CURSO: GOBERNANZA Y GESTIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

Unidad 6: Cumplimiento

Patricia Prandini y Raúl Saroka
DOCENTES

Índice

- Contexto
- Definición
- Ejemplos
- La función de cumplimiento
- Algunos estándares técnicos

De qué se trata

- Cumplimiento (del inglés *compliance*) define el conjunto de procedimientos y buenas prácticas adoptadas por una entidad para gestionar riesgos operativos y legales.
- Se lo asocia con el cumplimiento normativo, pero es mucho más que eso.
- En un contexto creciente de riesgos asociados a la transformación digital, consiste en establecer mecanismos de prevención, gestión, control y reacción frente a los riesgos.
- El cumplimiento de las reglas no debe ser realizado solo para evitar sanciones, sino debe convertirse en un mecanismo para el tratamiento de datos personales y la información sensible.

Concepto

Cumplimiento es un concepto que refiere a **actuar de acuerdo con las leyes, regulaciones, protocolos, estándares y especificaciones**. El costo del "no cumplimiento" puede ser civil, penal, financiero o afectar la imagen y reputación de la organización. (Ej: SOX)

Fuente: Governance, Risk and Compliance Handbook - Anthony Tarantino, PhD

Cumplimiento es la **práctica corporativa** que busca asegurar la adherencia y salvaguarda de los procedimientos y otros aspectos normativos.

Fuente: "La inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo" – Jeimy Cano

Concepto

Cumplimiento es la adherencia a directivas y requerimientos definidos por ley y por regulaciones, así como a los **requisitos voluntarios resultado de obligaciones contractuales y políticas internas, incluyendo también la capacidad de demostrar dicha observancia**.

Fuente: "A conceptual model for interated governance, risk and compliance"
Vicente y Mira da Silva

Nota: El Informe COSO sobre Control Interno establece, como uno de sus objetivos: "el cumplimiento de las leyes y reglamentaciones aplicables", poniendo este concepto como uno de los ejes del sistema de control interno.

Alcance

:

Cumplimiento de LEGISLACIÓN

- Cumplimiento de leyes y regulaciones sobre seguridad de la información
- Obligatorias para la organización según industria, país, actividad, etc.

Cumplimiento de NORMATIVA INTERNA

- Implantación y cumplimiento de normas internas sobre seguridad de la información.
- Obligatorias para la organización por decisión de sus cuerpos directivos, gerenciales y técnicos.

La función de cumplimiento

Según el Comité de Basilea es: ***Una función independiente que identifica, asesora, alerta, monitorea y reporta los riesgos de cumplimiento en las organizaciones****, es decir, el riesgo de recibir sanciones por incumplimientos legales o regulatorios, sufrir pérdidas financieras, o daños a la reputación por fallas de cumplimiento con las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas.*

La función de cumplimiento se refiere a todas las personas que tienen alguna actividad o responsabilidad relacionada y no sólo a un sector de la organización en particular.

La función de cumplimiento

- **Identifica** riesgos de incumplimiento, evalúa su impacto y los clasifica según su severidad y probabilidad de ocurrencia;
- **Monitorea,** verificando conformidades;
- **Asesora** como resultado de la evaluación del riesgo;
- **Alerta** sobre posibles incumplimientos;
- **Reporta** casos de no conformidad al Directorio

Fuente: La Función de Compliance – CP Martín Svarzman
http://www.iaia.org.ar/revistas/elauditorinterno/04/articulo1.html

Responsabilidades de la función

- **Identificar y evaluar los riesgos de cumplimiento asociados al negocio**, incluyendo los relacionados al desarrollo de nuevos productos y prácticas comerciales;
- **Establecer una guía** sobre la adecuada implementación de las leyes, reglamentaciones y estándares mediante políticas, procedimientos y otros documentos como manuales de procedimientos y códigos de conducta internos;
- **Advertir a la gerencia** sobre las leyes, reglas y estándares aplicables, informar sobre consecuencias de incumplimientos y divulgar mejores prácticas;
- **Asesorar a los responsables de los procesos internos** en la identificación de deficiencias en las políticas y procedimientos y formular propuestas de mejora;
- **Monitorear y probar conformidades** en forma regular, identificando casos de no conformidad con el consecuente reporte de deficiencias a la alta gerencia;
- **Ejercer responsabilidades específicas sobre cumplimiento normativo** en casos importantes para la industria, por ejemplo las normas de prevención del lavado de dinero para los Bancos;
- **Capacitar** a los colaboradores en el cumplimiento de las leyes y reglamentaciones; y
- **Atender a representantes de entes externos** (reguladores, inspectores, etc.)

Fuente: La Función de Compliance – CP Martín Svarzman – http://www.iaia.org.ar/revistas/elauditorinterno/04/articulo1.html

Por qué es importante

- **Cumplimiento Legal**
  Las empresas están sujetas a leyes y regulaciones relacionadas con la seguridad de los datos, privacidad de la información, protección de la propiedad intelectual y otros aspectos relacionados con la tecnología.

- **Protección de datos sensibles**
  En un entorno en el que la información se ha convertido en uno de los activos más valiosos de las organizaciones, es crucial garantizar la seguridad y confidencialidad de los datos sensibles.

Por qué es importante

- **Mitigación de riesgos**
  El cumplimiento permite identificar y mitigar riesgos asociados con el uso de la tecnología, mediante la implementación de normativas y buenas prácticas.

- **Confianza del usuario**
  La adopción de medidas de cumplimiento genera confianza a usuarios y socios. Al seguir buenas prácticas y cumplir regulaciones aplicables, la organización se presenta como un socio confiable y comprometido con la seguridad de los datos y la privacidad de la información.

Por qué es importante

- **Eficiencia operativa**
  Al establecer políticas y procedimientos claros, se optimizan los procesos internos, se reducen los errores y se aumenta la productividad. Además, el cumplimiento normativo facilita la auditoría y el monitoreo de los sistemas tecnológicos, ayudando a detectar y corregir posibles desviaciones o vulnerabilidades.

Cómo mejorar el cumplimiento

Políticas y procedimientos claros

- Establecer políticas y procedimientos claros incluye el desarrollo de políticas de seguridad de la información, de uso responsable de los sistemas, etc., así como procedimientos para el manejo de incidentes y protección de datos personales, entre otros. Además, estos procedimientos deben comunicarse al personal y a los terceros involucrados y ser parte de la capacitación.

Evaluaciones de riesgo

- Realizar evaluaciones de riesgo periódicas ayuda a identificar y mitigar las posibles vulnerabilidades y amenazas en el entorno tecnológico y tomar acciones preventivas y correctivas.

Cómo mejorar el cumplimiento

Capacitación y concientización

- Todo el personal, incluyendo los directivos deben entender la importancia de cumplir con regulaciones y políticas internas, así como los riesgos asociados con cualquier incumplimiento. La capacitación debe incluir entre otros, temas de seguridad de la información, privacidad de los datos y buenas prácticas.

Uso de herramientas seguras

- El uso de herramientas seguras, como la criptografía y la firma electrónica, por ejemplo, permite proteger la información. La organización debe proveer estas herramientas y capacitar en su uso.

Cómo mejorar el cumplimiento

Monitoreo y supervisión continua

- El monitoreo continuo de los sistemas es esencial para garantizar el cumplimiento normativo. Estas actividades permiten identificar posibles desviaciones, evaluar la efectividad de los controles implementados y corregir cualquier problema o brecha de seguridad.

Riesgo de incumplimiento

El riesgo de incumplimiento es la **incapacidad de una organización para prevenir, detectar, corregir y mantener la comprensión de los riesgos actuales y/o emergentes**, que afecten la operación y/o sus objetivos estratégicos de mediano y largo plazo.

La función de cumplimiento **vigila el riesgo de no cumplimiento**, que potencia escenarios relacionados con sanciones, errores u omisiones, multas, etc., y advierte a la organización respecto a la aplicación sistemática de malas prácticas, que pueden ocasionar incidentes, pérdida de valor y compromiso de la estrategia.

Fuente: "La inseguridad de la Información:
Motivador de la Práctica de Cumplimiento Corporativo" – Jeimy Cano

Atributos de la función de cumplimiento

Autoridad

Responsabilidad

Competencia

Objetividad

Disponibilidad de recursos

Fuente: “La inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo” – Jeimy Cano

Atributos de la función de cumplimiento

Autoridad

- Función adecuadamente ubicada en la estructura organizacional
- Nivel jerárquico que asegure su independencia y le permita incorporar prácticas para alcanzar un nivel de madurez apropiado.

Responsabilidad

- Capacidad para desarrollar, hacer funcionar e impulsar el programa de cumplimiento, en coordinación con profesionales de otras áreas que gestionan riesgos claves.

Competencia

- Ejercida por un profesional con conocimientos, experiencia y entrenamiento suficientes para lograr el desarrollo adecuado de la función.

Fuente: "La inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo" – Jeimy Cano

Atributos de la función de cumplimiento

Objetividad

- Implementada contemplando las presiones organizacionales en situaciones particulares
- Focalizada en asegurar las prácticas e informar los hallazgos a la instancia correspondiente.

Disponibilidad de recursos

- Asignación de recursos suficientes para llevar adelante la función, teniendo en cuenta el tamaño de la organización y la naturaleza de los riegos que enfrenta.

Fuente: “La inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo” – Jeimy Cano

Mediciones y métricas

Un **programa de cumplimiento efectivo** debe contemplar el establecimiento de **métricas** que permitan evaluarlo y mejorarlo.

Algunos interrogantes:

- ✓ ¿Estamos seguros de satisfacer en forma suficiente las necesidades de cumplimento?
- ✓ ¿Se están alcanzando los requerimientos de cumplimiento en forma más efectiva?
- ✓ ¿Cómo nos comparamos con otros?

Fuente: "Turning a Security Compliance Program Into a Competitive Business Advantage"-ISACA

El Factor Humano

Un programa de cumplimiento efectivo depende **de las personas, los procesos y la tecnología.**

Las **personas un factor crucial**. Un equipo hábil y motivado desarrollará el comportamiento esperado y adoptará las decisiones correctas, ejecutando acciones en forma oportuna.

Debe favorecerse el desarrollo de una cultura en la que se perciba que la responsabilidad de la gerencia general respecto al programa de cumplimiento se extiende a toda la organización.

Sistema de Gobierno y Cumplimiento

- ✓ Se requiere la **apropiación directa del programa de cumplimiento por parte de los responsables del gobierno y la gestión**.

- ✓ Solo se asegura un respaldo continuo cuando este programa se convierte en una **parte inherente del marco de gobierno de la seguridad de la información.**

Cumplimiento de estándares - PCI

El PCI Security Standards Council fue fundado por American Express, Discover Financial Services, JCB International, MasterCard y Visa, Inc.

Es un foro mundial abierto para la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas de tarjetas.

Objetivo: aumentar la seguridad de los datos de tarjetas de pago mediante la promoción de la educación y el conocimiento sobre las Normas de seguridad de la PCI.

- Norma de seguridad de datos (DSS)
- Norma de seguridad de datos para las aplicaciones de pago (PA-DSS)
- Requisitos de Seguridad de transacciones con PIN (PTS)

Cumplimiento de estándares - PCI

- ✓ Aplicable a entidades involucradas en el procesamiento de tarjetas de pago (comerciantes, responsables del procesamiento, emisores, proveedores de servicios y entidades que procesan, almacenan o transmiten datos de los titulares de tarjetas).

- ✓ Los requerimientos de cumplimiento varían según el volumen anual de transacciones, según 4 CATEGORÍAS (1 = mayor volumen de transacciones/mayores exigencias de seguridad).

- ✓ Según el caso, exige la realización de auditorías anuales, que suelen ser muy profundas y técnicas.

Cumplimiento de estándares-ISO 27001/2

Dos visiones del cumplimiento:

1. como adopción de buenas prácticas

2. como objetivo de la organización, que decide certificar ISO/IEC 27001

Cumplimiento de estándares-ISO 27001/2

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.31	Legal, statutory, regulatory and contractual requirements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection
5.32	Intellectual property rights	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem
5.33	Protection of records	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Defence
5.34	Privacy and protection of PII	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection

Cumplimiento de estándares-ISO 27001/2

ACTUALIZACIÓN INFORMÁTICA

5.35	Independent review of information security	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
5.36	Compliance with policies, rules and standards for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem
5.37	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

Cumplimiento de estándares-ISO 27001/2

Para certificar ISO 27001, una organización debe seguir los siguientes pasos:

1. **FASE 1** (Revisión de la documentación): se revisa la documentación sobre el alcance, la política y los objetivos del SGSI, la descripción de la metodología y el informe de evaluación de riesgos, la Declaración de Aplicabilidad, el Plan de tratamiento del riesgo, los procedimientos para el control de documentos, las medidas correctivas y preventivas y el informe de auditoría interna. Si falta alguno de estos elementos, significa que no está listo para la Fase 2.
2. **FASE 2** (Auditoría principal): busca determinar si la organización realmente está cumpliendo lo que dicen sus documentos y la ISO/IEC 27001. Se verifica que el SGSI se encuentra establecido en la organización.

Cumplimiento de estándares - COBIT

Experiencia requerida para funciones de cumplimiento

Descripción: Asegura que la gestión y el procesamiento de la información cumplan con la legislación, regulaciones, directivas y estándares internos y externos que le sean aplicables

Experiencia recomendada: Varios años de experiencia en seguridad de la información y en auditoría/cumplimiento, incluyendo:

- ✓ Auditoría, con exposición a leyes y regulaciones que deben ser cumplidas por la empresa
- ✓ Aseguramiento de que las prácticas seguridad de la información son efectivas, se aplican y se encuentran documentadas

Fuente: Cobit 5 for Information Security

Cumplimiento de estándares - COBIT

Conocimientos, habilidades técnicas y de comportamiento

Conocimientos:

- ✓ Estándares, guías y buenas prácticas de auditoría informática para asegurar que los sistemas del negocio se encuentran protegidos y son gestionados adecuadamente
- ✓ Técnicas de planificación y gestión de proyectos de auditoría
- ✓ Estándares de seguridad de la información
- ✓ Leyes y regulaciones locales vinculadas a la seguridad de la información

Habilidades técnicas: herramientas de auditoría y amplios conocimientos de TI

Comportamiento: Altos valores éticos, orientación a procesos, habilidades de negociación

Fuente: Cobit 5 for Information Security

Principales conclusiones - 1/2

- El concepto de gobierno de la Seguridad de la Información implica que **el negocio debe comprender y cumplir con una cantidad considerable de leyes, regulaciones, normas internas y estándares**

- El cumplimiento es **CLAVE** para la gestión corporativa del riesgo y el buen gobierno de la organización

- El cumplimiento requiere que la organización adopte **procedimientos alineados con las buenas prácticas**, incluyendo **controles internos** que protejan sus sistemas, procesos, información y el valor se sus activos

Principales conclusiones - 2/2

- Una falla en la integridad y consistencia de los controles sobre la infraestructura, los sistemas o los datos puede tener **un efecto significativo en la imagen corporativa o en el valor de sus activos**

- El cumplimiento en materia de TI no alcanza solo a algunos sectores en particular y los requerimientos de SI no se circunscriben exclusivamente al cumplimiento de la normativa de protección de datos

- Además de las sanciones, las consecuencias del incumplimiento pueden materializarse en potenciales obligaciones frente a terceros, daños en la reputación, pérdida de clientes, etc.

CURSO: GOBERNANZA Y GESTIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

Unidad 6: Cumplimiento

Patricia Prandini y Raúl Saroka
DOCENTES