ANÁLISIS DE SEGURIDAD DE SISTEMAS INFORMÁTICOS PARA LAS ELECCIONES DEPARTAMENTALES, REGIONALES Y MUNICIPALES 2021

RESUMEN EJECUTIVO CONCLUSIVO
ÓRGANO ELECTORAL PLURINACIONAL
FECHA: 14 DE MARZO, 2021

DREAMLAB
TECHNOLOGIES

1 RESUMEN EJECUTIVO

Durante los días 23 de febrero al 14 de marzo del año 2021, el equipo consultor de Dreamlab Technologies realizó pruebas correspondientes al Análisis de Seguridad de los Sistemas Informáticos para las Elecciones Departamentales, Regionales y Municipales 2021 solicitado por el ÓRGANO ELECTORAL PLURINACIONAL (OEP) con el fin de realizar una evaluación integral de Seguridad en la plataforma informática y la efectividad de los controles de seguridad que hayan sido implementados para preservar la seguridad de la Información.

Adicionalmente, de forma paralela y hasta fecha 14 de marzo del año 2021, el equipo consultor de Dreamlab Technologies realizó el acompañamiento en la corrección de vulnerabilidades y el retest a los hallazgos identificados sobre los activos marcados como prioritarios de cara a las elecciones subnacionales realizadas el día domingo 7 de marzo. Posteriormente a ello se continuó con la corrección sobre el resto de los elementos de riesgo crítico, alto y medio.

El análisis de seguridad se derivó en la ejecución de dos actividades:

- Pruebas de Penetración externas
- Pruebas de Penetración internas

Todas las pruebas se realizaron en modalidad caja negra (sin conocimiento previo de los elementos a analizar) y además en modalidad caja gris para lo cual se nos proporcionó tanto conectividad a la red interna como cuentas de acceso a los distintos aplicativos en la red interna. Resultado de las pruebas realizadas, se identificaron observaciones con distintos niveles de criticidad.

La evaluación externa permitió identificar hallazgos sobre los servicios expuestos a internet sobre los subdominios del OEP (*.oep.org.bo). La entidad solicitó priorización sobre los hallazgos que afectan a los servidores de cómputo que fueron utilizados durante la publicación de las elecciones subnacionales 2021, estos hallazgos priorizados fueron subsanados. También se realizaron pruebas de Denegación de Servicio sobre 3 portales del OEP: www.oep.org.bo, yoparticipo.oep.org.bo y computo.oep.org.bo, se evidencia que el servicio de protección WAF utilizado (Cloudflare), protege correctamente contra este tipo de ataques. Existe un conjunto de observaciones no relacionadas con estos subdominios que aún quedan

pendientes de resolución por parte del OEP detallados en los informes técnicos de análisis y seguimiento.

En la evaluación de la infraestructura interna se evidenció que se ha implementado una red independiente de la red de trabajo actual del personal interno del OEP, que además se encontraba aislada de conectividad a internet y que fué utilizada para el cómputo de resultados durante las elecciones subnacionales. En dicha red existen controles de seguridad como ser: un gestor de configuraciones y parches de seguridad, mecanismos de segregación de la red interna y antivirus instalado en los equipos que corren bajo Windows.

Durante la evaluación interna se identificaron hallazgos con distintos niveles de criticidad que debilitaban la seguridad en la infraestructura interna a nivel de estaciones de trabajo y servidores. El proceso de acompañamiento para su respectiva resolución, mitigó gran parte de los hallazgos en los rangos crítico, alto y medio, minimizando los vectores necesarios para una posible intrusión, siendo que las observaciones remanentes deberían ser controladas mediante monitorización durante los días de elecciones y además continuar trabajando sobre las observaciones remanentes, en los días posteriores al proceso de cómputo para fortalecer aún más la infraestructura.

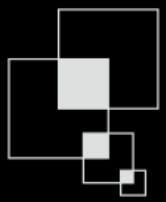
Este análisis, además, incluyó la revisión de aplicativos de escritorio para el procesamiento de actas y aplicativos web para presentación de resultados tanto de forma interna como a través de AWS, cuyas observaciones fueron mitigadas durante el proceso de acompañamiento. El aplicativo de consolidación de resultados aún no había sido publicado en internet, por lo que fue evaluado en ambiente interno de la red cómputo, sin observación alguna. Recomendamos además: habilitar, resguardar y monitorizar los registros de actividades de los sistemas en caso de generarse algún incidente.

Adicionalmente se realizó una revisión documental a las políticas de seguridad internas. Las cuales fueron generadas en septiembre de 2020, actualizadas y adaptadas a la fecha en función a las operaciones de la organización, se recomienda continuar la implementación del SGSI adaptándola además a los procesos del OEP fuera del periodo de elecciones.

Finalmente se realizó una inspección de los ambientes físicos en los cuales se evidencia una adecuada implementación de controles de seguridad y medidas de contingencia en caso de la materialización de distintas categorías de riesgos.

Los detalles técnicos, cuantificación de hallazgos, vulnerabilidades, observaciones, efectos y condiciones de las pruebas fueron presentados oportunamente en las fechas solicitadas por el OEP, así como los detalles de la corrección de hallazgos identificados y el retest, en los respectivos informes técnicos y ejecutivos, presentados en cumplimiento a nuestras obligaciones contractuales antes de la celebración del proceso electoral.

NICHT GLAUBEN, WISSEN.



DREAMLAB
TECHNOLOGIES