

Informe Preliminar de Configuraciones de la Infraestructura del Sistema Informático del PREP

**Informe preliminar de las pruebas y escaneos de vulnerabilidades,
así como de configuraciones del sistema informático del PREP del
IEE Sinaloa**

Descripción breve

Este documento contiene el resultado y la evidencia del escaneo de vulnerabilidades a los elementos de la solución de informática como parte de los servicios de auditoría de seguridad del sistema preliminar de resultados para el IEE Sinaloa

Roberto Luis Iriarte / Raime Alejandro Bustos

roberto@iriarte.net

raime.bustos@tec.mx

Jesús R. González / Juan Arturo Nolasco

jrgonza@gmail.com

jnolasco@itesm.mx

Índice

1	Introducción	2
2	Resumen Ejecutivo	3
3	Objetivos	4
4	Alcance	4
5	Criterios utilizados para la auditoría	4
6	Observaciones Preliminares	5
6.1	Hallazgos Pruebas Revisión Configuraciones	5
6.2	Pruebas Controles Físicos	6
6.3	Pruebas Escaneo Vulnerabilidades de Activos	7
6.4	Pruebas Soporte Operativo	10
Anexo I – Evidencias		11

Versión	Fecha	Descripción
1.0		
1.1	14-Abril-2021	Documento inicial preliminar de configuración e infraestructura
1.2	26/Abr/2021	Revisión general

Dictamen elaborado por: MSc. Jesús Raúl González Hernández en coordinación con el Dr. Juan Arturo Nolasco, Ing. Roberto Luis Iriarte Pablos y MSE Raime Alejandro Bustos Gardea.

1 Introducción

Este documento presenta los avances y resultados preliminares de la revisión de configuraciones y de los escaneos y análisis de vulnerabilidades del PREP para la jornada electoral del 2021.

Este documento se dará en cada iteración de pruebas que se de para llevarlo a una aceptación del 100% por lo que estos resultados se documentarán cada vez que se lleve a cabo el escaneo.

La sección de anexos documenta en cada uno los resultados de cada iteración con las firmas por parte del ente auditor y un representante del **IEE Sinaloa**. La tabla de resultados tiene sección de comentarios, si hay necesidad de agregar algún tipo de recomendación adicional, ésta estará incluida en esa misma sección de anexo.

2 Resumen Ejecutivo

Las pruebas y hallazgos se presentan en la siguiente tabla indexando la prueba con un resumen del resultado y su hallazgo, si acaso tuvo alguno. El detalle se puede revisar en la sección 6 de este documento.

Prueba	Resultado	Prueba	Resultado
SPI01 – Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	Aceptado	SPV01 – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso	Aceptado
SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Aceptado	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso	Aceptado
SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Pendiente	SPV03 – El escaneo de servicios hecho a la infraestructura no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS	Pendiente
SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla	Pendiente	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	Pendiente
SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones	Aceptado	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos	Pendiente
SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral	Pendiente	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	Pendiente
SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos	Aceptado	PRS01 – La OPL debe tener un manual de capacitación para el personal de captura	Aceptado
SPI08 – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas	Aceptado	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP	Aceptado
SPI09 – En los centros de captura no debe haber redes inalámbricas que conectan la infraestructura de captura o del OPL.	Aceptado	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta	Aceptado
SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos	Aceptado	PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros)	Pendiente
SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación	Aceptado	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos	Pendiente
SPI12 – Controles de acceso físico a los centros de captura	Aceptado	PRS06 – Tener los contratos con los proveedores de nube, así como los procedimientos de reporte en caso de eventos hacia ellos. (si se está utilizando Nube como repositorio operativo del PREP)	Pendiente
SPI13 – Control de acceso al sitio donde está la infraestructura del PREP	Aceptado	PRS07 – Tener la documentación del sistema PREP de la OPL actualizado y en resguardo por los encargados del área de tecnología de la OPL	Aceptado
SPI14 – Verificar si hay control de acceso a teléfonos móviles	Aceptado		

3 Objetivos

Este documento documenta los resultados preliminares de las pruebas para poder hacer la implementación de controles o medidas para poder cerrar los hallazgos en cuanto a vulnerabilidades y disminuir la superficie de riesgo que el PREP del **IEE Sinaloa** pueda tener al terminar la primera revisión.

4 Alcance

El alcance de las pruebas se estructura en la sección 6 de este documento en base a las siguientes partes:

- Revisión Configuraciones – Configuraciones y parámetros de los equipos involucrados en el PREP
- Escaneos de Activos – Revisión de vulnerabilidades de los sistemas operativos y aplicaciones
- Revisión de infraestructura – Revisión de infraestructura que soporta al PREP
- Controles físicos – Validación de controles físicos de la infraestructura e instalaciones
- Soporte Operativo – Revisión de los controles de soporte operativo a la operación del PREP

5 Criterios utilizados para la auditoría

Las tablas de la sección 6 documentaron resultados en función de los criterios de aceptación dados. En la sección de anexos se encuentra la evidencia de dichas pruebas. Cada prueba puede tener uno de tres tipos de resultados que pueden ser los descritos en la tabla siguiente

Resultado Prueba	Descripción de Criterio	Acciones
Aceptado	La prueba cumplió satisfactoriamente con los criterios de aceptación	La prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
Rechazado	La prueba no cumplió con los criterios de aceptación	La prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
Aceptado con Observaciones	La prueba cumplió con una parte de los criterios o cumplió totalmente con observaciones.	La prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no serían obligatoria su implementación y solo queda como sugerencia o recomendación.

6 Observaciones Preliminares

Las observaciones y recomendaciones se harán sobre el anexo correspondiente de pruebas que se esté realizando y bajo los criterios que se detallan por cada una de las. En esta sección se presenta un resumen, en función de los resultados y revisión de hallazgos, de los resultados de esta y su cumplimiento, así como hallazgos por clasificación que se de.

6.1 Hallazgos Pruebas Revisión Configuraciones

Para estas pruebas, en adición a que el personal técnico de la **IEE Sinaloa** proporcione la configuración en línea de comando o por interfaz gráfica para revisión, el ente auditor usará las herramientas necesarias (no intrusivas) para detectar mediante escaneos a los activos, las vulnerabilidades que puedan existir en los activos que pertenecen al PREP.

Resultados Preliminares Revisión de Configuraciones				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPI01 – Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	Revisar que la configuración bloquee puertos no usados, niegue por definición servicios y protocolos no utilizados	LA configuración debe tener incorporada la limitación de protocolos, direcciones que no se estén usando en la jornada electoral 2021	SSH, http (redirect), https, rsync entre webserver y el equipo que lo genera (son json). y un zip de cada corte. 3 cortes por hora (cada 20 minutos). Pendiente evidencia	Aceptado
SPI02 – Los equipos de comunicaciones sólo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Hay que confirmar que el acceso a los equipos de comunicaciones y redes solo se pueda dar por medio de SSH y no bajo otro protocolo (TELNET, HTTP u otro)	Acceso a los equipos de comunicaciones (FW, SW, Router) solo debe ser posible desde la red interna de la OPL	Consolas gráficas con acceso seguro por https	Aceptado
SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Obtener las versiones de los equipos de ruteo y switcheo para confirmar que las versiones son actuales y aun disponibles (no descontinuadas)	Las versiones de estos equipos deben estar aún en soporte por el fabricante	Switch Cisco SG220-26P en versión de firmware 1.1.4.1, la última es 1.1.4.8 Firewall Sonicwall NSA 2650, v6.5.1-5-6n actualizar a SonicOS 6.5.1.12-1n	Pendiente
SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla	Confirmar contratos de soporte y/o equipo de reemplazo en caso de falla	Deberá haber un contrato de soporte por un tercero o bien equipo en frío que pueda instalarse en caso de falla.	Firewalls, si hay, switches tienen smartnet (pólizas de soporte extendido), lo cubren por HA. Soporte si. Todo lo crítico si está en HA, a excepción de los CATD solo hay un switch y tienen a la mano un 2do por si se requiriera	Pendiente

			cambiarlo. Pendiente de habilitar HA el Firewall	
SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones	Entrar al equipo de comunicaciones y verificar la existencia de dos enlaces, configurados ya sea de manera activo-activo o activo-standby	Existencia de redundancia de sistemas de comunicaciones para continuidad de captura. Verificar tiempos de convergencia (desde caída hasta recuperación) durante simulacro	IBM ofrece varios carriers de contacto. CATD, enlaces redundantes con Telmex, Megared (Metrocarrier).	Aceptado
SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral	Verificar que exista una planta generadora eléctrica con UPS que mantiene interrumpido el flujo eléctrico en caso de falla de la red pública.	Existencia de planta eléctrica para en caso de corte. Verificar tiempos de corte (desde caída hasta recuperación) durante simulacro	Laptops, UPS y una planta externa para el día de la elección, en centro de captura y unas de menor capacidad en los CATD. Simulacro se realizó un día antes del simulacro del 30-mayo sin presencia de Ente Auditor	Pendiente
SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos	Entrar a los distintos activos y verificar la configuración y directorios donde se guarda la bitácora que esta esté habilitado	La función de bitácora deberá estar habilitada y sus archivos creados	Cumple, (fw, switches, ruteadores, SO).	Aceptado

6.2 Pruebas Controles Físicos

Resultados Preliminares Pruebas Controles Físicos				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPI08 – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas	Validar la existencia de un centro que permita la visualización de la operación y su desempeño y que desde este se pueda visualizar la totalidad de los elementos del sistema PREP	Existencia de un centro o grupo que se dedique a monitorear el funcionamiento adecuado de los sistemas del PREP	Cumple, se cuenta con área definida con monitoreo en línea por video de los CATDs y apoyo operativo por teléfono IP	Aceptado
SPI09 – En los centros de captura no debe haber redes inalámbricas que conectan a la infraestructura de captura o del OPL.	Escanear las redes inalámbricas para asegurar que no haya acceso a la red de estaciones de captura	De haber redes inalámbricas en los centros de captura, estas redes no pueden tener acceso a la red de captura	No hay redes inalámbricas que conectan al sistema Central PREP	Aceptado
SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos	Debe validarse que los ambientes de producción y de operación sean distintos y estén por separado	Los ambientes deben ser distintos y debe haber una clara segregación lógica y/o física entre estos ambientes.	Centro de Operaciones 10.3.0.0/24 Centro de Captura 10.3.101.0/24 Centro de datos 1 10.161.98.64/26 Centro de datos 2 10.161.101.64/26	Aceptado
SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación	El ambiente operativo del PREP en evaluación no debe compartir recursos con otros sistemas o plataformas, sus recursos deben ser únicos. <i>Este control aplica primordialmente hacia estados donde hay terceros involucrados en el desarrollo de PREP que lo hacen para otros estados</i>	Validación que el ambiente es único y que no hay compartición de recursos con otras plataformas.	Ambiente exclusivo en dos zonas distintas de IBM Cloud	Aceptado

SPI12 – Controles de acceso físico a los centros de captura	El centro de captura deberá estar resguardado con entrada controlada para evitar que haya personas ajenas a los trabajos durante la jornada	El control puede ser manual (registro), tarjeta, o pase para apertura automática	Control de acceso con tarjeta, registro sanitario de temperatura y registro de asistencia por sistema escaneando la credencial INE del personal. El propio IEES tiene su protocolo de entrada	Aceptado
SPI13 – Control de acceso al sitio donde está la infraestructura del PREP	Las aplicaciones que se estén utilizando para la jornada deberán estar activados sus puertos y no otros distintos a estos.	Las estaciones de captura deberán contar con el mínimo de privilegios y un control de contenido y de navegación en Internet	Estaciones de captura sin Wi-Fi, sin acceso a recursos del sistema operativo ni navegación por Internet. Utilizan IBM Cloud Referencia: https://cutt.ly/gbFfXQH	Aceptado
SPI14 – Verificar si hay control de acceso a teléfonos móviles	Debe haber un lugar donde registrar equipos móviles para control del acceso de estos	Registro de equipos móviles para evitar tenerlos en el área de captura	Está establecido la política que prohíbe el uso de celular durante el PREP, se recogerán para resguardo al principio del turno del Capturista y se le regresará solo al final del mismo.	Aceptado

6.3 Pruebas Escaneo Vulnerabilidades de Activos

Resultados Preliminares Escaneo Vulnerabilidades de Activos				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPV01 – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso	Entrar y escanear y listando los diversos activos del PREP para la cual debe existir la justificación de cada uno de ellos por parte de la OPL	Todos los activos listados deberán estar justificados con el servicio que desempeña dentro de la función del PREP	Servidores en IBM Cloud son sólo los productivos	Aceptado
SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso	Entrar y escanear y listando los diversos puertos de los activos del PREP para la cual debe existir la justificación de cada uno de ellos por parte de la OPL	Todos los puertos o servicios listados en los distintos activos deberán estar justificados con el servicio que desempeña dentro de la función del PREP	Los puertos activos en los servidores son solo los necesarios	Aceptado
SPV03 – El escaneo de servicios hecho a la infraestructura no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS	Mediante escaneo vulnerabilidades obtener las vulnerabilidades de los activos (sistemas operativos y aplicaciones) relacionados con el PREP, listando por la criticidad especificada por el estándar CVSS	Las aplicaciones y los sistemas operativos no deben tener vulnerabilidades críticas ni altas. Si tienen nivel medio, deberá existir contramedidas para esta. La lista completa de vulnerabilidades debe ser notificada hacia la parte responsable del OPL.		Pendiente
SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	Revisar en los resultados del escaneo que no haya explotaciones publicadas contra las vulnerabilidades encontradas. De ser así se deberán listar y comprobar que estas son explotadas en los controles SPP	En la obtención de la lista de vulnerabilidades no debe haber ninguna explotación existente para estas.		Pendiente

Bajo				Medio			Alto		Crítico		Servicios	Web
0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		web_Sinaloa_red.xlsx	Sinaloa.xlsx

Las vulnerabilidades encontradas se clasifican en base al estándar CVSS 3.1 (<https://www.first.org/cvss/specification-document>)

Nombre Servidor	Dirección IP	CVSS Score	Riesgo	Puerto	Descripción	Recomendación
Firewall SonicWall	187.216.65.254	9.4	Crítico		A buffer overflow vulnerability ¹ in SonicOS allows a remote attacker to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a malicious request to the firewall.	Actualizar el firmware del firewall a la versión recomendada v6.5.1.12-1n
sinapp01 sin-web1	10.3.0.222 10.3.0.224	9.8	Crítico	80, 443	Apache Web Server v2.4.6 presenta 41 vulnerabilidades, 6 alto-crítico, 5 presentes en servidores del PREP	Actualizar a la última versión disponible de The Apache Foundation, v2.4.46
sin-bd1 sinapp01 sin-web1	10.3.0.221 10.3.0.222 10.3.0.224	2.6	Bajo	22	SSH Server CBC Mode Ciphers Enabled	Vulnerabilidad de riesgo bajo y puerto restringido por Firewall y VPN. No acción recomendada

La documentación de vulnerabilidades por activo se presenta en la tabla anexa indicando el nivel de criticidad y riesgo, y los puertos habilitados en cada uno de los activos escaneados.

Recomendaciones:

En el caso de las vulnerabilidades encontradas:

1. Actualizar

¹ <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010>

Resultados Preliminares Escaneo Vulnerabilidades de Servicios Web

Prueba	Criterio Aceptación	Criterio Aceptación	Comentarios	Resultado
SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos	Mediante escaneo de vulnerabilidades y/o software de tipo DAST (para pruebas dinámicas de seguridad de aplicación) obtener las vulnerabilidades de los servicios WEB	Los hallazgos de este escaneo no deberán ser de severidad crítica o alta. De haber nivel medio, deberá existir contramedidas para esta. La lista completa de vulnerabilidades debe estar notificada hacia la parte responsable del OPL.	Se detectaron vulnerabilidades por protocolo de encriptación DES/3DES y TLS v1.0 activos	Pendiente
SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	Se confirmará que el sitio de publicación tenga un certificado válido y que el protocolo de SSL exista (El escaneo se hará desde Internet)	Certificado expedido e instalado y protocolo de cifrado deberá ser TLS1.2 o mayor	Protocolo TLS v1.0 contiene múltiples explotaciones. Referencia: https://cutt.ly/InsRvTZ	Pendiente

Los servidores de WEB se escanearon y se obtuvieron las siguientes vulnerabilidades

Nombre Servidor	Dirección IP	CVSS Score	Descripción	Recomendación
sinapp01	10.3.0.222	7.5	El webserver soporta protocolos de encriptación SSL de fuerza media	Deshabilitar los protocolos de encriptación DES/3DES
sinapp01	10.3.0.222	6.5	TLS Version 1.0 Protocol Detection	Deshabilitar protocolo TLS v1.1 e inferior
sin-web1	10.3.0.224	7.5	El webserver soporta protocolos de encriptación SSL de fuerza media	Deshabilitar los protocolos de encriptación DES/3DES
sin-web1	10.3.0.224	6.5	TLS Version 1.0 Protocol Detection	Deshabilitar protocolo TLS v1.1 e inferior
prepsinaloa.info	varias	6.5	TLS Version 1.0 Protocol Detection	Deshabilitar protocolo TLS v1.1 e inferior
sinapp01	10.3.0.222	4.3	Web Application Potentially Vulnerable to Clickjacking	Habilitar X-Frame-Options response header a una Content-Security-Policy 'frame-ancestors' response header en todas las respuestas de contenido.
sin-web1	10.3.0.224	2.6	Web Server Uses Basic Authentication Without HTTPS	Página pública, además no tendrá la autenticación el día de la elección.

El escaneo de servidores web externo, web interno y base de datos arrojó vulnerabilidades de nivel alto, medio y bajo las cuales no tienen impactos y se pueden resolver del siguiente modo:

1. Deshabilitar la autenticación de páginas por .htaccess
2. Habilitar los headers de respuesta X-Frame-Options
3. Deshabilitar TLS v1.1 e inferior en web servers
4. Deshabilitar protocolo de encriptación DES/3DES

6.4 Pruebas Soporte Operativo

Resultados Preliminares Pruebas de Controles del Soporte Operativo				
Prueba	Criterio Aceptación	Criterio Aceptación	Comentarios	Resultado
PRS01 – La OPL debe tener un manual de capacitación para el personal de captura	Verificar con la OPL la existencia de los manuales	Debe haber un manual disponible para el personal de captura	Cumple, se cuenta con una guía rápida para Capturista	Aceptado
PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP	Se revisará con la OPL la forma como se resuelven dudas o consultas en los distintos procesos del PREP	Debe haber un grupo de personas que atienden llamadas de aclaración de dudas o consultas de las distintas fases del proceso del PREP	Mesa de ayuda con teléfonos IP atendiendo en extensión 3500	Aceptado
PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta	Revisar con la OPL la existencia de dicha organización que permita resolver problemas de captura	Existencia de una mesa de servicio o de soporte para resolución de problemas o dudas en los distintos procesos del PREP así como resolución de las inconsistencias al momento de la captura.	Se cuenta con el módulo de verificación/validación MVEVAL	Aceptado
PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros)	Se deberá comprobar los contratos de soporte externo en caso de eventualidades en caso de que el sistema PREP haya sido elaborado por un tercero	Existencia de un contrato de soporte válido durante la fecha de la jornada electoral para el soporte de la plataforma PREP de la OPL.		Pendiente
PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos	Verificar con la OPL la existencia de contratos existentes con la matriz de escalación y tiempos de resolución por parte del proveedor de telecomunicaciones.	Tener contrato válido con soporte y con los procesos de reporte en caso de eventos, así como los niveles de servicio para resolución de incidentes en caso de que se llegue a reportar algo		Pendiente
PRS06 – Tener los contratos con los proveedores de nube, así como los procedimientos de reporte en caso de eventos hacia ellos. (si se está utilizando Nube como repositorio operativo del PREP)	Verificar con la OPL la existencia de contratos existentes con su matriz de escalación y tiempos estimados de resolución por parte del proveedor de nube (si se está utilizando Nube como repositorio operativo del PREP)	Tener contrato válido con soporte y con los procesos de reporte en caso de eventos, así como los niveles de servicio para resolución de incidentes en caso de que se llegue a reportar algo		Pendiente
PRS07 – Tener la documentación del sistema PREP de la OPL actualizado y en resguardo por los encargados del área de tecnología de la OPL	Verificar con la OPL la existencia de dicho documento de arquitectura y modelación del sistema	Mostrar evidencia de la existencia del documento	Documento PREPSIN_01_DOC_ARQUITECTURA_V1.pdf	Aceptado

Anexo I – Evidencias