Desmitificando el cumplimiento normativo

para responsables de seguridad y de tomar decisiones de TI

Introducción

La elaboración de marcos normativos y normas ha surgido de la necesidad de hacer frente a los retos y requisitos de la gestión de la tecnología de la información y la salvaguardia de los datos. Estos marcos y estándares no solo han evolucionado con el tiempo, sino que han sido moldeados por los avances tecnológicos y las amenazas emergentes de ciberseguridad. El desarrollo de marcos y normas ha sido impulsado principalmente por los siguientes factores:

- **Los organismos reguladores** están haciendo hincapié en la necesidad de que las organizaciones sean responsables de sus prácticas de ciberseguridad y cumplan con normas y reglamentos específicos.
- **Las ciberamenazas avanzadas** son cada vez más frecuentes y dañinas. A menudo, abarcan la sofisticación que alguna vez se limitó a las amenazas respaldadas por el Estado, pero que ahora están en manos de oportunistas y hacktivistas.
- **Infraestructuras críticas y servicios esenciales** (por ejemplo, sanidad, energía, finanzas) que son vitales para el funcionamiento de la sociedad y la economía. Esto incluye legislación federal, como la Ley de Notificación de Incidentes Cibernéticos para Infraestructuras Críticas (CIRCA) de marzo de 2022.
- **Falta de uniformidad** en las prácticas de ciberseguridad en los diferentes sectores y regiones. Los enfoques incoherentes pueden conducir a brechas en la seguridad y desafíos de cumplimiento.
- **La orden ejecutiva** para mejorar la ciberseguridad de la nación que fue aprobada por el presidente de los Estados Unidos en mayo de 2021.

Está claro que las organizaciones necesitan ser resilientes frente a las ciberamenazas, para garantizar que puedan continuar operando y recuperarse rápidamente de las interrupciones. Con la creciente cantidad de datos personales que se recopilan y procesan, existe una mayor necesidad de proteger estos datos de las ciberamenazas y las violaciones de datos. Los incidentes cibernéticos no solo tienen un impacto económico significativo, provocan pérdidas financieras y socavan la confianza en los servicios digitales para la economía en general, sino que en algunos casos pueden costar vidas, especialmente cuando la industria de la salud ha sido el objetivo.

El cumplimiento normativo es crucial para desarrollar la resiliencia organizacional. Las empresas que comprenden el alcance completo de sus riesgos reconocen que el cumplimiento no es solo una actividad de casilla, sino una parte fundamental de una estrategia de seguridad general. Al adherirse a las regulaciones e implementar las mejores prácticas de seguridad, las organizaciones pueden posicionarse mejor para resistir y recuperarse rápidamente de la mayoría de los incidentes cibernéticos. Este enfoque garantiza que, cuando se produzca una crisis, ya se hayan sentado las bases para una rápida recuperación.

1.

Ciberataques

Si la infraestructura digital de una empresa está siendo atacada, los efectos pueden ir mucho más allá de la simple pérdida de datos. El impacto del tiempo de inactividad, la pérdida de funciones básicas, las posibles interrupciones en las ventas y la forma en que se percibe a la organización son todos resultados potenciales de un incidente cibernético.

Dadas estas posibilidades, el impacto en la vida humana es el factor más importante a tener en cuenta. Dentro de las industrias de servicios financieros (FSI) y de atención médica (HC), las ciberamenazas pueden tener impactos que alteran la vida a nivel individual, con impacto en las facturas, los pagos y el acceso a atención médica, entre otros servicios críticos. Preocupaciones y riesgos como estos son una buena razón para que las organizaciones mejoren su postura de seguridad y cumplan las regulaciones de su industria.

Por qué es importante el cumplimiento

El cumplimiento implica adherirse a las leyes y regulaciones que se aplican a la industria y geografía de la organización. El cumplimiento normativo puede ayudar a reducir el impacto en su negocio, desde la pérdida de ingresos debido al pago de rescates hasta la interrupción operativa, la exposición a vulneraciones de datos, las multas regulatorias y el daño a la reputación. Los estándares de cumplimiento están cambiando rápidamente y continuarán haciéndolo. Es posible que las regulaciones desarrolladas hoy para cumplir con los objetivos actuales no funcionen en el futuro. Estar al tanto de los nuevos marcos de trabajo y regulaciones y sus nuevas expectativas es una forma segura de proteger a su organización.

Regulaciones frente a marcos de trabajo

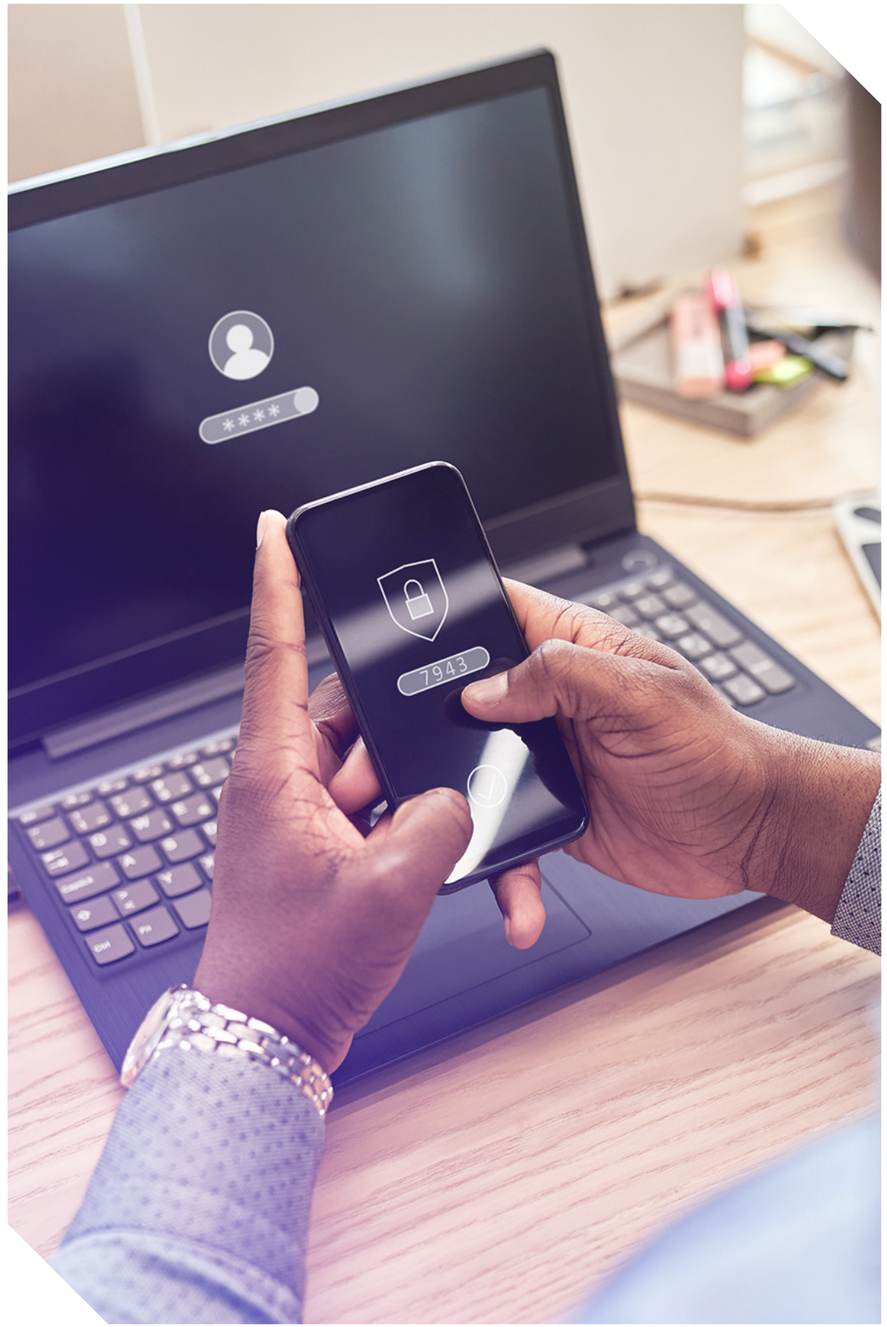
La diferencia fundamental entre las regulaciones y los marcos es lo que está tratando de lograr. Los marcos proporcionan un conjunto estructurado de directrices, mejores prácticas y estándares que las organizaciones pueden utilizar para gestionar y mejorar su postura de ciberseguridad. De otra forma, las regulaciones son requisitos legales impuestos por los gobiernos o los organismos reguladores para hacer cumplir un estándar mínimo de prácticas de ciberseguridad en todas las organizaciones. Algunas regulaciones ampliamente utilizadas incluyen:

- **RGPD** (Reglamento General de Protección de Datos): regulación de la Unión Europea para la protección de los datos y la privacidad.
- **HIPAA** (Ley de Portabilidad y Responsabilidad en Seguros de Salud: regulación de EE. UU. para proteger la información relacionada con la atención médica.
- **SOX** (Ley Sarbanes-Oxley): regulación de EE. UU. para prácticas financieras y gobierno corporativo.
- **PCI DSS** (Estándar de seguridad de datos de la industria de tarjetas de pago): estándares para proteger las transacciones con tarjeta de crédito.
- **FISMA** (Ley Federal de Administración de Seguridad de la Información): ley de EE. UU. para proteger la información gubernamental.

Regulaciones como estas funcionan en conjunto con los marcos de trabajo. Por ejemplo, los marcos de trabajo proporcionan la base para el cumplimiento de las regulaciones, y las regulaciones impulsan la adopción de marcos de trabajo. Los marcos de trabajo también ayudan a las organizaciones a ir más allá de los requisitos normativos mínimos y facilitan el cumplimiento y la auditoría, al tiempo que las normativas garantizan una seguridad de referencia coherente en todos los sectores. Estos son algunos marcos de trabajo ampliamente utilizados:

- **NIST Cybersecurity Framework (CSF):** proporciona un enfoque integral para gestionar los riesgos de ciberseguridad.
- **Controles CIS:** un conjunto de mejores prácticas para defenderse de las ciberamenazas.
- **COBIT:** proporciona un marco de trabajo para la gestión y el gobierno de TI, con un importante enfoque en los objetivos de control para TI, incluida la ciberseguridad.

Los marcos proporcionan las mejores prácticas para la gestión de la ciberseguridad, mientras que los reglamentos imponen normas mínimas para garantizar la seguridad básica en todos los sectores.



Gestión de riesgos y cumplimiento

Un enfoque basado en el riesgo comienza con una evaluación exhaustiva del riesgo. Este proceso debe implicar la participación de varias partes interesadas, incluidos los equipos de seguridad, el personal de TI, los expertos legales y los líderes empresariales.

Por ejemplo, un proveedor de servicios de atención médica puede identificar la protección de los registros médicos electrónicos (RME) como una prioridad máxima debido a la naturaleza confidencial de los datos y las posibles consecuencias de una infracción, como la pérdida de datos del paciente y las multas regulatorias según la HIPAA. Al priorizar la seguridad de los EHR, el proveedor puede centrar sus esfuerzos de cumplimiento en la implementación de controles que mitiguen los riesgos más significativos.

A medida que los requisitos normativos continúan aumentando en complejidad, las organizaciones recurren cada vez más a herramientas de gobernanza, gestión de riesgos y cumplimiento (GRC) para optimizar sus procesos de cumplimiento, mejorar la visibilidad y garantizar una monitorización y una mejora continuas.

Un enfoque de cumplimiento basado en el riesgo adapta los esfuerzos de seguridad a los riesgos únicos de cada organización, lo que garantiza que se prioricen las amenazas críticas.

Descripción general de las herramientas de GRC y sus beneficios:

Las herramientas de GRC están diseñadas para ayudar a las organizaciones a automatizar y gestionar diversos aspectos del cumplimiento, lo cual incluye el desarrollo de políticas, las evaluaciones de riesgos, el seguimiento de auditorías y la respuesta a incidentes. Estas herramientas ofrecen varios beneficios clave:

- **Administración de cumplimiento centralizada:** las herramientas de GRC permiten a las organizaciones consolidar las actividades de cumplimiento en una única plataforma.
- **Automatización de tareas de cumplimiento:** al automatizar las tareas rutinarias de cumplimiento, como la monitorización de los registros de acceso o la generación de informes de auditoría, las herramientas de GRC liberan un tiempo valioso.
- **Visibilidad y generación de informes mejorada:** las herramientas de GRC proporcionan visibilidad en tiempo real del estado de cumplimiento, lo que facilita a los responsables de seguridad el seguimiento del progreso, la identificación de brechas y la demostración del cumplimiento a los reguladores y auditores.
- **Monitorización y mejora continuas:** las herramientas de GRC facilitan la monitorización continua de lo que permite a las organizaciones identificar y abordar los problemas de forma proactiva en lugar de reactiva.

2.

Por qué es importante adoptar regulaciones de cumplimiento

El objetivo de comprender los riesgos de su organización y cómo puede hacer frente a ellos no es encontrar fallos. Más bien, es importante encontrar hechos para que pueda ayudar a su organización a protegerse y avanzar. Mientras que los ejecutivos podrían pensar que su organización está preparada y que sería ciberresiliente, la realidad podría ser muy diferente, poniendo a las organizaciones en riesgo.

Garantizar la participación y el compromiso de la junta directiva es la principal forma de lograr el cumplimiento. Las organizaciones deben fomentar una cultura de cumplimiento en toda la organización para reducir el riesgo. La gerencia es responsable de implementar los procesos y la tecnología de acuerdo con las regulaciones. Es importante dar un paso atrás y asegurarse de que las leyes y regulaciones se sigan en el contexto de la industria y la geografía de la empresa.

A medida que la industria continúa creciendo y cambiando, también lo harán las normas de cumplimiento y regulación. Sin embargo, no querrá que su empresa se retrase en el cumplimiento porque entonces correría el riesgo de ser negligente, y ahí es cuando un ejecutivo o miembro de la junta directiva está sujeto a medidas punitivas. Una interrupción o un ataque de ransomware podrían suponer sanciones económicas y daños a la reputación. Pero cuanto más madura sea su organización en términos de satisfacer los diferentes cumplimientos normativos, mayores serán las posibilidades de que pueda recuperarse rápidamente.

Cumplimiento normativo en todo el mundo

En todo el mundo, si nos fijamos en la legislación cibernética, existen más de 150 países con algún tipo de legislación cibernética. Algunos de ellos incluyen DORA en la UE, así como NIS/NIS2 en el Reino Unido. Japón tiene la FSA y en Oriente Medio están la NESA y las leyes de protección de datos DIFC. A nivel mundial, los países pueden recurrir al NIST. Cuando la gente en los EE. UU. piensa en ransomware y multas regulatorias, piensa en la Comisión de Seguridad y Exchange (SEC). A pesar de la amplia gama de opciones regulatorias, menos de 100 países cuentan con una regulación de infraestructura crítica. Esto demuestra que muchos países no se ocupan de la seguridad a un alto nivel, a pesar de que existe una necesidad muy real de centrarse en estos entornos de infraestructura crítica. Si nos fijamos específicamente en la industria sanitaria e incluimos la investigación y la biotecnología, a menudo tienen normas diferentes según el país.

Las regulaciones de cumplimiento garantizan que su organización esté preparada para incidentes cibernéticos, con la participación de la junta directiva crucial para fomentar una cultura de seguridad.

En qué se diferencian las industrias de servicios financieros y de atención médica

En los EE. UU., la Ley de Notificación de Incidentes Cibernéticos para Infraestructuras Críticas (CIRCA, por sus siglas en inglés) enumera 16 industrias críticas que deben cumplir diferentes regulaciones. Cuando la gente piensa en industrias críticas, normalmente piensa en represas, redes eléctricas y, obviamente, atención médica. La atención médica y los servicios financieros desempeñan un papel fundamental en la vida cotidiana de las personas en todo el mundo. Al observar los efectos negativos que la falta de cumplimiento de seguridad podría tener en las organizaciones de atención médica, el impacto afecta la vida de las personas.

La HIPAA es una de las principales regulaciones que viene a la mente cuando la gente piensa en el cumplimiento en la atención médica. La Regla de Privacidad HIPAA establece estándares nacionales para la protección de cierta información de salud, mientras que la Regla de Seguridad HIPAA establece un conjunto nacional de estándares de seguridad para proteger cierta información de salud que se conserva o transfiere en forma electrónica. Si un proveedor sanitario no está debidamente protegido o no cumple con la normativa, podría correr el riesgo de que los datos de sus pacientes se vieran comprometidos en caso de sufrir un ataque de ransomware.

En la industria financiera, una de las principales regulaciones es la GLBA, o la Ley Gramm-Leach-Bliley. Esta ley exige a las empresas financieras que ofrecen a los consumidores productos o servicios financieros, como préstamos, asesoramiento financiero o de inversión, o seguros, que expliquen sus prácticas de intercambio de información a sus clientes y que protejan los datos sensibles. Cuando una empresa financiera no cumple con los marcos o las regulaciones, corre el riesgo de enfrentar costos potenciales como pérdidas financieras materiales, multas, inestabilidad económica y daños a la reputación.

Las organizaciones deben adaptarse continuamente a las nuevas regulaciones para mantener el cumplimiento y adelantarse a la evolución de las amenazas de ciberseguridad.

3.

Recomendaciones de mejores prácticas e implementación

El cumplimiento no es una consideración de una sola vez. Los requisitos reglamentarios no son estáticos; evolucionan con el tiempo a medida que surgen nuevas amenazas y se actualizan las regulaciones. Como tal, hay algunas mejores prácticas para implementar para garantizar que su empresa se mantenga al tanto de todos los marcos y regulaciones cruciales.

Monitorización continua

La monitorización continua es un componente crítico de la administración eficaz del cumplimiento. Las herramientas de GRC facilitan la monitorización continua mediante la integración con la infraestructura de seguridad existente, como los sistemas SIEM (gestión de eventos e información de seguridad), para realizar un seguimiento del cumplimiento en tiempo real.

Por ejemplo, una empresa de servicios financieros sujeta a SOX puede utilizar una herramienta GRC para supervisar continuamente el acceso a los sistemas financieros, garantizando que sólo el personal autorizado tenga acceso a los datos financieros sensibles. Al integrar las herramientas de GRC en sus estrategias de ciberseguridad, las organizaciones pueden optimizar sus esfuerzos de cumplimiento, reducir el riesgo de incumplimiento y garantizar que sus prácticas de seguridad evolucionen en paralelo con los requisitos normativos.

Auditorías y evaluaciones periódicas

Durante un ataque, no será cuestión de si tiene un plan de respuesta ante incidentes. Debe *saber que* su plan funcionará. Una de las mejores maneras de garantizar esto es a través de las pruebas. Probar el plan de su organización y demostrar que la prueba tuvo éxito es la manera de garantizar el nivel de cumplimiento.

Pasos clave para el cumplimiento

Al observar qué regulaciones pueden implementar las organizaciones para convertirse en conformes, es importante adoptar un enfoque holístico. Cada parte de su organización puede tocar otro aspecto de su entorno. La planificación y la previsión desempeñarán un papel muy importante para garantizar el cumplimiento de su organización. Algunos pasos a tener en cuenta incluyen:

- **Desarrollar un proceso de gestión de riesgos:** esto implica identificar todos los riesgos potenciales de TI que podrían afectar a su negocio, así como evaluar sus vulnerabilidades.
- **Analice y priorice sus riesgos:** esto se puede hacer mediante el desarrollo de una estrategia de mitigación de riesgos y la capacitación de su personal.
- **Desarrolle un plan de respuesta ante incidentes:** en este plan, puede considerar aspectos como la transferencia de riesgos mientras mantiene la visibilidad y el análisis de su entorno.
- **Establecer una cultura de seguridad:** esto puede consistir en involucrar a todas las partes interesadas relevantes, elegir las tecnologías adecuadas y nunca olvidarse de documentar, documentar, documentar.

Desarrolle un proceso de gestión de riesgos, priorice los riesgos y establezca una cultura de seguridad para mantener el cumplimiento y mejorar la resiliencia.

Conclusión

El futuro del cumplimiento normativo se centrará en la resiliencia, y las organizaciones tendrán que anticiparse a las nuevas regulaciones y crear programas de cumplimiento adaptables y proactivos.

El panorama regulatorio es dinámico y es poco probable que el ritmo del cambio regulatorio se desacelere, particularmente a medida que los gobiernos y los organismos reguladores responden a los rápidos avances tecnológicos. Con esto en mente, la instrucción es que las organizaciones adapten los marcos de seguridad y continúen satisfaciendo el cumplimiento normativo. Un objetivo secundario sería la estandarización de las mejores prácticas de seguridad para llegar a un punto en el que las organizaciones alcancen una postura de seguridad aceptable.

En conclusión, el cumplimiento normativo es un proceso continuo que requiere esfuerzo, adaptación y colaboración.

No basta con lograr el cumplimiento; las organizaciones deben esforzarse por mantener y mejorar sus programas de cumplimiento frente a la evolución de las amenazas y las regulaciones. Los responsables de seguridad y TI desempeñan un papel crucial en este proceso, guiando a sus organizaciones hacia una estrategia de cumplimiento que no solo consiste en evitar sanciones, sino en construir una organización más fuerte y ciberresiliente. Al integrar el cumplimiento en la estructura de las operaciones y la cultura de la organización, y al mantenerse informadas y ágiles frente al cambio, las organizaciones pueden sortear las complejidades del panorama normativo con confianza y éxito.