1. Equipo de Arquitectura y Diseño de Seguridad

- Diseñar la arquitectura de seguridad de la organización, asegurando que las nuevas tecnologías y sistemas sean seguros.
- Trabajar con el equipo de desarrollo para integrar la seguridad en el ciclo de vida del desarrollo de software.
- Desarrollar y mantener las soluciones criptográficas para proteger los datos.

1

2. Equipo de Operaciones de Seguridad

- Supervisar las operaciones diarias del equipo SecOps.
- Monitorear las alertas de seguridad, investigar incidentes y responder a amenazas.
- Diseñar y mantener las herramientas y sistemas de seguridad.
- Atender la respuesta a incidentes de seguridad, coordinando con otros equipos para la contención y remediación.

2

3. Equipo de Gobernanza, Riesgo y Cumplimiento (GRC)

- Supervisar el cumplimiento de las políticas de seguridad y las normativas.
- Monitorear y asegurar que la organización cumple con las normativas y estándares de seguridad.
- Gestionar los riesgos de seguridad
- Desarrollar los procedimientos, normas y directrices

3

4. Equipo de Concientización y Capacitación en Seguridad

- Liderar los programas de formación y concientización en seguridad.
- Diseñar y entregar programas de capacitación en seguridad para los empleados.

4

Modelo de Organización de Seguridad de la Información

5

TI & SI

¿INTEGRADOS O SEPARADOS?

6

Razones a Favor de Separar TI de Seguridad Informática

1. Especialización: La seguridad informática requiere habilidades y conocimientos específicos que pueden diferir significativamente de los necesarios para la gestión de operaciones de TI. La separación permite que cada equipo se enfoque en su área de especialización.

2. Independencia en la Evaluación de Riesgos: Tener un equipo de seguridad independiente puede ofrecer una perspectiva objetiva sobre los riesgos y vulnerabilidades, evitando posibles sesgos que podrían surgir si ambos roles están bajo la misma dirección.

3. Prevención de Conflictos de Intereses: En una estructura separada, el equipo de seguridad puede monitorear y evaluar la infraestructura de TI sin conflictos de interés, asegurando que las políticas de seguridad se apliquen rigurosamente.

4. Mejora del Control y la Gobernanza: La separación puede fortalecer los controles internos y la gobernanza, proporcionando una capa adicional de supervisión y asegurando que las políticas de seguridad se mantengan independientes de las decisiones operativas de TI.

7

Razones a Favor de Integrar TI y Seguridad Informática

1. Coordinación Efectiva: Tener ambos equipos bajo una misma área facilita la coordinación entre operaciones y seguridad, asegurando que las medidas de seguridad se integren de manera efectiva en las operaciones diarias de TI.

2. Respuesta Rápida a Incidentes: La integración puede mejorar la capacidad de respuesta a incidentes, ya que los equipos están en estrecha comunicación y pueden actuar de manera más coordinada frente a amenazas y vulnerabilidades.

3. Visión Unificada: Una estructura integrada permite una visión unificada de la infraestructura de TI y su seguridad, lo que puede facilitar la implementación de políticas y prácticas consistentes.

4. Eficiencia de Recursos: Integrar ambos equipos puede reducir redundancias y optimizar el uso de recursos, evitando la duplicación de esfuerzos y mejorando la eficiencia operativa.

5. Cultura de Seguridad: La integración puede fomentar una cultura de seguridad en la que todos los miembros del equipo de TI están más conscientes y comprometidos con las prácticas de seguridad.

8

La situación varía según la organización y su tamaño, así como la industria en la que opera. Sin embargo, hay algunas tendencias comunes:

Empresas Grandes y Reguladas: En organizaciones grandes y altamente reguladas (como en sectores financieros o de salud), es más común ver una separación clara entre TI y seguridad informática. Esto es para cumplir con requisitos de gobernanza y para proporcionar una capa adicional de protección y control.

Empresas Medianas y Pequeñas: En organizaciones más pequeñas o en empresas que buscan optimizar recursos, a menudo se integran las funciones de TI y seguridad informática bajo un solo departamento o equipo. Esto facilita la coordinación y puede ser más económico.

9

Tendencias de Integración: Hay una tendencia creciente hacia la integración en muchas organizaciones debido a la necesidad de una respuesta ágil a las amenazas y la creciente complejidad de los entornos tecnológicos. La integración permite una gestión más cohesiva de la infraestructura y la seguridad.

En resumen, la decisión de separar o integrar TI y seguridad informática depende de las necesidades específicas y la estructura de cada organización. Ambos enfoques tienen sus ventajas y desventajas, y la elección suele reflejar el equilibrio entre la especialización, la coordinación y la eficiencia que cada organización busca lograr.

10

Tareas que un área de seguridad suele delegar en TI por razones de conveniencia o practicidad

- Gestión de Parches y Actualizaciones de seguridad
- Configuración y Administración de Firewalls y Sistemas de Seguridad Perimetral (IPS-IDS)
- Gestión de Identidades y Accesos (IAM)
- Copia de Seguridad y Recuperación de Datos (Backups)
- Monitoreo básico de Seguridad (SIEM)
- Gestión de Endpoints (antivirus, antimalware)
- Soporte de Seguridad de Primer Nivel
- Gestión de Software de Seguridad de Red

11

MISION Y FUNCIONES DEL AREA DE SEGURIDAD INFORMATICA

12

MISIÓN

Procurar (¿asegurar, garantizar?) la confidencialidad, integridad y disponibilidad de la información de la organización (¿?), protegiendo nuestros activos digitales de amenazas internas y externas, a través de la implementación y mantenimiento de medidas de seguridad robustas y actualizadas, asegurando así la continuidad de nuestros procesos y la confianza de nuestros clientes.

13

FUNCIONES

- Desarrollo e implementación de políticas de seguridad
- Gestión de riesgos
- Diseño e implementación de soluciones de seguridad
- Monitoreo y análisis de eventos de seguridad
- Concientización y capacitación al personal
- Gestión de incidentes de seguridad
- Cumplimiento normativo
- Contingencia y recuperación de desastres

14

MISIÓN Y FUNCIONES (RESPONSABILIDADES) DEL CISO

15

La misión del CISO

El CISO tiene como misión definir la estrategia global de Seguridad de la Información de la organización a su cargo, coordinar su materialización en todos los ámbitos de la misma, identificar el nivel de riesgo existente y promover una cultura de resiliencia en esta materia.

Para lograr el cumplimiento de dicha misión el CISO debe contar con dos aspectos fundamentales:

- Tener los conocimientos, competencias y experiencia necesarias
- Apoyo de la Alta Dirección, con una definición clara de ámbitos y responsabilidades.

16

16

- **Estrategia de Seguridad:**
  - Desarrollar una estrategia de seguridad integral que se alinee con los objetivos de negocio de la organización.
  - Identificar, evaluar y mitigar los riesgos de seguridad de manera continua (Gestión de Riesgos)
  - Desarrollar planes de respuesta a incidentes, recuperación de desastres y continuidad del negocio.
- **Gobierno de la seguridad:**
  - Integrar, y eventualmente presidir, comités de seguridad, y comunicar los riesgos y estrategias a la alta dirección.
  - Fomentar una cultura de seguridad en toda la organización a través de concientización y capacitación.
  - Presentar, exponer y justificar ante los niveles directivos los planes, programas, proyectos y resultados del área de seguridad informática.

17

- **Cumplimiento normativo:**
  - Asegurar que la organización cumpla con las regulaciones y estándares de seguridad aplicables (Cumplimiento: GDPR, PCI DSS, etc.).
  - Realizar monitoreos para verificar el cumplimiento de las políticas de seguridad.
- **Relaciones con otros departamentos:**
  - Trabajar en estrecha colaboración con otras áreas de la organización para integrar la seguridad de la información en los procesos de negocio.
- **Tecnología y herramientas:**
  - Evaluar, seleccionar e implementar las tecnologías y herramientas de seguridad adecuadas para proteger los activos de la organización.
  - Supervisar la gestión y mantenimiento de las herramientas de seguridad.

18

- **Gestión del área:**
  - Desarrollar, implementar y gestionar el SGSI.
  - Liderar el desarrollo de políticas, procedimientos, estándares y directrices de seguridad de la información actualizados, y supervisar su aprobación, difusión y mantenimiento.
  - Desarrollar y gestionar el presupuesto del área.
  - Gestión de talentos: desarrollar, orientar y gestionar un personal de alto rendimiento de seguridad de la información.
  - Desarrollar métricas de negocio para medir la eficacia del programa de gestión de seguridad y aumentar la madurez del programa con el tiempo.
- **Gestión de incidentes:**
  - Dirigir la respuesta a incidentes de seguridad, desde la detección hasta la recuperación.
  - Analizar los incidentes para identificar las causas raíz y mejorar las medidas de seguridad.

19

PERFIL DEL CISO (conocimientos, experiencia, estudios, habilidades)

Conocimientos: estudios formales, cursos de capacitación, dominio de la tecnología, marcos y estándares, arquitectura de seguridad, experiencia, trayectoria.

Habilidades personales: comunicación oral y escrita, negociación, liderazgo, manejo de expectativas, marketing.

Capacidad de gestión: trabajo en equipo, visión económica-financiera, administración de proyectos.

Conocimiento del negocio: organización, procesos, mercado, contexto.

20

Evolución del CISO

- **CISO tradicional vs. CISO moderno:**
  - Enfoque en la tecnología vs. enfoque en el negocio.
  - Rol reactivo vs. rol proactivo.
  - Habilidades requeridas.
- **Factores que han impulsado la evolución:**
  - Aumento de la complejidad de las amenazas.
  - Mayor dependencia de la tecnología.
  - Creciente importancia de la privacidad de los datos.
- **Tendencias actuales:**
  - CISO como socio estratégico del negocio.
  - Mayor enfoque en la gestión de riesgos.
  - Importancia de la cultura de seguridad.

21

DESAFÍOS MÁS COMUNES QUE ENFRENTAN LOS CISOs

- La escasez de talento
- La complejidad creciente de las amenazas
- La presión para hacer más con menos
- La resistencia al cambio
- La integración de la seguridad con los procesos de negocio
- La gestión de la fatiga de la seguridad

22

A quién reporta el CISO

- **Estructura organizacional típica:**
  - CEO
  - Director de Información (CIO)
  - CISO
- **Tendencias actuales:**
  - Reporte directo al CEO en organizaciones más maduras en seguridad.
  - Comité de seguridad para decisiones estratégicas.

23

¿De quién debe depender el CISO?

- Del tamaño de la empresa
- De la naturaleza del “compliance”
- De la naturaleza del Gobierno de la TI
- El nivel de madurez del programa de seguridad
- El nivel de madurez de la gestión del riesgo
- De la visión de la dirección
- De las características del CIO
- De las características personales del CISO

24

El CISO del futuro

- **Habilidades y conocimientos requeridos:**
  - Inteligencia artificial y machine learning.
  - Ciberseguridad en la nube.
  - Privacidad de los datos.
  - Resiliencia cibernética.
- **Desafíos futuros:**
  - Ataques más sofisticados.
  - Escasez de talento.
  - Presión para demostrar el valor de la seguridad.
- **Recomendaciones para el futuro del CISO:**
  - Desarrollo continuo de habilidades.
  - Colaboración con otros equipos.
  - Promoción de una cultura de seguridad.

25

Global CISO Forum

26

1. ASESOR DE SEGURIDAD DE CONFIANZA: Como CISO, necesita traducir los asuntos técnicos al lenguaje de la empresa. En otras palabras, ayudará a los ejecutivos y juntas directivas no tecnológicas a comprender cuestiones técnicas y a tomar decisiones informadas sobre los riesgos con confianza.

2. ESTRATEGA: Como CISO, debe involucrarse en el establecimiento de objetivos, la determinación de acciones para lograrlos y la movilización de recursos para ejecutar acciones priorizadas que deben estar estrechamente vinculadas a la estrategia comercial.

3. LÍDER: Como CISO, debe tener habilidades de liderazgo no solo para construir un equipo diverso inspirado y unido, sino también para dar ejemplo como modelo a seguir para crear una cultura de aprendizaje constante, innovación y colaboración activa.

27

4. MARKETER MODERNO El marketing moderno es la capacidad de aprovechar todas las capacidades de una empresa para brindar la mejor experiencia al cliente y así impulsar el crecimiento. Como CISO, debe difundir las capacidades de ciberseguridad entre los reguladores, los clientes potenciales, las aseguradoras y los socios comerciales, ayudando a conseguir nuevos negocios, reducir el costo de capital y mantener una licencia para operar.

5. AGENTE DE CAMBIO: Los CISO deberían poder crear una cibercultura en la que todos en la organización comprendan los riesgos cibernéticos y ayuden a mitigarlos.

6. INFLUENCIADORES: Los CISO deberían poder influir en las partes interesadas críticas para apoyar la transformación de la ciberseguridad.

28

5 formas de saber que no eres material CISO

Característica

28 de marzo de 2023 • 7 minutos

CSO y CISO | Gestión de riesgos

Los profesionales de la ciberseguridad que buscan el puesto más alto tienen las habilidades técnicas para convertirse en CISO, pero pueden preguntarse si tienen lo necesario para liderar un equipo y al mismo tiempo garantizar el apoyo de la administración y la junta directiva. Aquí hay cinco formas de saber si eres candidato a CISO o no.

29

Los conocimientos técnicos y la experiencia son obviamente enormes activos.

Un CISO eficaz tiene la capacidad de evaluar y seleccionar tecnología de seguridad, comunicarse con el personal técnico y tomar decisiones cruciales sobre la infraestructura y la arquitectura de seguridad.

La mayoría ya tiene experiencia liderando y gestionando personas, ha establecido relaciones con stakeholders relevantes dentro de la organización y ha vivido situaciones de crisis.

Saben cómo tomar decisiones rápidas e impulsar cambios en la organización.

Sin embargo, algunas cualidades podrían perjudicar el éxito como CISO.

Aquí hay cinco cualidades necesarias que si no la tienes , indican que probablemente no seas apto para ser CISO.

30

1. **Ser reacio al riesgo**: Por definición, la función de un CISO es gestionar el riesgo cibernético. Eso implica evaluar y gestionar el riesgo en toda la empresa y tomar decisiones basadas en esas evaluaciones.

2. **Queriendo hacerlo todo**: Los CISO son responsables de liderar y gestionar equipos de profesionales de seguridad. Como CISO, debes ser experto en gestionar personas y comunicarte eficazmente con los demás. Significa estar dispuesto a escuchar y considerar los comentarios de los demás.

3. **No te gusta hablar de negocios**: No eres apto para CISO si careces de una sólida comprensión de los requisitos y objetivos del negocio para desarrollar una estrategia de seguridad que se alinee con los objetivos de la organización.

31

4. **No puedes "vender" seguridad**: Ser CISO significa poder vender seguridad a la gerencia y a quienes controlan el dinero. Un CISO necesita poder articular y defender las razones para un mayor presupuesto de ciberseguridad o para un gasto adicional en un proyecto.

5. **Ser demasiado técnico**: Las habilidades técnicas son esenciales para una buena ciberseguridad. Pero ser demasiado técnico es un inconveniente porque indica que su enfoque como CISO probablemente favorecería el uso de tecnología en cada desafío de seguridad. La realidad es que, como líder de seguridad, su función realmente es gestionar el riesgo cibernético y, al mismo tiempo, permitir que su organización siga cumpliendo sus objetivos de negocio.

32

Acerca de los ejecutivos de Seguridad Informática

Los ejecutivos de seguridad de la información deben aumentar su comprensión del negocio y sus habilidades en la comunicación.

Los ejecutivos de seguridad de la información deben mantener informados a los ejecutivos del negocio a través de publicaciones acerca de la problemática de la SI.

Los ejecutivos de seguridad deben intervenir en la incorporación de TIC

El ejecutivo de SI y el auditor deben trabajar en equipo para evitar incorporar TI que no cumplan con los requisitos establecidos.

33

vCISO

"Los vCISO son una nueva solución a un viejo problema. Con un vCISO, las organizaciones pueden acceder a la experiencia que necesitan para alcanzar sus objetivos de ciberseguridad, sin las complejidades de contratación y los altos costos que normalmente conlleva un líder interno permanente en ciberseguridad."

Es **un profesional que presta sus servicios** a una empresa que lo contrata **por horas o tiempos definidos** y de una manera regular, casi siempre en forma remota.

34

VENTAJAS

- **Flexibilidad:** Los servicios de un vCISO se pueden ajustar a las necesidades y presupuesto de cada organización.
- **Experiencia:** Los vCISO suelen tener una amplia experiencia en diferentes sectores y tecnologías, lo que les permite ofrecer una visión más global de la seguridad.
- **Acceso a conocimientos especializados:** Las organizaciones pueden acceder a conocimientos especializados en ciberseguridad sin tener que contratar a un equipo completo.
- **Costos optimizados:** Contratar un vCISO suele ser más económico que tener un CISO a tiempo completo, especialmente para pequeñas y medianas empresas.

35

Rol y Perfil del CISO según CISCO

FING

36

CISO según CISCO

¿Qué es un CISO?

Un CISO, o director de seguridad de la información, es un ejecutivo de alto nivel que supervisa la seguridad informática, cibernética y tecnológica de una organización.

Las responsabilidades del CISO incluyen desarrollar, implementar y hacer cumplir políticas de seguridad para proteger datos críticos.

37

Las responsabilidades exactas variarán según la organización

Tradicionalmente, un CISO se centra en desarrollar y liderar el programa de seguridad de la información.

Esto implica proteger los activos, las aplicaciones, los sistemas y la tecnología de la organización y, al mismo tiempo, permitir y promover los resultados del negocio.

Otros deberes pueden incluir, pero no están limitados a:

•Desarrollar e implementar procesos y sistemas seguros utilizados para prevenir, detectar, mitigar y recuperarse de ciberataques.

•Educar y gestionar el riesgo tecnológico en colaboración con líderes empresariales

38

•Construir e impulsar una estrategia y un marco de ciberseguridad, con iniciativas para proteger los activos cibernéticos y tecnológicos de la organización.

•Evaluar y gestionar continuamente la postura de riesgo cibernético y tecnológico de la organización.

•Implementación y gestión del proceso de gobernanza, riesgo y cumplimiento cibernético (GRC)

•Reportando a los niveles más altos de la organización (el CEO y la junta directiva, o equivalente)

•Desarrollar, justificar y evaluar inversiones en ciberseguridad

•Desarrollar e implementar capacitación y educación continua sobre concientización sobre seguridad para los usuarios.

•Liderar operaciones de ciberseguridad e implementar protocolos de recuperación ante desastres y planes de continuidad comercial teniendo en cuenta la resiliencia empresarial

39

¿Cómo está evolucionando el papel del CISO y por qué?

- El papel del CISO se está expandiendo rápidamente y adquiriendo mucho más impacto. Los CISO interactúan con más frecuencia con otros ejecutivos de la alta dirección, como el director ejecutivo o el director financiero (CFO), así como con la junta directiva de forma casi continua.
- Muchos CISO lideran debates de alto nivel sobre la estrategia de seguridad y ayudan a los líderes empresariales a comprender las tendencias y los riesgos que afectan a la organización. Se espera que un CISO intervenga en todo lo relacionado con el riesgo tecnológico de la organización. Esto puede incluir la protección de la fuerza laboral remota, liderar la GRC en materia de ciberseguridad y gestionar de forma proactiva las operaciones de seguridad.
- Las empresas aprovechan la experiencia de un CISO sobre las complejidades de seguridad involucradas en acelerar la transformación digital, migrar a la nube, proteger la cadena de suministro y pasar al trabajo remoto e híbrido. También se les pide que informen sobre las medidas de seguridad y cumplimiento a las partes interesadas y a los reguladores.

40

¿Qué valor aporta un CISO?

Las organizaciones se benefician de la visión amplia de seguridad de un CISO. Este líder tecnológico comprende cómo se relacionan diversos aspectos de la seguridad con los sistemas, dispositivos y redes de TI en los que opera y depende la empresa.

Un CISO aplica su perspectiva única sobre seguridad para identificar riesgos de seguridad y recomendar estrategias para gestionarlos. Los CISO exitosos también pueden tomar problemas de seguridad complejos y describirlos en un lenguaje no técnico que ayude a los líderes y otras partes interesadas clave a comprender los impactos potenciales (buenos o malos) de esos problemas.

41

¿Qué habilidades debe tener un CISO?

La pasión por la tecnología de la información y el compromiso con el aprendizaje continuo son esenciales para el éxito como CISO, pero también lo es comprender cómo liderar a las personas.

Debido a que el rol del CISO es cada vez más destacado, estos profesionales deben tener sólidas habilidades de gestión, comunicación, liderazgo y negociación. La visión para los negocios también es una habilidad valiosa, ya que ayuda a los CISO a comprender mejor cómo la tecnología y la seguridad respaldan los objetivos comerciales.

Además, dadas las tendencias hacia la transformación digital y el trabajo remoto e híbrido, los CISO deben comprender la seguridad de las aplicaciones y la nube. También deben ser conscientes de los posibles riesgos de seguridad asociados con tecnologías emergentes como la automatización y el aprendizaje automático.

42

B I S O

43

BISO

Business **I**nformation **S**ecurity **O**fficer

“La próxima evolución del CISO”

44

Consultores relevantes dicen:

“No se puede conseguir la aceptación organizacional de la seguridad informática simplemente arrojándole tecnología “

"Cuando TI actúa como socio del negocio, en lugar de como consultor de tecnología o simple proveedor de servicios de TI, los beneficios son sorprendentes“

45

BISO a bordo: los embajadores cierran la brecha entre la ciberseguridad y los negocios

Un BISO es un mediador en un puente de doble vía, con presencia tanto en el mundo de la ciberseguridad como en el sector empresarial . El BISO traduce conceptos y conecta los puntos entre la ciberseguridad y las funciones empresariales para garantizar que los equipos estén sincronizados.

46

47

¿El BISO por arriba, al mismo nivel o por debajo del CISO?

48

Un BISO puede:

- Actuar como contacto de seguridad principal para el nivel directivo.
- Desarrollar y supervisar la implementación de políticas, procedimientos y controles de seguridad.
- Realizar evaluaciones de riesgos y gestionar la respuesta a incidentes de seguridad.
- Supervisar el cumplimiento de las normas de seguridad
- Gestionar presupuestos de seguridad

49

Conjunto de habilidades BISO

Sólida perspicacia empresarial: los directores de sistemas de información deben comprender y hablar el lenguaje empresarial. Deben ser capaces de explicar claramente el valor de las inversiones en ciberseguridad a los líderes empresariales que pueden no estar familiarizados con los detalles técnicos.

Sólidas habilidades técnicas: los BISO deben tener un conocimiento profundo de las tecnologías de ciberseguridad y de cómo pueden proteger los activos de su organización. También deben estar familiarizados con una amplia gama de sistemas y aplicaciones de TI.

Sólidas habilidades de comunicación: los BISO deben comunicarse eficazmente con el personal técnico y no técnico. Deben ser capaces de traducir conceptos técnicos complejos a un lenguaje sencillo y presentarlos de una manera que los responsables de la toma de decisiones puedan comprender.

Comprensión de los principios de gestión de riesgos: los BISO deben ser capaces de identificar, evaluar y priorizar los riesgos. También deben estar familiarizados con los principios de gestión de riesgos y cómo se aplican a la ciberseguridad.

Sólidas habilidades de gestión de proyectos: los BISO deben supervisar los proyectos desde su inicio hasta su finalización, estableciendo objetivos, cronogramas y presupuestos, y al mismo tiempo adaptándose a las amenazas cibernéticas emergentes. Para tener éxito, se requiere un profundo conocimiento tanto de la tecnología como de los negocios.

50

Según una encuesta de 2020 realizada por Forrester Consulting los ejecutivos de seguridad alineados con el negocio tienen ocho veces más probabilidades de tener una gran confianza en sus evaluaciones internas de seguridad y riesgo que sus pares más centrados en la tecnología.

En el mismo informe, los investigadores descubrieron que las organizaciones con una fuerte alineación entre la seguridad y el negocio tienen más del doble de probabilidades de emplear BISO o ejecutivos similares.

51

El BISO es vital en materia de ciberseguridad, ya que conecta los objetivos organizacionales con la protección contra amenazas cibernéticas en grandes entidades.

Colabora con líderes tecnológicos y empresariales para integrar la ciberseguridad en la planificación a largo plazo.

Los BISO actúan como intermediarios entre los equipos de seguridad y operativos, asesorando a los líderes y ofreciendo su experiencia en cumplimiento normativo, evaluación de riesgos y prevención de pérdida de datos.

Se aseguran de que la ciberseguridad se integre en las nuevas iniciativas tecnológicas desde el principio, en lugar de agregarse como una idea de último momento.

52

Históricamente, los equipos de seguridad y sus líderes pueden haber creado inadvertidamente barreras a la colaboración al presentarse como la voz más importante en la sala y dejar poco margen para la negociación sobre cuestiones de seguridad, un problema que se amplifica cuando se utiliza la jerga y la complejidad, a sabiendas o sin saberlo, para ofuscar las cuestiones.

La importancia de adoptar un enfoque empresarial respaldado por personas, procesos y tecnología está ganando una aceptación más amplia dentro de la comunidad de seguridad más humilde del presente.

Adoptar un enfoque de este tipo requiere un conjunto diverso de habilidades y competencias que no se encuentran fácilmente en las funciones de seguridad tradicionales.

53

El **marketing de la seguridad** es una consideración cada vez mayor para los líderes de seguridad.

Una relación más estrecha con el consumidor (la empresa) puede hacer que la seguridad sea más atractiva y demostrar su valor al comprender verdaderamente las motivaciones y necesidades de la empresa y adaptar la propuesta a esas necesidades.

El objetivo es llegar a un punto en el que la empresa "quiera" seguridad como línea de inversión, en lugar de que la seguridad sea vista como algo que "debe" o "deberá" tener.

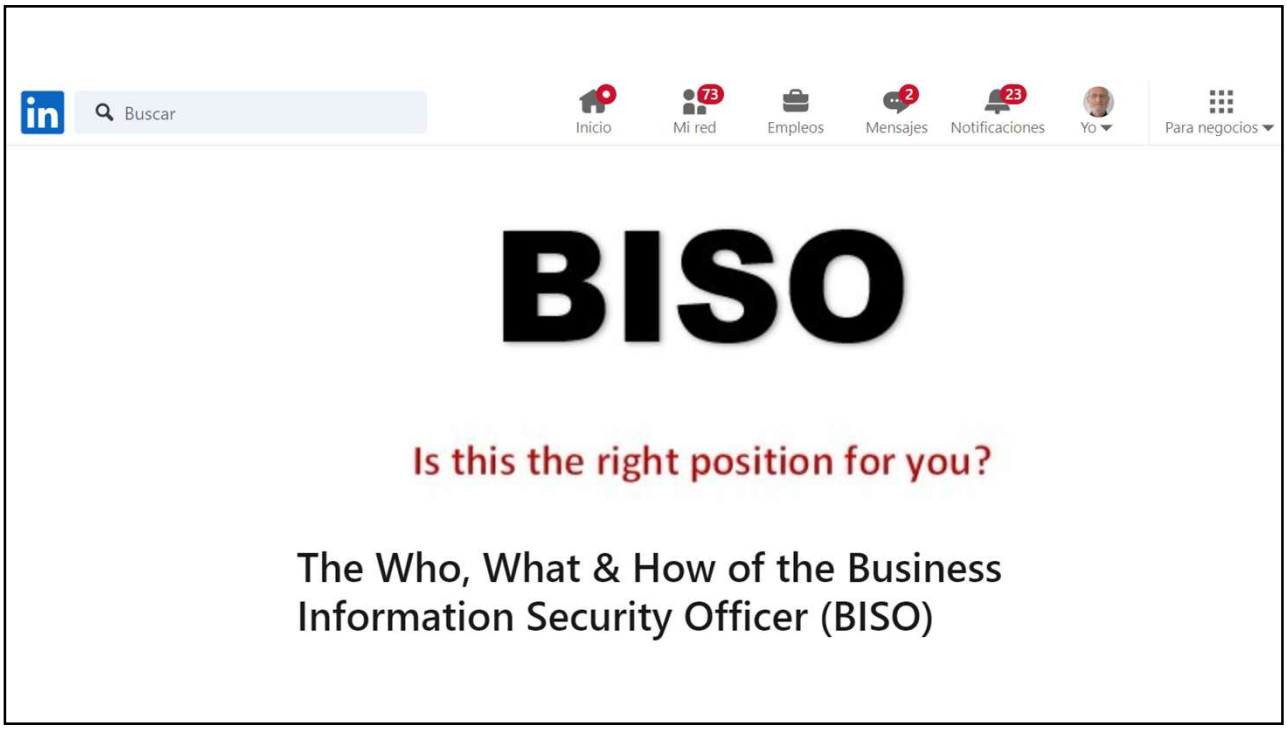
54

Los responsables de seguridad de la información empresarial (BISO) han ido ganando terreno durante años. El puesto está en auge y la demanda de BISO capacitados y con experiencia va en aumento.

Las búsquedas en Google de "Business Information Security Officer" han aumentado de unas 1.950 en enero de 2021 a 2.879 en enero de 2023.

Las publicaciones y los podcasts sobre ciberseguridad que cubren al BISO han aumentado drásticamente. Incluso hay un foro BISO en LinkedIn .

55



56