Seguretat de base de dades Versió Sprint 2.0

VIA – Vilanova Intelligent Airport

Index

Introducció:

Aquest informe especifica els requeriments de seguretat aplicables a la base de dades del projecte VIA – Vilanova Intelligent Airport (PTIN 19-2020). Queda obert a millores i suggerències per part del client empresarial, client tècnic, assessor metodològic i qualsevol altre membre dels equips del terminal 1

Actual: sprint 2.0 (-/04/2020)
Anteriors: sprint 1.0
Actualitzacions:

- Actualment la base de dades en un hosting AWS a la espera de un hosting definitiu
- S'han afegit a la tabla **Pasajeros** els camps *nom* i *password*

Consensuat:

- ❏ Usuaris
- ❏ Política de generació de contrasenyes
- ❏ Política general de la base de dades

Validat:

- ➢ Usuaris [pendent d'implementar]
- ➢ Política de generació de contrasenyes [pendent d'implementar]
- ➢ Política general de la base de dades [pendent d'implementar]

Usuaris:

Administrador de la base de dades:
És el que administra la BBDD en la seva totalitat amb dret a crear, borrar objectes i modificar a més pot concedir privilegis a altres usuaris (personal amb autorització) sobre els objectes que ha creat.

El admin del BBDD generarà els usuaris i contrasenyes del personal amb autorització i d'alta autorització a petició i/o autorització del responsable de RRHH (en el nostre cas, Responsable de Seguretat de BBDD de l'equip A1)

Nom d'admin: admin_VG_Aeroport@27BBDD (arbitrari)
Contrasenya: xxx (15 caràcters)

Política de generació de contrasenyes:
Les contrasenyes han de tenir almenys 15 caràcters, combinant lletres, números i símbols
No usar paraules reals, encara que estiguin a l'inrevés.
No es poden incloure dades obvies com el nom, data de naixement, etc.

Rols-usuaris de la base de dades(inf. proporcionada per l'equip A4):
Personal d'alta autorització: usuari amb dret a consultar i/o actualitzar, sense dret a crear o borrar objectes. (Pendent de consensuar)

Personal amb autorització: usuari amb dret a consultar i sense dret a crear o borrar objectes. (Pendent de consensuar)

Política general de la base de dades:
Accés per defecte: sense accés
Revisió permanent: modificació de contrasenyes cada mes per motius de seguretat
Física: accés a l'equip només per l'admin de la BBDD
SGBD: Identificació i autenticació (format)
.Usuari: nom.cognom1
.Contrasenya: xxx (15 caràcters) seguir política de generació de contrasenyes descrita prèviament

Annex: documentació rebuda per part de l'equip responsable A4

Sprint 1:

--FeedBack de la versió 1:
Usuaris:

Administrador de la base de dades:Ok
Política de generació de contrasenyes:Ok
Rols-usuaris de la base de dades(inf. proporcionada per l'equip A4):

¿A que haceis referencia con "personal de alta autorización" o con "personal con autorización"?
Política general de la base de dades: Ok a tot
Política de les còpies de seguretat BackUps: Excesiva, si lo hacemos con AWS ya tiene amazon copias más que suficientes.
Infraestructura requerida: No es responsabilidad nuestra hablar acerca de la infraestructura.
Privacitat(Informació confidencial de dades personals): Nosotros teníamos planeado hacer las notificaciones a los usuarios, pero esto es una notificación a un responsable. ¿Podrías especificar más a que os referis con este apartado?
Pla de contingència de BackUp: No es responsabilidad nuestra hablar acerca de la infraestructura.
Punts a revisar al realitzar el Pla de Contingència de Backup: No es responsabilidad nuestra hablar acerca de la infraestructura.

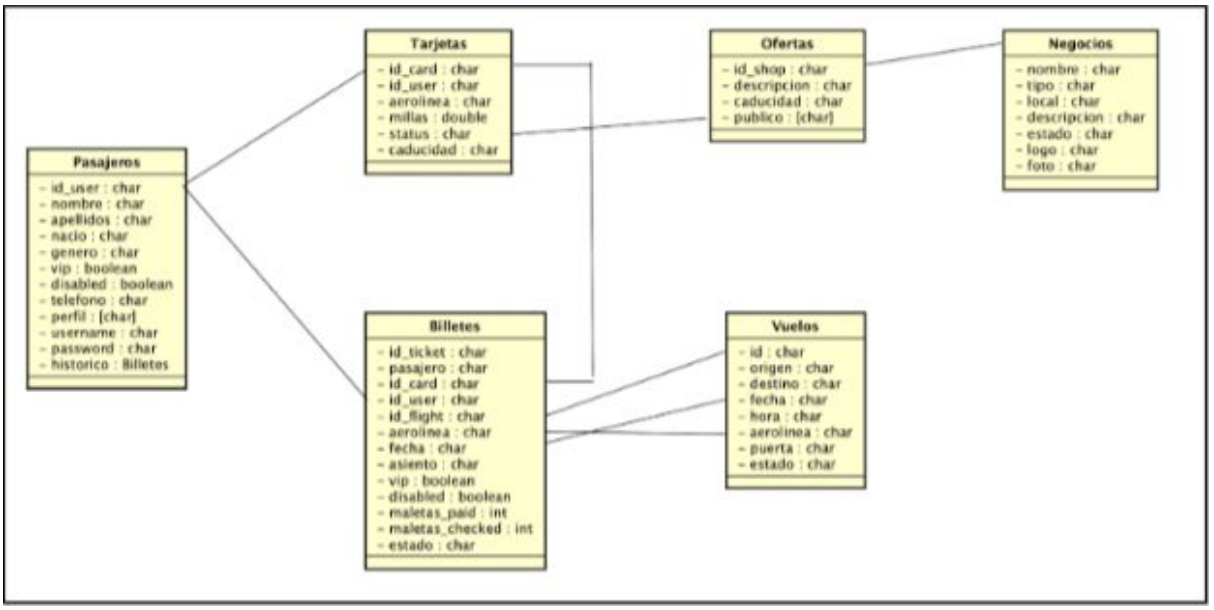
-Resposta:
"Privacitat(Informació confidencial de dades personals): Nosotros teníamos planeado hacer las notificaciones a los usuarios, pero esto es una notificación a un responsable. ¿Podrías especificar más a que os referis con este apartado?"
Me refiero a las notificaciones requeridas a un hipotético responsable designado por la administración del aeropuerto, externo al equipo informático, experto en LOPD y

responsable de todos estos asuntos. Esta figura es un requerimiento y una obligación por ley.
"¿A que haceis referencia con “personal de alta autorización” o con “personal con autorización”?"
Es la definición dada por vosotros mismos en el formulario del sprint 0 y confirmado en el formulario del sprint 1

--Formulari contestat:
·Definició de les característiques de la Base de dades i resum de la seva funcionalitat.(si n’hi ha de noves i/o diferents del sprint 0)
Base de dades:
·Definició de les característiques de la Base de dades i resum de la seva funcionalitat.
La base de dades és de tipus nosql i estarà basada en el SGBD Mongo DB. No tenim informació d’on estarà el hosting del SGDB. Guardarà informació dels passatgers, tendes, vols, restaurants, ofertes i altres necessitats que puguin sortir durant el desenvolupament
.
·Quines tecnologies heu utilitzat? (si n’hi ha de noves i/o diferents del sprint 0)
SGBD Mongo DB, hosting actual AWS a la espera de un hosting definitiu
·On creieu que farà falta seguretat en la base de dades? Heu començat a treballar en ella? (si n’hi ha de noves i/o diferents del sprint 0)
Accés i explotació de les dades personals per personal autoritzat d’alta autorització.
Accés i explotació d’altres dades per personal amb autorització

Creiem que s’hauria de fer una api que limités l’explotació de les dades al personal que no té alta autorització segons les diverses necessitats.
El disseny de les dades està tenint en compte de separar quines dades personals han de ser accesibles a quines persones.

·Amb quina informació confidencial treballeu? (si n’hi ha de noves i/o diferents del sprint 0)



Respecte al document anterior han afegit
Pasajeros
username
password
historico (de vuelos/billetes)
Vuelos
aerolinea
//
VOLS
id_flight: Número de vuelo (único en el día)
origen: aeropuerto de origen - Vilanova Intercontinental Airport
destino: aeropuerto de destino - Nombre completo del aeropuerto
fecha: fecha de salida
hora: hora de salida - en hora local
aerolinea: compañía operadora del vuelo
puerta: puerta de embarque
estado: En Hora, En Tierra, Embarcando, Retrasado, Cancelado, Cerrado, Cambio de puerta de embarque.
aerolinea: nom de la erolinea

PASSATGERS
id_user: numero de cliente - unico
nombre: nombre
apellidos: apellidos
nació: fecha de nacimiento
género: hombre/mujer
vip: bool para indicar si es vip o no
disabled: bool para indicar si es dependiente
username: nom d'usuari
password: password usuari s'ha de xifrar

historico: billete
TARJETES DE FIDELITZACIÓ
id_card: numero de tarjeta - unico
id_user: numero de cliente
aerolinea: compañía emisora de la tarjeta
millas: número de puntos acumulados en la tarjeta
status: status del viajero (gold/silver/bronce)
caducidad: fecha de caducidad de la tarjeta
DADES DE BITLLETS
id_ticket: numero de billete - unico
pasajero: nombre y apellidos del pasajero
id_card: numero de tarjeta de pasajero frecuente (puede ser vacio)
id_flight: id del vuelo
fecha: fecha del vuelo
asiento: asiento del vuelo
vip: bool para indicar si es vip o no
disabled: bool para indicar si el usuario es dependiente o no
maletas_paid: número de maletas facturables
maletas_checked: número de maletas facturadas
DADES DE NEGOCIS
id_shop: id del negocio - unico
nombre: nombre del negocio
tipo: tienda/restaurante (expandible a otros tipos)
local: localización del negocio
descripción: descripción del negocio si es restaurante (tipo de comida...) si es tienda (que venden....)
estado: abierto - cerrado - saturado
logo: ruta a la imagen del logotipo
foto: foto de la entrada del negocio
DADES D'OFERTES
id_offer: id de la oferta - único
id_shop: id del negocio
descripción: descripción de la oferta
caducidad: caducidad de la oferta

publico: a quien va dirigida (todos - vip - disabled

Versió Sprint 1.0

Index

- Introducció
- Usuaris
- Política general de la base de dades
- Política de les còpies de seguretat BackUps
- Infraestructura requerida
- Privacitat (Informació confidencial de dades personals)
- Pla de contingència de BackUp
- Punts a revisar al realitzar el Pla de Contingència de Backup
- Annex

Introducció:

Aquest informe especifica els requeriments de seguretat aplicables a la base de dades del projecte VIA – Vilanova Intelligent Airport (PTIN 19-2020). Queda obert a millores i suggerències per part del client empresarial, client tècnic, assessor metodològic i qualsevol altre membre dels equips del terminal 1

Actual: sprint 2.0 (-/04/2020)
Anteriors: sprint 1.0
Actualitzacions: -posa aquí les modificacions respecte al sprint anterior

Usuaris:

Administrador de la base de dades:
És el que administra la BBDD en la seva totalitat amb dret a crear, borrar objectes i modificar a més pot concedir privilegis a altres usuaris (personal amb autorització) sobre els objectes que ha creat.

El admin del BBDD generarà els usuaris i contrasenyes del personal amb autorització i d'alta autorització a petició i/o autorització del responsable de RRHH (en el nostre cas, Responsable de Seguretat de BBDD de l'equip A1)

Nom d'admin: admin_VG_Aeroport@27BBDD (arbitrari)
Contrasenya: xxx (15 caràcters)

Política de generació de contrasenyes:
Les contrasenyes han de tenir almenys 15 caràcters, combinant lletres, números i símbols
No usar paraules reals, encara que estiguin a l'inrevés.
No es poden incloure dades obvies com el nom, data de naixement, etc.

Rols-usuaris de la base de dades(inf. proporcionada per l'equip A4):
Personal d'alta autorització: usuari amb dret a consultar i/o actualitzar, sense dret a crear o borrar objectes.
Personal amb autorització: usuari amb dret a consultar i sense dret a crear o borrar objectes.

Política general de la base de dades:
Accés per defecte: sense accés
Revisió permanent: modificació de contrasenyes cada mes per motius de seguretat
Física: accés a l'equip només per l'admin de la BBDD
SGBD: Identificació i autenticació (format)
.Usuari: nom.cognom1

.Contrasenya: xxx (15 caràcters) seguir política de generació de contrasenyes descrita prèviament

Política de les còpies de seguretat BackUps:

Mensual: còpia completa externa
Còpia de seguretat de tots els arxius i carpetes en un dispositiu extern (ubicat en altre ubicació física)
Quinzenal: còpia completa local
Còpia de seguretat de tots els arxius i carpetes en un dispositiu local en una partició diferenciada
Diari: còpia incremental inversa Snapshot cada 24 hores
Realització programada de backups incrementals inverses tipus Snapshot perquè la seva restauració és més ràpida i es manté la capacitat de tornar a les versions anteriors per debugar errors a posteriori
Constant: còpia mirall entre node principal i node secundari Actualització S3.0
Tipus específic RAID 1 (disk mirroring), commutació immediata en cas de failover amb una alta disponibilitat en temps de recuperació

Infraestructura requerida:

Recolzament de nodes:

Sempre hi haurà un segon node que pot entrar en calent per substituir al principal en cas de fallada és a dir, per tenir un recolzament immediat en cas de fallada del principal. També hi haurà un tercer node net que farà el rol d'auxiliar

Encriptació de dades:

Es farà servir criptografia asimètrica (key-pairs) amb certificats, encara que l'ús d'algoritmes addicionals en les operacions de consultes pot fer disminuir el rendiment en l'accés a la base de dades, s'utilitzaran per reforçar la seguretat.
El servidor de CA (Certification Authority) serà independent del servidor de BBDD amb una generació de certificats de clau públicas originats per aquest servidor.
S'usaran algorismes d'encriptació RSA amb protocols TLS (Transport Layer Security).
El tamany de les claus públiques serà de 1024 bits que és el mínim amb el qual no es coneix un mètode eficient de factorització

Privacitat(Informació confidencial de dades personals):

-Tabla PASSATGERS
nombre: nombre
apellidos: apellidos
nació: fecha de nacimiento
género: hombre/mujer

-Protocol en cas de violació de dades personals:
En cas de violació de dades personals, segons l'article 33 de l'RGPD, *Notificació d'una violació de la seguretat de les dades personals a l'autoritat de control*, es farà un enviament d'un missatge d'avís al responsable designat en termes de privacitat per l'aeroport amb aquests camps:

Destinatari: responsable@email.org
Tema: Violació de dades personals
Body:
Data - hh/mm/ss
Descripció de la incidència així com el passatger/s i els seus camps afectats

Pla de contingència de BackUp:

Immediatament tras succeir un "desastre".
- Entrarà en funcionament el node secundari o de recolzament.

Durant la resolució de la situació.
- Mentres estigui el node de recolzament funcionant es buscarà la recuperació del principal i la posada en marxa d'un tercer, l'auxiliar, amb una restauració com a mirall del node secundari.

Després d'haver-se restablert el servei
- En cas de recuperació del node primari, aquést tornaria a ser el principal i el node secundari tornaria a ser de recolzament
- En cas de que no s'hagi recuperat el node primari, el node secundari passaria a convertir-se en el node primari i l'auxiliar en el secondari de recolzament. Alhora, es farà un enviament d'un missatge d'avís al responsable designat d'infraestructures amb aquests camps:

Destinatari: responsable@email.org
Tema: Node principal caigut
Body:
Data - hh/mm/ss
Prioritari, creació d'un node auxiliar net i preparat per la connexió
Guardat per a posterior revisió del node principal caigut i recuperació, si es pot, de la base de dades

També, es farà un enviament d'un missatge d'avís al responsable designat per l'aeroport en termes de privacitat amb aquests camps:

Destinatari: responsable@email.org
Tema: Caiguda del node principal
Body:
Data - hh/mm/ss

Descripció de la incidència així com de la localització de la base de dades. També s'informarà si està corrompuda i si hi ha hagut pèrdues i/o filtracions de dades personals.

Definició dels objectius de recuperació: Actualització S3.0

El RPO (Recovery Point Objective): Actualització S3.0

El RTO (Recovery Time Objective): Actualització S3.0

Freqüència de realització del Pla de Contingència de BackUp:

Recomanat fer un simulacre de restauració del Backup cada 6 mesos per donar compliment a la LOPD, verificar la funcionalitat del sistema i poder comparar resultats amb pròximes restauracions.

Plans de recuperació del BackUp de la base de dades: Actualització S3.0

Punts a revisar al realitzar el Pla de Contingència de Backup:

Revisió del repositorio de Backup: Millores S3.0
Estat dels discos durs
Espai disponible

Revisió de les tarees de BackUp: Millores S3.0
Anotació del tamany dels arxius de Backup
El.liminar còpies antigues per alliberar espai: còpies assegurades i prèviament autoritzades per el responsable designat per l'aeroport
Encriptació de les dades en totes les tarees que afecten el BackUp
Actualització de versions del software de BackUp
Notificacions: tenir actualitzats les adreces de mails dels corresponents responsables

Restauració de BackUps: Millores S3.0
Crear un entorn de TEST per restauració: Creació d'un servidor bessó a l'original independent per fer tests de restauració
Comprovar integritat dels arxius de restauració
Restaurar arxius individuals i apuntar temps de restauració.
Si la restauració fos fallida, resoldre el problema i, si no fos possible, s'el.liminaria i es faria un enviament d'un missatge d'avís al responsable designat per l'aeroport en termes de privacitat amb aquests camps:

Destinatari: responsable@email.org
Tema: Restauració fallida
Body:
Data - hh/mm/ss

Descripció de la incidència així com de la localització de l'arxiu de restauració.També s'informarà de l'el.liminació de l'arxiu corromput

Informe de resultats: Millores S3.0
Després de l'execució del Pla de Contingència, el responsable designat per l'aeroport rep un informe explicant la situació detallant:

- Tamanys dels fitxers de còpia
- Temps reals de restauració
- Percentatge d'èxit mensual de les tarees de restauració
- Gràfic actualitzat de la situació dels BackUps.
- Propostes de millora (si s'escau)

Annex: documentació rebuda per part de l'equip responsable A4

Sprint 0:

Base de dades:
·Definició de les característiques de la Base de dades i resum de la seva funcionalitat.
La base de dades és de tipus nosql i estarà basada en el SGBD Mongo DB. No tenim informació d'on estarà el hosting del SGDB. Guardarà informació dels passatgers, tendes, vols, restaurants, ofertes i altres necessitats que puguin sortir durant el desenvolupament
·Quines tecnologies heu utilitzat?
Veure apartat anterior
·On creieu que farà falta seguretat en la base de dades? Heu començat a treballar en ella?
Accés i explotació de les dades personals per personal autoritzat d'alta autorització.
Accés i explotació d'altres dades per personal amb autorització
Creiem que s'hauria de fer una api que limités l'explotació de les dades al personal que no té alta autorització segons les diverses necessitats.
El disseny de les dades està tenint en compte de separar quines dades personals han de ser accesibles a quines persones.
·Amb quina informació confidencial treballeu? (Dades dels usuaris, informació de la terminal…)
Fins ara guardem la següent informació:
VOLS
id_flight: Número de vuelo (único en el día)
origen: aeropuerto de origen - Vilanova Intercontinental Airport
destino: aeropuerto de destino - Nombre completo del aeropuerto
fecha: fecha de salida
hora: hora de salida - en hora local
aerolinea: compañía operadora del vuelo
puerta: puerta de embarque
estado: En Hora, En Tierra, Embarcando, Retrasado, Cancelado, Cerrado, Cambio de puerta de embarque.

PASSATGERS
id_user: numero de cliente - unico
nombre: nombre
apellidos: apellidos
nació: fecha de nacimiento
género: hombre/mujer
vip: bool para indicar si es vip o no
disabled: bool para indicar si es dependiente
TARJETES DE FIDELITZACIÓ
id_card: numero de tarjeta - unico
id_user: numero de cliente
aerolinea: compañía emisora de la tarjeta
millas: número de puntos acumulados en la tarjeta
status: status del viajero (gold/silver/bronce)
caducidad: fecha de caducidad de la tarjeta
DADES DE BITLLETS
id_ticket: numero de billete - unico
pasajero: nombre y apellidos del pasajero
id_card: numero de tarjeta de pasajero frecuente (puede ser vacio)
id_flight: id del vuelo
fecha: fecha del vuelo
asiento: asiento del vuelo
vip: bool para indicar si es vip o no
disabled: bool para indicar si el usuario es dependiente o no
maletas_paid: número de maletas facturables
maletas_checked: número de maletas facturadas
DADES DE NEGOCIS
id_shop: id del negocio - unico
nombre: nombre del negocio
tipo: tienda/restaurante (expandible a otros tipos)
local: localización del negocio
descripción: descripción del negocio si es restaurante (tipo de comida...) si es tienda (que venden....)
estado: abierto - cerrado - saturado
logo: ruta a la imagen del logotipo
foto: foto de la entrada del negocio
DADES D'OFERTES
id_offer: id de la oferta - único
id_shop: id del negocio
descripción: descripción de la oferta
caducidad: caducidad de la oferta
publico: a quien va dirigida (todos - vip - disabled ....)