LICITACION PÚBLICA INTERNACIONAL 10/17

IDENTITY MANAGER

CIRCULAR N°02 -ACLARATORIA CON CONSULTA-

La Plata, 02 de Noviembre de 2017

El Proyecto informa con motivo de una consulta recibida lo siguiente

Consulta: *¿Qué plataformas son las que se necesitan el control de acceso: Wlndows y UNIX/Linux,Mainframe?*

Respuesta: **Control de acceso para aplicaciones web contra los siguientes repositorios: Windows (es la misma cuenta que se tiene que aprovisionar para el acceso a la PC) Mainframe (es la misma cuenta que se tiene que aprovisionar para acceso de una terminal) LDAP (solo cuenta de aplicaciones) Cuentas privilegiadas sobre: Windows, Mainframe, Linux, AIX**

Consulta: *¿Se cuenta con alguna definición de políticas de control de acceso?*
Respuesta: **Para aplicaciones Web mediante roles. Cuentas privilegiadas: Windows:**

- **separación de administración de cuentas (seguridad)**
- **Administración de servidores y servicios (infraestructura)**
- **Administración de WorkStation (Microinformática)**

Linux: PAM LDAP, se dan permisos a los servicios según necesidad
Unix: PAM LDAP, se dan permisos a los servicios según necesidad

Consulta: *¿Se estará controlando el acceso hacia el Sistema Operativo o hacia Aplicaciones?*
Respuesta: **Ambos.**

Consulta: *En los puntos 8 y 9 se habla de aplicaciones web basadas en CAS1.0 y que deben*

integrarse con la solución de SSO ofertada. Es posible obtener más detalle de esta solución y todas aquellas que se requerirá considerar SSO?

Dar ejemplo de una aplicación y detallar lo siguiente:

Respuesta:

a. Tipo de aplicación - Cliente/Servidor o Web? ¿Apache-Tomcat? Webshpere, boss?

Las aplicaciones son Web. Existen distintas tecnologías: Java corriendo sobre WebSphere 8.5, .Net corriendo sobre IIS 7, Asp corriendo sobre IIS7, algunas aplicaciones de terceros corriendo sobre Apache2 (Moodle, Wordpress, Plone). Sharepoint.

b. Descripción de la aplicación (Funcionalidad, criticidad, etc.)

Se puede empezar por cualquiera de las aplicaciones web. Todas utilizan el cliente de SSO para autenticarse, el cual provee un mecanismo basado en CAS 1.

c. La aplicación es comercial o desarrollada

Las aplicaciones web Java y Net son desarrolladas internamente.

d. Donde se autentican los usuarios que acceden a la aplicación, (Ejemplo; BD, LOAP, etc.). Indicar versión

Los usuarios están definidos en Ldap de Tivoli Directory Server 6.3 (contribuyentes), Active Directory de Microsoft sobre Windows server 2008 R2 y RAFC de mainframe (empleados).

e. ¿Es posible acceder a los repositorios de usuarios mediante operaciones normales de read/write?

Sí, es posible a través de protocolo Ldap.

f. ¿Cuál es el diseño de la tabla/registro de usuarios y permisos? Por favor si existe más de una tabla/ registro, enviar el detalle y la función

Los usuarios no se almacenan sobre una base de datos. Los mismos están alojados en Ldap, Active Directory y RACF. Los permisos sobre las aplicaciones también están definidos sobre el mismo Ldap, con una estructura jerárquica que define Aplicación/roles/miembros.

g. La aplicación tiene embebida el formulario de autenticación? Explicar:

No, el formulario de autenticación lo tiene la aplicación de SSO. Las aplicaciones nunca tienen acceso a la contraseña del usuario. Las aplicaciones hacen uso de un cliente de dicho SSO que lo redirecciona a dicho formulario en caso que la persona no se encuentre autenticado.

h. Existe acceso a los códigos de desarrollo de la aplicación?

Si, todas las fuentes se encuentran guardadas en un versionador (cvs, git).

i. Sobre que servidor web está instalada la aplicación (ejemplo liS), indicar versión.

Como servidor web se tiene IIS 7 y apache 2 (según la aplicación)

j. Sobre que aplicación server está instalada la aplicación (ejemplo WAS), indicar versión.

WAS 8.5

k. Sobre qué sistema operativo está instalada la aplicación (solo aplica para aquellas Web)

En el caso de Websphere sobre AIX. En el caso de IIS sobre Windows Server 2008, Apache2 sobre Debian 9.

l. Detallar sistema operativo y CPU donde está instalada la aplicación.

Contestado en los puntos anteriores.

m. Es utilizado o es deseable incorporar a futuro algún método de autenticación robusta, (Token, certificados, biométricos, otros)

Si, sería deseable contar con dicha capacidad a futuro.

n. Detallar si es necesario incorporar niveles de autenticación, ejemplo; Nivel 1 – solo user/password, Nivel 2 - user/password y Certificado, Nivel 3 - user/password y biométrico, etc.

Se está pensando en poder contemplar el uso de niveles de autenticación. Además de los nombrados también en base a como se validó al contribuyente al momento de otorgarle su contraseña (ejemplo todo virtual nivel 1, presencial nivel 2, etc).

o. Detallar si es necesario controlar el acceso a las aplicaciones por algún atributo o criterio:

- Atributo del usuario, ejemplo; cargo, oficina, IP Origen, fecha, horario, otros, cuales?

Es necesario que la aplicación de control de acceso sea capaz de evaluar atributos del usuario. En principio oficina que tiene asignada el mismo.

p. ¿Es necesario controlar el número de sesiones SSO?

Un mismo usuario no es necesario que se controle, si se loguea más de una vez.

Sí, es necesario contar con un mecanismo para limitar la cantidad total de sesiones establecidas sobre una aplicación (se usa en días de vencimientos cuando los equipos no soportan la carga).

q. ¿Cuántos dominios se están considerando implementar para SSO? Indicar cuáles son.

Si se refieren a dominios de Active Directory, es solo uno.

Para el caso de aplicaciones existen estos dominios actualmente en producción: www.arba.gov.ar, www1.arba.gov.ar, www2.arba.gov.ar, www3.arba.gov.ar, www4.arba.gov.ar, www.arba.gob.ar, www1.arba.gob.ar, www2.arba.gob.ar, www3.arba.gob.ar, www4.arba.gob.ar

r. ¿Los dominios a implementar SSO, son todo parte de ARBA?

Si se refieren a dominio de Active Directory está contenido todo dentro de ARBA.

Para aplicaciones Web se debe implementar para todos los dominios.

s. ¿Es necesario implementar Federación?

Es necesario contar con dicha funcionalidad para poder proveer a otros organismos de los mecanismos de autenticación de ARBA, así como también en algunos casos utilizar la autenticación de otros organismos para ingresar a aplicaciones de ARBA.

Consulta: *En el punto 1.38 indica que "La solución debe incluir un generador de contraseñas random para que los administradores puedan periódicamente cambiar contraseñas de ciertas cuentas de manera automática.*

a- ¿Estas cuentas a las cuales los administradores cambiarán contraseñas de forma random, son cuentas de servicios? Por favor entregar un ejemplo

Respuesta: **Cuentas de usuarios**

Consulta: *En el punto 1.18 indica que "El/los productos ofrecidos deben proveer módulos de integración "Out of the Box" con los siguientes sistemas: Windows AD, Exchange, LDAP v3, MS SQL, ORACLE, RACF".*

a- ¿Cuentan con Alta Disponibilidad para Exchange? ¿La alta disponibilidad de Exchange la tienen configurada a través del uso de un DAG?

No está en alta disponibilidad.

b- Para el caso del AD ¿Cuántos Domain Controles tienen?

Un Domain. Dos domain controlers.

c- Para el caso LDAP v3 ¿Cuántos LDAP se integrarán?

Dos.

d- ¿Cuántas instancias de MSQLy Oracle se van a estar integrando?

15 instancias MSQL y 13 Oracle

e- Para todos estos módulos de integración:

f- ¿Hay un ambiente de desarrollo para poderse integrar**?**

Sí.

Consulta: *En el punto 1.96 Indica "EI sistema de Identity Management debe poder integrarse con otros sistemas mediante Web Serviees (REST) a SOAP"*

a- ¿Hasta con cuántos sistemas se tiene que integrar Identity Managment?

La idea es que el identity esté preparado para poder conectarse con cualquier sistema mediante el uso de servicios web (SOAP o Rest).

b- ¿Cuántos estarían integrándose en el alcance de este proyecto?

En una primera instancia se debería conectar contra el sistema de recursos humanos (SIAPE), el cual expone actualmente mediante tres servicios SOAP las funcionalidades: padrón completo de empleados, listado de la estructura jerárquica del organigrama, novedades.

Consulta: *En el punto 2.32 indica que "la solución deberá soportar aquellas casas de SSO donde la provisión de usuario y contraseña sea requerida pero no suficiente, ya que existen aplicaciones Legacy que requieren que el usuario defina con qué perfil desea acceder."*

a- ¿Estas aplicaciones legacy son del tipo Web?

Sí, dichas aplicaciones son Web.

b- ¿Dónde almacenan sus usuarios?

Dichos usuarios están almacenados en Ldap y Active Directory.

Consulta*: En el punto 2.44 se indica que ~Debe soportar autenticación contextual (basada en riesgo), ej: si viene desde china, forzar un segundo factor, mientras que si accede desde un dispositivo que ya utilizó previamente y está en Argentina, entonces le pido la clave."*

¿ARBA cuenta con una solución de segundo factor?

No.

• En caso de sí, ¿cuál?

• En caso de no, ¿es necesario ofertar una?

Sí.

Consulta: *¿Qué sistema ERP está considerado?*

No hay sistema ERP.

Consulta: *¿Cuántos dominios de active se desean implementar?*

Respuesta: **Uno.**

Consulta: *Entregar detalle de las aplicaciones, sistemas operativos y sistemas a los cuales se desea aprovisionar.*

a. Repositorio de usuarios que utiliza cada una de las aplicaciones mencionadas y versiones, es decir dónde son almacenados los usuarios y sus atributos.

Ldap

b. Versión del sistema operativo

AIX 701

c. Versión de las Base de datos

MSQL: 2012 y 2008 R2. ORACLE 11g R2.

Consulta: *10. Para aquellas aplicaciones que se tiene una base de datos propietaria:*

a. ¿Se tendrá acceso a las tablas del BD?

Si en cuanto a propietario se refieren a aplicaciones que no fueron desarrolladas por nosotros (Moodle, Wordpress, Plone, Sharepoint), no hay problemas que accedan a las mismas.

b. ¿Es posible acceder al BD en forma remota?

Habría que estudiar en qué caso estarían necesitando acceder en forma remota a dichas bases y con qué fin. Cabe aclarar que todo lo que es la implementación y capacitación se realice de forma presencial en el edificio de Arba de calle 7 y 45, en conjunto con el Departamento de Seguridad para una mejor transferencia de los conocimientos.

c. Se tiene el conocimiento de la estructura del BD, dependencias, SP y cuáles son los campos necesarios para que un usuario este operativo?

Sobre dichos sistemas que no fueron realizados por ARBA, no conocemos el detalle de sus DB.

Consulta: *¿Se cuenta con la matriz y/o definición, delegación de funciones entre múltiples aéreas/departamentos/edificios o la administración se realizará de forma centralizada (un solo Departamento que proporciona servicios de aprovisionamiento a todos los sistemas)?*

Respuesta: **La Organización cuenta con un Departamento de Seguridad Lógica que se encarga de esta tarea.**

Consulta: *Para la solución de aprovisionamiento ¿Qué tipo de usuarios se manejarán dentro de la solución (usuarios internos, clientes, proveedores, usuarios externos)?*
Respuesta: **Usuarios internos, contribuyentes, usuarios externos y proveedores.**

Respuesta: *¿Cuántos servidores estarán involucrados para la implementación del proceso de Administración de Usuarios Privilegiados?*
Respuesta: **Servidores Windows (distintas versiones): 70 / Servidores Linux: 90 / Servidores AIX: 15.**

Consulta: *¿Cuántas cuentas por servidor estarán contemplándose para este proceso?*
Respuesta: **Cuenta Administrador: 1 por cada servidor (en este caso se contempla un usuario root (Linux/Unix) y/o Administrador (Windows).**
Cuenta de usuarios: 100 usuarios con acceso a las consolas de los servidores (varios deptos. Seguridad/Infra/DB/Hard y Soft/Implementacion/Desarrollo con distintos permisos, algunos administradores y otros usuarios con permisos puntuales.) Este número es aleatorio por servidor.

Consulta: *¿La administración de accesos y privilegios se maneja mediante el uso de perfiles y/o roles?*
Respuesta: **Sí.**

Consulta: *¿Cuántos roles y/o perfiles existen?*
Respuesta: **600 roles web y 500 perfiles de aplicaciones natural (host).**

Consulta. *Existen reglas de segregación de funciones y cómo son aplicadas y controladas?*
Respuesta: **Existe una segregación de funciones a nivel de estructura de organigrama y en las aplicaciones en función de los roles que tienen definidos.**

Consulta: *En caso de tener la definición de roles y privilegios, ¿en qué formato o donde está la definición?*
Respuesta: **Ldap, en grupos de AD y perfiles de Natural Security.**

Consulta: *¿La definición de roles y privilegios la tienen disponible para todos los sistemas considerandos en el proyecto?*
Respuesta: **Sí.**

Consulta: *¿El proceso de alta/baja/modificación de usuarios es automático o manual?, explicar este proceso.*
Respuesta: **Se contesta en los puntos 25 y 26.**

Consulta: *Existe una nomenclatura de nombre estándar para todas las plataformas (ejemplo: ¿userid = nombre+apellido)?*
Respuesta: **No, en el caso de active directory sí se cuenta con una definición de nombre.apellido (aunque no todos los usuarios hoy cuenten con esa definición y se está en un proceso de migración). En el caso de los usuarios externos (contribuyentes, municipios, etc) los mismos son identificados mediante el CUIT. En el caso de RACF se tiene la limitación de 6 caracteres.**

Consulta: *¿Esta definición es igual para todos los sistemas o cada sistema tiene su propia nomenclatura?*
Respuesta: **Se contestó en el punto anterior.**

Consulta: *¿Cuántos atributos de usuario son requeridos administrar en la solución de aprovisionamiento?*
Respuesta: **La intención es que la herramienta pueda soportar todos los atributos que sean necesarios. En principio el código de la oficina en donde trabaja el empleado, nivel de certificación (como obtuvo clave en caso de contribuyente), si la persona es externa o interna a la organización.**

Consulta: *¿Existe una política de contraseña única para todas las plataformas?*
Respuesta: **No, actualmente las distintas plataformas de usuarios tienen distintas políticas de contraseñas. Lo ideal sería unificar dicho criterio con la implementación de la herramienta.**

Consulta: *¿Existen flujos definidos que controlan el alta y baja de usuarios?*
Respuesta: **Si, existe una integración contra el sistema de recursos humanos. En dicha integración se detecta si hay un alta o baja de empleado.**

Consulta: *Estos flujos son manuales, automáticos o una combinación, favor describir:*
Respuesta: **Es una combinatoria de manual y automática. Automático toda aquella que está dentro del flujo normal de ingreso de una persona. Manual como vía de excepción, altas tempranas, o sea todos aquellos casos que por algún motivo todavía no fueron dados de alta en el sistema de recursos humanos. Cabe aclarar que, ese es el circuito actual pero la idea es mejorar dichos procesos junto con la implementación de la herramienta.**

Consulta: *¿Existe claridad de los aprobadores para estos flujos?*
Respuesta: **La idea es volver a revisar dichos procesos con el fin de mejorar el procedimiento.**

Consulta: *¿Se desea tener control de las cuentas privilegiadas?*
Respuesta: **Sí, se desea tener el mayor control posible sobre dichas cuentas.**

Consulta: ¿Con cuántos Datacenter cuenta hoy ARBA? *En caso de tener varios Datacenters, las implementaciones de las soluciones deben estar activo/activo o activo/pasivo.*
Respuesta: **Se cuenta con un solo Datacenter.**

Consultas: SOLUCIÓN DE ANÁLISIS DE EVENTOS EN SEGURIDAD (SIEM)

Consulta: *¿Respecto al requerimiento de alta disponibilidad, es necesario que se considere una arquitectura tolerante a fallas en esta etapa?*
Respuesta: **No es necesario en el caso que su fallo no impida el funcionamiento correcto de la red y sus servicios.**

Consulta: *Respecto al manejo de integridad, es posible utilizar otros mecanismos, diferentes a los mencionados en el requerimiento? Ejemplo: La utilización de métodos de ofuscación y acceso restringido a la base de datos (propietaria) de la solución para garantizar la integridad*
Respuesta: Puede ser, mientras cumpla la funcionalidad de poder detectar quién y qué se modificó en un dato especifico.

Consulta: *Respecto al análisis forense de los eventos procesados, ¿cuánto es el tiempo de almacenamiento requerido para dichos eventos?*
Respuesta: **El tiempo estimado son 3 meses.**

Consulta: *Respecto al análisis de Vulnerabilidades, se desea que la herramienta de correlación se integre con herramientas de vulnerability Assesment, para usar esa información con un elemento de correlación basada en riesgo?*
Respuesta: **Sí. Principalmente con la solución Security Center/Nessus de Tenable.**