Ciberseguridad de los Datos

Proyecto de Seguridad Centrada en el Dato

ÍNDICE

Descripción del Proyecto

El proyecto de seguridad centrado en el dato de la administración del Principado de Asturias posee una serie de componentes mixtos que pretenden una evolución no sólo técnica, sino más allá organizativa y cultural. Así mismo no es posible asociarlo a un único proyecto individual y contratación, sino que posee repercusiones cruzadas entre diversas actuaciones que se centralizan en el Servicio de Seguridad, Datos e Inteligencia Artificial como director del proceso. Aun así el peso organizativo y de compromiso de alto nivel es crucial para definir este proyecto de modo global.

El origen del modelo de trabajo es incorporar el dato como activo unitario de referencia, para que tomado de partida, realizar la dotación adecuada de seguridad ante cualquier incorporación o modificación del mismo. Esta propuesta surge de una evolución natural. Por Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia del Principado de Asturias dentro de su Dirección General de Sector Público, Seguridad y Estrategia Digital se asigna la responsabilidad de la ciberserguridad dentro de su Servicio de Seguridad.

La descripción de sus atribuciones incluye: *"El Servicio de Seguridad ejerce las funciones de dirección, diseño, desarrollo, implantación y mantenimiento de los programas y políticas de seguridad en materia de sistemas de información para todos los ámbitos de la Administración del Principado de Asturias. Le corresponde el control de riesgos en sistemas de información, la puesta en marcha de medidas correctivas para su reducción, así como la redacción y seguimiento del cumplimiento de normativas y estándares que se desarrollen en materia de tecnologías de la información y comunicaciones"*.

Posteriormente en el Decreto 35/2020, de 2 de julio, de primera modificación del Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica

básica de la Consejería de Presidencia, varía las atribuciones del Servicio de Seguridad y Datos. Destacar entre las variaciones específicas de nuevas atribuciones del Servicio donde incorpora:

"*Se encarga de definir la arquitectura de bases de datos más adecuada a la política de gestión del dato en el Principado de Asturias y establece los modelos de normalización y eficiencia en el almacenamiento de los datos de todos los ámbitos de la Administración del Principado de Asturias. Asimismo, genera los cuadros de mando necesarios para dar respuesta a las necesidades de gestión y diseña las políticas de explotación de los datos*".

Es ya con esta modificación de estructura en la que se unen en el mismo Servicio todas aquellas atribuciones relativas a ciberseguridad junto a la de gestión del dato, y es en este momento cuando se identifica la capacidad estratégica de coordinar la seguridad del dato unificada y optimizada durante todo el ciclo de vida en lo que respecta a Ciberseguridad, Seguridad del Dato y Protección del Dato con una visión integrada. Es destacable además la simplificación que se identifica para integrar operativamente las diferentes normativas que aplican de modo práctico, así como ser ágiles ante las evoluciones que se esperan.

Esta situación es la que permite consolidar la idea de abordar una apuesta de trabajo mediante un proyecto que ordene, planifique y centralice el objetivo de una seguridad centrada en el dato y que sirva de acelerante en la propia optimización en Ciberseguridad.

La línea de trabajo se ha visto reforzada una vez más organizativamente en el Decreto 73/2023, de 18 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia, Reto Demográfico, Igualdad y Turismo. En el mismo se establece un refuerzo de una Dirección General Tecnológica, la Dirección General de Estrategia Digital e Inteligencia Artificial en la que su Servicio de Seguridad y Datos evoluciona al Servicio de Seguridad, Datos e Inteligencia Artificial.

Este servicio posee en esta norma entre otras las siguientes atribuciones "*1. El Servicio de Seguridad, Datos e Inteligencia Artificial ejerce las funciones de dirección, diseño,*

desarrollo, implantación y mantenimiento de los programas y políticas de seguridad en materia de sistemas de información para todos los ámbitos de la Administración del Principado de Asturias.

Le corresponde el control de riesgos en sistemas de información, la puesta en marcha de medidas correctivas para su reducción, así como la redacción y seguimiento del cumplimiento de normativas y estándares que se desarrollen en materia de tecnologías de la información y comunicaciones. Asimismo, es el responsable de la actualización y aplicación de los procedimientos, procesos y metodologías que aseguren la calidad, tanto de los productos como de los servicios que se presten.

2. Además se encarga de definir la arquitectura de bases de datos más adecuada a la política de gestión del dato en la Administración del Principado de Asturias y establece los modelos de normalización y eficiencia en el almacenamiento de los datos de todos los ámbitos de la Administración del Principado de Asturias desarrollando estrategias que fomenten la economía del dato. Asimismo, genera los cuadros de mando necesarios para dar respuesta a las necesidades de gestión y diseña las políticas de explotación de los datos, junto con los mecanismos de automatización y robotización".

En este entorno es el que confirma esta apuesta de seguridad centrada en el dato, y no solo en el dato estático, sino en su vertiente incluso generativa unida en un Servicio unitario a la Seguridad.

El objetivo del proyecto es la dotación de procedimientos, medios de gestión, herramientas y prácticas para que toda actuación sobre el dato esté asociada y sea disparador de las acciones a nivel de seguridad que desde su partida se precisen. Utilizando la incorporación y evolución prevista de la Oficina del Dato, y su uso posterior a nivel de Inteligencia Artificial se inicia la capacidad de que con el inicio de cada actuación esta posea de modo natural y controlado todas las garantías, evaluaciones y medias de seguridad que se precisen en función de su uso de modo integrado.

En diversas ocasiones por evolución o ante la actualización de sistemas obsoletos es cuando se produce su evaluación integral a efectos de seguridad, sobre todo en la vigente dado el carácter dinámico de la misma, en vez de ser abordado en un inicio como parte y mantenido, produciendo ineficiencias y dificultades para asociar las medidas correspondientes de seguridad una vez tomadas decisiones técnicas frente a hacerlo de inicio. Mediante este proyecto se pretende que la Oficina del Dato y todo su funcionamiento integre la seguridad de modo nativo e inmediato, siendo por

tanto un disparador de la seguridad añadido a los ya vigentes de ciberinteligencia, certificación de sistemas, gestión de riesgos, vulnerabilidades, normativa, etc. El carácter dinámico y continuo de las actuaciones sobre el Dato que recibirá una Oficina del Dato supone el punto de engarce perfecto para su aplicación.

Existen diversos marcos de referencia y normativas que incluyen cuestiones de seguridad en el marco de los datos Dmbok, Normas Une, etc, que forman parte del cuerpo organizativo de las Oficinas del Dato pero que podrían no llegar a recoger la complejidad que supone la seguridad en el entorno público a nivel normativo unido a unos únicos recursos tecnológicos. La adaptación directa a la organización y la partición directa de seguridad en los procesos correspondientes del dato se considera una opción con un gran recorrido de eficiencia y mejora de resultados.

Repercusión para el ciudadano y las Administraciones

La repercusión a nivel general es la incorporación y verificación de Ciberseguridad que se asocia ante cualquier incorporación de datos o modificación de los modelos existentes, lanzando de modo inmediato la revisión y dotación de los modelos adecuados.

Es por tanto una mejora de los servicios y calidad de los mismos dado que la Ciberseguridad y sus medidas no deben ser entendidas como una disciplina estanca, sino como los facilitadores internos que asocian un servicio de calidad, seguro, eficiente y resiliente entre otros.

Equipo de desarrollo y proveedores

El equipo de Desarrollo participante es el compuesto por el equipo del Dato y Seguridad, mediante un coordinador con alta experiencia en diversos sectores, así

como un equipo de cuatro miembros altamente especializados en disciplinas que recogen desde las bases de datos, a analítica y modelos de reporting, como de seguridad a nivel de análisis de riesgos, cibervigilancia y cumplimiento normativo.

A nivel de proveedores el soporte principal lo supone el lote de Seguridad del CGSI, Centro de Gestión de Sistemas de Información que da soporte al funcionamiento básico de tecnología. Dentro de este se encuentra el equipo especializado de Consultoría, Analítica y Cumplimiento Normativo, que recoge la gestión, procedimientos y organización necesaria para obtener los niveles de seguridad requeridos. Este equipo guía la evolución de los restantes equipos especializados de ciberinteligencia, gestión de incidentes, gestión de vulnerabilidades y gestión de equipos de seguridad, todos ellos coordinados por un gestor único interlocutor.

Esta contratación ha sido adjudicada al proveedor Telefónica.

Valoración económica

Este proyecto está asociado dentro de los trabajos de cobertura de Ciberseguridad, un pliego con valor económico de casi 6 M de Euros sin Iva en un periodo de cuatro años, de los cuales serían imputables a este proyecto específico 300.000 Euros en nueve meses.

Así mismo posee relación con el pliego de la Oficina del Dato en cuanto al equipo que construye la visión completa de la implantación de la misma y en la que figura la seguridad como un elemento de integración que será el objeto procedimental de integración y adaptación a este nuevo modo de trabajo. El modelo organizativo objetivo pretende la integración de ambas especialidades en trabajos para mantenimiento de la seguridad del dato. Este último pliego posee un valor económico

de poco más de 900.000 Euros en un año y que se encuentra en situación ya avanzada.

Plazos de cumplimiento

La Oficina del Dato y su implantación posee un plazo de un año de implantación, actualmente cercana a su finalización y donde se recogen los procedimientos de seguridad a asociar a la misma. Los trabajos reales de seguridad centrada en el dato se encuentran en su fase inicial de conformado y definición específica con un plazo estimado de 9 meses, coordinados con el resto de objetivos del equipo durante el mismo, con el objetivo que tras su finalización y prueba piloto se pueda incorporar en el funcionamiento natural de la Oficina del Dato como producto del proyecto de Seguridad centrada en el Dato.