https://colorbrewer2.org/
- CyberSaint. (2023, octubre 5). *The best cybersecurity dashboards: 5 key features for success*.

  https://www.cybersaint.io/blog/the-best-cyber-security-dashboards
- Datawrapper. (s.f.). *Datawrapper Blog*.

  https://blog.datawrapper.de/
- **Directiva (UE) 2022/2555** del Parlamento Europeo y del Consejo de 14 de diciembre de 2022.

  https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555
- Fer, S. (2004). *Show me the numbers: Designing tables and graphs to enlighten*. Analytics Press.
- Few, S. (2006). *Information dashboard design: The effective visual communication of data*. O'Reilly Media.
- Few, S. (2009). *Now you see it: Simple visualization techniques for quantitative analysis*. Analytics Press.
- Few, S. (2013). *Information dashboard design: Displaying data for at-a-glance monitoring*. Analytics Press.
- Google. (s.f.). *Looker Studio Help Center*.

  https://support.google.com/looker-studio
- Jit.io. (s.f.). *Continuous security monitoring (CSM) tools*. https://www.jit.io/resources/appsec-tools/continuous-security-monitoring-csm-tools
- Knaflic, C. N. (2015). *Storytelling with data: A data visualization guide for business professionals*. Wiley.

- Material Design. (s.f.). *Data visualization guidelines*. Google. https://m3.material.io/foundations/data-visualization
- Microsoft. (s.f.). *Power BI Documentation*. https://learn.microsoft.com/power-bi/
- National Institute of Standards and Technology (NIST). (s.f.). *Cybersecurity Framework*.

  https://www.nist.gov/cyberframework
- Secureframe. (2023, junio 30). *Cybersecurity dashboards: What they are and how to use them*.

  https://secureframe.com/blog/cybersecurity-dashboards
- Smartosh. (2022, mayo 10). *Indicadores preventivos (leading) o lagging: ¿Cuál es la diferencia?*.

  https://www.smartosh.com/indicadores-preventivos-leading-o-lagging/
- Splunk. (2025). *The CISO Report 2025*. Splunk Inc.
- Sprinto. (2023, marzo 8). *Cybersecurity dashboards: Why they matter and what to track*.

  https://sprinto.com/blog/cybersecurity-dashboards/
- Tableau. (s.f.). *Visual best practices guide*. https://www.tableau.com/learn/whitepapers/visual-best-practices
- TechTarget. (2023, agosto 2). *Top ERM software vendors to consider*. https://www.techtarget.com/searchcio/feature/Top-ERM-software-vendors-to-consider
- The Noun Project. (s.f.). *Icon library*.

  https://thenounproject.com/
- TuDashboard. (s.f.). *¿Qué es un indicador lagging y leading?*. https://tudashboard.com/que-es-un-indicador-lagging-y-leading/

- Tufte, E. R. (2001). *The visual display of quantitative information*. Graphics Press.
- How CISOs Can Take Advantage of the Balanced Scorecard Method.https://www.isaca.org/resources/news-and-trends/industry-news/2024/how-cisos-can-take-advantage-of-the-balanced-scorecard-method
- MIT Sloan – Cuadro de Mando Balanceado para la Resiliencia Cibernética. https://cams.mit.edu/wp-content/uploads/Balanced-Scorecard-Dashboard-for-Cybersecurity.pdf
- NIST – Desarrollo de un Cuadro de Mando de Ciberseguridad. https://csrc.nist.gov/CSRC/media/Presentations/Creating-a-Cybersecurity-Scorecard/images-media/Developing%20a%20Cybersecurity%20Scorecard.pdf
- Wikipedia. (s.f.). Ciclo de Deming.

  https://es.wikipedia.org/wiki/Ciclo_de_Deming

Anexo I.

Metodología del proyecto

A la hora de desarrollar la presente guía, se ha seguido la metodología que se muestra continuación:

La presente metodología busca dotar al CISO y la Alta Dirección de indicadores clave (KPIs y KRIs) que permitan una comprensión clara, objetiva y accionable del estado de la ciberseguridad en la organización. A través de un proceso estructurado, se analizan necesidades, se seleccionan indicadores relevantes y se diseñan herramientas eficaces para su visualización y seguimiento.

a) Fases de desarrollo

En esta etapa, se trata de hacer un análisis de la situación actual, para identificar los requisitos en materia de ciberseguridad. Para ello es clave comprender el impacto de

los riesgos de ciberseguridad en el negocio para poder identificar los indicadores relevantes para dicho propósito y evaluar el estado actual del reporting en la organización (periodicidad, consistencia, adaptabilidad a los interlocutores, etc.).

Es esencial considerar que la Alta Dirección no participa del detalle técnico, por lo que los indicadores seleccionados deben responder a un enfoque ejecutivo.

Las fases de desarrollo son las siguientes:

b) Diagnóstico inicial y análisis de requerimientos

Se persigue identificar cuáles son los requerimientos cuando hablamos de seguridad y protección de la información.

Con carácter general, la Alta Dirección debe comprender cómo los riesgos en materia de ciberseguridad pueden afectar al normal funcionamiento de su organización, qué recursos deben dedicar para mitigar ese riesgo y cómo realizar el seguimiento de forma continua. Así mismo, resulta fundamental su comprensión del marco normativo con el que la organización debe cumplir y contar con las herramientas necesarias para monitorizar el cumplimiento del mismo.

Sin embargo, no es labor de la Alta Dirección participar en el día a día de las actividades de ciberseguridad y protección de la información, ni tener un conocimiento técnico específico.

Todo ello, deberá ser tenido en cuenta a la hora de seleccionar los indicadores adecuados en la siguiente fase.

c) Identificación de indicadores relevantes

Los indicadores que utilicemos para el reporte a la Alta Dirección deben cumplir con las siguientes características:

- **Medibles**, con definiciones y fórmulas claras
- **Comparables** con valores históricos, para poder disponer de una escala temporal y con otras referencias externas para poder interpretar los datos con precisión
- **Relevantes**, alineados con negocio, deben aportar no informar.
- **Comprensibles** en cuanto a su propósito de medida respecto al objetivo deseado y entendibles por parte de los interlocutores a los que se presentan

- **Escalables y adaptables**, de forma que puedan manejar una cantidad creciente de componentes y puedan adaptarse a un panorama de amenazas cambiante
- **Accionables**, para dar soporte a la toma de decisiones

De esta forma, los indicadores que identifiquemos servirán para estar al tanto de forma objetiva del estado de la seguridad y tomar decisiones a nivel táctico, operacional y/o estratégico.

Así mismo, a la hora de identificar los indicadores significativos para nuestra compañía, no debemos perder de vista su relevancia estratégica (que puede variar de una organización a otra). Esto es clave para garantizar que los objetivos de seguridad están alineados con los objetivos estratégicos de la organización, identificando las principales áreas de riesgo para la estrategia empresarial y definiendo un plan de acción para mitigar dicho riesgo.

d) Evaluación del estado actual de reporting

En la última fase de desarrollo, evaluamos el estado actual del reporting de las organizaciones.

Partimos de la base de que no basta con presentar información, sino que este debe ser accionable y servir para la toma de decisiones estratégicas en lo relativo a la ciberseguridad y la protección de la información. Por tanto, a la hora de evaluar el estado actual del reporting debemos hacemos preguntas como:

- ¿La información es relevante para el negocio?
- ¿Es clara y entendible por los interlocutores (que no tendrán un perfil técnico)?
- ¿Está enfocada en los indicadores que hemos identificado?
- ¿Es efectiva a la hora de medir el grado de avance en la consecución de los objetivos?

Todo ello, nos ayudará a identificar la idoneidad del reporte actual y las áreas de mejora para conseguir la eficacia deseada. El reporte debe ser eficaz, claro y centrado en aportar valor al negocio.

No hay que olvidar que, en la medida en la que se avance en la percepción del CISO como una figura integrada dentro de la Alta Dirección, su misión será no solamente proteger a la compañía, sino también ser un habilitador del negocio mediante una gestión del riesgo cíber plenamente alineada con sus objetivos estratégicos de negocio. Por tanto, su comunicación debe ser clara, efectiva y alineada con el negocio;

presentando el estado de la ciberseguridad de la organización mediante reportes ejecutivos y cuadros de mando directos, relevantes y entendibles por parte de los interlocutores del negocio.

e) Diseño y desarrollo del sistema de indicadores y reporting

Una vez hemos evaluado la situación actual en lo relativo a los indicadores y reporting, se trata de desarrollar el sistema de indicadores y reporting deseado mediante la selección de los indicadores relevantes y el diseño de las herramientas efectivas. Podemos distinguir las siguientes fases:

f) Selección de indicadores clave (KPIs y KRIs)

Los indicadores se dividen principalmente en dos grandes tipos:

- KPIs - Key Performance Indicators
- KRIs - Key Risk Indicators

Los KPIs miden el grado de avance de una compañía, área, proceso, etc. en relación con unas metas preestablecidas. Su objetivo principal por tanto es proporcionar información que permita tomar decisiones y realizar acciones concretas.

Los KRIs por su parte tienen como objetivo identificar y medir los riesgos potenciales que podrían afectar a la consecución de las metas de la compañía.

Ambos por tanto deben ser medibles, integrados con los objetivos específicos de la organización, temporales y comparables.

Además, los KPIs seleccionados también deben ser alcanzables, realistas y basados en la capacidad efectiva de la organización. De nada serviría definir unos objetivos que no fueran alcanzables con un esfuerzo razonable.

Dado que los KRIs buscan anticiparse a posibles riesgos futuros, también vamos a exigir que sean predictivos; para poder usarlos como un sistema de alerta temprana y anticiparnos a los riesgos antes de que estos se materialicen.

Conviene también destacar la importancia de la regulación y el marco normativo en la selección de los KPIs y KRIs adecuados. Dependiendo del sector de actividad de la organización, su tamaño o ámbito geográfico pueden aplicarse una serie de regulaciones generalistas o sectoriales que deben tenerse en cuenta a la hora de seleccionar los indicadores adecuados.

g) Diseño de herramientas y cuadros de mando

Como vimos anteriormente, la comunicación del CISO con la Alta Dirección debe ser directa, clara, concisa y alineada con el negocio. Por tanto, las herramientas de reporting y cuadros de mando que se diseñen también deben cumplir con estas características.

Podemos definir los siguientes principios de diseño:

- Relevancia estratégica, presentando información alineada con las prioridades estratégicas de la compañía y evitando caer en el error de diseñar métricas técnicas
- Claridad y Concisión, con lenguaje ejecutivo, sin argot técnico y abordando los objetivos esenciales
- Enfoque en KPIs/KRIs, estos últimos deben ser el pilar principal de todo reporting. Seleccionando como vimos aquellos relevantes a los objetivos de negocio; transformando los datos que presentan en información accionable
- Visibilidad de riesgos y oportunidades, proyectando posibles escenarios futuros e identificando no sólo riesgos potenciales sino también oportunidades (la ciberseguridad como habilitador del negocio)

Los cuadros de mando deben permitirnos sintetizar la información en visualizaciones claras y concisas que permitan evaluar el estado general de la ciberseguridad y de la protección de la información vinculadas con el negocio. De esta forma, la Alta Dirección podrá tomar decisiones informadas en el ámbito que nos ocupa.

Por tanto, el diseño visual se convierte en un aspecto fundamental de la eficacia del reporte. Una visualización bien diseñada mejora la comprensión, reduce el tiempo de análisis y permite focalizar la atención en los elementos más relevantes del negocio. Por tanto, el diseño visual también deberá cumplir con los siguientes principios:

- Claridad; facilitando la comprensión y evitando la saturación de información y visual
- Elección adecuada de gráficos para cada ocasión, que facilite su interpretación
- Codificación visual coherente, manteniendo la consistencia en todo el reporte del código visual escogido, evitando así la fatiga o pérdida de atención de la audiencia
- Narrativa guiada; el orden de presentación de los elementos, su agrupación y énfasis deben guiar a la audiencia hacia las conclusiones principales

- Evitar la sobrecarga de información, presentando los datos clave y evitando un esfuerzo mental excesivo por parte de la audiencia para interpretar los datos

h) Validación y ajustes del estándar

Hoy en día, la figura del CISO está sometida a elevada presión regulatoria y de cumplimiento por lo que cualquier indicador y cuadro de mando debe estar debidamente validado y ajustado al marco normativo que la empresa ha decidido seguir y las diferentes regulaciones que puedan ser aplicadas.

i) Implementación y capacitación

Una vez seleccionados, validados y diseñados los indicadores deberemos implementarlos.

j) Integración con herramientas existentes

Dentro del ciclo de vida de los indicadores para la Alta Dirección y una vez los hemos definido, validado e implementado, está el proceso de cálculo de estos. Hoy en día, la tecnología actual permite calcular prácticamente en tiempo real y mostrar los indicadores y cuadros de mandos directamente desde una plataforma digital.

k) Pruebas y evaluación

Como buenos profesionales en la gestión del riesgo, no deberíamos utilizar ningún indicador y/o cuadro de mandos que no haya sido probado y validado. Cada indicador debe ser contrastado con su definición, pregunta que responde y fórmula de cálculo. Una buena práctica es revisarlo internamente y luego compartirlo con colegas de confianza de otras áreas para que hagan de “abogado del diablo” y realicen una validación externa e independiente.

Anexo II.

Plantillas de reportes y cuadros de mando

Este anexo proporciona ejemplos y plantillas prácticas para ayudar al CISO a estructurar y presentar la información sobre ciberseguridad a la Alta Dirección. Se incluyen formatos sugeridos para reportes periódicos, cuadros de mando visuales y reportes especiales para situaciones críticas o extraordinarias. Además, se incluyen recomendaciones específicas sobre elementos que resultan especialmente relevantes para distintos perfiles directivos como CEO, CIO, CFO y otros.

1. **Plantilla para Reporte Ejecutivo Mensual**
   - **Página de portada**

     Título: Reporte Ejecutivo Mensual de Ciberseguridad
     Fecha: [Mes - Año]
     Responsable: [Nombre y Cargo del responsable]
     Área: [Ej. Seguridad de la Información]

   - **Resumen ejecutivo**

     Breve descripción (máx. 300 palabras) con las conclusiones clave del mes:
     Estado general de la seguridad.
     Principales incidentes o eventos.
     Recomendaciones estratégicas.
     Tendencias o cambios significativos.

   - **Evolución de Indicadores Clave (KPIs)**[4]

[4] *Incluir gráficas si es posible para mostrar evolución de cada KPI.*

KPI	Indicador	Resultado Actual	Mes Anterior	Tendencia	Observaciones
KPI 1	Nº de incidentes por gravedad (Alta/Media/Baja)	[###/###/###]	[###/###/###]	▲/▼	[Notas breves]
KPI 2	Tiempos medios de respuesta y resolución	[hh:mm:ss]	[hh:mm:ss]	▲/▼	[Notas]
KPI 3	% de sistemas críticos parcheados	[%]	[%]	▲/▼	[Notas]
KPI 4	Nivel de cumplimiento normativo (ISO 27001, GDPR, etc.)	[% o semáforo]	[%]	▲/▼	[Notas]
KPI 5	Concienciación del personal (% éxito en phishing simulado)	[% que hizo clic]	[%]	▲/▼	[Notas]

- Riesgos y Oportunidades identificados.

Tipo	Descripción	Impacto	Probabilidad	Mitigación / Acción propuesta
Riesgo	[Descripción del riesgo]	Alto/Medio/Bajo	Alta/Media/Baja	[Acciones]
Oportunidad	[Mejora o herramienta identificada]	Alto/Medio/Bajo	Alta/Media/Baja	[Acciones]

- Próximos pasos y acciones requeridas.

AC1: Revisión de políticas de acceso antes de [fecha]

AC2: Actualización de inventario de activos críticos

AC3: Campaña de concienciación fase 2 – [fecha]

AC4: Evaluación de solución X para [necesidad]

AC5: Reunión con proveedores críticos – [fecha]

2. **Plantilla para Cuadro de Mando Integral**
   - Diseño visual en una sola página (Dashboard ejecutivo)
   - Indicadores organizados por categoría

Categoría	Indicador	Valor actual	Meta	Semáforo	Comentario / Contexto
Gestión de Incidentes	• Número de incidentes • Tipo de incidentes (malware, acceso, etc.) • Severidad promedio				• Ej. Alta incidencia en endpoints móviles • Clasificación por categoría más común • Escala 1–5 o crítica/alta/media/baja
Cumplimiento normativo	% cumplimiento regulatorio		100%		Según auditoría o autoevaluación
Resiliencia y continuidad	• RTO (Tiempo objetivo de recuperación) • RPO (Punto objetivo de recuperación) • Disponibilidad de sistemas críticos (%)				• En horas • Frecuencia de backups • Ej. sistemas productivos clave
Concienciación y capacitación	• Tasa de participación en capacitaciones (%) • Tasa de éxito en simulacros (phishing, etc.)				• Basado en asistencia a sesiones • % que no cayó en el señuelo
Estado de riesgo	KRI más relevantes				Riesgos identificados con mayor impacto
Estado de seguridad general	% desviación de la línea base				Cambios detectados respecto a configuración

   - Alertas visuales con semáforos (verde, amarillo, rojo)

Verde ✅: dentro del umbral aceptable o superando la meta.

Amarillo ⚠️: cerca del umbral o con leves desviaciones.

Rojo ❌: fuera de los límites aceptables.

- Anotaciones breves y contexto explicativo.

Sección	Descripción / Instrucciones
1. Introducción y contexto	Breve resumen del trimestre: eventos relevantes, entorno de amenaza, cambios organizacionales
2. Análisis Comparativo	Comparación de KPIs actuales vs. trimestres anteriores. Incluir gráficos si es posible. Ejemplo: Evolución de incidentes, cumplimiento, tiempos de respuesta.
3. Evolución de Riesgos Estratégicos	Mapa de riesgos actualizado: alta, media, baja. Indicar cambios respecto a trimestres anteriores. Puede incluir tabla de riesgos o gráfico de burbujas.
4. Iniciativas Estratégicas	Estado de proyectos clave: nombre, objetivo, avance (%), desafíos, próximos pasos.
5. Impacto en el Negocio	Cómo las actividades de ciberseguridad contribuyeron o impactaron en operaciones clave. Ej.: Reducción de riesgos, mejora de cumplimiento, continuidad operativa.
6. Proyecciones y Escenarios Futuros	Análisis de tendencias futuras: amenazas emergentes, necesidades presupuestarias, roadmap.

3. Plantilla para Reporte Trimestral Estratégico

*Incorpora **tablas comparativas** y **gráficos de línea o barra** para el análisis de evolución.*

*Aplica **códigos de colores** o **señalización visual** para resaltar riesgos y logros*

4. Plantilla para Reporte de Incidentes Críticos

Sección	Descripción / Instrucciones
1. Identificación del Incidente	• **Fecha y hora** de detección del incidente. • **Sistemas afectados**: Indicar qué sistemas se vieron comprometidos.
2. Impacto del Incidente	• **Impacto financiero**: Pérdidas estimadas, costos de recuperación. • **Impacto operacional**: Procesos o actividades interrumpidas. • **Impacto reputacional**: Efecto en la imagen de la empresa o confianza del cliente.
3. Análisis de Causa Raíz	• **Causa principal** del incidente. • ¿Qué vulnerabilidad o error permitió el incidente? • Descripción detallada de cómo ocurrió.
4. Respuesta Inmediata Ejecutada	• **Acciones inmediatas** tomadas al detectar el incidente. • ¿Cómo se contuvo el incidente? • ¿Se activaron protocolos de emergencia?
5. Lecciones Aprendidas	• **Lecciones clave** obtenidas del incidente. • ¿Qué aspectos funcionaron bien? • ¿Qué falló y por qué?
6. Recomendaciones	• **Acciones preventivas** para evitar futuros incidentes similares. • Mejora en políticas, procedimientos o tecnologías.
7. Acciones Preventivas a Realizar	• **Plan de mejora a implementar**: cambios en procesos, tecnologías o recursos humanos. • **Fechas y responsables** de cada acción a realizar.

Indice	Fecha y Hora	Sistemas afectados	Impacto Financiero	Impacto Operacional	Impacto Reputacional	Causa Raíz	Respuesta Ejecutada	Lecciones aprendidas	Recomendaciones	Acciones preventivas
Incidente 1	01/05/2025 14:00	Sistema de pagos	50,000	Caída de servicios por 3 horas	Pérdida de clientes potenciales	Vulnerabilidad en el sistema de autenticación	Se deshabilitó acceso, análisis forense	Mejorar autenticación multifactor	Revisar procesos de seguridad en plataformas críticas	Mejorar autenticación multifactor, realizar auditorías periódicas
Incidente 2	12/06/2025 10:30	Base de datos	30,000	Interrupción de consultas	Daño a la confianza de clientes	Inyección SQL en base de datos	Restauración desde backups, parches aplicados	Mejorar validación de entradas, revisión de firewall	Revisión de configuración de seguridad en bases de datos	

5. Ejemplos visuales recomendados para cuadros de mando

Tipo de Gráfico	Uso Principal	Ejemplo Visual
Gráfico de Líneas	Mostrar tendencias a lo largo del tiempo	Evolución de incidentes mensuales
Gráfico de Barrasl	Comparar diferentes categorías	Comparación de incidentes por tipo (phishing, malware)
Velocímetro/ Semáforo	Mostrar estado actual de un KPI o proceso	Nivel de cumplimiento normativo (rojo, amarillo, verde)
Mapa de Calor	Análisis de riesgos en diferentes áreas o sistemas	Riesgo por departamento (color más intenso para mayor riesgo)
Diagrama Circular	Mostrar proporciones de un todo	Porcentaje de incidentes por gravedad (grave, medio, leve)

6. Elementos clave para perfiles específicos:

- **CEO (Chief Executive Officer):**

  Objetivo: Proveer una visión estratégica del impacto de la ciberseguridad en la organización a nivel de continuidad, reputación y cumplimiento.

  Elementos clave:

  - Impacto de incidentes críticos sobre la continuidad del negocio:
    - Descripción: Resumen de los incidentes críticos y su efecto en las operaciones clave de la organización.
    - Visualización:
      1. Gráfico de líneas que muestra la frecuencia de incidentes a lo largo del tiempo y su impacto en la continuidad de los servicios.
  - Riesgos estratégicos que afectan la visión global:

- Descripción: Los principales riesgos estratégicos que podrían comprometer la visión a largo plazo de la organización (por ejemplo, ataques a sistemas críticos).
- Visualización: Mapa de riesgos con la clasificación de los más críticos (alto, medio, bajo).

- Cumplimiento regulatorio y riesgos reputacionales:
  - Descripción: Cómo los incidentes de seguridad están afectando el cumplimiento con normativas regulatorias y la imagen corporativa.
  - Visualización: Gráfico circular o de barras para mostrar el porcentaje de cumplimiento normativo o incidentes que afectaron la reputación.

- Progreso y efectividad del programa estratégico de ciberseguridad:
  - Descripción: Estado del programa de ciberseguridad, incluyendo las iniciativas estratégicas y sus resultados.
  - Visualización: Indicadores de progreso o gráficos de barras para mostrar el avance de cada proyecto.

Elementos Clave	Descripción	Visualización recomendada
Impacto de incidentes críticos sobre la continuidad del negocio	Efectos de incidentes críticos en las operaciones clave.	Gráfico de líneas con impacto de incidentes a lo largo del tiempo..
Riesgos estratégicos que afectan la visión global	Principales riesgos que podrían afectar la visión a largo plazo.	Mapa de riesgos clasificados por gravedad (alto, medio, bajo).
Cumplimiento regulatorio y riesgos reputacionales	Cumplimiento con regulaciones y su impacto en la reputación.	Gráfico circular o de barras mostrando el cumplimiento y riesgos
Progreso y efectividad del programa estratégico de ciberseguridad	Estado y avance de las iniciativas estratégicas en ciberseguridad.	Indicadores de progreso, gráficos de barras o diagramas de Gantt.

- **CIO (Chief Information Officer)**

Objetivo: Proveer una visión técnica y operativa sobre el estado de los sistemas tecnológicos, incidentes, y la efectividad de las medidas de ciberseguridad implementadas.

- ☐ Estado operativo de los sistemas tecnológicos
  - Descripción: Proveer un resumen sobre la disponibilidad, funcionamiento y estado general de los sistemas tecnológicos clave. Incluye información sobre el rendimiento de las infraestructuras críticas, como servidores, redes y bases de datos.
  - Visualización recomendada:
    1. Gráfico de barras o semáforo que indique el estado operativo de cada sistema clave (verde = operativo, amarillo = en mantenimiento, rojo = inactivo o con problemas).

- ☐ Tiempos de respuesta y resolución de incidentes
  - Descripción: Medir la efectividad en la respuesta ante incidentes. Esto incluye los tiempos medios de respuesta y resolución para diferentes tipos de incidentes (por ejemplo, incidentes críticos de ciberseguridad).
  - Visualización recomendada:
    1. Gráfico de líneas que muestre los tiempos de respuesta y resolución a lo largo del tiempo.
    2. Indicadores de velocidad o medidores que muestren el tiempo promedio frente a los objetivos establecidos (idealmente en color verde para dentro del objetivo, amarillo y rojo para fuera del objetivo).

- ☐ Porcentaje de sistemas críticos actualizados y parcheados
  - Descripción: Indicar qué porcentaje de los sistemas críticos de la organización han recibido actualizaciones y parches de seguridad para mitigar vulnerabilidades.
  - Visualización recomendada:
    1. Gráfico circular que muestre la proporción de sistemas críticos actualizados versus los pendientes.
    2. Barra de progreso que refleje el porcentaje de sistemas actualizados frente a la meta de actualización.

- Impacto técnico y operacional de incidentes recientes
  - Descripción: Mostrar cómo los incidentes recientes han afectado el rendimiento y la operatividad de los sistemas tecnológicos. Esto puede incluir el tiempo de inactividad o las repercusiones en la productividad.
  - Visualización recomendada: Gráfico de barras que muestre el número de incidentes y el tiempo de inactividad por incidente.

  Diagrama de dispersión que relacione el impacto en términos de tiempo y los sistemas afectados.

Elementos Clave	Descripción	Visualización recomendada
Estado operativo de los sistemas tecnológicos	Disponibilidad y funcionamiento de los sistemas clave.	Gráfico de barras o semáforo (verde = operativo, amarillo = en mantenimiento, rojo = problemas).
Tiempos de respuesta y resolución de incidentes	Tiempos medios de respuesta y resolución de incidentes críticos.	Gráfico de líneas con tiempos de respuesta y medidores comparando con el objetivo.
Porcentaje de sistemas críticos actualizados	Porcentaje de sistemas clave con parches y actualizaciones de seguridad.	Gráfico circular o barra de progreso mostrando sistemas actualizados versus pendientes.
Impacto técnico y operacional de incidentes recientes	Impacto de los incidentes recientes en la operatividad y el rendimiento de los sistemas.	Gráfico de barras con el impacto de cada incidente, tiempo de inactividad y servicios afectados.

- CFO (Chief Financial Officer):

El objetivo de los **elementos clave para el CFO (Chief Financial Officer)** es proporcionar una visión financiera clara sobre los costos, inversiones y retornos relacionados con la ciberseguridad, y cómo estos impactan en el negocio. El CFO necesita tomar decisiones informadas basadas en datos financieros precisos, y los informes deben ayudar a entender cómo la ciberseguridad influye en las finanzas de la organización. Los objetivos específicos son:

- **Evaluar los Costos Asociados a Incidentes y Gestión de Riesgos**:

El CFO necesita entender cuánto está costando a la organización la gestión de incidentes de seguridad, tanto en términos de gastos directos (por ejemplo, recuperación, multas) como en costos indirectos (pérdida de productividad, daños reputacionales).

El objetivo es identificar áreas en las que se pueda mejorar la eficiencia en la gestión de incidentes para reducir costos.

- **Medir el Retorno de Inversión (ROI) en Medidas de Ciberseguridad:**

  El CFO necesita ver si las inversiones realizadas en ciberseguridad están proporcionando valor tangible a la organización. Este indicador ayuda a determinar si las inversiones están evitando costos más altos, como la pérdida de datos, fallos operacionales o daños reputacionales.

  El objetivo es demostrar que la ciberseguridad no solo es un gasto, sino una inversión que mejora la eficiencia y reduce riesgos financieros.

- **Asegurar el Cumplimiento Normativo Financiero:**

  El CFO debe asegurarse de que la empresa cumpla con las regulaciones financieras relacionadas con la seguridad de la información y la privacidad (por ejemplo, GDPR, SOX). No cumplir con estas regulaciones puede resultar en sanciones o daños financieros.

  El objetivo es evitar multas y garantizar que la organización esté alineada con los requisitos regulatorios, minimizando los riesgos legales.

- **Monitorear el Presupuesto Asignado versus el Gasto Efectivo en Seguridad:**

  El CFO necesita realizar un seguimiento de cómo se está utilizando el presupuesto de ciberseguridad y asegurarse de que los recursos asignados se utilicen de manera eficiente.

El objetivo es asegurar que el presupuesto para ciberseguridad se esté gastando de manera efectiva y que las desviaciones del presupuesto sean identificadas y corregidas.

Elementos Clave	Descripción	Visualización recomendada
Costes asociados a incidentes y gestión de riesgos	Costos directos e indirectos derivados de incidentes de seguridad.	Gráfico de barras comparando costos de diferentes tipos de incidentes.
Retorno de inversión en medidas de ciberseguridad	Medición del ROI de las inversiones en ciberseguridad.	Gráfico de barras o columnas mostrando la relación entre costos y beneficios.
Cumplimiento normativo financiero	Estado del cumplimiento con normativas regulatorias financieras.	Gráfico circular o de barras mostrando el porcentaje de cumplimiento.
Presupuesto asignado versus gasto efectivo en seguridad	Comparación entre el presupuesto asignado y el gasto real en ciberseguridad.	Gráfico de barras comparando presupuesto frente al gasto real.

- Comité de Dirección:

  Objetivo: Proporcionar una visión integral del estado general de la ciberseguridad en la organización, permitiendo a los miembros del Comité de Dirección tomar decisiones estratégicas informadas sobre la protección de los activos y la continuidad del negocio.

  - Resumen ejecutivo del estado general de seguridad
    - Descripción: El Comité de Dirección necesita una visión global sobre cómo la ciberseguridad está siendo gestionada dentro de la organización. Esto incluye un resumen claro del estado general de las medidas de seguridad, las amenazas actuales y cómo estas son gestionadas.
    - Visualización recomendada:
      1. Resumen en formato de texto con gráficos de apoyo: Un informe breve y conciso con los puntos más relevantes, apoyado por gráficos como barras, líneas o semáforos que

representen el estado general de la seguridad en un formato claro y fácil de digerir.

2. Ejemplo visual: Un semáforo o gráfico de barras para representar el estado de los sistemas de seguridad: verde (seguro), amarillo (atención requerida), rojo (riesgo elevado).

☐ **Principales indicadores clave (KPIs) y evolución**

- Descripción: El Comité de Dirección necesita entender cómo la organización está evolucionando en términos de ciberseguridad. Esto se logra a través de los principales indicadores clave de desempeño (KPIs), que deben ser monitoreados a lo largo del tiempo.
- Visualización recomendada:
  1. Gráfico de líneas o columnas: Mostrar la evolución de KPIs clave como el número de incidentes, el tiempo medio de resolución, el porcentaje de sistemas parcheados, etc.
  2. Indicadores tipo velocímetro o semáforo: Para mostrar el nivel de cumplimiento o el estado de los KPIs en tiempo real.

☐ **Riesgos emergentes y planes de mitigación**

- Descripción: Los miembros del Comité de Dirección deben estar al tanto de los nuevos riesgos cibernéticos que podrían amenazar a la organización, y conocer los planes de acción que se están implementando para mitigarlos.
- Visualización recomendada:
  1. Mapa de riesgos (Heatmap): Un mapa de calor donde los riesgos son representados por colores según su nivel de gravedad (rojo para alto, amarillo para medio, verde para bajo).
  2. Diagrama de burbujas o gráfico de radar: Para visualizar los riesgos emergentes y sus impactos, y cómo los planes de mitigación están siendo aplicados.

☐ **Progreso en formación y concienciación del personal**

- Descripción: El Comité de Dirección debe entender cómo se están llevando a cabo las iniciativas de concienciación y formación en ciberseguridad, lo que es esencial para reducir los riesgos humanos.
- Visualización recomendada:
  1. Gráfico de barras o columnas: Mostrar la tasa de participación en programas de formación, con un desglose de los módulos completados y los resultados (porcentaje de éxito).

2. Gráfico circular: Para mostrar el porcentaje de empleados que han completado la formación en comparación con los que aún no han sido capacitados.

Elementos Clave	Descripción	Visualización recomendada
Resumen ejecutivo del estado general de seguridad	Visión global del estado de la ciberseguridad en la organización.	Gráfico de barras, semáforo o resumen ejecutivo con indicadores visuales.
Principales indicadores clave (KPIs) y evolución	Evolución de KPIs clave a lo largo del tiempo (número de incidentes, etc.).	Gráfico de líneas o columnas mostrando la evolución de los KPIs.
Riesgos emergentes y planes de mitigación	Identificación de nuevos riesgos y planes de acción para mitigarlos.	Mapa de riesgos (Heatmap) o diagrama de burbujas/radar.
Progreso en formación y concienciación del personal	Progreso en la formación y concienciación en ciberseguridad de los empleados.	Gráfico de barras/columnas o gráfico circular mostrando tasas de participación.

Estas plantillas deben adaptarse a las características específicas de cada organización y actualizarse periódicamente para mantener su relevancia estratégica y operativa.

Anexo III.

Normativas relacionadas

Este anexo presenta los principales marcos normativos, estándares y guías de referencia actuales que justifican la necesidad de implantar indicadores de ciberseguridad en la organización. Estas referencias permiten a la CISO seleccionar, justificar y comunicar indicadores clave de rendimiento (KPI) y de riesgo (KRI), alineados con los requisitos regulatorios y de buenas prácticas.

Las referencias se agrupan por su naturaleza normativa, técnica o metodológica, con una tabla resumen que facilita su aplicación práctica.

1. Normativas europeas y nacionales

Estas normativas definen obligaciones de seguridad y evaluación continua aplicables a organizaciones públicas, privadas y de sectores regulados.

- Directiva NIS2 (Directiva (UE) 2022/2555)
  Establece obligaciones en materia de ciberseguridad para entidades esenciales e importantes. Refuerza el papel de la Alta Dirección como responsable última de los riesgos.
- Reglamento DORA (Reglamento (UE) 2022/2554)
  Obliga a entidades financieras a implementar medidas de resiliencia digital y a medir su eficacia.
- Reglamento sobre ciberresiliencia (CRA)
  Exige que los productos con componentes digitales integren la ciberseguridad desde el diseño y durante todo su ciclo de vida.
- Reglamento General de Protección de Datos (RGPD) (*Reglamento (UE) 2016/679*)
  Establece medidas técnicas y organizativas cuya eficacia puede evaluarse mediante indicadores.
- Esquema Nacional de Seguridad (ENS) (*Real Decreto 311/2022*)
  Marco obligatorio para el sector público español. Establece niveles de seguridad y controles que deben ser monitorizados.
- Ley 8/2011, de protección de infraestructuras críticas
  Impone la obligación de adoptar planes y medidas de seguridad basadas en riesgos, cuya efectividad debe controlarse.

2. Estándares internacionales y marcos técnicos

Estos estándares proporcionan estructuras ampliamente reconocidas para establecer, medir y mejorar la seguridad de la información y la continuidad del negocio.

- ISO/IEC 27001:2022
  Norma internacional para establecer un sistema de gestión de seguridad de la información (SGSI).
- ISO/IEC 22301:2019
  Define requisitos para la gestión de la continuidad del negocio, incluyendo tiempos de recuperación (RTO y RPO).
- ISO 31000:2018
  Proporciona principios y directrices para la gestión del riesgo en cualquier tipo de organización.
- NIST Cybersecurity Framework v2.0 (2024)
  Marco de ciberseguridad estructurado en seis funciones: gobernar, identificar, proteger, detectar, responder y recuperar.
- CIS Controls v8
  Lista priorizada de controles críticos para mejorar la defensa de los sistemas de información.
- COBIT
  Marco de gobernanza de TI que alinea los objetivos empresariales con la medición del desempeño y del riesgo.

3. Regulaciones sectoriales específicas

Determinados sectores están sometidos a normativas particulares que requieren control y evidencia cuantificable.

- EBA Guidelines (EBA/GL/2019/04 – ICT Risk, BA Reporting Framework)
  Obligan a entidades del sector bancario a evaluar y monitorizar el riesgo TIC y de seguridad.
- PCI DSS v4.0
  Norma de seguridad para proteger los datos de tarjetas de pago, con controles y métricas asociadas.
- HIPAA Security Rule (45 CFR Part 164)
  Norma federal de Estados Unidos que regula la protección de información sanitaria electrónica.

4. Guías de referencia y buenas prácticas

- Cyber Green Proof (ISMS Forum)
  Propuesta para evaluar el impacto ambiental y la eficiencia de los controles de ciberseguridad.
- Guías del CCN-CERT sobre indicadores

Recomendaciones para organismos públicos y operadores estratégicos sobre medición y seguimiento de controles.

5. Estándares y marcos específicos sobre indicadores

Norma Framework	Enfoque	Tipo de indicadores	Aplicación principal
ISO/IEC 27004	Seguridad de la información	KPIs, eficacia de controles	Guía de métricas para evaluar la eficacia de los controles de seguridad según ISO 27001.
ISO/IEC 27014	Gobernanza de seguridad	KPIs estratégicos	Orienta a la Alta Dirección en la supervisión de la estrategia de seguridad.
NIST SP 800-55	Medición de rendimiento	Eficacia, eficiencia, impacto	Establece y gestiona métricas de rendimiento en seguridad.
NIST CSF v2.0	Ciberseguridad general	Funcionales, madurez	Marco estructurado con foco en medición y mejora continua.
COBIT 2019	Gobierno de TI	KPIs y KRIs	Alinea métricas de TI con objetivos estratégicos del negocio.
MITRE ATTACK / D3FEND	Ciberdefensa táctica	Indicadores tácticos	Permite construir indicadores técnicos sobre amenazas y defensas.
ENISA Metrics Guidelines	Evaluación europea	KPIs, madurez	Guías de ENISE en materia de medición de seguridad para a UE.
Balanced Scorecard aplicado a ciberseguridad	Gestión estratégica	KPIs organizativos	Alinea la seguridad con la estrategia mediante una visión integral del desempeño.

Anexo IV.

Herramientas y recursos recomendados

a) Herramientas para visualización efectiva de información

La visualización de información en los reportes dirigidos a la Alta Dirección debe cumplir una función clara: transmitir mensajes clave de forma comprensible, rápida y eficaz.

b) Plataformas de visualización de datos

A continuación, se detallarán algunas herramientas genéricas que son muy prácticas y que permiten aplicar los principios de diseño visual y presentación de la información descritos anteriormente. Ejemplos de estas herramientas, que permiten crear visualizaciones impactantes, limpias y alineadas con las mejores prácticas de diseño visual serían:

Herramienta	Descripción	Casos de uso recomendado	Idoneidad reporting Alta Dirección
Tableau	Potente herramienta de BI. Permite dashboards interactivos y narrativas visuales.	Visualización de KPIs estratégicos y analíticos.	Alta
Power BI	Integración nativa con Microsoft 365. Ideal para entornos corporativos.	Reportes tácticos y operacionales.	Alta (especialmente en entornos Microsoft)
Canva / Visme	Ambas son herramientas de diseño gráfico con plantillas visualmente limpias.	Gráficos individuales o material visual para informes.	Alta
Flourish	Especializada en gráficos narrativos interactivos.	Storytelling visual enfocado a audiencias no técnicas.	Alta
Looker Studio	(Google) Gratuita, útil para dashboards simples y de rápida implementación.	Cuadros de mando para seguimiento periódico.	Media - Alta
Grafana	Especializada en monitorización en tiempo real	Orientada a indicadores operativos	Media (óptima para KPIs operativos)

*A tener en cuenta que estas herramientas son una referencia actual y que están sujetas a las leyes de mercado. Esto es, tienen su propio ciclo de vida, nacen, se desarrollan, evolucionan y/o pueden desaparecer y emerger otras nuevas referencias.

> Estas soluciones permiten integrar los principios de claridad, coherencia visual y narrativa estructurada en cualquier informe o presentación ejecutiva.

c) Herramientas especializadas en reporting de ciberseguridad

Existen también soluciones diseñadas específicamente para la visualización y comunicación de indicadores de seguridad. A modo de ejemplo:

- **SecurityScorecard**: Ofrece calificaciones de seguridad fácilmente comprensibles y visualizaciones comparativas del estado de seguridad de la organización. Ideal para comunicar posicionamiento respecto a competidores o estándares del sector.
- **BitSight Security Ratings:** Similar a SecurityScorecard, permite visualizar métricas de seguridad externas comparativas y evolución temporal, facilitando la conversación sobre **riesgos de terceros** con la Alta Dirección. Su caso de uso es muy específico.
- **Dashboards** de **SIEM** (como **QRadar**, **Splunk**, Microsoft **Sentinel**):
  - Configurables para mostrar indicadores de alto nivel.
  - Permiten drill-down para análisis detallados cuando sea necesario.
  - Ofrecen plantillas predefinidas para reporting ejecutivo.
  - Integran múltiples fuentes de datos de seguridad y podemos integrarlas adicionalmente con plataformas ITSM para enriquecer esos datos.
- **Plataformas GRC (Governace, Risk & Compliance):** Las plataformas GRC facilitan la integración de datos de riesgo y cumplimiento, y son muy útiles para el reporting a Alta Dirección.

d) Recursos para garantizar un diseño efectivo de informes

e) Plantillas y frameworks de reporting

Son útiles para mantener la coherencia visual y minimizar el tiempo de desarrollo de informes:

- **NIST Cybersecurity Framework Dashboard Templates**: Plantillas alineadas con los cinco pilares del NIST CSF (Identificar, Proteger, Detectar, Responder, Recuperar), facilitando la comunicación de madurez y progreso.
- **CIS Control Visualization Templates**: Recursos visuales para reportar el estado de implementación de los CIS Controls, con codificación de colores coherente y niveles de cumplimiento claramente definidos.

- **ISO 27001 Compliance Dashboards**: Muestran el estado de controles y no conformidades de manera visualmente eficaz, agrupados por dominios para facilitar la comprensión ejecutiva.

f) Recomendaciones de paletas cromáticas y codificación visual

Se usan para garantizar la coherencia visual y mejorar la interpretación intuitiva. A continuación, se pueden ver algunas posibles recomendaciones de paletas por tipo de información:

Tipo de información	Paleta recomendada*	Justificación
Niveles de riesgo	Gradiente Verde-Amarillo-Naranja-Rojo	Universalmente reconocible, permite identificación rápida de áreas críticas
Cumplimiento normativo	Azules y grises, con acentos en amarillo/rojo para excepciones	Transmite profesionalidad y formalidad, adecuado para contextos regulatorios
Indicadores de progreso	Verdes de distintas intensidades	Comunica avance positivo y crecimiento
Alertas y amenazas	Escala monocromática con acentos en rojo	Permite destacar lo urgente sin saturar visualmente

*Nota de accesibilidad: Asegurar que todas las paletas son comprensibles para personas con daltonismo. Herramientas como Color Oracle pueden ayudar a verificar la accesibilidad de las visualizaciones.

g) Guías y bibliotecas adicionales de diseño visual

Para que el diseño visual facilite la comprensión y no sea una barrera cognitiva, se indican a continuación algunas guías y bibliotecas que ayudarán a mejorar el diseño visual de estas presentaciones. Algunas que se pueden mencionar, de entre las actuales, son:

Recurso	Utilidad principal
ColorBrewer 2.0	Selección de paletas accesibles (daltónicos, impresión, etc.).
Material Design	Sistemas de diseño de Google con principios de UX/UI.
Noun Project / FontAwesome	Repositorios de iconos estandarizados y reconocibles.
Storytelling with Data (Cole Nussbaumer)	Libro y blog con ejemplos aplicados a reporting empresarial.
Datawrapper Blog / Highcharts Examples	Repositorios de casos de uso de gráficos bien diseñados.

h) Mejores prácticas para implementación

La selección de herramientas debe acompañarse de un proceso estructurado para garantizar la efectividad de los reportes:

i) Proceso de implementación recomendado

- Mapeo de audiencias y necesidades:
  - Identificar los diferentes stakeholders (CEO, CFO, Consejo, etc.)
  - Documentar sus preocupaciones específicas y nivel de detalle requerido
  - Establecer frecuencia ideal de reporting por audiencia
- Inventario de fuentes de datos:
  - Catalogar las fuentes disponibles (herramientas de seguridad, sistemas GRC, etc.)
  - Evaluar calidad, completitud y frecuencia de actualización
  - Identificar brechas de información
- Prototipado y validación:
  - Desarrollar prototipos de dashboards para cada audiencia
  - Validar con un grupo reducido de usuarios representativos
  - Refinar en base a feedback antes de la implementación completa
- Establecimiento de ciclo de mejora continua:
  - Recopilar feedback regularmente sobre utilidad y claridad

- Revisar KPIs trimestralmente para verificar relevancia
- Mantener el dashboard actualizado con nuevas amenazas y prioridades estratégicas

j) Recomendaciones para optimizar el impacto

Crear niveles de información: Partir de indicadores de alto nivel con posibilidad de profundizar en detalles ("drill-down") según demanda.

Incorporar benchmarks: Cuando sea posible, incluir comparativas con industria o estándares reconocidos para contextualizar el desempeño.

Balancear métricas técnicas y de negocio: Vincular indicadores técnicos con impactos en negocio para mejorar la relevancia en Alta Dirección.

Simplificar de forma inteligente: No confundir simplicidad con simplismo; buscar representaciones visuales que transmitan complejidad de forma accesible.

Este enfoque estructurado, combinado con las herramientas adecuadas, garantizará que los reportes a la Alta Dirección no solo informen, sino que faciliten decisiones estratégicas fundamentadas en materia de ciberseguridad.

k) Recomendaciones de uso. Claves prácticas

Por último, algunas prácticas clave que pueden ayudar al CISO:

- **Construir visualizaciones con propósito:** cada gráfico debe responder a una pregunta o reforzar un mensaje clave.
- **Adaptar las visualizaciones al público:** no es lo mismo reportar a un CFO que a un Comité de Dirección o a RRHH.
- **Aplicar la regla de los 5 segundos:** si no se entiende el mensaje principal en 5 segundos, el gráfico debe rediseñarse.
- **Menos, es más:** evitar dashboards saturados. Priorizar calidad sobre cantidad de información visual.
- **Actualizar las visualizaciones:** asegurar que los datos estén actualizados y sean relevantes para el ciclo de decisiones.

CyberIndicatorsFrameworks: el CISO y la Alta Dirección

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

Una iniciativa de

isms forum CSC CYBER SECURITY CENTRE