Raconteur

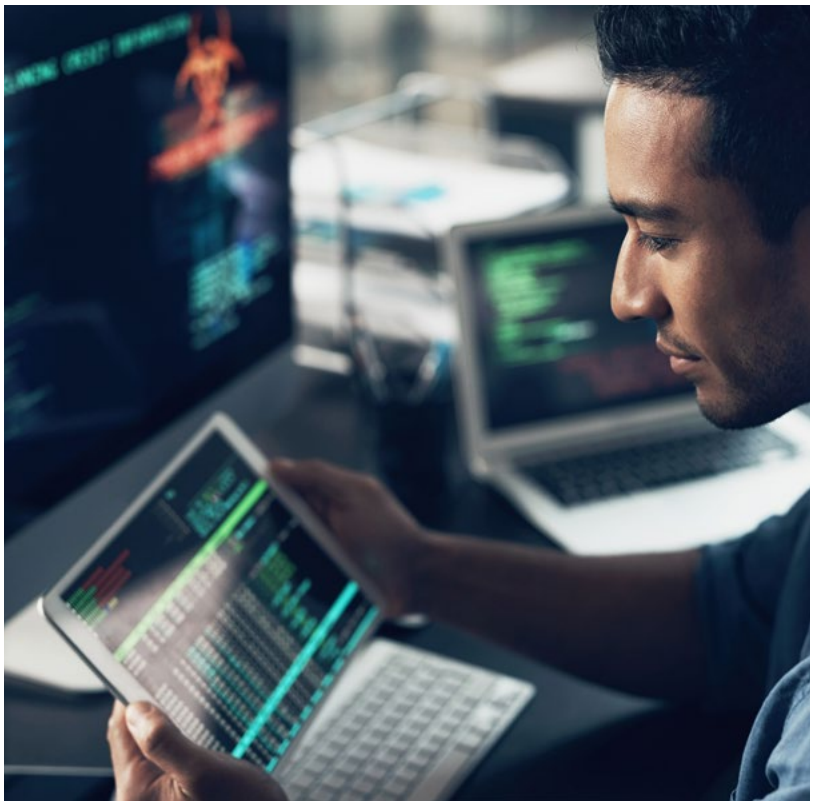
Éxito probado: por qué los líderes deben dominar el cumplimiento digital

digicert®

Contenidos

Lista de comprobación para transformar el cumplimiento normativo: cinco jugadas clave para lograr la excelencia en seguridad a largo plazo

A medida que las normativas en materia de ciberseguridad redefinen el riesgo empresarial, los líderes deben aprender a convertir las crecientes obligaciones en materia de seguridad en una ventaja comercial. Siga los cinco pasos de esta hoja de ruta para alcanzar la excelencia en términos de cumplimiento.



Con la aparición de normativas en materia de ciberseguridad que están transformando el panorama empresarial global y el auge de los nuevos marcos de cumplimiento, las empresas están sometidas a una presión sin precedentes que las está obligando a transformar su estrategia de seguridad y pasar de la defensa reactiva a la ventaja estratégica.

Los líderes se enfrentan a un reto complejo: ante unos ciberataques cada vez más sofisticados, el cumplimiento normativo ha dejado de ser una tarea administrativa y se ha convertido en un factor diferenciador crítico para el negocio. La pregunta ya no es si las empresas deben actuar o no, sino la rapidez con la que son capaces de adaptarse.

Además de evitar infracciones e interrupciones en los sistemas, las empresas que gestionan su seguridad digital de manera proactiva establecen operaciones resilientes que pueden adaptarse rápidamente a las nuevas normativas como el Reglamento DORA. Ante el aumento de las amenazas digitales, garantizar un cumplimiento normativo sólido ha pasado a ser un

elemento indispensable de unas buenas prácticas empresariales.

Además, se avecinan cambios en los requisitos de cumplimiento normativo. El Reglamento de Resiliencia Operativa Digital (DORA) comenzó a aplicarse en su totalidad el 17 de enero de 2025 y está transformando el sector de los servicios financieros de la UE y sus proveedores de TIC.

Al mismo tiempo, se espera que el proyecto de ley de resiliencia y seguridad cibernéticas (CS&R) del Reino Unido se presente en el parlamento este año (2025), por lo que la postura del Reino Unido estaría alineada con la Directiva NIS2 de 2022 de la UE. Ambas iniciativas establecen claramente qué responsabilidades tienen los directivos a la hora de supervisar la gestión de los riesgos de ciberseguridad.

En palabras de Patrick Beckman Lapré, director y especialista en confianza digital de DigiCert: «Para lograr la excelencia en seguridad, es fundamental que la empresa sea lo más resiliente posible. Partiendo de la base de que es imposible controlarlo todo, podemos prepararnos para saber cómo minimizar las consecuencias que puede tener un ciberataque tanto para los clientes como para la empresa».

Los líderes globales de gestión de riesgos y seguridad necesitan un enfoque estructurado para abordar un panorama de seguridad que no deja de cambiar. Sin embargo, para convertir los requisitos complejos y duplicados de las diferentes reglas en estrategias útiles, es necesario establecer una hoja de ruta clara y transformar el modelo de negocio digital.

Estos son los cinco pasos básicos que cualquier líder debe seguir para que los requisitos regulatorios dejen de ser una carga y se conviertan en una ventaja competitiva y, al mismo tiempo, preparar las operaciones para futuras auditorías.

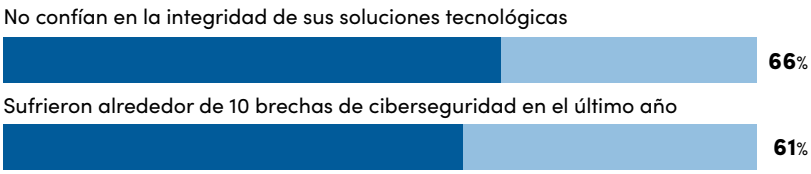
01 Entienda su inventario de activos digitales

Saber qué activos digitales forman parte del entorno es fundamental para garantizar una ciberseguridad eficaz. Si desean recopilar todas las piezas del rompecabezas y crear una radiografía detallada de su entorno, los líderes pueden recurrir a la detección de activos automatizada, la supervisión continua y funciones que les permitan obtener una visibilidad clara de las conexiones de terceros.

«Los activos pueden incluir PC, servidores, aplicaciones, certificados digitales, reglas de cortafuegos, empleados o servicios externos.

A medida que las ciberamenazas y los requisitos regulatorios evolucionan, las empresas deben adoptar estrategias sólidas para defenderse con eficacia

Porcentaje de líderes a los que les preocupa la ciberseguridad



Deloitte 2024

Si no se cuenta con un inventario completo de los activos, nunca se sabrá con certeza si los controles de ciberseguridad están protegiendo todo lo que deberían», explica Simon Lawrence, director y cofundador de i-confidential, una consultora de ciberseguridad y riesgo.

«Por ejemplo, si un servidor no está registrado en la base de datos de gestión de la configuración (CMDB), el escáner de vulnerabilidades no sabrá de su existencia, por lo que es posible que algunas vulnerabilidades críticas pasen desapercibidas», añade Lawrence.

Al elaborar el esquema del ecosistema de TIC, es necesario agrupar los activos y relacionarlos con los sistemas de la información que los utilizan, ya que esto permite establecer un orden de prioridad en función de su criticidad para el negocio. Esta priorización tiene en cuenta el impacto empresarial que podría tener un ataque a un sistema de la información, un escenario que pone en peligro tanto la reputación empresarial como la personal.

«Contar con una vista que indique el nivel de criticidad es fundamental, ya que es una forma de evitar que las empresas no inviertan lo suficiente en los sistemas más críticos e inviertan demasiado en sistemas de menor riesgo, lo que dejaría los sistemas críticos expuestos a riesgos cibernéticos significativos», destaca Lawrence.

Y añade: «Esto también puede mermar la eficacia de la seguridad operativa. Por ejemplo, si una empresa está siendo atacada, los encargados de la respuesta a incidentes no dispondrán de la información que necesitan para centrarse en los sistemas más críticos».

02 Perfeccione la arquitectura del control del acceso y los permisos

La arquitectura del control del acceso requiere establecer permisos detallados para definir con precisión los recursos a los que pueden acceder los usuarios, así como las acciones que pueden realizar. Para abordar esta tarea, puede recurrir a la gestión del acceso basado en roles (RBAM), con la que los permisos se asignan a roles específicos, en lugar de a usuarios individuales, lo que simplifica la administración y reduce los riesgos de seguridad.

Un control del acceso eficaz se basa en una verificación rigurosa de la identidad. Para ello, verificación rigurosa de la identidad. Para ello, los líderes pueden utilizar certificados digitales para los usuarios, los dispositivos y las cargas de trabajo. Estos certificados sirven de credenciales de confianza para autenticar las identidades en toda la infraestructura empresarial.

Cuando una empresa implementa la verificación de la identidad basada en certificados, el seguimiento automatizado del ciclo de vida de los certificados se convierte en una herramienta crucial para gestionar estas identidades digitales desde la emisión del certificado hasta su renovación y revocación. Gracias a la automatización, podrá asegurarse de que los certificados no caducan de forma imprevista y de que se revocan inmediatamente cuando ya no son necesarios.

El sistema mantiene registros de auditoría detallados de todas las interacciones del sistema, con el objetivo de ofrecer visibilidad sobre quién accede a qué recursos y cuándo lo hace. Esta información es fundamental para supervisar la seguridad y cumplir los requisitos normativos.

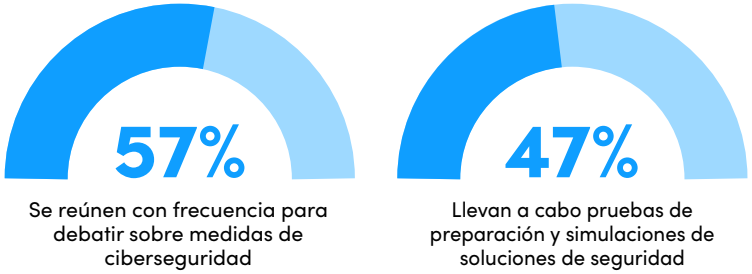
La arquitectura debe ser compatible con las actualizaciones dinámicas para poder responder a los cambios empresariales sin poner en riesgo la integridad de la seguridad. Para ello, es necesario contar con flujos de trabajo automatizados para las solicitudes de acceso, las aprobaciones y las revocaciones, lo que garantiza que todas las actualizaciones se realicen a tiempo y, al mismo tiempo, evita el acceso no autorizado.

Las actualizaciones continuas y una definición clara de las responsabilidades del equipo son clave para lograr un buen control del acceso. Sin un proceso eficaz que automatice las tareas y contemple el factor humano, el control del acceso puede convertirse en un riesgo empresarial, en lugar de en un activo para mejorar la seguridad.

La gestión del control del acceso no es una medida puntual, sino un proceso que debe supervisarse y controlarse de forma continua teniendo en cuenta diversos factores, por ejemplo, las nuevas contrataciones o los empleados que abandonan la empresa y que podrían llevarse datos con ellos.

Los líderes deben contar con sistemas de seguridad resilientes que estén preparados para superar con facilidad cualquier auditoría de cumplimiento

Porcentaje de líderes que afirman tener un equipo directivo que se muestra proactivo a la hora de tomar medidas de ciberseguridad



Deloitte 2024

03 Establezca y desarrolle marcos de incidentes precisos

La respuesta a incidentes de ciberseguridad concierne tanto al equipo directivo como a los encargados de las operaciones de seguridad, y ambos desempeñan una función esencial en ella. «La eficiencia y eficacia de la respuesta inicial determinan la gravedad de las consecuencias operativas, reputacionales o financieras que pueda tener un ataque», apunta Katherine Kearns, responsable de Servicios Proactivos para la región EMEA de la consultora S-RM.

Mitigar estos retos exige dominar desde el principio la colaboración entre los responsables de la toma de decisiones estratégicas y los técnicos de respuesta.

> **Si no se cuenta con un inventario completo de los activos, nunca se sabrá con certeza si los controles de ciberseguridad están protegiendo todo lo que deberían.**

Kearns opina que realizar ejercicios de respuesta de forma periódica ofrece una oportunidad para poner en práctica competencias críticas y ver cómo funcionan las responsabilidades en un entorno de pruebas seguro. Después, los equipos pueden tener en cuenta todo lo aprendido en el ejercicio para mejorar sus planes de respuesta a incidentes de ciberseguridad.

«Un ejercicio de respuesta eficaz pone a prueba capacidades clave como la continuidad empresarial, la gestión de los recursos, la recuperación de los sistemas, la gestión de las amenazas, las comunicaciones y el cumplimiento normativo», añade Kearns.

04 Implemente controles de cumplimiento automatizados

Al sustituir la supervisión manual por la garantía que brinda la automatización, los líderes tienen la certeza de que están preparados para superar cualquier auditoría, además de poder demostrar a sus socios que su empresa gestiona el riesgo de manera eficaz en todo momento.

Aún más importante es medir la eficacia de los controles de ciberseguridad para poder corregir cualquier carencia o punto débil en tiempo real y garantizar la seguridad y la conformidad de las operaciones empresariales de manera continuada.

Aunque, por lo general, las empresas implementan tecnologías de seguridad, no suelen invertir mucho tiempo en realizar controles para comprobar que dichas tecnologías sigan siendo eficaces, lo que abre la puerta a que los ciberataques burlen las defensas de la empresa.

«Los controles suelen medirse mediante pruebas. Normalmente, estas actividades toman una muestra de los activos para determinar si se están aplicando los controles pertinentes. Por lo general, las pruebas se hacen una o dos veces al año y, aunque este enfoque puede ofrecer información sobre la eficacia y la conformidad del control, también tiene limitaciones», opina Lawrence.

Y añade: «Por ejemplo, estas pruebas no analizan todos los activos, por lo que, si existiese alguna carencia relacionada con el control en los activos que no se han incluido en la muestra, esta no se detectaría. Las pruebas de control también deben hacerse con cierta frecuencia, ya que, de lo contrario, las empresas quedan expuestas a las vulnerabilidades de seguridad hasta que se ejecuta la siguiente prueba, lo que puede ser hasta un año después. Por último, las pruebas de control son caras y se hacen de forma manual, por lo que las empresas medianas y de mayor tamaño deberán tener equipos que se dediquen en exclusiva a esta tarea si quieren tener una cobertura de pruebas adecuada».

Para solucionar estos retos, las empresas pueden recurrir a la supervisión continua de controles (CCM). Con la CCM, pueden hacer pruebas de control para detectar puntos débiles en todos los activos del entorno de forma automatizada, además de elegir si quieren realizar los controles semanal o diariamente.

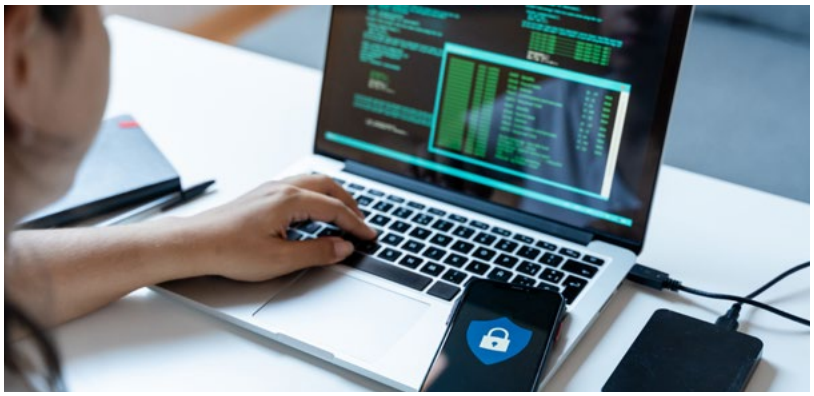
05 Adapte su estrategia de ciberseguridad a los requisitos a nivel global

Las empresas que operan a nivel global deben atender a múltiples requisitos de ciberseguridad en distintas jurisdicciones que, por si fuera poco, no dejan de evolucionar. Para ello, es necesario que entiendan las particularidades de cada región en lo que respecta a la elaboración de informes y las obligaciones complejas que establecen las normativas.

Implementar marcos escalables, como la norma ISO 27001 o el CSF del NIST, puede ayudarle a optimizar los procesos de cumplimiento normativo en las distintas jurisdicciones de manera significativa.

También es muy importante que cree puestos dedicados a hacer un seguimiento de los cambios normativos y las amenazas emergentes mediante evaluaciones continuas.

Los equipos regionales suelen enfrentarse a desafíos parecidos, por lo que la coordinación entre departamentos es fundamental para evitar tener procesos de cumplimiento normativo fragmentados o duplicados.



DORA: una nueva oportunidad para aprovechar el potencial de las soluciones de seguridad

Los procesos de cumplimiento normativo manuales dejan vulnerables a las empresas, por lo que sus líderes deben priorizar la adopción de soluciones de seguridad automatizadas.

A pesar del aumento de los riesgos en los entornos digitales, muchas empresas siguen utilizando procesos de cumplimiento normativo manuales en lugar de apostar por sistemas de seguridad automatizados, lo que las deja vulnerables a errores que les pueden salir muy caros, al agotamiento de los recursos y a posibles incumplimientos que amenazan la continuidad del negocio.

Llevar un seguimiento manual de los cambios normativos puede aumentar el riesgo de incumplimiento, lo que podría acarrear sanciones y, en última instancia, la pérdida de la confianza digital y daños irreparables a la reputación de la empresa.

Con la introducción del Reglamento de Resiliencia Operativa Digital (DORA) y la previsión de Deloitte de que el 57 % de los líderes aumentarán el presupuesto de ciberseguridad en los próximos 12-24 meses, establecer una estrategia de cumplimiento normativo es una prioridad cada vez más apremiante en la agenda de los directivos.

Gestión del coste-eficacia

Patrick Beckman Lapré, director y especialista en confianza digital de DigiCert –un proveedor global de soluciones de PKI y gestión del ciclo de vida de los certificados para empresas– explica que la transformación digital contribuye a reducir drásticamente el trabajo manual y los costes asociados, lo que permite a los directivos centrarse en desarrollar estrategias que les otorguen una ventaja competitiva.

«Los costes derivados de los errores, las ineficacias y las sanciones pueden superar con creces los ahorros que se cree obtener con los métodos manuales. Con estos métodos, estamos limitados a responder una vez que ya ha sucedido algo, ya que no ofrecen ningún tipo de información que permita prever los posibles daños».

Explica también que la agilidad criptográfica –la capacidad de una empresa de cambiar rápidamente de un método de seguridad y cifrado de datos a otro– es fundamental para lograr una ventaja competitiva.

«La criptografía protege la información convirtiéndola a formatos codificados seguros. En la situación actual, las empresas deben pasar de la reactividad a la proactividad. Para ello, necesitan un inventario completo de sus herramientas criptográficas y la capacidad de sustituir rápidamente las soluciones vulnerables antes de que sean explotadas», relata Lapré.

Y añade: «Los líderes deben ser capaces de anticipar las situaciones que pudieran darse y, de producirse un problema, necesitan contar con los controles y los procesos necesarios para minimizar las interrupciones».

La seguridad y el cumplimiento no son acciones puntuales, sino un compromiso permanente. Las plataformas de automatización ofrecen supervisión en tiempo real para alertar a las empresas de los posibles riesgos y activar respuestas proactivas mucho más rápido.

Los sistemas de gestión de certificados digitales responden rápidamente a los cambios normativos y a la introducción de normas nuevas como el reglamento DORA para garantizar que nada se pase por alto y que las empresas no se enfrenten a multas ni a otras consecuencias derivadas de las infracciones normativas.

Estos sistemas supervisan y gestionan los certificados de seguridad digitales automáticamente, lo que ayuda a los líderes a detectar y corregir problemas de seguridad antes de que ocasionen interrupciones(que es uno de los requisitos clave de las nuevas normas de seguridad que establece el reglamento DORA).

Una transformación digital que empieza desde arriba

Las ventajas para la empresa de adoptar tecnologías de cumplimiento digital están claras: desde mejoras de la eficiencia hasta un proceso de toma de decisiones más rápido y basado en informaciónobjetiva. Sin embargo, para que estas iniciativas lleguen a buen puerto, es necesario contar con el compromiso de la cúpula.

«Para muchas empresas, la digitalización es una cuestión puramente técnica –asegura Lapré–. Muchas veces, nombran a un CISO sin pararse a pensar demasiado en lo que significa realmente la ciberseguridad. Sin embargo, los directivos y ejecutivos sénior deben implicarse y ser plenamente conscientes de cuanto está sucediendo».

«Son ellos quienes deciden dónde se gasta el dinero. Cuando se les pide financiación para algo que no saben con certeza cuándo sucederá, suelen inclinarse más por invertir en proyectos que saben que generarán valor en tres meses. La alta dirección debe entender que no invertir en cumplimiento en materia de ciberseguridad digital puede tener consecuencias nefastas para el negocio, porque perdería su confianza digital», apunta Lapré.

Una confianza digital reinventada

Mantener un cumplimiento digital sólido ayuda a obtener ventajas empresariales clave, como la detección temprana de violaciones de datos, la protección de activos de IP valiosos y la mejora de la confianza del cliente.

Más allá de proteger la propiedad intelectual y los datos personales, estas medidas transforman las inversiones en seguridad en fidelidad del cliente e iniciativas que generan valor para la empresa a largo plazo.

> **Con una estrategia de cumplimiento digital, las empresas obtienen una protección mejorada y, por consiguiente, una mayor confianza digital.**

«Lo que hace la normativa es obligar a las empresas a cuidar a sus clientes –señala Lapré–. Da igual que se trate de un proveedor de servicios o de una institución financiera: todas deben mitigar los riesgos y garantizar que las transacciones empresariales por internet sean más seguras y de confianza».

«Hoy en día, con todo esto de la IA, sabemos que se ha vuelto mucho más difícil determinar si algo es real o falso, lo que podría hacer mucho daño a los negocios», explica Lapré.

Y añade: «Elegir un socio de soluciones digitales estratégico garantiza la solidez de los procesos y de los controles y, además, amplía las funciones de seguridad sin necesidad de contratar más personal».

Superar los nuevos desafíos

«Cada auditoría es una nueva oportunidad de mejora. En DigiCert, realizamos 26 auditorías anuales que abarcan todos los aspectos de nuestro negocio y nuestra presencia internacional. Esto es una garantía de confianza, porque sabes que la empresa con la que vas a trabajar cuenta con los procesos necesarios para mitigar el riesgo al máximo», comenta Lapré.

Aunque es imposible evitar por completo todos los riesgos cibernéticos, seguir una estrategia de ciberseguridad robusta contribuye a evitar pérdidas económicas y a garantizar que la reputación de la empresa permanezca intacta.

«Las amenazas cibernéticas son cada vez más inteligentes y las normativas en torno al cumplimiento, cada vez más complejas y engorrosas. Con una estrategia de cumplimiento digital, las empresas obtienen una protección mejorada y, por consiguiente, una mayor confianza digital».

«Ignorar la necesidad de sustituir los procesos manuales por una estrategia digital es un riesgo grandísimo que ninguna empresa se puede permitir correr», sentencia Lapré.

Por qué la eficacia de su estrategia de cumplimiento normativo está en manos de su equipo

Una estrategia de ciberseguridad sólida puede ayudar a proteger el futuro de las empresas, pero su eficacia depende de que los equipos estén formados en cumplimiento normativo y entiendan el papel que tienen en la confianza digital.

A pesar de las cuantiosas inversiones que se hacen en herramientas de cumplimiento digital, los errores humanos siguen siendo el origen de muchas de las violaciones de seguridad a nivel mundial. Según Verizon, en el 68 % de las infracciones que se registraron en 2024 intervino el factor humano.

Este desequilibrio entre las funciones tecnológicas y las habilidades de los empleados pone de relieve una verdad innegable: la eficacia de la ciberseguridad no depende solo de que las empresas implementen las herramientas adecuadas, sino también de que los equipos sepan cómo utilizarlas.

Los directivos deben entender que es igualmente necesario invertir en formación sobre cumplimiento normativo para los empleados como en soluciones tecnológicas de defensa. Este enfoque equilibrado garantiza que los equipos sean capaces de implementar las medidas de seguridad de forma eficaz y de mantenerlas con el paso del tiempo, lo que da lugar

a una estrategia de defensa sólida frente a las ciberamenazas en evolución.

Si quiere anticiparse y sobreponerse a estos desafíos digitales complejos, tenga esta máxima siempre presente: la eficacia de su estrategia de ciberseguridad es, ni más ni menos, la del equipo que la implementa.

Hacer énfasis en la responsabilidad colectiva

El cumplimiento en materia de ciberseguridad es una responsabilidad colectiva que traspasa las cuatro paredes del departamento de TI y se extiende a toda la empresa. A medida que los requisitos regulatorios ganan complejidad, las empresas deben formar equipos de cumplimiento normativo más diversos que abarquen un amplio abanico de competencias.

Para cumplir las normativas sobre ciberseguridad modernas, es necesario contar con la visión de todos los niveles de la empresa, por lo que la responsabilidad digital ya no es solo cosa de los equipos de TI. Cualquier miembro del equipo puede aportar competencias y puntos de vista esenciales para garantizar un cumplimiento normativo eficaz.

«El papel que tienen los diferentes miembros de un equipo en distintos niveles suele pasarse por alto y, sin embargo, ha demostrado ser crucial en un momento en el que la complejidad de las normativas es cada vez mayor –señala el Dr. Tommaso De Zan, responsable sénior de Gobernanza de Datos de Access Partnership, una consultora de políticas tecnológicas–. Los líderes deben formar equipos completos que estén preparados para adoptar procesos de seguridad sólidos y tengan una actitud proactiva, ya que constituyen un valor añadido».

Estar al día de los cambios en las normativas es un reto constante que pone a prueba hasta a los equipos de cumplimiento más organizados. Por ese motivo, priorizar la mejora de las competencias al ritmo al que cambian los riesgos es un elemento clave que los negocios deben tener en cuenta.

Cada día surgen requisitos nuevos en los distintos sectores y regiones, lo que da lugar a una compleja trama de reglas que los equipos deben supervisar, interpretar e implementar. Para abordar esta tarea con éxito, las empresas no pueden depender únicamente de la supervisión de los equipos de cumplimiento normativo, sino que deben contar con la implicación real de todos los departamentos para mantener los estándares y adaptarse a los nuevos requisitos.

Forjar una cultura basada en el cumplimiento normativo

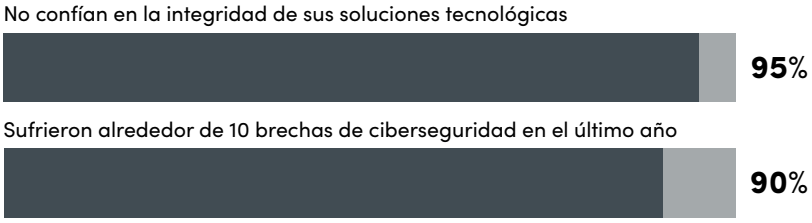
El cumplimiento normativo ha dejado de ser una medida puntual que se implementa para cumplir con un requisito y se ha convertido en un elemento esencial que los equipos deben integrar y seguir desarrollando. Para que sea eficaz, el cumplimiento debe convertirse en una responsabilidad compartida, y los equipos tienen que dejar de ver la seguridad como un requisito más y empezar a incorporarla a sus flujos de trabajo.

Esto ayudará a que las empresas cumplan los requisitos de seguridad necesarios para aprovechar las ventajas de la digitalización y establezcan una concienciación sobre la seguridad a largo plazo.

Casey Ellis, consultor que presta servicios a agencias de seguridad nacional de EE. UU., el Reino Unido y Australia, defiende que, para que el cumplimiento normativo sea realmente valioso, este debe darse de forma natural e incorporarse sistemáticamente a unas operaciones empresariales sólidas.

Para garantizar el éxito a largo plazo, los líderes tienen que dejar de ver el cumplimiento como un mero trámite y forjar una cultura adaptativa basada en el aprendizaje

Porcentaje de líderes que han adoptado un enfoque basado en el aprendizaje sobre cumplimiento en toda la empresa



Deloitte 2024

> **Los líderes deben formar equipos completos que estén preparados para adoptar procesos de seguridad sólidos y tengan una actitud proactiva, ya que constituyen un valor añadido.**

«Cuando se implementa de la forma adecuada, el cumplimiento normativo es eficaz y no interfiere en el desarrollo del negocio –explica Ellis–. El objetivo final es que el cumplimiento sea una motivación intrínseca, en lugar de una fuerza extrínseca. Para lograrlo, pueden llevarse a cabo diferentes acciones, como lanzar una campaña de concienciación en materia de seguridad en todos los departamentos, reconocer los logros y buscar formas de convertir la excelencia en seguridad en un factor diferenciador en el mercado. Todas estas herramientas ayudan a situar el cumplimiento normativo en el centro de la cultura corporativa».

Mejorar y actualizar las competencias

Los cambios en las preocupaciones relativas a la privacidad y la evolución de las amenazas digitales complican aún más el cumplimiento normativo. Los equipos deben entender cómo afectan los nuevos riesgos a sus obligaciones normativas, por lo que deben formarse y adquirir nuevas competencias continuamente.

Sin embargo, muchas empresas tienen dificultades para ofrecer una formación sobre cumplimiento adecuada y actualizada a sus empleados debido a limitaciones presupuestarias y de personal.

«Garantizar un presupuesto aceptable para ofrecer programas de cumplimiento normativo de alta calidad puede entrar en conflicto con otras prioridades del negocio, y crear marcos de cumplimiento normativo aplicables en distintas jurisdicciones no hace sino añadir más complejidad al asunto», reconoce De Zan.

Y añade: «Sin embargo, es probable que lo más complicado sea lograr una adopción generalizada en toda la empresa, ya que esto implica cambiar el comportamiento de los trabajadores y propiciar una cultura de cumplimiento que cale en los empleados de todos los niveles».

Además de ofrecer formación, las empresas deben asegurarse de que los empleados retienen y aplican los conocimientos sobre seguridad que han adquirido. Para ello, pueden hacer evaluaciones y ofrecer programas de refuerzo de forma continuada, ya que las acciones puntuales no son suficientes.

Para garantizar el cumplimiento normativo, las empresas deben adoptar un enfoque integral que permita que los empleados se conviertan en guardianes digitales. La forma más eficaz de hacerlo es integrando el cumplimiento normativo en los flujos de trabajo diarios, con el objetivo de crear un entendimiento común que vaya más allá de la formación tradicional.

«Es una tendencia que no solo observamos en empresas, sino también en organismos de supervisión y auditores externos –comenta Lapré–. Por ejemplo, en los Países Bajos, el tamaño de los equipos responsables de supervisar las normativas se ha duplicado o incluso triplicado en los últimos dos o tres años, y esto es algo que seguirá acentuándose, ya que la tendencia es que se sigan publicando más normativas y se sigan fijando nuevos estándares».

Y añade: «Las empresas necesitarán contratar empleados con las competencias necesarias para revisar, implementar y controlar las nuevas normativas, por lo que se espera un aumento de la demanda de talento en esas áreas».

Reinventar las mejores prácticas

Capacitar a los equipos para que se adapten rápidamente a los cambios regulatorios sin renunciar a la eficiencia operativa ni la creatividad es un reto continuo, pues existe la posibilidad de que los equipos se sientan coartados por los requisitos normativos, lo que se traduce en una mayor reticencia o retrasos a la hora de implementar actualizaciones.

Según Ellis: «Lo ideal sería que las empresas aplicasen la seguridad basándose en sus propios modelos de amenazas y riesgos. Sin embargo, como estos modelos son dinámicos y muchas veces las empresas no los entienden bien, el cumplimiento normativo juega una función de vital importancia para reducir los errores humanos, ofrecer orientación sobre mejores prácticas y compensar esas carencias».

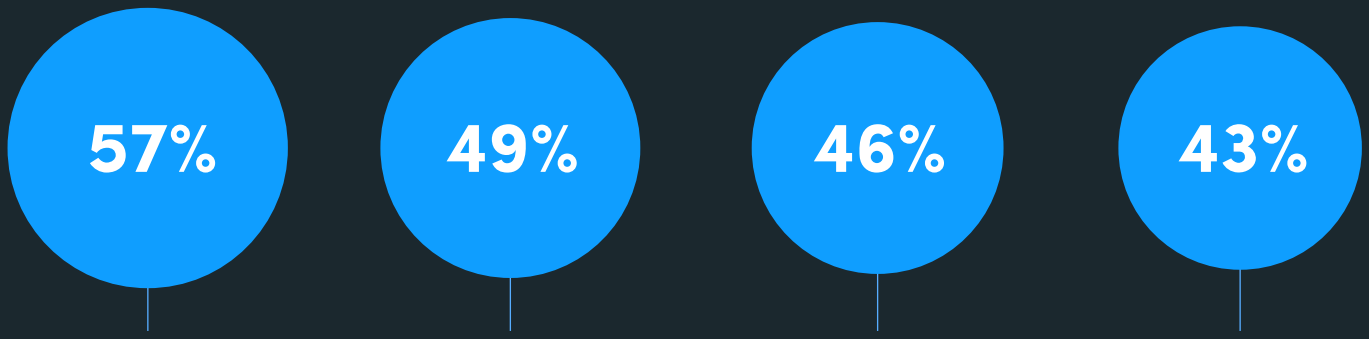
«La selección cuidada de proveedores, la priorización basada en los puntos fuertes de la empresa y los esfuerzos para alinear los objetivos de las unidades de negocio encargadas de los ingresos y la generación de productos constituyen tanto un reto como una oportunidad para lograr la excelencia y diferenciarse», sentencia Ellis. ●

Una nueva era regulatoria: el futuro del cumplimiento cibernético

De los reglamentos sobre cumplimiento a los requisitos de ciberseguridad: ¿cómo pueden los líderes hacer frente a las crecientes exigencias de las normativas, transformar los marcos de riesgo y lograr una gobernanza sólida?

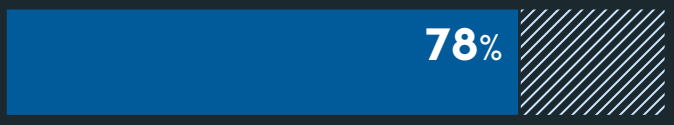
Dar una respuesta eficaz a los cambios en los marcos y la regulación cibernética puede ayudar a los directivos a mantener la ventaja competitiva de sus empresas

Porcentaje de líderes que opinan que el cumplimiento eficaz ofrece una ventaja competitiva

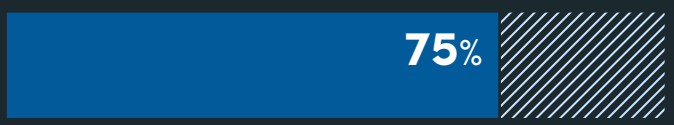


A medida que aumentan las exigencias en materia de cumplimiento, la ciberseguridad ha pasado de ser un asunto exclusivo de TI a una cuestión capital para la junta directiva

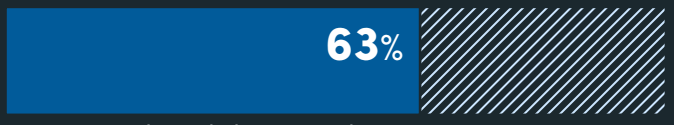
Porcentaje de grandes empresas en las que la ciberseguridad es una prioridad en la agenda de los directivos



Envían actualizaciones trimestrales sobre ciberseguridad a los directivos sénior



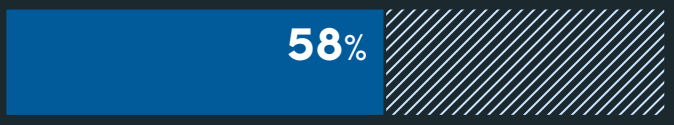
Tratan la ciberseguridad como una prioridad de primer nivel para los directivos sénior



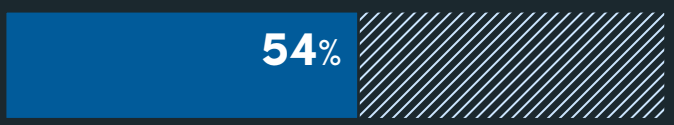
Tienen miembros de la junta y directivos sénior cuyas funciones y responsabilidades incluyen la ciberseguridad de manera explícita

Los líderes que quieran blindar sus operaciones de cara al futuro deben invertir tanto en herramientas de seguridad como en campañas de concienciación sobre el cumplimiento para los empleados

Porcentaje de directivos que han establecido prioridades relativas a la seguridad para los próximos dos años



Mejorar la concienciación de los empleados en materia de ciberseguridad



Mejorar la protección de la información

Consolidar y simplificar las soluciones y herramientas de seguridad

digicert®

DigiCert es un líder global en **confianza digital**. Gracias a él, tanto los usuarios individuales como las empresas pueden utilizar Internet con la tranquilidad de saber que su **presencia en el mundo digital** está protegida. La plataforma de confianza digital, **DigiCert® ONE**, protege los sitios web, los accesos y comunicaciones empresariales, el software, las identidades, el contenido y los dispositivos para que las empresas respondan a toda una gama de necesidades en materia de confianza pública y privada con una visibilidad y un control centralizados. Su galardonado software y su liderazgo en el sector de los estándares, la asistencia y las operaciones convierten a DigiCert en el proveedor de confianza digital al que recurren las grandes empresas de todo el mundo.

Para obtener más información, visite **www.digicert.com/es** o siga a **@digicert**

Raconteur

Editor: Larnie Hur
Design: James Lampard, Samuele Motta
Contributors: Alison Coleman

Although this publication is funded through advertising and sponsorship,all editorial is without bias and sponsored features are clearly labelled.
For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net