PROCESOS DE SEGURIDAD ALINEADOS CON EL 'NEGOCIO': ADMINISTRACIÓN ELECTRÓNICA Y TECNOLOGÍAS DE CERTIFICACIÓN

Dentro del gobierno de las Tecnologías de la Información, la seguridad ha de convertirse en una actividad importante e integrada en él, como oportunidad de mejora de los procesos de negocio dando soporte a la integridad de la información, continuidad del negocio y protección de los activos de información.

Para ello, y mientras muchos nos hallamos en "construcción de la Seguridad", en diferentes caminos y estados de madurez, hacia una seguridad adecuadamente definida en la organización, luchamos por compaginar las oportunidades que nos brinda el negocio para impulsar la seguridad con la construcción de la Gestión de Seguridad.

He de constatar, antes de continuar, que el término "negocio", lo voy a utilizar como terminología general usada en seguridad, ya que en la administración, no es aplicable hablar de negocio, sino de Servicio Público.

Los elementos y factores que posibilitan el desarrollo de la construcción y el posicionamiento de la seguridad vienen dados por el Marco Legislativo, Política de Seguridad, Plan Director de Seguridad para la Construcción del Sistema de Gestión de Seguridad de la Información (SGSI) , Definición y gestión de los Servicios y Procesos de Seguridad…

Pero la realidad es que con frecuencia, la seguridad se impulsa cuando existen proyectos de seguridad que son de gran interés para *la dirección*/*el negocio* y cuando se participa en los Proyectos de Planes Estratégicos o Directores de Sistemas de Información.

En estas tesituras, y en el marco de la e-administración en que se ve involucrada la administración en general, tenemos la oportunidad de colaborar para prestar una mejora en el proceso de negocio. En estos momentos podemos considerar la e-administración como uno de los factores que dinamizan e impulsan la seguridad en la administración.

Es evidente que el marco regulatorio recientemente aprobado, impulsa el uso de las tecnologías de certificación, y abre los servicios de la administración al uso de estos medios:

- Legislación sobre Facturación electrónica: Orden EHA/962/2007, Orden PRE/2971/2007.
- Ley 30/2007 de Contratos del Sector Público.
- Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

En especial, la Ley de Acceso nos ofrece y facilita el camino para desarrollar la administración electrónica. Es una gran oportunidad para las administraciones que se hallan en el camino de mejorar sus procesos y procedimientos internos y las relaciones con los ciudadanos.

Un reto subyacente de la ley es proveer de los mecanismos necesarios para que la ciudadanía confíe en el e-acto administrativo al igual que confiaba en los actos clásicos soportados en papel. Es esta una ley muy garantista con la intención de generar confianza en el canal electrónico, donde de los 46 artículos que tiene la Ley, en 28 (un 60%) se referencia la identidad digital, firma electrónica o seguridad jurídica. Además, brinda el desarrollo de las técnicas y tecnologías criptográficas aplicadas a la seguridad de la información y procesos asociados a ella, como elemento de ayuda a la generación de la confianza suficiente que elimine o minimice los riesgos asociados a la utilización de tecnologías de la información.

> Para alinear la seguridad con el 'negocio', tenemos que proporcionar un marco o guía que ayude a establecer y tipificar los requisitos de seguridad de los procesos o trámites electrónicos. La transformación de la actividad administrativa a medios electrónicos ha de proporcionar las garantías y medidas de seguridad adecuadas y proporcionales a la naturaleza y circunstancias de los distintos trámites y actuaciones.

Pero todos conocemos el riesgo existente, cuando aparecen necesidades tecnológicas no aposentadas, de particularizar en cada proceso la implantación de toda una tecnología desarrollando desde el inicio toda su problemática, y de aplicar distintas soluciones para abordar un mismo problema. El "desparrame" de soluciones adoptadas nos llevan a no tener control de la seguridad de la información y a perder eficiencia.

Es muy importante alinear las necesidades de una administración en el uso de las tecnologías criptográficas. Las vías para conseguirlo son el desarrollo de normativas criptográficas que pauten las bases y el uso de estas tecnologías criptográficas, la definición de una arquitectura única para las funciones asociadas a la identificación, la firma y el documento digital, y la participación en proyectos de Planes Globales de Administración electrónica, desarrollando los siguientes aspectos:

Normas de Seguridad de la Información

Lo que se puede aportar en primera instancia, es la generación de las normas y procedimientos criptográficos para evitar la diversidad de criterios aplicados en la organización. Las Normas, han de ir dirigidas en dos caminos:

– En base a los controles que desarrolla la ISO 17799, pero extendidas a la realidad criptográfica:

- Pautas base de generación, gestión, custodia y uso de claves y certificados digitales.
- Pautas de cifrado.
- Pautas de firma digital, estándares y uso en la organización.
- Pautas de identidad digital y representación, estándares y uso en la organización.
- Pautas del documento electrónico (formatos, metadatos, política de preservación,...).
- Pautas de generación de evidencias electrónicas.
- Pautas para la interoperatividad.

– En base a la seguridad del trámite y proceso:

Para alinear la seguridad con el negocio, tenemos que proporcionar un marco o guía que ayude a establecer y tipificar los requisitos de seguridad de los procesos o trámites electrónicos. La transformación de la actividad administrativa a medios electrónicos ha de proporcionar las garantías y medidas de seguridad adecuadas y proporcionales a la naturaleza y circunstancias de los distintos trámites y actuaciones. De acuerdo y alineado con los responsables de estos procesos en la organización, esta guía ha de incorporar las consideraciones a tener en cuenta para conseguirlo.

Arquitectura común

Hay que desarrollar plataformas centrales y comunes para toda la organización donde se realicen las acciones básicas asociadas a la identidad, firma y documento electrónico sobre los que se apoyen los componentes de administración electrónica, los tramites y procedimientos, siempre diferenciadas de los procesos de la administración electrónica:

La firma electrónica, validación de certificados y de firmas electrónicas, sellado de tiempo, almacenamiento y gestión de certificados digitales y claves privadas en red, digitalización segura de documentos en papel, impresión segura de documentos digitalizados, firmas automatizadas, portafirmas, sistema de trazabilidad, gestión de *logs* y evidencias, aprovisionamiento y gestión del ciclo de vida de los certificados digitales, custodia y preservación del documento y el expediente electrónico, cifrado de información, gestión de la publicación de documentos a la sede electrónica...

Estas funciones se han de proporcionar mediante productos, herramientas o desarrollos a medida y siempre usando funciones que actualmente ya proporcionan agentes externos (Catcert/RED.es,...). Los departamentos de arquitectura y desarrollo tendrán que abastecer, en base a requerimientos de seguridad, de desarrollos completos e integraciones de productos y de proveedores externos de servicios de certificación.

Procesos de Seguridad

En el camino hacia la gestión de la seguridad en que muchos nos encontramos, hemos de definir líneas de actuación de seguridad que hagan visible, de forma sencilla a modo de eslogan, las actuaciones de seguridad encaminadas a alinearse con los intereses de la organización. Una de ellas es, sin duda, la relativa a las técnicas y tecnologías aplicadas a la seguridad de la información: criptografía y procesos asociados a ella.

> Se requiere habilidad para combinar las urgencias del desarrollo e implantación del plan estratégico para la administración electrónica con las fases de implantación de las funciones a cubrir, y tecnologías asociadas a criptografía, certificación y firmas digitales.

Plan Estratégico de Sistemas de Información

Es necesaria una visión estratégica adecuada, un interés a nivel de organización para desarrollar la administración electrónica, a través de iniciativas y planes estratégicos, y éstos han de contemplar la seguridad para prevenir de los riesgos existentes en la utilización de los nuevos medios y tecnologías.

Se requiere habilidad para combinar las urgencias del desarrollo e implantación del plan estratégico para la administración electrónica con las fases de implantación de las funciones a cubrir, y tecnologías asociadas a criptografía, certificación y firmas digitales.

Es clave coordinar bien las implantaciones de funcionalidades básicas asociadas a la identificación y firma digital según el plan de implantación de la administración electrónica, así como definir fases de implantación a abordar. Convencer de la importancia de esto es nuestro trabajo.

> Nuestras visiones de seguridad, nuestra idea de cómo ha de ser, no siempre concuerda ni puede imponerse en una organización de repente. Debemos aprovechar las inquietudes del negocio para alinearnos con él, y crear sinergias luego de los proyectos en la gestión de la seguridad.

Conclusiones

Nuestras visiones de la seguridad, nuestra idea de cómo ha de ser ésta, no siempre concuerda ni puede imponerse en una organización de repente.

Debemos aprovechar las inquietudes del negocio para alinearnos con él, y crear sinergias luego de los proyectos en la gestión de la seguridad. Así, la administración electrónica si es estratégica para una Administración, nos posibilita adquirir seguridad en los activos de información estableciendo en diversos puntos criterios y buenas prácticas de seguridad, a través de normativas y arquitecturas razonables. ■

Neus Bellavista Arimany
Responsable de Seguridad
Institut Municipal d'Informatica
AYUNTAMIENTO DE BARCELONA