SERVICIO DE CONSULTORÍA POR PRODUCTO - FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA - ELECCIONES JUDICIALES

ÓRGANO ELECTORAL PLURINACIONAL
BOLIVIA

RESUMEN EJECUTIVO

INFORME DE FORTALECIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA (HARDERING) Y MONITOREO Y SEGURIDAD PERSISTENTE

La seguridad no es un producto, es un proceso constante

CamWave
Comunicaciones Unificadas

Powered by
EthicalHacking
Consultores

INFORME CONSOLIDADO

FORTALECIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA (HARDENING)

MONITOREO Y SEGURIDAD PERSISTENTE

RESUMEN EJECUTIVO

Cliente	Órgano Electoral Plurinacional
Proyecto	SERVICIO DE CONSULTORÍA POR PRODUCTO - FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA - ELECCIONES JUDICIALES 2024
Fecha	23 - diciembre - 2024

Av. Villegas No. 6450 - Zona Irpavi - Telf. (591 - 2) - 2723644 - info@camwave.com.bo
La Paz - Bolivia

Tabla de contenido

Av. Villegas No. 6450 - Zona Irpavi - Telf. (591 - 2) - 2723644 - info@camwave.com.bo
La Paz - Bolivia

INFORME FINAL CONSOLIDADO
SERVICIO DE CONSULTORÍA POR PRODUCTO
FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA
ELECCIONES JUDICIALES 2024

Introducción

En cumplimiento del contrato administrativo y los términos de referencia establecidos por el Órgano Electoral Plurinacional de Bolivia (OEP), se realizaron las actividades correspondientes al servicio de consultoría por producto. Este informe consolida los resultados obtenidos en las fases de "Fortalecimiento de Infraestructura Tecnológica (Hardening)" y "Monitoreo y Seguridad Persistente" realizadas en el marco del proceso electoral de las Elecciones Judiciales 2024.

1. Fortalecimiento de Infraestructura Tecnológica (Hardening)

1.1 Objetivo: Endurecer las políticas y condiciones de seguridad de la infraestructura tecnológica para evitar escalaciones de privilegios en caso de vulneraciones.

1.2 Actividades Realizadas:

- Identificación de procesos y servicios en ejecución
- Identificación de cuentas de usuario
- Revisión de reglas de filtrado y lista de control de accesos
- Protección frente a ataques físicos o de hardware
- Configuración de contraseñas
- Protección de cuentas de administración
- Fortalecimiento de credenciales de usuarios
- Restricción de instalación de software y hardware en base a políticas de seguridad
- Habilitación de sistemas de auditoría y monitoreo de logs de servidores y equipo perimetral
- Aseguramiento de consolas de administración, pantallas de logueo y accesos remotos
- Administración de paquetes de instalación, parches de seguridad en servidores y equipos
- Aseguramiento de código fuente y software
- Configuración y afinamiento de reglas en firewalls y software de seguridad

Av. Villegas No. 6450 - Zona Irpavi - Telf. (591 - 2) - 2723644 - info@camwave.com.bo
La Paz - Bolivia

- Implementación de esquemas de seguridad DMZ en base a infraestructura del OEP.

1.3 Resultados Clave:

- Las credenciales utilizadas tienen la robustez adecuada en longitud y complejidad.
- Los servidores cuentan con los servicios necesarios y actualizaciones recientes.

---

2. Monitoreo y Seguridad Persistente

2.1 Objetivo: Implementar un monitoreo efectivo de la infraestructura tecnológica para garantizar la identificación, análisis y mitigación de eventos relevantes durante el proceso electoral.

2.2 Actividades Realizadas:

- Instalación de software de monitoreo y defensa.
- Instalación de agentes para monitoreo y defensa, remotos.
- Configuración de logs de eventos de sistema operativo, servicios web, dispositivos de red, antivirus, firewalls, active directory, etc.
- Identificación de puertos y servicios de forma pasiva y activa.
- Identificación de tecnologías vulnerables.
- Identificación de vulnerabilidades web.
- Identificación de correos electrónicos comprometidos.
- Identificación de redes sociales comprometidas.
- Despliegue gráfico de infraestructura externa e interna
- Despliegue de tableros de monitoreo de infraestructura y eventos.
- Monitoreo, alertas y defensa persistente (24/7) durante el proceso electoral, cómputo oficial de resultados, hasta su conclusión.
- Capacitación al personal del OEP para acceso y consulta a la plataforma de monitoreo
    - **22 equipos internos:** Sistemas de cómputo no accesibles al público.
    - **5 equipos externos:** Incluyen 4 servidores para las páginas departamentales y 1 para la página principal del OEP.
- Configuración de logs para sistemas operativos, servicios web, dispositivos de red, antivirus, firewalls y Active Directory.

Av. Villegas No. 6450 - Zona Irpavi - Telf. (591 - 2) - 2723644 - info@camwave.com.bo
La Paz - Bolivia

- Identificación de riesgos y vulnerabilidades, incluyendo puertos y servicios activos, tecnologías vulnerables y correos electrónicos comprometidos.
- Visualización y seguimiento mediante tableros de monitoreo y despliegue de gráficos de infraestructura interna y externa.
- Monitoreo persistente 24/7 durante el proceso de cómputo oficial.
- Capacitación al personal del OEP para el uso de la plataforma de monitoreo y entrega de credenciales de acceso.

2.3 Resultados Clave:

- Instalación exitosa de agentes de monitoreo en 22 servidores internos y 5 externos.
- Centralización de logs en un servidor único para facilitar el análisis.
- Identificación y gestión de 33 eventos registrados durante el monitoreo, ninguno de los cuales comprometió la estabilidad o integridad del sistema.
- Capacitación exitosa del personal del OEP para el uso de la plataforma de monitoreo.

2.4 Conclusiones: El monitoreo continuo permitió garantizar la estabilidad del sistema durante el proceso electoral, fortaleciendo la capacidad de análisis y respuesta del equipo técnico del OEP.

---

3. Conclusión General:

El servicio de consultoría por producto alcanzó los objetivos establecidos, fortaleciendo la infraestructura tecnológica del OEP y garantizando la estabilidad durante el proceso electoral. Las acciones realizadas y los resultados obtenidos sientan una base sólida para futuras mejoras en la seguridad y operatividad del sistema.

Av. Villegas No. 6450 - Zona Irpavi - Telf. (591 - 2) - 2723644 - info@camwave.com.bo
La Paz - Bolivia