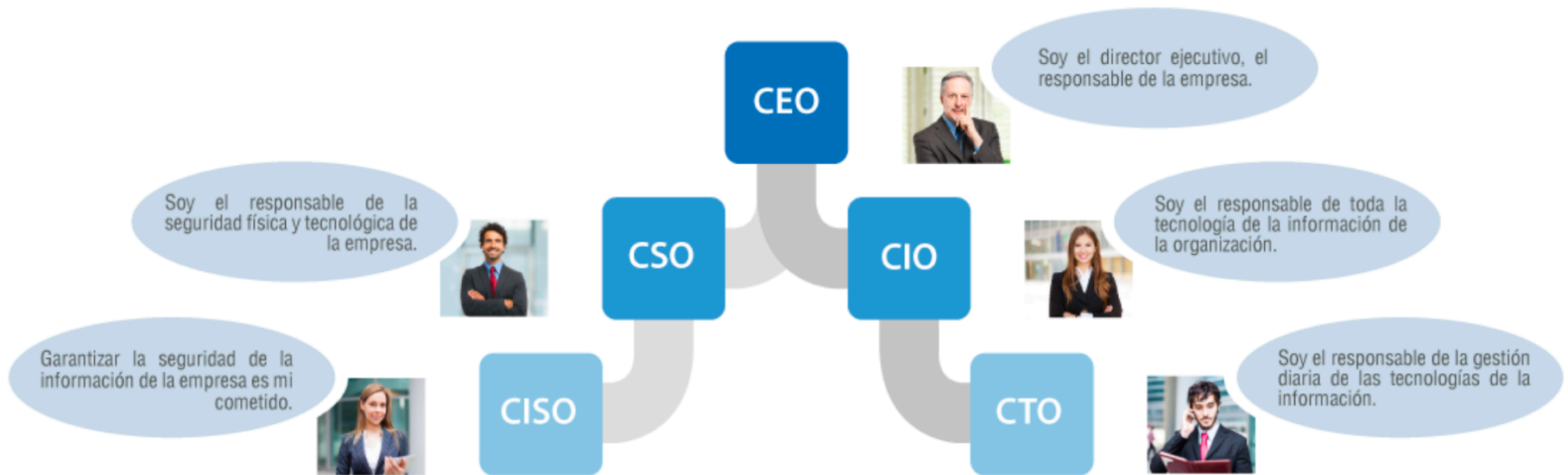


FIGURAS DIRECTIVAS

CIO, CISO

Figuras directivas relacionadas con la seguridad de la información



CEO

- **El CEO (Chief Executive Officer).**
 - Es el director ejecutivo, el gerente, el cargo más alto dentro del organigrama de la organización. Es el responsable final de las acciones que se lleven a cabo dentro de la empresa, de su desempeño y su eficiencia.
 - Su función principal es la de supervisar y velar porque la estrategia definida en la empresa cumpla con la consecución de los objetivos de la organización, además de sembrar los principios y pilares básicos a seguir dentro de la empresa.
 - El CEO tiene una importante relación con el CIO, debido a que las estrategias de las empresas están estrechamente ligadas al ámbito de las tecnologías de la información.

CIO

- **El CIO (Chief Information Officer)**
 - Es el gerente de sistemas o director de tecnologías de la información.
 - Reporta directamente al CEO, y se encarga básicamente de que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados.
 - Además, se encarga de
 - mejorar los procesos de tecnologías de la información de la organización,
 - gestionar el riesgo y la continuidad de negocio,
 - controlar el coste en infraestructura de tecnologías de la información,
 - alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos,
 - y establecer mejoras e innovaciones de soluciones y productos.

CTO

- **El rol del CTO (Chief Technology Officer)**
 - en un rol similar al CIO pero más “técnico”.
 - Se entremezclan con las funciones de los CIO.
 - Es un director técnico, siendo su responsabilidad la gestión del día a día de las tecnologías de la información.

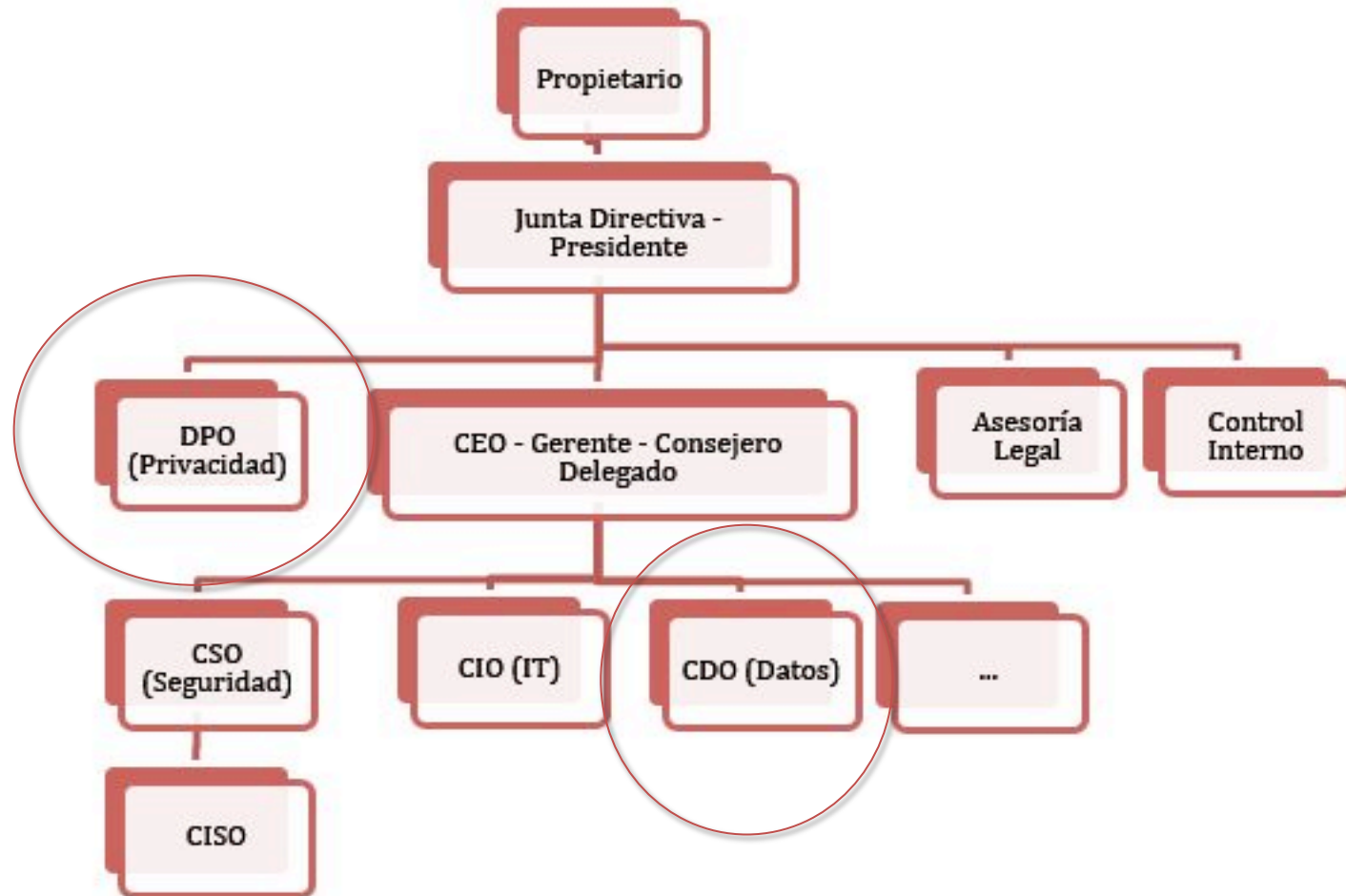
CSO

- El CSO (Chief Security Officer) es el responsable de la seguridad de la organización.
- Al CSO a veces se le denomina responsable de seguridad corporativa.
- El rol del CISO suele estar más centrado en aspectos de seguridad de la información, mientras que al CSO se le requiere:
 - Tener una visión de negocio que comprenda los riesgos que afronta la organización y cómo tratarlos.
 - Entender la misión y los objetivos de la empresa y asegurarse de que todas las actividades son planificadas y ejecutadas para satisfacer dichos objetivos.
 - Comprender las necesidades normativas, la gestión de la reputación de la organización y las expectativas de los usuarios.
 - Establecer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las tecnologías de la información.
 - Estar al tanto de los cambios normativos, debiendo informarse de las consecuencias para las actividades de la organización y proponiendo las medidas oportunas para adecuarse al nuevo marco normativo.
- Cuando existen CSO y CISO, el CISO reporta al CSO y el CSO a la dirección.

CISO

- El CISO (Chief Information Security Officer) es el director de seguridad de la información.
- Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio.
- El rol de CISO podemos decir que en general, sus responsabilidades incluyen:
 - Generar e implantar políticas de seguridad de la información.
 - Garantizar la seguridad y privacidad de los datos.
 - Supervisar la administración del control de acceso a la información.
 - Supervisar el cumplimiento normativo de la seguridad de la información.
 - Responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.
 - Supervisar la arquitectura de seguridad de la información de la empresa.

Nueva figura del Delegado de Protección de Datos



DPO y DPD

- El **DPO** es fundamentalmente un asesor para el cumplimiento del RGPD. Estos son dos posibles encajes:
 - El **CISO** o el **CDO**, otro «*Chief XXX Officer*» o un empleado a otro nivel, podría ser también el DPD siempre que no intervengan en determinar los fines y medios del tratamiento, y que se implementen las garantías de ausencia de conflicto de intereses.
- Si el DPD se designa como figura independiente, el **CISO** y el **CDO** podrán «descargar» la responsabilidad de supervisión y asesoramiento sobre el RGPD en esta persona.
- En este caso, al no ser desempeñadas las funciones de DPD junto con otras funciones, será más fácil demostrar la ausencia de conflicto de intereses.