## Desayunos ASTIC

# Gestión de la Gobernanza, el riesgo y el cumplimiento en las AAPP

**POR MAOLE CEREZO**
REDACTORA JEFE DE BOLETIC
**FOTOS** AITOR DIAGO

Evento patrocinado por

EMC²

La división de seguridad de EMC presentó en un desayuno de trabajo, el pasado mes de junio, su solución Archer, un software para la el gobierno, la gestión del riesgo y el cumplimiento, conceptos que en las organizaciones cada vez cobran más importancia.


Fidel Pérez, Director Comercial de RSA, la División de Seguridad de EMC comenzó su intervención ahondando sobre la herramienta que "ofrece la gobernanza de los objetivos corporativos, permite conectar entre sí las políticas, los riesgos y las normativas que deben cumplir, tanto a nivel global, como de detalle". La herramienta facilita "el cumplimiento de los objetivos en estos apartados, teniendo un único repositorio centralizado donde se maneja todo lo relacionado con riesgos, cumplimientos, políticas, incidentes..." Todo ello se realiza a través de "un framework o marco de trabajo que tiene un desarrollador de aplicaciones muy sencillo, donde se dispone de los cuadros de mando e informes a todos los niveles: se maneja el control de acceso, las notificaciones, el estado »

**Antonio Pérez de Lema**

**Aurora Clemente de EMC**

**Carlos García**

de situación de cualquier campaña que se lance, los flujos de trabajo, y lo más importante, permite la integración con nuestras aplicaciones".

Para el directivo, utilizando este framework "hemos construido un conjunto de soluciones o módulos para resolver distintas problemáticas de la empresa: un gestor de políticas, un gestor de amenazas, un gestor de empresa o Enterprise Management (que nos permite conectar los activos de nuestra organización a todos los niveles), un gestor de riesgos, un gestor de continuidad de negocio (RSA Archer permite centralizar planes de continuidad de negocio para saber que hay que hacer en caso de desastres, cómo lanzar de forma automática todos los procesos y mantenerlos actualizados), un gestor de proveedores que se alimenta con información derivada del control de riesgos, un gestor de personal, un gestor de auditorías y un módulo relativo a la gestión del cumplimiento normativo". Una aplicación importante de RSA Archer es que "podemos tener la cobertura necesaria para el Esquema Nacional de Seguridad".

Gartner habla de tres dominios principales dentro del GRC: el de TI, el financiero y el legal, y Pérez se "atrevió" a "incluir un cuarto, el de operaciones". En el dominio de TI, "introducimos los conceptos de controles (contraseñas), riesgos (el acceso no autorizado a un sistema), incidentes (una fuga de información), amenazas (un ataque de hacking) y activos (información)". Estos conceptos "son comunes para cualquier organización pero ¿tienen sentido en las Administraciones Públicas? Nosotros creemos que sí". Por otra parte, "contemplando todas las normativas que se han de cumplir, pensamos que las soluciones de GRC tienen mucho que aportar en las AAPP".

Una vez presentada la herramienta, los directivos TIC de la AAPP plantearon sus cuestiones y comenzó abriendo el debate Francisco Antón, Presidente del Patronato de la Fundación ASTIC: "nosotros somos los responsables de implementar la herramienta y para convencer a nuestros superiores de sus bondades necesitamos argumentos convincentes, puesto que ellos no entiende de seguridad y no lo contemplan entres sus preocupaciones... ¿Contáis con alguna experiencia?

RSA Archer, detalló Pérez "no tiene que ver solo con la seguridad TI, si no con la gestión de riesgos de cualquier tipo en la organización. En las instituciones financieras, por ejemplo, el tema de los riesgos operacionales es fundamental porque se refleja en el balance: en función de mi nivel de riesgos tengo que provisionar más o menos fondos. Hay ejemplos de casi cualquier tipo de compañía

en la que la gestión de riesgos es fundamental".

Un tema importante en, en el caso de la AAPP, "son los riesgos relativos a la gestión de proveedores. Si tenéis mucho negocio con un proveedor no fácilmente sustituible, puede estar impactando en el riesgo de vuestra organización de manera muy importante. Hay compañías que, al más alto nivel, están empleando estas soluciones de GRC".

Respondiendo a Francisco Antón, Carlos Senac, del Ministerio de Defensa argumentó que "el mayor riesgo para nuestra organización sería no sacar adelante la tarea, ahí puede estar el quid de cómo venderlo a nuestros mayores. El mapa de riesgos es una representación gráfica que podría ser útil y que permitiría a nuestro Director General percibir, en un solo vistazo, que es lo que está en juego". Si bien, este tipo de herramientas "van dirigidas a nuestra gestión, uno de los instrumentos más útiles para elevarlo a otras esferas sería las representaciones gráficas de la herramienta". Refiriéndose al cumplimiento, Senac señaló que "el más importante sería, en estos tiempos de crisis, cumplir con lo básico". Por último planteó a EMC "¿A qué has llamado mapa de riesgos?"

Un mapa de riesgos "lo entendemos como una representación o listado de los riesgos de la organización ordenados según su probabilidad de ocurrir y su impacto en el negocio. Una vez desarrollado este mapa de riesgos, se tiene una clara visión de que procesos son los básicos (porque tienen mayor impacto o son más probables de ocurrir), para comenzar a trabajar sobre ellos".

Según compartió Serafín Hernández, del Comisionado del Mercado del Tabaco, para él la herramienta "además de para presentar informes a nuestros superiores, nos puede servir para estudiar nuestro estado de situación". Ante el cambio de gobierno que se avecina, es conveniente saber "hasta qué punto nuestra infraestructura es ágil y puede adaptarse a nuevas directrices políticas".

Fidel Pérez le comentó que "RSA Archer es un framework o marco de trabajo sobre el que es muy sencillo desarrollar, ir añadiendo módulos o configurar en caso de cambios de políticas. Es completamente ágil"

¿Cómo se integraría nuestro sistema con los vuestros?, porque la integración, "según has expuesto, tendría tres patas: por un lado con el software comercial pre existente, con nuestro software corporativo (múltiple, muy variado y con muchas tecnologías) y la integración con las plataformas corporativas" intervino Javier Gil, del Ministerio de Defensa.

Desde EMC explicaron que "básicamente tenemos »

**Carlos Maza**

**Carlos Senac**

**Carmen Cabanillas**

**Enrique de Frutos**

**Fidel Pérez de RSA-EMC**

**Gerardo Herrero**

tres procedimientos de integración: uno a través de la importación vía ficheros para realizarla una sola vez; una integración vía fichero de forma periódica y otra tercera a través de un API o webservice con capacidad de hablar con cualquier tipo de aplicación viva para poder importar datos en tiempo real". Cualquiera de estas opciones "pretendemos que sean extraordinariamente sencillas de ejecutar sin tener que programar nada".

¿Con Archer podemos definir, gestionar, objetivos, políticos, estructura organización y facilitarnos la definición de estrategias? Porque, según me parece haber entendido, la seguridad es una pequeña parte de lo que ofrece la herramienta ¿es así? Carlos García, del MICIN.

Como detalló el directivo de RSA, La división de seguridad de EMC, la herramienta RSA Archer pretende "manejar todo lo que tiene que ver con la gobernanza de las TI. Podemos utilizar las políticas definidas por alguna normativa, que puede referirse a continuidad de negocio o a riesgos, o simplemente, con normativas que definamos nosotros de cómo debe ser el equipamiento de nuestros sistemas, nuestros procesos de back up, nuestros procesos de personal, nuestras estrategias...etc." En definitiva, "todo lo que tiene que ver con el cumplimiento y con los riesgos asociados". La herramienta "incluye las políticas más estándar de la ISO, o todos los puntos de control, de los cuales, algunos tienen que ver con seguridad pero otros muchos no. También incorpora una parte importante relativa al cumplimiento y a las políticas en el mundo virtual (políticas de la Cloud Alliance)"

Gerardo Herrero, del Ministerio de Fomento, compartió con los presentes que "en cuanto al tratamiento de la información, en la AAPP queda mucho por hacer: los riesgos no están implantados en los sistemas; los bienes Públicos, el Patrimonio del Estado, no está asegurado.... Veo interesante Archer para implementar nuevas políticas púbicas en este sentido". El directivo puso el ejemplo de su utilidad para el caso concreto de la regularizaron que tuvo lugar, tiempo atrás, con los inmigrantes que llegaron a nuestro país. A la vez, planteó "vincular la calidad a la parte de seguridad, en cuanto al cumplimiento de los objetivos de los sistemas de información se refiere".

RSA Archer posibilita, según Fidel Pérez, "los procesos de gestión y monitorización de campañas, de gestión de auditorías enfocadas hacia la calidad o el cumplimiento normativo clásico". La solución "no es más que un gran repositorio, con unas herramientas software alrededor, que puedes dirigir según tus necesidades a temas de seguridad, de TI, de calidad... Se pueden definir unas polí-

ticas de calidad, unos puntos de control de esas políticas, unos cuestionarios para medir ese grado de calidad, etc".

Enrique de Frutos del MICIN, apuntó que "un tema importante y nos preocupa a los directivos TIC es, en qué momento nos llegan a nuestros departamentos los requisitos, las órdenes y la definición de nuestras aplicaciones, y en numerosas ocasiones, nos llegan con el BOE". En este sentido "si sería interesante tener un repositorio, una gestión de esa normativa y unos dashword que reflejaran como nuestras aplicaciones hacen posible que la organización cumpla con esa normativa, de manera que traslademos al negocio de los ministerios y de los organismos lo que hay por detrás, nos vendría bien para gestionar todo lo que hay detrás de esa normativa". Sería "una herramienta muy útil, para hacer ver al negocio todo lo que cuelga de una normativa legal y como la maquinaria TI da el servicio en la organización".

Concretamente, coincidió Fidel, "esa es una de las soluciones o módulos que ofrecemos: el gestor de políticas, que permite tener conectadas a cada una de las áreas de la organización, en un repositorio único, todas las políticas que nos afectan y garantizando, que todos los empleados, conocen esa política. Están formados en ella y, si cambia, la herramienta difunde inmediatamente los cambios a todos los involucrados. Esta es una de las funciones estándar de la solución RSA Archer".

Francisco Antón, del Ministerio de Educación, se interesó por conocer cuál es el alineamiento con las ISOS, ITIL...

La herramienta RSA Archer "tiene contenidos y plantillas, como las normas ISO, que están pre-cargadas en la herramienta con todos los puntos de control necesarios. Lo que se necesita es adecuarlas a la estructura de cada organización. En cuanto a la gestión de riesgos, la herramienta utiliza la metodología COSO (similar a la ISO 30.000) que permite importar, una vez que se tiene el mapa de riesgos. Otros de los contenidos pre-cargados en la herramienta es el Esquema Nacional de Seguridad", informó Fidel Pérez.

Carmen Cabanillas, del Ministerio de Educación preguntó si la herramienta recoge COBIT. Y en relación de las auditorías, ¿a parte de un repositorio, tenéis definidos puntos de control, supervisión, flujos?

EMC aclaró que, "si recoge COBIT y, más que en la parte de auditoría, en la de cumplimiento donde están definidos los puntos de control. En la ISO 27.000 tienes más de cuatro mil puntos de control".

¿Dónde se instala RSA Archer? Preguntó Carlos García, del MICIN. »

**Javier Gil**

**José Antonio Arozarena**

**Francisco Antón**

**José María Museros**

**José Ramón García**

**Manuel Alonso**

Archer, tal y como aclaró Pérez, se instala "en casa del cliente o en la nube. Nosotros tenemos la posibilidad de vender la solución como software as a service que corre en data center nuestros y a través de una suscripción". En caso de catástrofes, "lo mejor es esta última opción".

Los tres pilares a los que EMC se refirió: gobernanza, riesgo y cumplimiento, fueron objeto de análisis por parte de Andoni Pérez de Lema, de la IGAE. Para éste, "el riesgo es muy complejo de valorar, porque se han de contemplar sus dos componentes, impacto y vulnerabilidad. El impacto de una materialización de una amenaza es conocido, pero la vulnerabilidad es un parámetro estadístico y para conocerlo bien habría que tener un sistema de modelización o una base de datos histórica muy grande". Su intervención concluyó con una pregunta para EMC: ¿Cómo mide el riesgo?

Fidel Pérez explicó que "la herramienta tiene una librería matemática que ayuda a hacer todo tipo de cálculos, y en cada uno de los segmentos, el cálculo de los riesgos lo realizan los expertos en la materia y hay metodologías para ello".

¿Podrías darnos referencias de algún caso concreto que esté empleando Archer?, intervino Francisco Antón.

La solución funciona "en cualquier proceso de la empresa, por ejemplo, Fedex gestiona todas las investigaciones de pérdidas de paquetes con Archer".

José Antonio García del Ministerio de Educación, se refirió a Archer como una "solución que los TIC proponemos para perfeccionar la organización y se interesó por conocer "¿Qué recursos se necesitan para implementar la solución, a nivel de instalación, licencia, recursos humanos?

El día a día, "no consume prácticamente recursos, pero su implantación si exige un proceso previo de consultoría para ofrecer la información a la herramienta, en función de lo que queramos hacer con ella" respondió Fidel Pérez.

La herramienta ¿permite jugar con una pirámide de distintos objetivos?, ¿se puede contemplar dentro del mapa de riesgos poder agregar o desagregar?, preguntó Pablo Burgos, del Ministerio de Industria.

Según EMC, "éste es una de los principales puntos fuertes de la herramienta, la capacidad de agregación y desagregración, así como la vista a todos los niveles. Si nos limitamos a la gestión de riesgos, RSA Archer tiene dos métodos de trabajo para la creación del mapa de riesgos: una metodología de arriba abajo, que define cuales son los grandes objetivos y los riesgos que están asociados a sus incumplimientos; y otra metodología, de

abajo arriba, donde básicamente a través de campañas de entrevistas, encuestas y cuestionarios automáticos se evalúa el comportamiento de nuestros empleados con respecto al tema que nos preocupe".

Carlos Maza, del Ministerio de Industria, se refirió al potencial de estas herramientas "como escaparate de visibilidad de lo que se está haciendo en los departamentos de TI", así como "a la implicación que ello tiene para la organización". A la vez se interesó por conocer un ejemplo "de qué tipo de cuadro de mandos, relacionados con la gobernanza más que con riesgos, que se puede extraer con la herramienta para presentar a un nivel intermedio, como un Secretario de Estado, y que lo sienta como parte consustancial del negocio y de la actividad del ministerio y no como algo puramente técnico".

La herramienta permite "integrar en un único punto toda la información disponible, proporcionando un mapa o cuadro de mando en el que se puede tener visibilidad de indicadores de todo tipo, como por ejemplo, el número de acciones que está realizando el ciudadano, el crecimiento de la utilización de las páginas web, los procesos que fallan o no, las quejas... " Una de las soluciones empaquetas en la herramienta es "la gestión de incidentes, que te permite leer incidentes de múltiples dispositivos de seguridad y hacer una integración para presentar un estado de incidentes al nivel más alto y realizar las desagregaciones que se necesiten", expuso Pérez.

En el debate salío a colación el workflow, parte que podría utilizarse para mecanizar procesos de negocio de informes a la gerencia. Fidel Pérez recordó que "una parte muy importante de la herramienta es la automatización de los procesos de workflow o flujos de trabajo, lo que elimina una gran cantidad de esfuerzo y horas de trabajo".

Por último, Francisco Antón, cerró las intervenciones interesandos por "la inversión necesaria para implementar RSA Archer. A lo que Fidel Pérez respondió que "se dimensiona por usuarios de la herramienta y su inversión está por debajo de las decenas de miles de euros".

**Pablo Burgos**

**José Antonio García**

**Santiago Domínguez**

**Serafín Hernández**