Resumen Ejecutivo

Servicio de consultoría por producto para fortalecimiento y monitoreo de infraestructura tecnológica para las elecciones generales 2020

Entorno de Trabajo

Cliente	Órgano Electoral Plurinacional
Proyecto	CD-POE-R N° 144/2020 (2DA CONVOCATORIA) SERVICIO DE CONSULTORIA POR PRODUCTO PARA FORTALECIMIENTO Y MONITOREO DE INFRAESTRUCTURA TECNOLÓGICA PARA LAS ELECCIONES GENERALES 2020
Fecha	04-Nov-2020

Índice

1. Antecedentes 3
2. Periodo de la Consultoría 3
3. Alcance de la Auditoría 3
4. Desarrollo de la Auditoría 4
   4.1 Wazuh 4
   4.2 Kibana 4
   4.3 Elasticsearch 4
   4.3 Pentest365 4
5. Conclusiones 6

1. Antecedentes

Por invitación del OEP nos presentamos a través de nuestro Partner en Bolivia CAMWAVE SRL, a la licitación CD-POE-R N° 144/2020 (2DA CONVOCATORIA) SERVICIO DE CONSULTORIA POR PRODUCTO PARA FORTALECIMIENTO Y MONITOREO DE INFRAESTRUCTURA TECNOLÓGICA PARA LAS ELECCIONES GENERALES 2020, la cual fue adjudicada a nuestro Partner a través del cual realizamos todo el trabajo de consultoría de seguridad para la auditoria y monitoreo de la Elecciones Generales 2020.

2. Periodo de la Consultoría

Previamente a la puesta de agentes en cada servidor, los servidores no externalizaban ningún tipo de información acerca de su funcionamiento, tráfico o movimiento, por lo tanto, su comportamiento no podía ser observado ni mucho menos monitorizado. Cada servidor tiene un sistema operativo, funcionamiento y objetivo distinto, es así que el punto de vista de la monitorización para cada uno, no siempre es similar.

3. Alcance de la Auditoría

De acuerdo a lo solicitado y contratado por parte del OEP, el alcance se desglosa en los siguientes puntos:

1. **Análisis de intrusión interna, externa a la infraestructura de Cómputo Oficial**
   1.1. ANALISIS DE INTRUSIÓN EXTERNA
   Análisis de intrusión desde internet, simulando ser un atacante externo, con conocimientos de las aplicaciones objetivo del cliente
   1.2. ANÄLISIS DE INTRUSIÓN INTERNA
2. **Corrección de Vulenrabilidades**
   Una vez identificadas las vulenrabilidades brindar el apoyo a través de nuestro Ciber-SOC con los manuales de remediación o recomendaciones de remediación de los hallazgos identificados.

3. **Fortalecimiento de Infraestructura Tecnológica (Hardening)**
   Apoyar a la DNTIC en el fortalecimiento de la infraestructura tecnológica para eliminar los vectores de ataque y reducir el riesgo tecnológico de ataques o fallas de la infraestructura electoral.

4. **Monitoreo y Seguridad Persistente**
   Plataforma de seguridad implementada por nuestra empresa para el monitoreo persistente 24/7 y defensa ante ataques a la infraestructura tecnológica utilizada para la difusión rápida de resultados y el cómputo oficial de resultados. Dicho monitoreo fue ejecutado durante el proceso electoral hasta su conclusión y confirmación del OEP

El objetivo en términos específicos busca cumplir con los siguientes aspectos:

- Seguimiento de los eventos críticos de los sistemas.
- Seguimiento de logs o registros de los servicios web.
- Almacenamiento de toda la información extraída de los seguimientos.
- Visualización en tiempo real de la información a la que se hace el seguimiento
- Dashboard de eventos de monitoreo en tiempo real

4. Desarrollo de la Auditoría

La auditoría se realizó de forma normal a través de tecnologías especializadas para este tipo de trabajo como son Wazuh, Kibana, Elasticsearch y Pentest365. Las cuales se describen a continuación para una mayor comprensión de este reporte.

4.1 Wazuh

Es un sistema para la detección de intrusos e irregularidades a nivel de host, entre muchas de sus funcionalidades según el caso se pueden citar los siguientes:

- Seguimiento de la salud del host (activo o inactivo)
- Seguimiento de registros
- Seguimiento de eventos
- Seguimiento de logs

4.2 Kibana

Panel de código abierto para la visualización de la información.

4.3 Elasticsearch

Servidor de búsquedas, con un motor de búsqueda incorporado, dicho motor es sumamente versátil y rápido, brindando la posibilidad de realizar consultas o búsquedas instantáneamente.

4.3 Pentest365

Plataforma de auditoría persistente para identificar vulnerabilidades y riesgos en infraestructuras tecnológicas tanto a nivel de aplicaciones web, infraestructuras web, servidores, sistemas operativos y dispositivos de red.

Dentro el desarrollo de la Auditoría se identificaron diferentes incidentes tanto de Seguridad como de Monitoreo, los cuales fueron subsanados en su momento por el personal técnico de la DNTIC en apoyo con nuestros especialistas.

A nivel de incidentes de ciberseguridad en cuanto al sistema de cómputo, se encontraron 7 vulnerabilidades presentadas en diferentes días previos al día de la elección, las mismas fueron reportadas inmediatamente y se trabajo junto con el personal de la DNTIC para parchar y subsanar las vulnerabilidades.

Todas las 7 vulnerabilidades reportadas en el sistema de cómputo SCORC fueron debidamente parchadas y subsanadas antes del inicio de las elecciones generales.

Para el monitoreo de las Elecciones Generales se desplegaron agentes de monitoreo en toda la infraestructura local de la DNTIC, en todos los servidores de transacción, bases de datos y también en la infraestructura de servidores de transmisión de actas alojados en Amazon.

Durante el monitoreo de las Elecciones Generales, se registraron 44 incidentes que reportamos inmediatamente al personal de la DNTIC asignado al proyecto de monitoreo, quienes oportunamente respondieron a nuestras alertas explicando el porqué de las mismas cooperando para bajar la criticidad o eliminar los fasos positivos.

Todos los incidentes reportados y sus consecuentes respuestas por parte de la DNTIC se encuentran en los reportes de monitoreo que se entregaron en fecha al OEP.

Dentro las protecciones a nivel de infraestructura, se configuró una en red confinada basada en seguridad de direcciones MAC con los TED’s y se implementó un mecanismo de replicación de resultados en la red interna y externa (AWS), las cuales fueron monitoreadas 24/7.

Como protocolo de seguridad en base a la ISO 27001, se desarrolló un protocolo de congelamiento y puesta en cero del sistema, previo al proceso electoral.

Nuestro equipo de expertos trabajó arduamente con los funcionarios de la DNTIC para realizar un fortalecimiento de la infraestructura electoral llevando a cabo varias pruebas de carga, pruebas de estrés y configuraciones de seguridad en toda la infraestructura electoral.

Durante el monitoreo ocurrieron algunos incidentes que requirieron la presencia de nuestros auditores para presenciar y asegurar procesos técnicos de la DNTIC, como empresa auditora donde nuestro protocolo permitió identificar el tipo de procedimiento a realizar, identificar a los presentes y grabar o tomar las evidencias necesarias para preservar todo el acto informático.

5. Conclusiones

- Nuestro servicio y la entrega de los reportes según el contrato se presentaron en tiempo y en las fechas indicadas en el contrato para cumplir con el mismo.
- El monitoreo del sistema de producción se realizó desde el 18 de octubre hasta el 24 de octubre, previo a esto se instalaron los agentes a los equipos que la DNTIC determinó para el funcionamiento del sistema de cómputo.
- Los eventos que se generaron durante el proceso electoral fueron explicados por el equipo de DNTIC de manera oportuna.
- Todas las vulnerabilidades reportadas dentro la auditoría fueron subsanadas oportunamente por la DNTIC y con el apoyo de nuestros especialistas antes del inicio de las Elecciones Generales.
- Se implementaron múltiples controles de seguridad en la infraestructura electoral para mantener un adecuado nivel de seguridad durante las elecciones.
- Durante todo el proceso electoral se mantuvo un adecuado nivel de comunicación entre la empresa auditora y el personal de la DNTIC.
- Durante la jornada del 20 de Octubre participamos como parte auditora del procedimiento del potenciamiento del servidor de base de datos de la pagina web externa de resultados para que la misma pueda soportar mayor cantidad de peticiones o visitas en línea. Este procedimiento se realizó delante de la prensa, del personal de la DNTIC y de nuestro equipo de auditores donde la pagina web no se paró en ningún momento.
- Todos los registros de auditoría reposan con su debido backup

Trazabilidad:

Fecha de Entrega	04-11-2020
Elaborado por	Alvaro Andrade Gonzalo Nina Diego Bagur