Unidad 11: La dirección de seguridad
BLOQUE III – La gestión del ciberriesgo como un proceso

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. El director de seguridad y su equipo.
2. El buen director de seguridad.
3. Comunicación del ciberriesgo.

1. El director de seguridad y su equipo

- Hace unos 25 ó 30 años que se comenzó a discutir la figura del director de seguridad con una función similar a la que tiene hoy en día.
  - Efecto 2000, atentados de septiembre del 2001.
- Se trataba de una figura puramente técnica, que se centraba mucho en la protección de los activos fundamentales, los datos y los sistemas de información que los procesaban.
  - Mediante cifrado, protección del perímetro y fortificación o bastionado de servidores.
  - Chief Information Officer (CIO).

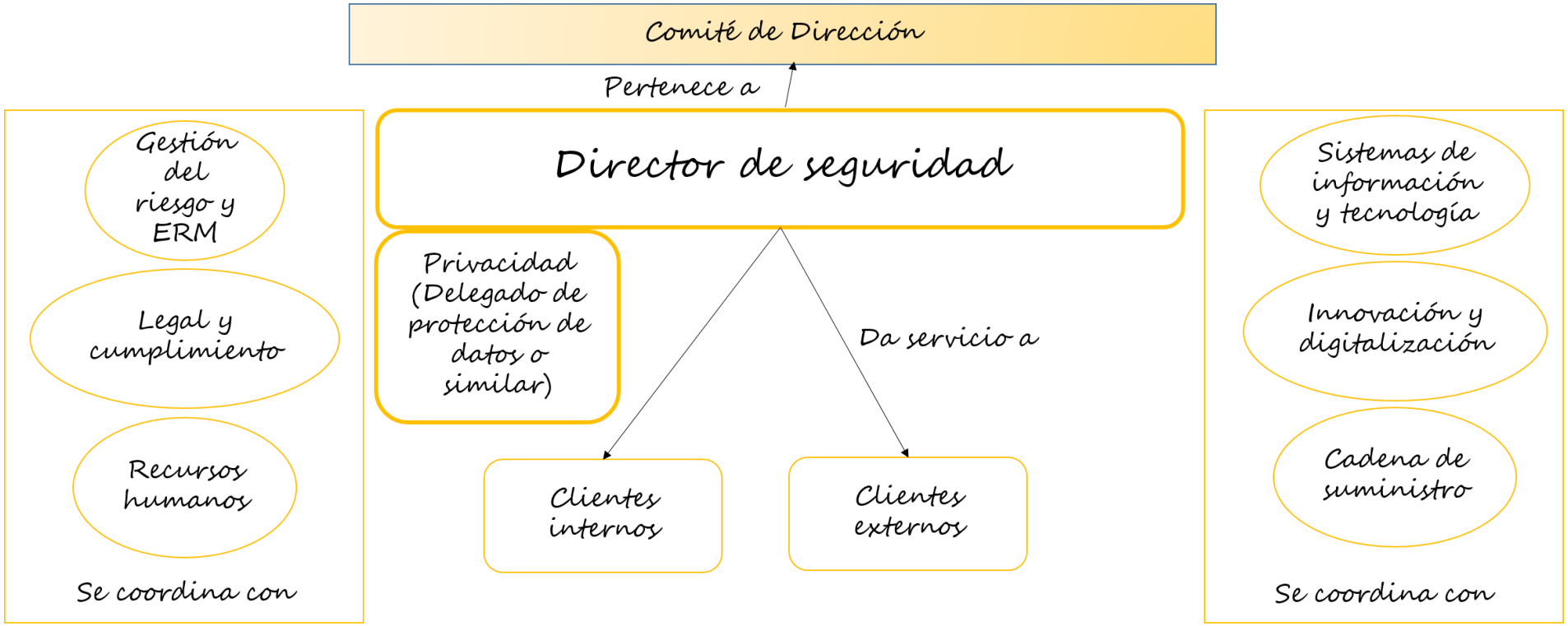
1. El director de seguridad y su equipo

- El rol del director de seguridad ha evolucionado mucho en estos años.
  - Chief Information Security Officer (CISO) o Chief Security Officer (CSO).
- Su perfil sigue siendo muy técnico pero se debe complementar con habilidades de comunicación y con una comprensión en profundidad del negocio y de sus objetivos.
  - Suele reportar directamente al CEO o a un consejero delegado y ocupa un puesto muy importante y de liderazgo en la mayor parte de los consejos de dirección

1. El director de seguridad y su equipo

- Distintos perfiles.
  - Ingeniero vs abogado vs economista.
- Distintas posiciones en el organigrama.
  - Dependiendo del CEO, del CTO, del CIO.
- Distintos enfoques.
  - Virtual vs interno. A tiempo parcial vs a tiempo completo.
- Distintas responsabilidades y recursos disponibles.

1. El director de seguridad y su equipo



Gestión del riesgo	Recursos humanos	Cumplimiento
Coordinar los procesos de evaluación y análisis de riesgos.	Preparar planes de formación y concienciación.	Mantener listado de obligaciones de cumplimiento.
Proponer mitigaciones y controles.	Revisar historial de nuevas contrataciones.	Coordinar a los departamentos y funciones afectados por estas obligaciones y darles soporte.
Planificar el despliegue de las mitigaciones y controles. Coordinación de Programas.	Fomentar la cultura de seguridad mediante políticas y procedimientos de seguridad.	Mantener el contacto con autoridades y grupos de interés.
Tecnología	**Comunicación**	**Respuesta a incidentes y continuidad del negocio**
Diseñar, desplegar, mantener, actualizar, etc. mitigaciones y contramedidas para prevención.	Redacción y actualización de documentos de seguridad.	Coordinar la respuesta a incidentes desde la notificación hasta el pos-incidente, obteniendo lecciones aprendidas que sirvan para la mejora continua.
Diseñar, desplegar, mantener, actualizar, etc. mecanismos de detección.	Comunicación interna, vertical y horizontal.	Gestionar acciones legales y recoger evidencias digitales.
Gestión de presupuesto, adquisiciones, su-contrataciones, cadena de suministro.	Comunicación externa con terceras partes, socios, proveedores, clientes, etc.	Garantizar niveles comprometidos de continuidad y coordinar la recuperación.

1. El director de seguridad y su equipo

- En organizaciones con recursos, el director tiene un equipo con diferentes perfiles:
  - Arquitectos de seguridad, con capacidad para comprender las amenazas que corre la organización y de diseñar y construir arquitecturas tecnológicas seguras y de decidir cuáles son los controles y contramedidas más adecuados en cada escenario.
  - Ingenieros de seguridad, con capacidad para identificar y analizar las vulnerabilidades presentes en la organización y de proteger y defender sus activos frente a posibles amenazas desplegando, configurando, etc. los controles y contramedidas más adecuados en cada caso. Es muy importante que alguno de estos miembros del equipo sea capaz de planificar y gestionar proyectos.
  - Administradores de seguridad, con capacidad para mantener y operar de manera cotidiana estos controles y contramedidas.

1. El director de seguridad y su equipo

- Analistas de seguridad, con capacidad para producir, revisar y evaluar la información que proviene de distintas fuentes y procesos y convertirla en inteligencia que permita evaluar y gestionar el ciberriesgo.
- Desarrolladores e ingenieros del software con capacidad para producir herramientas y software seguro. Este perfil es especialmente importante en el caso de organizaciones que proporcionen o comercialicen sus propios productos o servicios.
- Investigadores, forenses y en general, profesionales con capacidad para detectar incidentes de seguridad y responder adecuadamente cuando se producen.
- Responsables de cumplimiento, auditores y asesores en aspectos legales.
- Responsables de formación y concienciación.
- Responsables de adquisiciones, gestión de proveedores y de la cadena de suministro.

2. El buen director de seguridad

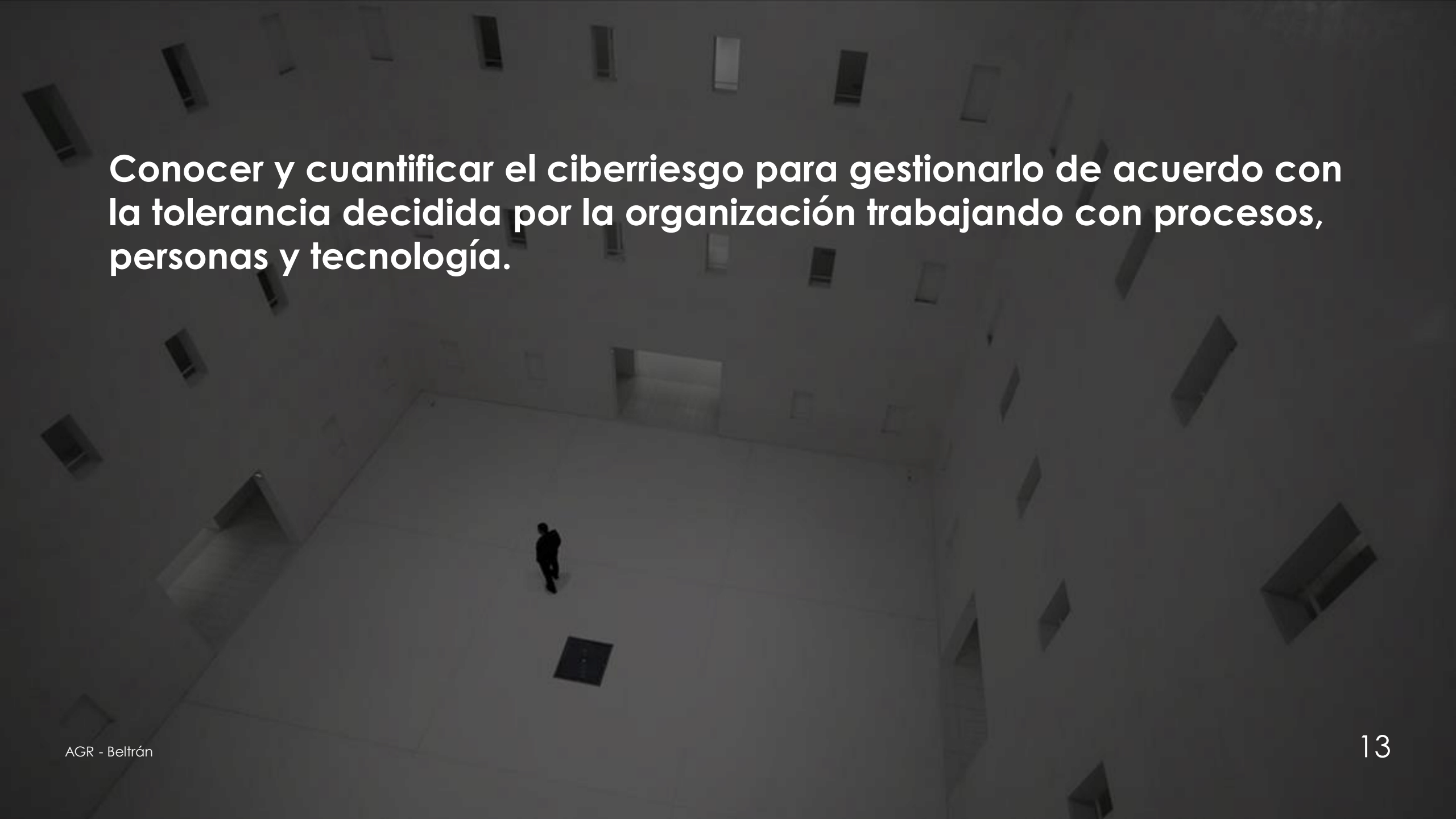
- Deber ser relevante:
  - Capaz de resolver problemas reales y de demostrar que las iniciativas que pone en marcha tienen un impacto y gestionan el ciber-riesgo de manera adecuada.
  - Capaz de cuantificar, para demostrar con indicadores de diferente naturaleza que el trabajo realizado es útil y que hoy se está mejor que ayer, que se ha mitigado, evitado o transferido riesgo invirtiendo los recursos disponibles donde era necesario.
  - Capaz de asumir responsabilidades y de tomar decisiones, priorizando y defendiendo las prioridades decididas con argumentos sólidos y soportados por evidencias.
  - Capaz de transmitir que es el experto, que se puede contar con él, que es de fiar, que escucha y que es útil.
  - Capaz de aportar y construir.

2. El buen director de seguridad

- Debe ser realista:
  - Capaz de mantenerse al día y actualizado.
  - Manejar bien el contexto interno, tanto desde el punto de vista del negocio (con el que tiene que estar siempre alineado, debe ser un habilitador) y de las operaciones, como del tecnológico.
  - Conocer bien a esos clientes internos y sus expectativas, limitaciones, etc. así como el nivel de madurez de la organización y las implicaciones que éste tiene en su función.
  - Capaz de detectar quiénes son sus aliados y quiénes van a ser una barrera. Debe ser capaz de distinguir qué peleas merece la pena luchar en cada momento.
  - No debe asumir más responsabilidades de las que le corresponden, comprendiendo bien su situación, su función y qué se espera de él o ella.

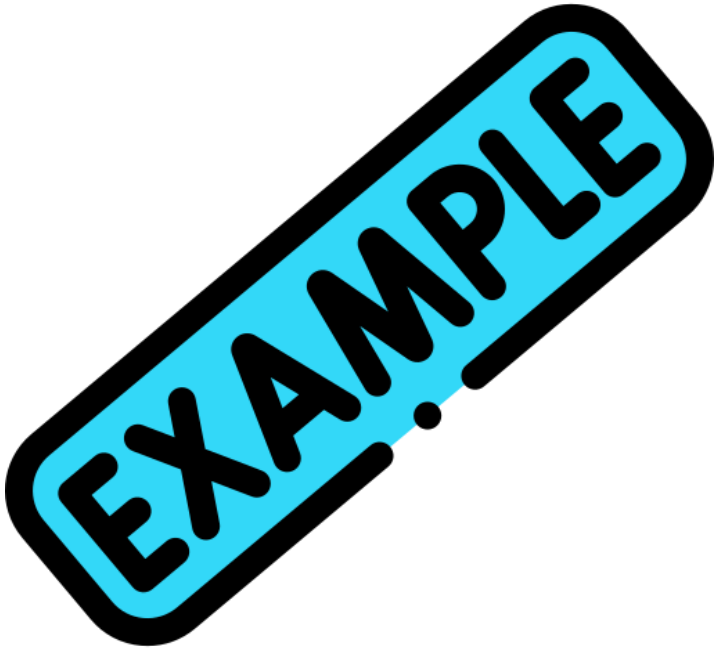
2. El buen director de seguridad

- Debe ser líder:
  - Capaz de gestionar un equipo con funciones, perfiles y responsabilidades muy variados.
  - Motivar y guiar a la organización, en los momentos buenos pero sobre todo en los malos.
  - Traducir de lenguaje técnico a lenguaje de negocio y viceversa,
  - Buen comunicador, didáctico.
  - Capaz de anticiparse a los riesgos que vendrán y estar preparado.
  - Capaz de planificar a corto, medio y largo plazo (de nuevo, priorizar).
  - Capaz de trabajar en un contexto en el que existe un adversario, algo que no es habitual en otros puestos de dirección.



Conocer y cuantificar el ciberriesgo para gestionarlo de acuerdo con la tolerancia decidida por la organización trabajando con procesos, personas y tecnología.

3. Comunicación del ciberriesgo



3. Comunicación del ciberriesgo

- Resumen ejecutivo:
  - Aséptico vs convincente.
  - Explicativo/introductorio vs numérico/avance de resultados vs recomendaciones.
  - Sólo texto vs gráfico.
  - Esquemático vs redactado.
  - Audiencia homogénea vs heterogénea.

3. Comunicación del ciberriesgo

- Consejos:
  - Lo primero es tomar todas las decisiones de la diapositiva anterior según de qué se trate.
  - Hilo conductor: qué quiero contar, a qué nivel, cómo quiero hacerlo, a dónde quiero llegar, cuál es el objetivo.
  - Comenzar por un esqueleto: número de párrafos, una idea por párrafo muy sencilla.
    - Ir desarrollando esta idea hasta dejar escrito cada párrafo.
  - Si hay figuras o tablas ¿a qué texto sustituyen? ¿merece la pena?
    - Trabajar esta parte gráfica adecuadamente, visualización.
  - Normalmente, es lo último que se escribe.

3. Comunicación del ciberriesgo

- Más:
  - Evitar jerga técnica y acrónimos.
  - Pero también definiciones vagas o textos que no aporten nada (no tienen que estar ahí).
  - Seguir la estructura del documento de alguna forma suele ser buena idea, ayuda al lector a ubicarse.
  - Encontrar el tono y mantenerlo (personal o impersonal, siempre el mismo tiempo verbal).
  - Una vez escrito, ver cómo se puede resumir todavía más.
  - Tras leerlo, tiene que quedar alguna conclusión clara.

Para leer e investigar…

1. "2021 Global Chief Information Security Officer (CISO) Survey", Heidrick & Struggles (2021).
2. "SURVEY ANALYSIS REPORT: Chief Information Security Officers' (CISO) Challenges & Priorities", ECSO (2021).

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/
- Figuras:
  - "Dirección de seguridad y gestión del ciberriesgo" Fernando Sevillano y Marta Beltrán. Colección Ciberseguridad, editorial RaMa. 2021.