OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Proceso Electoral 2023 2024 Veracruz
Mi voz, mi voto, mi elección

ANÁLISIS DE CIBERSEGURIDAD

Unidad Técnica de Servicios Informáticos

Xalapa, Ver., a 29 de enero de 2024

Contenido

I. Presentación

La Unidad Técnica de Servicios Informáticos (UTSI) del Organismo Público Local Electoral del Estado de Veracruz (OPLE Veracruz), con fundamento en lo previsto en el artículo 25, incisos a), b), c), l) y q) del Reglamento Interior del OPLE Veracruz, tiene entre sus atribuciones de atender los temas en materia informática, cómputo y telecomunicaciones que se requieran para las actividades del proceso electoral, así como la de evaluar y gestionar los riesgos en la implementación de sistemas informáticos, siendo estos sistemas resultado de la coadyuvancia y solicitud por parte de las áreas del OPLE Veracruz.

En ese sentido y derivado del Acuerdo **OPLEV/CG127/2023** por el cual se reforman, derogan y adicionan diversas disposiciones del Reglamento para las Candidaturas a cargos de elección popular para el estado de Veracruz de Ignacio de la Llave y el Informe sobre la factibilidad de la implementación del Sistema de Registro de Candidaturas Locales (SRCL) que emiten la Dirección Ejecutiva de Prerrogativas y Partidos Políticos y la Unidad Técnica de Servicios Informáticos, en el que señala que la UTSI será la responsable de realizar un análisis de la ciberseguridad en torno al sistema antes mencionado.

En ese sentido, el presente análisis de ciberseguridad tiene como propósito el lograr identificar los activos del OPLE Veracruz involucrados en la implementación del SRCL y con ello, protegerlos para que la información recolectada se encuentre segura, así como el poder definir y establecer las medidas de ciberseguridad que se tienen contemplada.

Lo anterior, para poder definir las medidas tecnologícas y físicas que se implementan en el SRCL tendientes a garantizar la seguridad de la información y la estabilidad del sistema.

II. Análisis de ciberseguridad

La ciberseguridad es un conjunto de buenas prácticas utilizadas para proteger los sistemas, las redes, las aplicaciones de software, los datos y los dispositivos de accesos no autorizados que podrían formar parte de ciberataques coordinados y otras amenazas digitales maliciosas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización.

Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial. En este contexto, la ciberseguridad trata de proteger la información confidencial de las organizaciones y salvaguardar la integridad de los sistemas. Los ciberataques pueden tener como objetivo acceder, modificar o destruir datos vitales.

La obligación de mantener un entorno de ciberseguridad eficaz y confiable, minimza la vulnerabildad del sistema lo cual es logrado al implementar medidas de ciberseguridad robustas. Esto incluye la protección de los datos contra accesos no autorizados y la prevención de interrupciones en sistemas clave debido a actividades de red no deseadas.

La implementación efectiva de la ciberseguridad por parte del OPLE Veracruz implica una combinación de protección a nivel de personas, procesos y tecnología. Esto asegura no solo la seguridad de los datos y sistemas, garantizando que los datos y servicios estén protegidos contra amenazas digitales.

En ese sentido, la UTSI del 23 al 29 de enero del presente año realizó la investigación y revisión de los activos relacionados con la implementación del SRCL y para el presente análisis de ciberseguridad se revisará lo concerniente a la seguridad de la red, la seguridad de aplicaciones y la seguridad física, en los siguientes términos:

- Los sistemas operativos y la arquitectura de la red que conforman la seguridad de su red. Puede incluir protocolos de red, cortafuegos, puntos de acceso inalámbricos, hosts y servidores.
- La seguridad de las aplicaciones de software que se enfoca en mantener el software y los dispositivos libres de amenazas.

- Por su parte, la seguridad física se refiere al control del acceso físico a los ordenadores y otros dispositivos.

a. Seguridad de la red

Sistema operativo

El SRCL se encuentra implementado en los activos propios del OPLE Veracruz, se cuenta con un sistema operativo de uso empresarial basado en Linux el cual brinda alto nivel de seguridad para las aplicaciones, contando con las últimas actualizaciones, mismas que contienen comprobaciones periódicamente en sus vulnerabilidades y creando parches de seguridad.

Se cuenta con un programa Oracle VM Manager el cual genera respaldo del sistema operativo, base de datos y configuraciones, por lo que en caso de pérdida o alteración indebida de la información se utilizará el respaldo creado por el programa antes citado.

Los servidores donde se almacenen programas y datos tienen cuentas con diferentes privilegios, teniendo particular cuidado en el nivel de restricción sobre instalación de software o modificación de la información.

Arquitectura de red y Protocolos de la web

Se cuenta con un firewall físico con los siguientes servicios: Prevención de intrusos (IPS), antivirus, filtros DNS, filtros de correos, firewall de aplicaciones web, control de aplicaciones y control de usuarios. Estas plataformas también proporcionan control de aplicaciones, prevención de pérdida de datos, enrutamiento dinámico para IPv4 e IPv6, NAC punto final y la inspección del tráfico cifrado con SSL.

b. Seguridad de las aplicaciones de software

El SRCL es una herramienta informática de desarrollo propio por el personal del OPLE Veracruz, el cual fue desarrollado bajo una plataforma de PHP y con un framework de Laravel versión 10.

Laravel es un framework de código abierto cuya utilidad está en desarrollar aplicaciones y servicios web usando uno de los lenguajes más populares en internet: el PHP. Este framework permite contar con una protección contra vulnerabilidades comunes como el cross-site scripting (XSS) y los ataques de inyección de código.

La configuración realizada en el SRCL, desde al framework Laravel evitará vulneraciones comunes como el cross-site scripting (XSS) y los ataques de inyección de código; los cuales son una vulnerabilidad de seguridad que permite a un atacante inyectar en un sitio web código malicioso del lado del cliente, siendo este código ejecutado por las víctimas y permite a los atacantes eludir los controles de acceso y hacerse pasar por usuarios.

Bases de datos

Ahora bien, a nivel de la base de datos se contempla como medida de seguridad el establecimiento de UUID (Universal Unique Identifier), el cual es un valor de 128 bits que se utiliza para identificar de forma única objetos o entidades, utilizado para en este caso dentro de las tablas del modelo entidad-relación de la base de datos del SRCL, los cuales proporcionan mayor seguridad en protección a las rutas de acceso a los datos.

Claves de acceso

El SRCL es una herramienta web restringida, es decir, si bien esta en una liga pública en internet, el acceso está restringido por medio de credenciales de acceso, que de acuerdo con el Proceso Técnico Operativo (PTO) definitivo por la Dirección Ejecutiva de Prerrogativas y Partidos Políticos (DEPPP) los usuarios que podrán contar con credenciales serán:

1. Partidos Políticos o Candidaturas independientes
    a. Autorizador
    b. Capturista/Digitalizador
2. Candidaturas independientes
    a. Autorizador/Capturista
3. Dirección Ejecutiva de Prerrogativas y Partidos Políticos
    a. Revisor

b. Supervisor

c. Administrador general

4. Consejerías Electorales, Secretaria Ejecutiva y el área asignada por el INE

   a. Consulta

En términos de lo antes señalado cada usuario maneja un perfil que le permite realizar actividades dentro del SRCL, dichos perfiles limitan a su vez el acceso a funciones más complejas, las cuales están delimitadas conforme a la establecido por la DEPPP en el PTO.

El único usuario de alto nivel es el Administrador general de la DEPPP, el cual tiene todos los permisos para realizar modificaciones en el sistema, así como las configuraciones de arranque para los distintos procesos de registro de las candidaturas, acorde con el PTO.

En el caso de los partidos políticos, coalición y candidaturas independientes en el PTO se establece que el otorgamiento de las credenciales quedará sujeto a la solicitud de manera oficial de las cuentas de acceso al sistema y está previsto dentro del mismo SRCL que la DEPPP, bajo su estricta responsabilidad, cree y entregue a las y los interesados las claves de acceso al sistema.

En ese sentido, cada usuario del sistema cuenta con sus credenciales de acceso: usuario y contraseña; en ese tenor, es importante puntualizar que la contraseña es generada por el SRCL y tiene una extensión de 10 caracteres, que incluyen números, letras mayúsculas y minúsculas, aunado a ello se encuentra cifrada para evitar posibles intrusiones.

c. Seguridad física

Los servidores donde se almacenen programas y datos tienen cuentas con diferentes privilegios, teniendo en particular cuidado en el nivel de restricción en la instalación de software.

El acceso al área de servidores se encuentra restringido solo a personal autorizado y en un espacio bajo llave; además de que los equipos están configurados para el cierre de sesiones tras un determinado tiempo de inactividad.

Se contempla la implementación correcta de procesos de autenticación y autorización, de tal forma que solo los usuarios autorizados tienen acceso restringido a funciones y datos necesarios. Se establece en los permisos de los usuarios el principio de privilegios mínimos, garantizando que los usuarios y sistemas solo tengan acceso a los recursos necesarios para realizar sus funciones.

Aunado a lo anterior, se tienen contemplado dentro de la seguridad física los siguientes aspectos para la continuidad de operaciones:

- Redundancia de infraestructura en caso de falla de hardware para el servidor de aplicación y la base de datos.
- Servicio secundario de respaldo de internet.
- instalación eléctrica con tierra física apropiada con la correcta polaridad de los contactos para evitar contratiempos relacionados con el suministro eléctrico.
- Fuentes de alimentación ininterrumpida (UPS) con regulador integrado, de manera que, ante una posible variación en el suministro eléctrico, el equipo de cómputo esté debidamente protegido y pueda continuar su operación.
- Extintores (basados en CO2 y Polvo Químico Seco).

El presente análisis se rinde en la Ciudad de Xalapa, Veracruz a los 29 días del mes de enero del 2024.

Ing. Rafael González Ortiz
Titular de la Unidad Técnica de
Servicios Informáticos