Caso de éxito

La Universidad de Sevilla garantiza la continuidad de sus activos tecnológicos

www.abast.es

La Universidad de Sevilla es una institución pública de educación superior e investigación con un Campus global constituido por más de 25 centros, propios y adscritos, y con una amplia oferta formativa que incluye más de 150 títulos, 77 grados y dobles grados, y 81 másteres oficiales. Ha confiado en el equipo de consultoría y auditoría de ABAST para desarrollar un Plan de Contingencia orientado a la continuidad de sus activos tecnológicos, garantizando así la protección de la información considerada como crítica y, a la vez, generando la capacidad operativa necesaria para minimizar el impacto de un hipotético desastre que los afectara.

Antecedentes

El Servicio de Informática y Comunicaciones (S.I.C) de la Universidad de Sevilla ofrece un amplio catálogo de servicios tecnológicos de soporte e infraestructura orientados a las principales actividades del organismo: docencia, investigación, gestión y administración. La apuesta tecnológica de la Universidad de Sevilla, acorde a su posición destacada en el ranking de Universidades españolas, requería asegurar, no sólo la continuidad de estas operaciones, sino también la información que se genera en cada uno de estos ámbitos, al constituir su activo de mayor valor.

El proyecto

Creación de una CMDB

Debido a la necesidad de constituir un repositorio de datos unificado, el proyecto se inició con la creación de una CMDB única para todo el S.I.C. Una vez seleccionado el producto OneCMDB, se trabajó conjuntamente en el establecimiento y definición de los elementos de configuración (CI) que formarían parte de esta CMDB, y en las categorías que constituirían el detalle de los mismos. A partir de la carga inicial, este repositorio sería utilizado como base para el posterior poblamiento de la herramienta EAR/PILAR en la fase de análisis de riesgo dentro del proyecto de continuidad.

Análisis de Impacto (BIA)

Constituida la CMDB, se partió de la revisión de la documentación existente y de la información obtenida mediante entrevistas con miembros del S.I.C para identificar los principales procesos de negocio de la Universidad de Sevilla, los servicios de TI que los soportan y sus dependencias, estableciendo un catálogo definido de servicios de TI agrupados por categorías y por ámbito de aplicación. A continuación se estimó su impacto hipotético a partir del uso potencial que de ellos realiza cada colectivo y se determinó, para cada uno de ellos, sus respectivos tiempos objetivos de recuperación (RTO y RPO). Estos valores establecen los requisitos de continuidad para los sistemas de información de la U. de Sevilla.

Análisis de riesgos

Con los datos de la fase anterior se elaboró un análisis detallado de riesgos utilizando, como aproximación metódica para determinar el riesgo, la herramienta EAR/PILAR (metodología MAGERIT). Los resultados de este análisis ofrecieron una "instantánea" de la situación actual y pusieron de manifiesto aquellos ámbitos de mejora en los que se debe hacer foco, todo ello enmarcado en un sistema de gestión que facilita el seguimiento y gestión del riesgo de forma continua.

Una de las acciones de mejora más destacadas que se llevaron a cabo a partir de los resultados de este análisis fue la adecuación del actual CPD.

Estrategias de recuperación

Conjuntamente con el equipo técnico de ABAST, el siguiente paso se orientó a definir, a alto nivel, qué estrategias tecnológicas debería implantar la Universidad de Sevilla para asegurar los requisitos de continuidad identificados en las fases anteriores. Para ello se identificaron aquellas estrategias preventivas y paliativas que servirían para cumplir con los objetivos propuestos de la forma más óptima y eficiente posible, teniendo en cuenta también la diversidad de la infraestructura existente. Así se propuso un escenario futuro para implantar una serie de medidas técnicas y organizativas a corto, medio y largo plazo que garantizan la protección de los activos de la organización.

Plan de recuperación ante desastres

Con el objetivo de establecer un plan operativo para hacer frente a los diversos escenarios de desastres, se generó el denominado Plan de Recuperación ante Desastres. En él se detallan claramente las actividades a realizar, las funciones y obligaciones del personal implicado y el plan de comunicación. Todo ello consigue que la organización trabaje de forma coordinada y eficiente para la recuperación los activos.

Beneficios

Con la realización del proyecto, la Universidad de Sevilla ofrece a sus distintos colectivos los medios necesarios para asegurar el desarrollo de su actividad en un entorno seguro, garantizando tanto la protección de sus datos como de la tecnología que los explota (HW y SW). Se asegura, de este modo, que en caso de desastre dispone de los mecanismos, procedimientos y organización necesarios para mitigar su potencial impacto, entendiendo como tal no sólo las posibles pérdidas económicas y de imagen derivadas, sino también la pérdida del esfuerzo docente e investigador que le otorga su actual prestigio.

Universidad de Sevilla

La Universidad de Sevilla es una institución pública de educación superior e investigación que cuenta con una comunidad universitaria formada por más de 70.000 estudiantes, 4.400 profesores y 2.400 profesionales de la administración y servicios.

El Campus global está constituido por 25 centros propios y otros centros adscritos que se distribuyen por la ciudad de Sevilla.

ABAST – Área de Seguridad TI

ABAST cuenta con un área especializada que ofrece posiblemente uno de los portfolios de servicios y soluciones de Seguridad TI más completo del mercado español, pues cubre todos los aspectos relacionados con infraestructura de seguridad TI, continuidad y disponibilidad, auditoría y control, y gobierno de la seguridad TI.

Aportamos una gran experiencia en la realización de planes de contingencia de TI, planes de continuidad del negocio y planes directores de seguridad; en auditorías y consultorías relacionadas con ISO2700X, LOPD, ENS y otros estándares o regulaciones; y en auditorías de seguridad basadas en test de intrusión (hacking ético).

Por otro lado, nuestras alianzas con los fabricantes líderes nos permiten ofrecerle las soluciones más avanzadas de seguridad. Una extensa gama de soluciones de extremo a extremo que dan respuesta a las amenazas de seguridad en los ámbitos de endpoint, red, aplicaciones, datos y personas, así como la gestión de la infraestructura de seguridad TI.

Estos servicios y soluciones podemos ofrecérselos también como servicio gestionado bajo el concepto de Oficina de Seguridad.

Para más información:
seguridad@abast.es

abast
www.abast.es · info@abast.es

Tel. 933 666 900
Fax 933 666 910
Carrer Equador 39-45
08029 Barcelona

Tel. 914 061 601
Fax 914 061 604
Calle de la Basílica 19, 9° B
28020 Madrid

Tel. 97 170 68 82
Calle Fluviá 1, Bajos dcha.
Despacho 25 (Son Fuster)
07009 Palma de Mallorca