Gartner

Visión de liderazgo para 2022

Tres importantes prioridades estratégicas para los directores de seguridad y gestión del riesgo

Autor: Chris Howard, director de Investigación, Gartner

Nos vamos adentrando en 2022 conscientes del peaje que ha supuesto la pandemia mundial en términos humanos, pero sabemos también que ha significado un periodo de inflexión en el que algunas actitudes y normas de nuestra vida y nuestro trabajo han cambiado para siempre.

La convivencia con la COVID-19 ha acrecentado la conciencia social, así como la demanda de equidad con los colectivos infrarrepresentados.

Las empresas también han cambiado. Para muchas organizaciones, la pandemia ha actuado como catalizador de iniciativas de digitalización en el intento de adaptarnos a las demandas de empleados, clientes y otras partes interesadas que, tras haber optado por lo virtual forzados por las circunstancias, se erigen ahora en defensores de esta modalidad.

Los compradores B2B están satisfechos con el canal digital, sin representantes comerciales; los consumidores B2C adquieren los productos directamente en las plataformas de las redes sociales; los empleados se han dispersado físicamente y se comunican de forma asincrónica... y las infraestructuras de Tecnología de la Información deben velar por la empresa a pesar de nuestra forma actual de funcionar “cuando sea, como sea y donde sea”.

No es extraño que la sensación de desgaste empiece a notarse en ti y en todo tu equipo, y ahora es más importante que nunca priorizar el tiempo y la energía.

Desde tu cargo de responsabilidad llevas meses adaptándote a sucesivos cambios y aportando soluciones a gran velocidad. No es extraño que la sensación de desgaste empiece a notarse en ti y en todo tu equipo, y ahora es más importante que nunca priorizar el tiempo y la energía. Para ayudarte, el ebook Visión de liderazgo de Gartner ofrece una guía de primer nivel (avalada por nuestra investigación basada en datos) para que los responsables y sus equipos sepan canalizar sus esfuerzos.

Nos entusiasma anunciar que la información específica que venimos proporcionando a nuestros diferentes clientes está disponible ahora en forma de extractos para toda la comunidad empresarial. Esperamos que pueda ayudarte a centrar los debates con tu equipo, tus compañeros y otros responsables para ganar agilidad y eficacia en el diagnóstico de las prioridades y las acciones. Te será muy útil para consolidar tus planes estratégicos para 2022.

Chris Howard
Director de Investigación, Gartner

Tarea 1: redefine la función del responsable de ciberseguridad...

Actualmente, las unidades de negocio y las personas gozan de capacidad para tomar decisiones importantes sobre su destino digital y, en ocasiones, estas se traducen en malos resultados de seguridad. Los responsables de seguridad y gestión del riesgo (SRM) se sienten atrapados entre un entorno de amenazas cada vez más agresivas y la expectativa poco realista de no interferencia del director de seguridad de la información (Chief Information Security Officer, CISO) en el sistema informático de la unidad comercial. Los directores de seguridad de la información (Chief Information Security Officers, CISOs) eficaces reconocen estos malentendidos y trabajan activamente para corregirlos en 2022 y en el futuro.

Concepto de liderazgo equivocado	Redefinición
 “El CISO previene las violaciones de seguridad”.	 “El responsable facilita la gestión del riesgo”.
 “El ciberriesgo es un problema de seguridad”.	 “El ciberriesgo es un riesgo de la empresa/organización”.
 “La seguridad es un obstáculo para la velocidad”.	 “La seguridad posibilita unos productos ágiles y seguros”.

… y céntrate en generar valor

n = 129 CISO

Fuente: Encuesta sobre eficacia del CISO de Gartner de 2020

Tres desafíos y acciones para el director de seguridad y gestión del riesgo

La pérdida de control

Uno de cada cinco trabajadores se considera experto en tecnología digital desde la COVID-19. El **49 %** de los CISO “ineficaces” asumen las expectativas poco realistas de las partes interesadas.

Los consejos exigen valor

Una de cada 10 organizaciones está creando comités especializados en ciberseguridad al nivel del consejo de administración. Los consejos de administración identifican el riesgo de ciberseguridad como la segunda mayor fuente de amenazas para la empresa.

La arquitectura de malla de ciberseguridad ha evolucionado

Si los terminales, los ciudadanos digitales y los activos de TI van a ubicarse en cualquier parte, entonces los controles de ciberseguridad deberán estar a la altura.

Acciones para el responsable de SRM

Desarrolla una cultura basada en el criterio digital que se adapte a la evolución de las necesidades de talento.

Prioriza las relaciones con los clientes y aquellas dirigidas al mercado y céntrate en actividades que generen valor.

Elige tecnologías de ciberseguridad que ofrezcan altos niveles de capacidades de integración, automatización y orquestación.

Fuente: Gartner

Consigue decisores competentes en toda la organización

Todos los empleados son ahora ciudadanos de una democracia digital. El equipo de seguridad y gestión del riesgo debe dotarlos de procesos y guías que les animen a transitar por rutas seguras. Enseñar criterio digital de esta manera es la respuesta más práctica frente al riesgo que conlleva el fenómeno de la informática ciudadana.

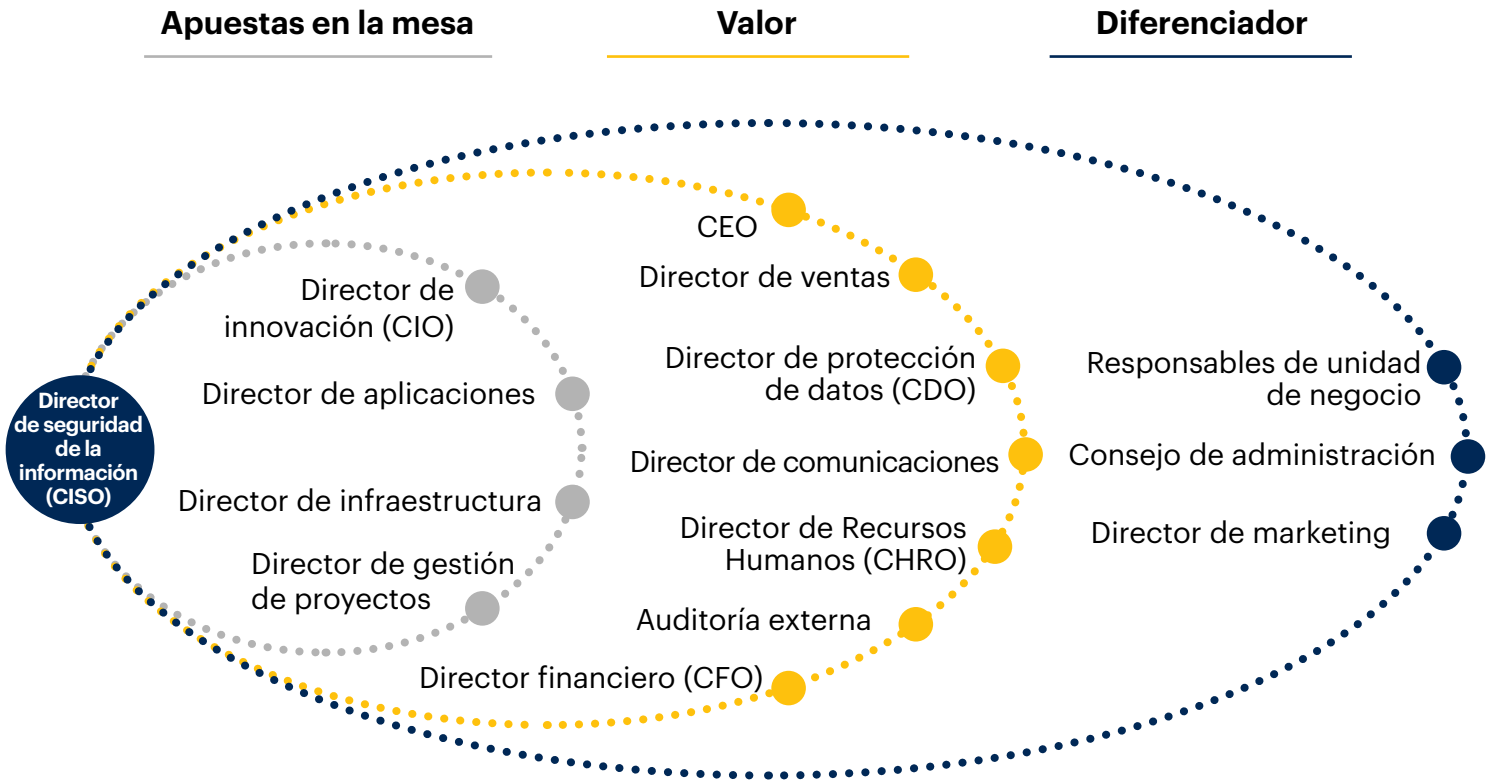
Actividades de seguridad	Fiabilidad baja	Fiabilidad media	Fiabilidad alta
Evaluación de riesgos	Conducida por seguridad	Autoaplicada, con revisión de seguridad	Autoaplicada
Control de la implementación	A cargo de seguridad	Seguridad implementa los controles de los riesgos altos	A cargo de los grupos
Solicitud de excepciones	Emitida por seguridad	Efectuada de forma independiente, en un rango de riesgos predefinido; revisión por homólogos	Efectuada de forma autónoma, en un rango de riesgos predefinido
Verificación	Revisiones de seguridad frecuentes	Revisiones solo en casos importantes	Autoverificación

A medida que los ciudadanos digitales demuestran unos niveles más altos de fiabilidad, disminuye la necesidad de actividades de gobernanza centralizada.

El objetivo último del buen criterio digital es el autoservicio.

Fuente: adaptación del caso de estudio de un cliente

Establece relaciones transformadoras fuera de TI



Resulta esencial establecer relaciones con los responsables de unidades de negocio y con los directores de ventas y de marketing, puesto que es en estas áreas donde el incremento del uso de la tecnología está llevando a tomar más decisiones y más variadas sobre el riesgo de la información. Existe una diferencia de órdenes de magnitud entre el número de CISO con un rendimiento máximo y aquellos con un rendimiento mínimo que mantienen reuniones frecuentes con estas partes interesadas de gran repercusión.

Fuente: Gartner

Prioriza de tres a cinco áreas con elevado valor comercial

Concéntrate en el número relativamente pequeño de actividades que ofrecen mayor rentabilidad marginal sobre la inversión de tiempo y recursos, y haz coincidir estas elecciones con el replanteo de tu misión.

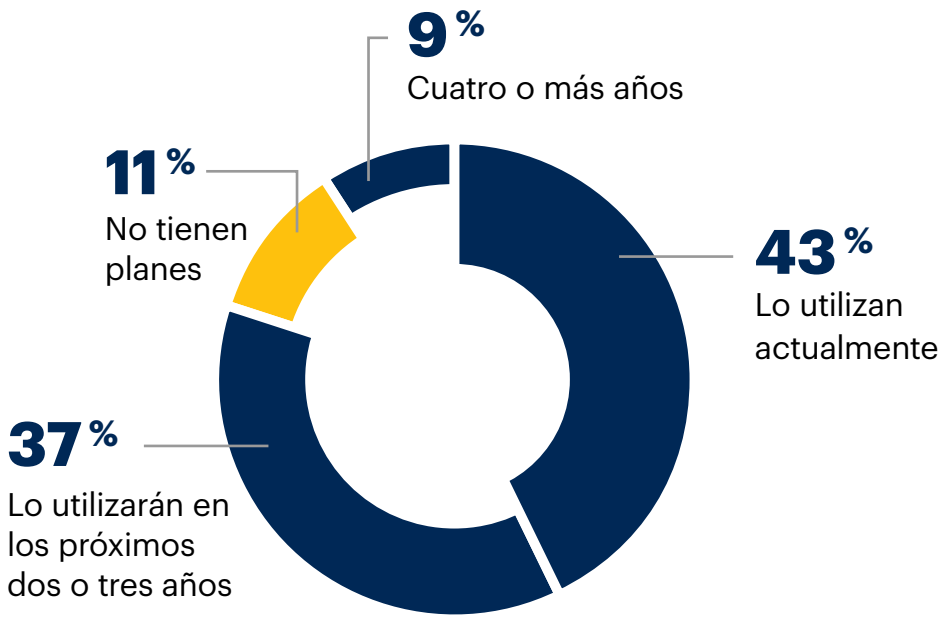
Deja claro a los clientes internos que no es tu función resolver todos sus problemas, pero que vas a identificar y abordar los más significativos.

Valor comercial	Impacto en los ingresos	Rentabilidad	Reducción del riesgo
Los 3-5 principales servicios, aplicaciones o iniciativas de TI que repercuten en el valor	Sistemas transaccionales	Productividad	Tiempo de inactividad operativa
	Atención al cliente	Eficiencia	Deterioro de reputación
	Carro de la compra	Optimización de plantilla	Cumplimiento normativo y auditoría
	Sistemas CRM	Optimización de activos	Seguridad operativa y de datos
	Entrada de pedidos	Uniformidad del nivel de servicio	Reparación de vulnerabilidades
	Atención al cliente		

Prioriza entre tres y cinco elementos bajo tu responsabilidad y control que tengan más impacto en las prioridades del valor comercial.

Fuente: Gartner

Utiliza soluciones ofrecidas desde la nube por su facilidad de redimensionarse, integrarse y automatizarse



El 80 % de las organizaciones encuestadas ya tienen o prevén tener un producto de ciberseguridad como servicio en los próximos dos o tres años.

n = 396, todas las respuestas, excluidas "no sabe, no contesta"
P. ¿Alguno de los productos de seguridad de la información de tu organización se ofrece "como servicio"?
Fuente: Encuesta sobre tendencias en la adopción de soluciones de seguridad e IAM de Gartner de 2020

Información objetiva y procesable

Descubre estos recursos y herramientas complementarios para responsables de seguridad:

Herramienta

IT Score de Gartner

Lleva a cabo un análisis comparativo de los procesos y actividades esenciales para potenciar tu departamento.

Más información

Herramienta

Gartner BuySmart™

Reduce costes, evita trampas y compra tecnología con confianza.

Más información

Hoja de ruta

Hoja de ruta para la madurez de la seguridad de la información

Crea un programa maduro para reducir con eficacia el riesgo de la ciberseguridad.

Descargar ahora

Ebook

Tres pasos para que los empleados dejen de morder el ciberanzuelo

Conciencia a tus empleados del riesgo digital para gestionar los ciberataques.

Descargar ahora

¿Ya eres cliente?
Accede a aún más recursos en el portal de clientes. Iniciar sesión

Más.

Obtén información útil y objetiva para satisfacer tus principales prioridades. Nuestras herramientas y nuestra experiencia permiten tomar decisiones más rápidas e inteligentes y mejorar el rendimiento. Contacta con nosotros para hacerte cliente:

EE. UU.: +1 855 811 7593

Internacional: +44 (0) 3330 607 044

Hazte cliente

Más información sobre Gartner para responsables de Tecnología de la Información en
gartner.es/es/tecnologia-de-la-informacion

Recibe las últimas novedades

Gartner®