

Documento

Versión 1.0 – 19/ENERO/2018

ID: PLAN-13

Plan de Seguridad PREP 2018

PREP 2018 OPL SINALOA



Enero 2018

Confidencialidad del Documento

© 2018 Informática Electoral. Todos los derechos reservados. El contenido de este documento es propiedad de Informática Electoral, cualquier reproducción parcial o total, está estrictamente prohibida si no se hace con el permiso estricto y por escrito de Informática Electoral. Este documento está sujeto a cambios. Cualquier comentario, corrección o pregunta deberán ser dirigidos al autor. http://informaticaelectoral.com/aviso_de_privacidad.pdf



Contenido

0	Prefacio	3
1	Introducción	4
2	Infraestructura e Información	4
2.1	Control de usuarios y Contraseñas con privilegios de operación	4
2.2	Comunicación cifrada de información	4
2.3	Implementación de Red segura para terminales de captura y estructura de Servidores	4
2.4	Mecanismos de redundancia de información y comunicación	4
2.5	Bitácora de Operaciones	4
2.6	Diagrama de Operación del Sistema	5
3	Personal	5

0 Prefacio

Control de versión y administración del documento:

Es responsabilidad del lector asegurarse de tener la última versión de este documento. Cualquier pregunta acerca del mismo deberá ser dirigida al propietario de este documento.

Autor de este documento:

El contacto principal para preguntas y observaciones acerca de este documento es:
Lucilda Berenice Angulo Rodríguez
IE®

Confidencialidad:

La información contenida en este documento deberá tratarse como información privada y confidencial. Esta información no deberá ser divulgada a otras personas que no estén involucradas en el proyecto **PREP 2018 – OPL SINALOA**.

Historia de cambios en el documento:

Fecha	Versión	Descripción	Autor
Enero 2018	1.0	Creación del documento	Lucilda Berenice Angulo Rodríguez

Firmas de Autorización:

Elaboró:	Revisó:	Aprobó:
Lucilda Berenice Angulo Rodríguez Auditoria y Mejora Continua	David Raymundo Aguirre Cabrales Auditoria y Mejora Continua	Jesús Oscar Crespo Palazuelos Director IE



1 Introducción

Este documento tiene como finalidad proporcionar la información sobre los mecanismos de seguridad que son necesarias implementar para el proyecto PREP 2018.

2 Infraestructura e Información

2.1 Control de usuarios y Contraseñas con privilegios de operación

Al ser el PREP un sistema en línea, es necesario que cuente con un mecanismo de acceso, por lo cual se implementará un estricto control y generación de las cuentas de usuario correspondientes. Como segundo nivel de seguridad en este rubro, es preciso señalar que el PREP contemplará diversos privilegios de operación en las cuentas de usuario que se generen, contemplando aspectos, por ejemplo, un usuario de captura del Distrito V, no podrá acceder y capturar casillas e información del Distrito IV, los usuarios de tipo "Consulta", como su nombre lo indica, no podrán capturar información, entre otros.

2.2 Comunicación cifrada de información

Para fortalecer los mecanismos de envío de la información a través de Internet, se implementará en el PREP la comunicación a los servidores del sistema a través de protocolos seguros, en específico HTTPS. Dicho protocolo es el mecanismo estándar a nivel internacional en materia de sistemas de comercio electrónico y servicios bancarios en línea.

2.3 Implementación de Red segura para terminales de captura y estructura de Servidores

A la par del uso de protocolos cifrados para el envío de la información, se establecerá una red privada entre los equipos de cómputo instalados en los CATDS y en oficinas centrales del IEES con los servidores virtuales del PREP. Cabe señalar que solamente los equipos que estén dados de alta en dicha red privada podrán acceder al sistema, incrementando con ello su nivel de seguridad.

2.4 Mecanismos de redundancia de información y comunicación

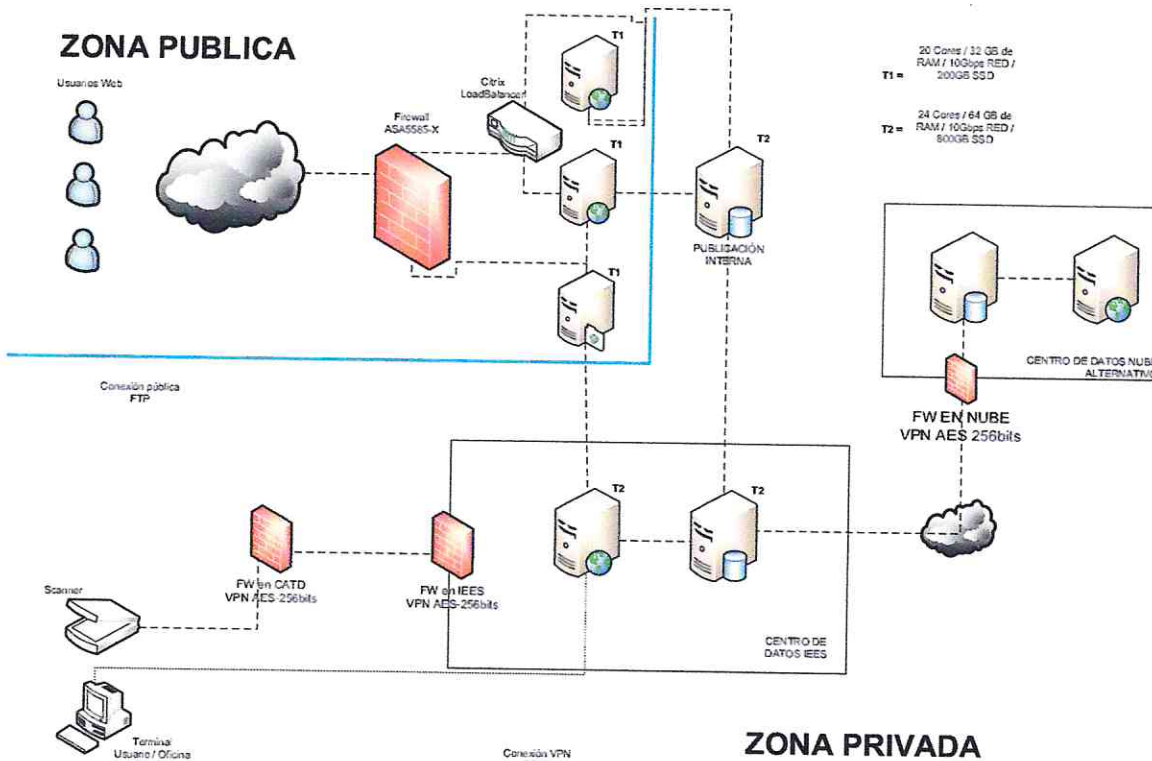
En caso de existir cortes de señal de Internet en algún componente de la red privada, cada CATD contará con un enlace alterno para mantener comunicación con los servidores del sistema.

2.5 Bitácora de Operaciones

Todo sistema de captura con múltiples usuarios debe contar con un control y/o bitácora de operaciones realizadas en el sistema, que incluya desde fecha y hora de ingresos y salidas del

sistema hasta registro de operaciones de captura y consulta de todos los usuarios que tengan contraseña válida para utilización del sistema.

2.6 Diagrama de Operación del Sistema



3 Personal

Se implementará una estrategia para asegurar que el acceso a los CATD sea restringido a solo el personal autorizado por el proveedor y el OPL, para ello deberán portar un gafete personalizado que será proporcionado por la empresa.

No se permitirá el uso de dispositivos móviles de comunicación o fotográficos al interior de las instalaciones, para esto se instalarán 2 líneas de Voz IP a las Oficinas de Coordinación.



