



The Security Division of EMC

White paper

La tormenta de reglamentación que se avecina



¿Qué función desempeñará la reglamentación para evitar otro desplome financiero a nivel global?

La constante crisis financiera que se ha apoderado del mundo desde la mitad del año 2008 probablemente dé lugar a una gran cantidad de nuevas reglamentaciones globales. La naturaleza de esta falla exige un nuevo enfoque en las reglamentaciones que impulsarán

requerimientos de transparencia y adopción de administración de riesgos. Las organizaciones en todo el mundo deberán administrar de manera eficiente estas nuevas reglamentaciones a fin de alcanzar el cumplimiento de normas y continuar siendo competitivas.

Contenido

I.	A la vista	Página 1
II.	La ruta hacia el destino	Página 1
III.	Presura global	Página 1
IV.	Imitación: ¿amiga o enemiga?	Página 2
V.	Una guía histórica	Página 2
	Gobierno. Ejemplo basado en eventos: Sarbanes-Oxley	Página 3
	Gobierno. Ejemplo de mejores prácticas: HIPAA	Página 3
V.	Ejemplo de la industria: PCI	Página 3
VI.	Cumplimiento de normas: el arte de hacer lo mínimo	Página 3
VII.	Escenarios:	Página 4
	Enfoque centrado en los riesgos	Página 4
	Controles	Página 4
	Requerimientos de creación de informes	Página 4
VIII.	Impacto para los departamentos de tecnología de la información	Página 5
IX.	Recomendaciones	Página 5
	Identificar y rastrear procesos humanos	Página 5
	Aprovechar controles actuales para ayudar a automatizar el proceso de evaluación	Página 5
	Reglamentaciones de mapa cruzado	Página 5
	Comunicar métricas claves a líderes ejecutivos, unidades de negocios y auditores	Página 6
	Acerca de RSA	Página 6

I. A la vista

Ante la presencia constante del desplome financiero global en tiempo real, los Gobiernos de todo el mundo trabajan para controlar la crisis a diario en un intento de restaurar la estabilidad y la confianza en el mercado. A medida que los esfuerzos comienzan a mostrar resultados, las conversaciones están cada vez más centradas en la manera de evitar que esto suceda otra vez.

En medio de una oleada de fuertes opiniones de expertos y populares, se prevé la aparición de una gran cantidad de reglamentaciones bien intencionadas que aumenten la transparencia corporativa y la administración de riesgos. No obstante, a diferencia de muchas medidas reglamentarias vistas en los últimos 30 años, la nueva oleada de reglamentaciones será amplia, abarcará múltiples industrias verticales y, lo que es aún más importante, será de naturaleza y cobertura globales.

Con la ayuda de los Gobiernos de países individuales y las zonas de colaboración económica para apuntalar los negocios afectados, cada uno está comenzando a establecer sus propias expectativas con respecto a las reglamentaciones futuras. El Gobierno de los Estados Unidos, uno de los más importantes proveedores de rescate financiero, sugiere la creación de un “regulador de riesgos sistémicos” para las organizaciones, algo que otros países también están imitando. Al igual que con los esfuerzos reglamentarios anteriores, los departamentos de tecnología de la información de las empresas deben prever que tendrán que enfrentar una carga significativa de nuevas reglamentaciones.

II. La ruta hacia el destino

Desde una perspectiva simplista, existen dos causas fundamentales para la crisis actual: avaricia desenfrenada y riesgo no administrado. Se prevé con seguridad que ambos factores serán enfrentados en las próximas reglamentaciones. Dejaremos de lado la avaricia para los fines de nuestro análisis y nos referiremos al riesgo no administrado, que representa un punto de interés muy probable para las nuevas reglamentaciones. Esto puede requerir que las empresas proporcionen visibilidad sin precedentes de los riesgos relacionados con sus negocios, más allá de la exposición financiera inmediata.

A diferencia de muchos esfuerzos reglamentarios previos, las empresas deben esperar una respuesta gubernamental amplia entre las distintas industrias verticales. Si bien, en la crisis actual, determinadas industrias verticales han sufrido mayores niveles de exposición y pérdida que otras, los Gobiernos y

organismos de supervisión fueron sorprendidos por el alto grado de interconexión que puede existir entre los diferentes negocios. El hecho de saber que las empresas son “demasiado grandes para fallar” a causa de su magnitud, con frecuencia independiente de su enfoque de negocios tradicional, significa que las reglamentaciones futuras dejarán a muy pocos fuera de su alcance en relación con el cumplimiento de normas exigido.

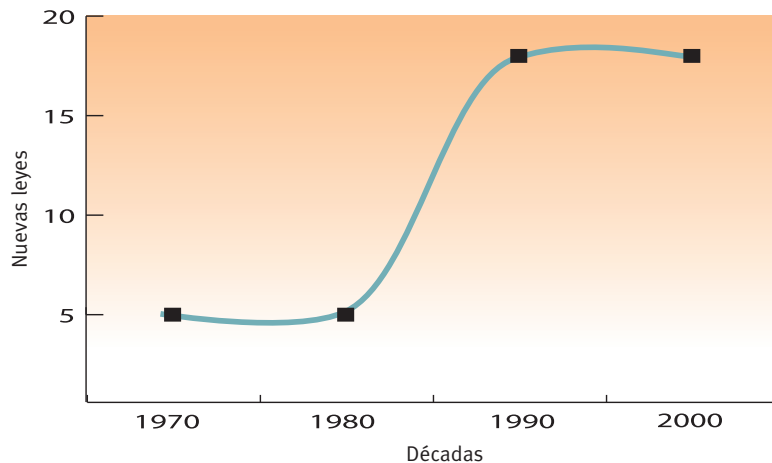
III. Presura global

En el gráfico que se muestra a continuación, se puede ver la cantidad de leyes globales nuevas que se centran en la protección de datos. Entre estas se incluyen leyes estadounidenses (como la GLBA, la HIPAA y la SB1386) y leyes internacionales (como la PIPDA, de Canadá, y la Ley de Privacidad de Nueva Zelanda). La década de 1990 representó una explosión en la actividad para las nuevas leyes: cada año, se sumaron alrededor de 20 nuevas reglamentaciones que cualquier organización internacional debe seguir y cumplir.

El crecimiento anual de estas reglamentaciones ha sido constante en los últimos años, dado que las leyes de protección de datos se convirtieron en prácticamente universales a nivel mundial, y los tiempos de auge económico con frecuencia se dieron con menos interés reglamentario. Con la crisis económica actual, las organizaciones deben estar preparadas para un regreso al crecimiento desenfrenado de las reglamentaciones, similar al visto en la década de 1990.

Tal como lo demuestra el gráfico, el crecimiento fue amplio debido a que cada Gobierno ingresó en el negocio de la reglamentación. Más adelante, es probable que la velocidad de las nuevas reglamentaciones se presente en un torrente y no en una curva de crecimiento. El nuevo crecimiento reglamentario modelará una pronunciada curva ascendente (palo de hockey) con una meseta que aparecerá relativamente rápido.

TREINTA AÑOS DE LEYES DE PROTECCIÓN DE DATOS



No debemos esperar ver un momento de calma de múltiples reglamentaciones mediante la presencia de una sola supervisión global. En las zonas económicas combinadas, como la Unión Europea, existe una mayor posibilidad de reglamentaciones combinadas. Aun así, si la carencia de coordinación actual en los diversos esfuerzos y enfoques de rescate financiero ofrece algún indicio del futuro, son probables las reglamentaciones individuales para cada país.

Ciertas prácticas aceptadas de contabilidad, como GAAP, pueden proporcionar vehículos de cumplimiento de normas para sus dominios; pero dichas prácticas no son universales y, debido a su enfoque específico, no proporcionarán una respuesta integral a las preguntas de los organismos reglamentarios. Los marcos de trabajo y los enfoques para las mejores prácticas de TI, como ISO 27002 y 27003, pueden ofrecer guías; pero requerirán que las organizaciones, en efecto, los implementen y los mapeen de manera adecuada a las nuevas reglamentaciones.

IV. Imitación: ¿amiga o enemiga?

Si se tienen en cuenta el alcance mundial de la crisis actual y la cantidad de Gobiernos individuales implicados en las actividades de rescate financiero, resulta razonable esperar que cada uno genere sus propias reglamentaciones. Según la manera en que los Gobiernos enfrenten la creación de reglamentaciones y la manera en que las organizaciones enfrenten las auditorías, la ley de cumplimiento de normas puede resultar mucho más costosa que la ley Sarbanes-Oxley o el acuerdo Basel II.

El análisis de las reglamentaciones actuales en relación con la tecnología de la información indica un alto grado de superposición en los controles y las directivas de control. De hecho, aproximadamente el 80% de las reglamentaciones globales relacionadas con TI comparten objetivos y directivas de control. Esto apunta a dos realidades: cuando hay un conjunto limitado de causas, con frecuencia hay un conjunto finito de opciones de corrección; por otra parte, cuando los gestores de las políticas reglamentarias encuentran trabajos similares, prefieren basarse en estos precedentes.

Un excelente ejemplo de los Gobiernos que, mutuamente, imitan sus reglamentaciones puede encontrarse en las leyes de información de identificación personal de los Estados Unidos. California inició la tendencia con el proyecto de ley 1386 del senado y el proyecto de ley 1298 de la asamblea. Estos proyectos de ley, que fueron sancionados en 2003, exigían que las organizaciones protegieran la información confidencial de sus clientes (incluidos el número de seguro social de los Estados Unidos, la dirección y la fecha de nacimiento) y que los notificaran en caso de pérdida o exposición de los datos. En pocos meses, la mayoría de los estados de este país aprobaron leyes similares. Los análisis de estas leyes muestran una similitud considerable con la ley de California, con retoques relativamente menores en relación con la definición de información de identificación personal y la definición de incumplimiento. Efectivamente, el cumplimiento de normas conforme a la reglamentación de California representa el cumplimiento de normas establecido por la mayoría de las leyes estatales posteriores.

La superposición reglamentaria resulta útil para una organización solo si la organización pretende aprovechar esta idiosincrasia. Debido a la velocidad con la que los Gobiernos responderán con nuevas reglamentaciones a medida que mengüe esta crisis, las empresas deberán prever y anticipar una superposición considerable con las reglamentaciones actuales y anteriores.

V. Una guía histórica

El uso del contexto histórico para los esfuerzos e impactos reglamentarios nos permite agrupar vagamente las reglamentaciones anteriores en dos categorías simples: gubernamentales e industriales. Dentro de las reglamentaciones gubernamentales: Resulta útil realizar una subdivisión aún mayor en dos categorías de reglamentaciones: “basadas en eventos” y “mejores prácticas”. Comúnmente, las reglamentaciones gubernamentales basadas en eventos son respuestas a fallas de índole significativa en el sector privado. Las reglamentaciones gubernamentales de mejores prácticas son casos en los que, en un momento dado, el Gobierno identifica una tendencia que causa preocupación y ofrece supervisión antes de que se produzca un evento negativo considerable.

Las reglamentaciones de la industria con frecuencia son intentos de proporcionar creación interna de políticas a fin de evitar o demorar la supervisión y la reglamentación gubernamentales.

Debido a la velocidad con la que los Gobiernos responderán con nuevas reglamentaciones a medida que mengüe esta crisis, las empresas deberán anticipar una superposición considerable con las reglamentaciones actuales y anteriores.

Lo que hará que estas nuevas reglamentaciones sean algo único será la concentración en el riesgo.

Gobierno. Ejemplo basado en eventos: Sarbanes-Oxley

Tras la anterior depresión económica de 1999, el Gobierno federal de los Estados Unidos, consciente del escándalo de Enron/WorldCom, incorporó la Ley Sarbanes-Oxley para lidiar con las empresas que cotizaban en bolsa. El objetivo de esta ley es que los ejecutivos claves asuman la responsabilidad de sus declaraciones financieras y que firmen de manera efectiva sus propias órdenes de arresto en caso de que se detecten irregularidades en los libros contables. La Sección 404, relacionada con los controles eficaces, proporcionó una cantidad considerable de material de marketing y oportunidades de generación de ingresos para las empresas de seguridad de TI. Una consecuencia imprevista de esta ley fue que varias empresas se privatizaron a fin de eludir el cumplimiento de normas establecido por Sarbanes-Oxley. Su motivo no era eludir la exposición a contabilidad financiera inadecuada; de hecho, varias empresas optaron por pasarse al sector privado tras muchos años de cumplimiento de normas conforme a SOX. En lugar de esto, buscaban eludir el *costo* del cumplimiento de normas que generó esta tendencia. Específicamente, los montos de siete cifras que las empresas públicas deben pagar anualmente para garantizar el cumplimiento de normas pueden constituir la diferencia entre ganancia y pérdida.

Gobierno. Ejemplo de mejores prácticas: HIPAA

La Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) es un ejemplo en el que el Gobierno federal de los Estados Unidos identificó tendencias clave que ponían en riesgo la privacidad de la información y los registros médicos de las personas. Esta situación precipitó el hecho de que la HIPAA estableciera requerimientos claves relacionados con la manera en que los proveedores de salud ofrecían seguridad física y digital para preservar la confidencialidad de los pacientes. No obstante, el incentivo más importante para que el Gobierno implementara la HIPAA

fue el potencial ahorro en los costos asociado con la accesibilidad de la ley. Una limitación clave de la HIPAA ha sido un modelo de financiación que limitó la aplicación proactiva durante muchos años.

Ejemplo de la industria: PCI

El Estándar de Seguridad de Datos de la Industria del Pago con Tarjetas (PCI DSS) es uno de los ejemplos más conocidos de reglamentaciones de la industria. La PCI fue establecida y aplicada por Visa® y MasterCard® a fin de garantizar que los comerciantes y los procesadores de pagos emplearan buenas prácticas de seguridad para la protección de la información de los titulares de tarjetas. Es una práctica altamente prescriptiva en cuanto al control de TI y exige opciones y requerimientos de tecnología específicos. Si la crisis financiera actual hubiese impactado parcialmente en lugar de causar un impacto directo, la supervisión del Gobierno podría haberse evitado mediante una serie de reglamentaciones de la industria.

Surge una interrogante en cuanto a si alguno de estos casos históricos puede usarse para indicar futuras reglamentaciones en el contexto de la crisis económica actual. Es seguro decir que la clase de reglamentaciones se incluirá en la categoría de las gubernamentales basadas en eventos. Debido a la velocidad con que se necesitan nuevas reglamentaciones, habrá una superposición más importante con las reglamentaciones y los marcos de trabajo actuales. Lo que hará que estas nuevas reglamentaciones sean únicas será la concentración en el riesgo. Si bien una gran cantidad de reglamentaciones globales actuales se centra en el riesgo financiero, se ha cuestionado su eficiencia, y se requieren y se desean nuevos enfoques.

VI. Cumplimiento de normas: el arte de hacer lo mínimo

El enfoque hacia el cumplimiento reglamentario desde la perspectiva de la organización promedio con frecuencia puede resumirse como “el arte de hacer lo mínimo”. En lugar de que las reglamentaciones externas sean vistas como una oportunidad para superar las expectativas, con frecuencia se reducen a una negociación con los auditores sobre el enfoque que se debe emplear para las mejoras de auditoría del año siguiente. Esto significa que, comúnmente, las auditorías son vistas como simples “aprobaciones” según las cuales se evaluará a la organización en la auditoría del año próximo.

Este ha sido el enfoque dominante desde que se generalizaron el cumplimiento reglamentario y la manera en que se ejecuta el cumplimiento de normas en una organización típica. Actualmente, la evaluación del cumplimiento de normas y la ejecución de auditorías continúa siendo una tarea manual ardua con portapapeles y cuestionarios manuales que representan las tecnologías modernas. Si bien se han desarrollado e implementado herramientas como escáneres de vulnerabilidad y soluciones de administración de eventos e información de seguridad como ayuda para agregar la carga en la organización de TI, el acto del cumplimiento de normas, en gran medida, continúa basándose en procesos humanos.

Por medio de un desempeño mínimo, las organizaciones han podido mantener bajo el costo de las evaluaciones del cumplimiento reglamentario. No obstante, el proceso muestra claramente tensiones que se traducirán en fallas a corto plazo. El modelo funcionó cuando la cantidad de reglamentaciones era relativamente baja y el alcance de las auditorías asociadas era limitado. El crecimiento anual compuesto de las reglamentaciones en el mundo ha hecho que las evaluaciones humanas pierdan eficacia y se vuelvan costosas hasta un nivel prohibitivo debido al simple hecho de que los humanos se adaptan de manera deficiente. En un ambiente de presupuestos reducidos y congelamiento de las contrataciones, las reglamentaciones adicionales irrumpirán sistemáticamente en las organizaciones de TI, a menos que las organizaciones cambien la manera en que se ejecutan las evaluaciones de auditoría.

VII. Escenarios:

¿Cuáles son algunos escenarios que probablemente se presentarán en los meses y años próximos a medida que surjan protecciones en un intento de evitar otra falla sistemática? Dado que faltan precedentes en esta área, la bola de cristal es ambigua, pero no es enteramente incierta.

Si bien gran parte de la crisis económica actual tiene sus raíces en una falta de supervisión adecuada de los riesgos, es improbable que las nuevas reglamentaciones apunten a una sola industria. Lo que la crisis ha dejado en exposición es el alto grado de interconexión e independencia en la empresa global, sin importar su enfoque principal de negocios. Esto significa que las nuevas reglamentaciones serán amplias y de largo alcance, y se extenderán a la interconectividad que define la infraestructura de TI actual.

Para la organización de TI, estas son las tres áreas con menos probabilidades de sufrir un impacto inmediato a causa de la nueva serie de reglamentaciones.

El crecimiento anual compuesto de las reglamentaciones en el mundo ha hecho que las evaluaciones humanas pierdan eficacia y se vuelvan costosas hasta un nivel prohibitivo.

Enfoque centrado en los riesgos

Las organizaciones deben prever que el cumplimiento de normas basado en preguntas que se pueden responder con “sí” o con “no” dará lugar a una concentración en los riesgos en la que se tendrá en cuenta el estado actual del sistema, pero la probabilidad de los eventos también constituirá un factor. Esto impulsará la necesidad de contar con planes de moderación y contingencia que puedan modelarse en función de eventos de falla. En lugar de intentar enfrentar todos los puntos débiles, las vulnerabilidades y las amenazas, las organizaciones deben establecer prioridades y enfrentar los problemas en función del nivel de riesgo al que están expuestas.

Controles

El ambiente actual de los controles empresariales probablemente será suficiente para muchas de las nuevas reglamentaciones. Las pequeñas y medianas empresas deberán comenzar a adoptar algunas de las herramientas más tradicionales de las “grandes empresas”. Esto incluye controles como autenticación de múltiples factores, separación de deberes y prevención de pérdida de datos. Debido a la nueva actitud centrada en los riesgos, los puntos de aplicación y las capacidades tradicionales deberán mejorarse para generar información y métricas en un contexto más amplio.

Requerimientos de creación de informes

La creación de informes sobre riesgo es diferente a la creación de informes sobre cumplimiento de normas. Los departamentos de TI deben prever que sus sistemas de cumplimiento de normas tradicionales deberán evolucionar para crear informes sobre análisis de brechas, simulaciones y probabilidades. Además, los informes deberán orientarse a equipos ejecutivos más grandes, que incluyan al director financiero y al director ejecutivo.

El golpe más duro de estas nuevas reglamentaciones serán las empresas con operaciones globales y un conjunto diverso de ofertas entre las industrias verticales. Estas organizaciones deberán satisfacer las expectativas de múltiples Gobiernos nacionales y organismos de la industria a fin de continuar operando en sus países e industrias respectivos.

VIII. Impacto para los departamentos de tecnología de la información

Al igual que los eventos reglamentarios importantes del pasado, como la HIPAA, la GLBA y la PCI, el impacto de las próximas reglamentaciones generará una carga desconocida y desafiante para el departamento de TI. Es probable que se requieran controles adicionales para moderar el riesgo considerado pertinente conforme a las nuevas reglamentaciones. Es mucho más probable aún que deba evolucionar la manera en que se utilizan los controles actuales.

Es probable que la amenaza más importante para las organizaciones de TI no radique en la implementación de controles específicos adicionales, sino en los inmensos volúmenes de evaluaciones que deberán ejecutar. Las organizaciones de TI deben prever que sus cargas de evaluaciones de cumplimiento de normas aumentarán considerablemente sus requerimientos de tiempo y de tamaño del equipo. Como se mencionó anteriormente, la carga actual de auditorías y evaluaciones ha conducido el departamento de TI promedio hacia un punto de quiebre. Las nuevas reglamentaciones solo aumentarán esta presión.

En el ambiente presupuestario actual, es poco probable que se aprueben grandes cantidades de contrataciones para llevar a cabo las evaluaciones manuales de cumplimiento de normas. En lugar de esto, las organizaciones deberán comenzar la transición hacia la automatización de este proceso en el futuro inmediato.

El objetivo debe ser crear un modelo sostenible para evaluar y comunicar el cumplimiento de normas en un conjunto de reglamentaciones amplio, cambiante y cada vez mayor.

IX. Recomendaciones

Las próximas reglamentaciones son inevitables. El líder estratégico de TI las verá como una oportunidad para reformar un sistema quebrado de evaluación y seguimiento del cumplimiento de normas. El enfoque en una organización centrada en los riesgos, en lugar de una centrada en el cumplimiento de normas, ha sido un objetivo de maduración de los departamentos de TI durante muchos años. El interés reciente en el riesgo debe ser explotado por los departamentos de TI (específicamente por el área de seguridad de TI) para impulsar la maduración de una empresa basada en los riesgos.

El objetivo debe ser crear un modelo sostenible para evaluar y comunicar el cumplimiento de normas en un conjunto de reglamentaciones amplio, cambiante y cada vez mayor. Para lograr esto, se deben priorizar cuatro iniciativas específicas.

Identificar y rastrear procesos humanos

El costo más significativo para una empresa en relación con las evaluaciones de cumplimiento reglamentario radica en las personas que deben ejecutar, rastrear y administrar el proceso. Además de representar un problema de escalación lineal, los equipos grandes centrados en comprobar configuraciones y marcar casillas limitan la capacidad de una organización de mejorar su modelo de madurez. Esto posiciona a una organización en una rueda de hámster metafórica en relación con el cumplimiento de normas.

Aprovechar controles actuales para ayudar a automatizar el proceso de evaluación

La mayoría de los departamentos de TI empresariales cuentan con componentes claves implementados que pueden ayudarlos a automatizar el proceso de evaluación reglamentaria. Las organizaciones deben realizar un análisis y un inventario detallados de sus capacidades. Deben solicitarles a sus proveedores que ayuden a enfrentar los requerimientos de cumplimiento de normas basado en los riesgos mediante sus ofertas de productos.

Reglamentaciones de mapa cruzado

Las organizaciones deben usufructuar la similitud entre las reglamentaciones globales de TI. Con las reglamentaciones de mapa cruzado, una empresa puede realizar una sola evaluación y, al mismo tiempo, cumplir con muchas reglamentaciones. Mediante la adición de las directivas comunes, un equipo de evaluación solamente deberá concentrarse en los elementos diferentes en caso de que se requieran nuevas auditorías. Además, mediante la integración de las nuevas reglamentaciones en el mapa cruzado, la organización de TI puede modelar el impacto de las nuevas reglamentaciones una vez que son propuestas. También puede proporcionar conocimientos sobre el costo del cumplimiento de normas a medida que se planifican nuevos negocios geográficos o entradas verticales.

Comunicar métricas claves a líderes ejecutivos, unidades de negocios y auditores

Se deben enviar informes regulares y tableros a los gerentes ejecutivos, los líderes de las unidades de negocio y los auditores para su análisis conjunto. Dentro de la empresa, se deben evaluar y rastrear los requerimientos reglamentarios para cada negocio. Se deben informar las tendencias y se debe establecer un plan de trabajo de madurez para el progreso de los informes en función de los objetivos. Es fundamental que se comuniquen métricas significativas en el contexto del negocio.

Resulta imposible conocer lo que depara el futuro para la reglamentación en el mundo. Es seguro suponer que la constante histórica de mayor reglamentación global se mantendrá para el futuro previsible y que veremos un pico en las nuevas reglamentaciones emitidas por Gobiernos y e industrias, más probablemente en los próximos 6 a 18 meses. Las organizaciones no deben suponer que se sentirán abrumadas. El área de TI puede aprovechar esta situación para cambiar el foco de interés desde el cumplimiento de normas puntuales hacia un enfoque centrado en los riesgos. Con una buena planificación y una buena preparación, las organizaciones estarán preparadas para enfrentar la gran cantidad de reglamentaciones que ofrecerá el futuro.

Acerca de RSA

RSA, la División de Seguridad de EMC, cuenta con personal especializado en seguridad centrada en la información, lo que permite proteger la información durante todo su ciclo de vida. RSA permite a los clientes asegurar de manera rentable los recursos de información críticos y las identidades en línea (en el lugar y en la etapa en que se encuentren), y administrar la información y los eventos de seguridad para aliviar la carga que impone el cumplimiento de normas.

RSA ofrece soluciones líderes de la industria en cuanto a verificación de identidad y control de acceso, encriptación y administración de claves, administración del cumplimiento de normas e información de seguridad, y protección contra fraudes. Estas soluciones brindan confianza respecto de millones de identidades de usuarios, las transacciones que realizan y los datos que se generan. Para obtener más información, consulte www.RSA.com (visite el sitio web de su país correspondiente) y www.EMC.com (visite el sitio web de su país correspondiente).

RSA y RSA Security son marcas registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC es una marca registrada de EMC Corporation. Todos los demás productos o servicios mencionados son marcas comerciales de sus respectivos dueños. ©2009 RSA Security Inc. Todos los derechos reservados.

REGULS WP 0609



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

