24 de Julio de 2018

CONVOCATORIA PARA EL INGRESO EN LA ESCALA DE GESTIÓN DE SISTEMAS E INFORMÁTICA, DE LA UNIVERSIDAD PABLO DE OLAVIDE DE SEVILLA

(Resolución de 21 de noviembre de 2017- BOE 227 de 27 de Noviembre de 2017)

SEGUNDO EJERCICIO

NO ABRA ESTE CUADERNILLO HASTA QUE SE LE INDIQUE.

SUPUESTO PRÁCTICO 1

Una conocida Universidad española ha sufrido recientemente un episodio que ha alcanzado una notable atención mediática, relacionada con la presunta intervención de un empleado en un caso de publicación de datos personales. El trabajador interino en cuestión, perteneciente al Área de Estadística y Gestión Operativa, había sido cesado con anterioridad, pero esta circunstancia no había sido trasladada con la suficiente agilidad a las aplicaciones de gestión, a las que el trabajador pudo seguir accediendo días después de su cese. Esta circunstancia permitió que, utilizando una VPN que tenía configurada en casa (convenientemente autorizada al estar inscrito en un programa piloto para la implantación del Teletrabajo aún vigente), extrajera datos de las aplicaciones de gestión para finalizar un trabajo pendiente, haciendo uso de sus privilegios de acceso y almacenando los datos en su ordenador personal. El ordenador ha sido atacado por un software malicioso y, como resultado, los datos personales de numerosos estudiantes, junto con sus calificaciones y sus direcciones postales, han sido publicados en un portal web de acceso público, al ser una de las alumnas hija de un alto cargo del gobierno de la comunidad autónoma.

Este desagradable episodio ha provocado, además de un notorio deterioro de la imagen de la Universidad, un intenso debate interno que ha puesto de manifiesto la debilidad del proceso de gestión de identidades y, en particular, el control de acceso a las aplicaciones de la institución. En este debate han quedado en entredicho tanto el Servicio de Informática, como los gestores encargados de trasladar a los sistemas informáticos la información de ingreso, cese, matriculación, anulaciones, nuevas contrataciones, así como los órganos de gestión de la política informática de la institución, que priorizaron proyectos tecnológicos de más visibilidad, desatendiendo proyectos de seguridad que podrían haber evitado el problema suscitado, o reducido su impacto.

Como consecuencia, la Rectora de la Universidad, una vez apagados los ecos de la noticia, ha solicitado al Gerente y al Vicerrector de Transformación Digital una atención prioritaria a la revisión de estos sistemas de gestión.

Es Vd. el responsable de organizar el sistema de gestión de la identidad corporativa para el acceso a los recursos electrónicos (tanto aplicaciones como otros servicios que puedan requerir autenticación previa y/o gestión de privilegios).

El sistema deberá tener en cuenta, al menos, los siguientes requisitos:

R1: **COLECTIVOS**. La Universidad cuenta con una comunidad de usuarios variable, formada por diversos colectivos con distintas necesidades de acceso a recursos electrónicos. Por simplificar, convendremos los siguientes:

- Personal de Administración y Servicios (de carácter permanente y eventual)
- Personal Docente e Investigador (de carácter permanente y eventual).
- Estudiantes de Grado, Postgrado, Doctorado y Formación Permanente (la vinculación de los estudiantes con la Universidad es de duración variable, según la duración de los estudios).

- Otros (empresas colaboradoras que prestan sus servicios en el campus, becarios). Con una vinculación de otra naturaleza, pero que les habilita para el uso de determinados servicios electrónicos.

Una misma persona puede pertenecer a más de un colectivo simultáneamente. Por ejemplo, un miembro del PAS podría ser también estudiante.

R2: **AUTORIZACIÓN**. En razón del cargo que la persona ocupe en el organigrama de la institución, o del colectivo al que pertenezca, una persona puede también tener acceso a una aplicación o servicio concreto. Por ejemplo, el sistema Portafirmas es accesible a todos los cargos de gobierno (Gerente, Rectora, Vicerrectores y Vicerrectoras, etc..), cualquier estudiante tiene acceso a un servicio de consulta de expediente, y cualquier miembro del colectivo PAS o del PDI tiene acceso a un servicio de consulta de nómina.

Una persona puede tener autorización para acceder a una aplicación en razón de su puesto de trabajo, para cumplir las funciones encomendadas por la Universidad.

También se conceden autorizaciones nominales (que no dependen del colectivo o del cargo; están dirigidas a personas concretas). Ej: Carmelo Cotón tiene acceso a la aplicación de mantenimiento de salas en razón de un trabajo autorizado para la medición del rendimiento del equipamiento audiovisual.

R3: No todas las aplicaciones tienen posibilidad de controlar la AUTORIZACIÓN internamente. En estos casos, la autorización debe controlarse de forma externa.

R4: AUTENTICACIÓN Las aplicaciones y servicios electrónicos universitarios pueden clasificarse (desde el punto de vista de las necesidades de autenticación) en los siguientes bloques:

- Aplicaciones o servicios públicos (sin necesidad de autenticación).
- Aplicaciones o servicios sin posibilidad de delegación de autenticación (dispone de bases de datos o tablas internas con las credenciales de acceso).
- Aplicaciones o servicios con posibilidad de delegación de autenticación LDAP.
- Aplicaciones o servicios con posibilidad de delegación de autenticación basada en servidores especializados (basados en aserciones u otros: SAML2, CAS, etc.).

R5: **PERFILES DE ACCESO**. Para completar el ejercicio considere que las aplicaciones NO tienen perfiles de acceso. Es decir, todos los autorizados a acceder a una aplicación disponen de los mismos privilegios en dicha aplicación y pueden, por tanto, acceder y gestionar la misma información.

APARTADO UNO. Diseñe un diagrama entidad-relación que describa la realidad planteada.

APARTADO DOS: Suponga el siguiente requisito adicional:

R6: Buena parte de los servicios y aplicaciones que requieren control de acceso se encuentran dentro del alcance de cobertura del Esquema Nacional de Seguridad (ENS), y están categorizados como de nivel MEDIO.

Ha adoptado usted la decisión de almacenar de forma centralizada todas las operaciones de AUTENTICACIÓN en las aplicaciones y servicios electrónicos para cumplir los requisitos que exige el ENS.

Enumere los campos que formarían parte de dicho registro de operaciones; descríbalos BREVEMENTE indicando su función; describa una (sólo una) de las actividades que, de forma obligatoria, debe realizar sobre el fichero o ficheros que contenga(n) los registros de operaciones de acuerdo con el nivel de protección que se exige.

APARTADO TRES:

R7: Para evitar que los usuarios deban recordar un número excesivo de pares "usuario/contraseña", se pretende utilizar un sistema de login único.

A) Dibuje un diagrama con los componentes de un Sistema de Gestión de Identidad que resuelva los requisitos R1 a R7. Dibuje sus relaciones. Describa los componentes brevemente. No es preciso que descienda al nivel hardware ni proposiciones de software concreto.

   Puede enriquecer la solución con componentes que no estén directamente orientados a satisfacer los requisitos comentados, pero siempre que estén relacionados con la gestión de la identidad en un ámbito corporativo.

B) Describa una de las formas de resolver el requisito R3.

C) Explique qué componentes o funciones debemos perfeccionar y atender con rigurosidad para mitigar el riesgo de que pueda suceder de nuevo el incidente descrito en el primer párrafo de este supuesto.

APARTADO CUATRO:

Se plantea la siguiente cuestión: las Pruebas de Evaluación de Bachillerato para el Acceso a la Universidad (PEvAU) se celebrarán dentro de dos meses en la Universidad y este año la Tarjeta Oficial de Calificaciones quiere distribuirse electrónicamente.

Le proponen incluir a los estudiantes que deben hacer la prueba en su Universidad, como un colectivo adicional en su Sistema de Gestión de Identidad (ver requisito R1), propuesta a la que usted se niega al valorar las ventajas y desventajas técnicas.

Su negativa provoca que los participantes en la PEvAU no puedan disfrutar del procedimiento de reparto de credenciales que tiene diseñado para s

u Universidad, credenciales que son indispensables para que los estudiantes accedan al servicio electrónico preparado para el acceso a su tarjeta.

Diseñe un sistema para el reparto de credenciales a los estudiantes de la PEvAU que considere, al menos, una vía de reparto no presencial. Suponga que dispone de los datos básicos de identificación de los todos alumnos, y de la mayoría de los teléfonos y direcciones de correo electrónico personal.

Realice cuantas suposiciones adicionales necesite para realizar este supuesto.

SUPUESTO PRÁCTICO 2

La Universidad va a realizar una convocatoria de formación para su personal, tanto PDI como PAS. Para poder realizarla su personal debe rellenar un formulario en el portal del usuario, solicitando los cursos que desea hacer.

El personal debe indicar un orden de preferencia de los mismos y la Universidad pondrá un límite de cursos a solicitar (por ejemplo, podrán solicitar un máximo de 10 cursos) y un límite de horas de los mismos a realizar (por ejemplo, un límite de 50 horas de cursos por solicitante).

Los cursos ofertados tendrán entre sus características unas horas de impartición, su tipología, si son presenciales, virtuales o mixtos y el personal que tendrá preferencia para recibirlos.

Finalmente, considere que estos cursos tendrán un coste asociado a los mismos que tendrán que sufragar las personas que se apunten a los mismos, teniendo en cuenta que las personas que sean familia numerosa tendrán una exención de pago consistente en un 50 % del precio del curso.

Se pide que se diseñe un aplicativo que realice la inscripción a los cursos; esta aplicación consistirá en un formulario que recogerá los datos personales del inscrito una vez identificado, así como los cursos que desea realizar; la asignación de los cursos a realizar ponderando tiempo trabajado, escala / grupo y nivel; también indicará una forma de pago de estos cursos una vez asignados.

Se pide que realice lo siguiente:

1) Proponga cómo se va a realizar la autenticación del inscrito a los cursos, teniendo en cuenta que la universidad tiene un sistema de gestión de identidad donde consta todo su personal.
2) Realice un diseño del esquema de datos a utilizar.
3) Realice un diseño estructurado del programa, utilizando diagramas de flujo, pseudocódigo, lenguaje natural o cualquier otra técnica de diseño.
4) Una vez que se ponga en producción esta aplicación, como gestiona datos personales a través de un formulario web de recogida de información que se almacena y se trata en una base de datos interna, y para evitar la ejecución remota de código, el acceso indebido o cualquier otro ataque al aplicativo o los datos, describa brevemente cinco de los riesgos más críticos que deben ser revisados antes de entrar en producción y sus consecuencias.

Para realizar este supuesto puede contar con:

- Se tiene acceso al sistema de gestión de identidad de la Universidad.
- Se tiene acceso a la base de datos de recursos humanos de la Universidad.
- Se tiene acceso a una pasarela de pago online.
- Para la comprobación de la condición de familia numerosa, se tiene acceso a un webservice de la Junta de Andalucía donde se indica este aspecto de una persona.

Realice cuantas suposiciones necesite adicionales a este enunciado para realizar la resolución del supuesto.