



Recomendaciones de Seguridad para Procesos Electorales

Guía v1.1



Contenido

del Documento



Este documento pretende dar una serie de lineamientos y recomendaciones que consideramos importantes para llevar acabo unas elecciones con un nivel de seguridad recomendable y genere confiabilidad de los resultados.



- ✓ El Proceso Electoral
- ✓ El Software Electoral
- ✓ Código fuente o Licencia
- ✓ Características
- ✓ Componentes de Seguridad
- ✓ Capacitación
- ✓ El Hardware Electoral
- ✓ Infraestructura Local
- ✓ Infraestructura Cloud
- ✓ Jurisdicción y Competencia
- ✓ Ciberseguridad y Monitoreo
- ✓ Previo a las Elecciones
- ✓ Durante las Elecciones
- ✓ Despues de las Elecciones
- ✓ Transporte de Actas Físicas
- ✓ Consideración de Tiempos
- ✓ El Equipo Técnico
- ✓ Disclaimer Legal



El Proceso Electoral

El proceso electoral es organizado por el Tribunal Supremo Electoral, como una entidad autónoma, administrada por un consejo ciudadano compuesto por su presidente y sus Vocales, quienes deben actuar siempre con certeza, legalidad, independencia, imparcialidad, máxima publicidad, transparencia y objetividad; quienes se manejarán de acuerdo con lo que dispone la Constitución Política de Estado (CPE) y Código Electoral Boliviano.



1

EI Software

Electoral



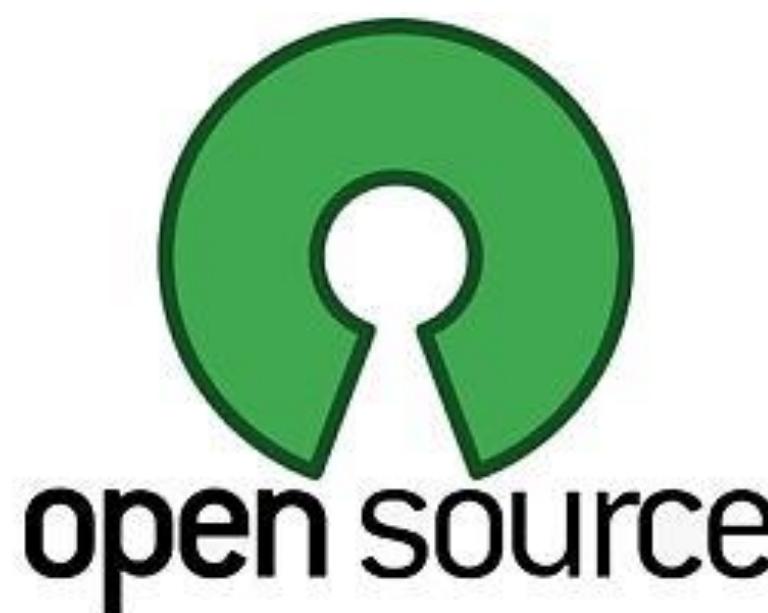
Código Fuente o Licencia de Software

```
    'role_id' => $role_details['id'],
    'resource_id' => $resource_details['id'],
);
if ( $this->rule_exists( $resource_details['id'], $role_details['id'] ) {
    if ( $access == false ) {
        // Remove the rule as there is currently no need for it
        $details['access'] = !access;
        $this->sql->delete( 'acl_rules', $details );
    } else {
        // Update the rule with the new access value
        $this->sql->update( 'acl_rules', array( 'access' => $access ) );
    }
}
foreach( $this->rules as $key=>$rule ) {
    if ( $details['role_id'] == $rule['role_id'] && $details['access'] == false ) {
        if ( $access == false ) {
            unset( $this->rules[ $key ] );
        } else {
```

En caso de que el software sea, desarrollo propio o desarrollo tercionalizado, se recomienda contar siempre que se pueda, con el código fuente para poder darle soporte al mismo, mejorarlo, actualizarlo o para tareas de auditoría de código seguro.



En caso de que se adquiera una licencia de uso de un software electoral el mismo se recomienda que sea de uso ilimitado durante toda la elección, que incluya soporte, mantenimiento, capacitación y transferencia de conocimiento a personal técnico del Tribunal Electoral que permita a estos administrar el software durante las elecciones y no dejar 100% el control a la empresa fabricante del software.



Otra opción es el Software Open Source para procesos electorales, donde el componente de seguridad es auditado y testeado por una gran cantidad de desarrolladores. uno de los inconvenientes es que debe implementarse por lo menos con 4 a 6 meses previos a las elecciones ya que requiere bastante configuración, adecuación y pruebas de funcionalidad para que se adecue a cada proceso electoral específico.

Características del Software Electoral

Cualquier software electoral que se deseé utilizar, debe contribuir a crear elecciones rápidas, flexibles y exactas. Que permita identificar comportamientos sospechosos o fraudulentos de forma sencilla, controlar grandes cantidades de información con facilidad y exactitud, preservando siempre la disponibilidad, trazabilidad, integridad y seguridad de la información almacenada.

El software electoral que se utilice debería apoyar mínimamente en los siguientes procesos:

- ✓ Documentación del Software Electoral
- ✓ Transferencia de conocimiento al TSE
- ✓ Despliegue
- ✓ Votación
- ✓ Escrutinio
- ✓ Consolidación
- ✓ Proclamación de Candidatos
- ✓ Backup de Bases de Datos
- ✓ Auditoría



Componentes de Seguridad del Software Electoral

Cualquier software electoral que se deseé utilizar, debe cumplir con las siguientes recomendaciones de Seguridad para considerarse apto para manejar cualquier tipo de proceso electoral:

- ✓ Comunicaciones Cifradas
- ✓ Utilizar algoritmos de cifrado conocidos
- ✓ No utilizar algoritmos de cifrado propios
- ✓ Certificación de haber sometido el software a una auditoria de seguridad o pruebas de Penetración
- ✓ Manejar un módulo de Seguridad de la aplicación
- ✓ Manejar Integridad de las Bases de Datos
- ✓ Generar Registros de Auditoría (logs)
- ✓ Código Fuente documentado (Si el código se entrega)
- ✓ Proveer infraestructura ideal donde funciona el software
- ✓ Si posee Aplicación Móvil, debe hacer sido auditada bajo OWASP Mobile mínimamente.
- ✓ Si posee hardware de Biometría debe ser certificado seguro
- ✓ Monitoreo persistente 24/7 (Previo / Durante y Despues del computo electoral)
- ✓ Equipo de Blue & Red Team (Respuesta y Reacción ante incidentes de Seguridad)
- ✓ Balanceadores de Carga
- ✓ Protección anti Denegación de Servicios



Capacitación

La capacitación o transmisión de conocimiento es otro de los factores primordiales al momento de escoger un software electoral ya que la empresa propietaria o desarrolladora deberá garantizar la correcta capacitación al personal del Tribunal Electoral para que estos puedan administrar al 100% todo el proceso electoral y que la empresa desarrolladora solamente brinde tareas de soporte o mantenimiento a la plataforma:

- ✓ *La empresa desarrolladora del software debe garantizar la correcta transmisión de conocimiento al órgano electoral*
- ✓ *Es recomendable que las capacitaciones sean en el mismo idioma del país donde se llevarán acabo las elecciones para reducir la curva de aprendizaje.*
- ✓ *El idioma del software es otro punto primordial al momento de transferir conocimiento a los operadores que administrarán la plataforma.*
- ✓ *Las capacitaciones deben incluir varios simulacros hasta el 100% de las actas para poner a prueba tanto al software electoral como a los RRHH entrenados.*
- ✓ *Las capacitaciones deben incluir varios simulacros, para identificar posibles fallas o malas configuraciones del software electoral.*
- ✓ *Las capacitaciones deben cubrir al 100% del personal y operadores que participaran del proceso electoral.*

2

EI Hardware

Electoral



Infraestructura Local

Por temas de Administración, mantenimiento, soporte y sobre todo seguridad, la infraestructura de servidores, redes y comunicaciones, debe estar dentro del mismo Data Center del Tribunal Electoral, para lo cual se deben considerar los siguientes aspectos:

- ✓ Auditoría de Seguridad a la infraestructura de Redes y Comunicaciones que se usará en las Elecciones
- ✓ Remediación y Hardening de Infraestructura de Redes y Comunicaciones que se usará en las Elecciones
- ✓ Auditoría de Seguridad a la infraestructura de Servidores que se usará en las Elecciones.
- ✓ Remediación y Hardening de Infraestructura de Servidores que se usará en las Elecciones.
- ✓ Confinamiento de la red de comunicación con los Tribunales Departamentales Electorales
- ✓ Configuración de Port Mirroring con cada computadora autorizada en cada TED.
- ✓ Comunicación únicamente por VPN's con cada TED



Infraestructura Cloud

Jurisdicción y Competencia

Por temas de Jurisdicción y competencia ante cualquier eventualidad donde el gobierno, un organismo internacional o una empresa de auditoría, necesiten acceder a los Registros de Eventos (Logs) de los servidores utilizados en la elección se recomienda que:

- ✓ La Nube que se vaya a utilizar ya sea Pública o Privada, se encuentre dentro del territorio nacional, donde se tenga jurisdicción y competencia.
- ✓ El proveedor de la Nube Pública o Privada, mantenga un infraestructura certificada tipo TIER III recomendablemente o en su caso TIER II.
- ✓ El proveedor de la Nube Pública o Privada, mantenga otro IDC redundante a no menos de 7 Kilómetros de distancia.
- ✓ El proveedor de la Nube Pública o Privada, provea tanto soluciones bajo licenciamiento como soluciones de Software Libre dentro sus servicios
- ✓ El proveedor de la Nube Pública o Privada, provea un servicio de Soporte 24/7 especialmente para todo el proceso electoral

3

Ciberseguridad Y Monitoreo



Previo a las Elecciones

Como parte de las tareas preparatorias para las elecciones electorales se recomiendan las siguientes tareas:

- ✓ Contratación de una empresa de Ciberseguridad como contraparte de la empresa que brinda el software electoral. Esta recomendación aplica con mas fuerza si el software es desarrollo propio o a medida.
- ✓ Poner el Software Electoral bajo Pruebas de Penetración Controladas o Ethical Hacking como se conoce por su nombre en Ingles.
- ✓ Identificar todas las posibles fallas y vulnerabilidades para reportarlas oportunamente al desarrollador del software y este tenga tiempo de parcharlas adecuadamente.
- ✓ Poner nuevamente bajo Pruebas de Penetración, cada vez que el software ha sido parchado, para verificar que las remediaciones fueron correctamente implementadas o todavía persisten las vulnerabilidades o se crearon nuevas a partir del parche aplicado.
- ✓ Poner la infraestructura de Red, Comunicaciones y Servidores, bajo Pruebas de Penetración Controladas o Ethical Hacking como se conoce por su nombre en Ingles.
- ✓ Desplegar y realizar pruebas de funcionalidad de todo el sistema de monitoreo de seguridad instalado.
- ✓ Validar que los controles de seguridad implementados no entran en conflicto con el software electoral
- ✓ Ejecutar protocolo de Seguridad en servidores y BBDD para inicio de la Votación Electoral

Durante las Elecciones

Como parte de las tareas a ejecutarse durante las elecciones electorales se recomiendan las siguientes tareas:

- ✓ Monitoreo persistente 24/7 de toda la infraestructura electoral tanto local como Cloud
- ✓ Registro de incidentes de seguridad
- ✓ Reportes periódicos del perímetro de seguridad y alertas generadas
- ✓ Monitoreo del flujo de datos que llegan tanto del extranjero como de los TEDs
- ✓ Análisis de tendencias por direcciones IP's en el flujo de datos
- ✓ Validación automatizada de IP's autorizadas para enviar datos
- ✓ Monitoreo persistente del control de accesos a la infraestructura
- ✓ Monitoreo persistente de conexiones a las bases de datos
- ✓ Monitoreo persistente de integridad de configuraciones
- ✓ Puesta en ejecución del Plan de Comunicación y notificación Interna

Después de las Elecciones

Como parte de las tareas posteriores a las elecciones electorales se recomiendan las siguientes tareas:

- ✓ Continuar monitoreando todos los accesos a toda la infraestructura electoral aun después de terminado el computo.
- ✓ Solicitar la ejecución del protocolo de Backup de las Bases de Datos, siempre en presencia de un responsable de la Dirección Nacional de Tecnología del Órgano Electoral, de la empresa de Auditoría de Seguridad y del responsable del Software Electoral.
- ✓ Generar los Hashes de integridad de los backups de bases de datos con un algoritmo que no este deprecado y se encuentre vigente como ser SHA-512
- ✓ Solicitar la ejecución del protocolo de Backup del Sistema de Monitoreo, con su correspondiente hash de integridad, siempre en presencia de un responsable de la Dirección Nacional de Tecnología del Órgano Electoral, de la empresa de Auditoría de Seguridad y del responsable del Software Electoral.
- ✓ Validar que se cumplan todos los protocolos y controles de seguridad implementados

4

Transporte de Actas Físicas



Transporte de Actas

Es obligación del Tribunal Electoral brindar las medidas necesarias para proteger el transporte de las Actas Físicas, por lo cual presentamos algunas recomendaciones:

- ✓ *No permitir que el transporte de las actas se realice en vehículos personales de los Jefes de mesa*
- ✓ *Brindar transporte seguro de actas a través de la asignación de un vehículo militar o policial.*
- ✓ *Permitir que en el vehículo de transporte pueda subir por lo menos 3 representantes de 3 partidos diferentes*
- ✓ *De ser posible incorporar una cámara web en cada vehículo militar o policial para el transporte de actas*
- ✓ *Mejorar la seguridad de los sobres precintados para el transporte de actas*

5

Consideración De Tiempos



Consideración de Tiempos

Algunas recomendaciones de tiempos a tomar en cuenta para una correcta implementación de un proceso electoral:

- ✓ *Obtener el software electoral por lo menos con 3 meses antes de las elecciones para poder hacer las pruebas y configuraciones necesarias.*
- ✓ *Realizar la capacitación y transferencia de conocimiento del software electoral a los operadores del OEP por lo menos con 2 meses de tiempo.*
- ✓ *Realizar las pruebas de Seguridad y Auditoría al software electoral por lo menos 2 meses antes de las elecciones para que exista un tiempo prudente para la remediación de las vulnerabilidades encontradas.*
- ✓ *Realizar las pruebas de funcionalidad por lo menos un mes antes con frecuencias de 4 veces por semana.*

6

El Equipo

Técnico



El Equipo Técnico

Consideramos que es primordial para acortar la brecha de aprendizaje, un equipo con un alto grado de conocimiento técnico que pueda facilitar tanto la transmisión de conocimiento hacia los operadores del software electoral, como la implementación, configuración y despliegue de capacidades hasta la puesta en marcha de todo el proceso de votación electoral.

Este equipo debe contar con expertos en ciertas áreas tecnológicas como ser:

- ✓ Ciberseguridad (Web, Mobile, Reversing)
- ✓ Redes y dispositivos de Capa 3
- ✓ Bases de Datos
- ✓ Big data y Analítica
- ✓ Monitoreo de Seguridad
- ✓ Firewalls, IDS, IPS
- ✓ DevOps

7

Disclaimer

Legal



Disclaimer Legal

El presente documento no pretende ser una guía oficial para llevar acabo un proceso electoral, sino un conjunto de directrices y recomendaciones que por nuestra experiencia y únicamente desde nuestro punto de vista vemos necesarias para brindar mas confianza y seguridad a un proceso electoral.

Es por esta razón que deseamos compartir esta primer versión y el documento queda abierto a nuevas interpretaciones, correcciones o aportes de mejora desde el repositorio <https://github.com/aandradex/Elecciones-Seguras> o a través del correo info@ehcgroup.io

Fin

Este documento esta liberado bajo la Licencia Attribution-ShareAlike 4.0 International de Creative Commons.



Esta licencia permite a otros remezclar, retocar, y crear a partir de esta obra, incluso con fines comerciales, siempre y cuando de el crédito al autor original y se licencien sus nuevas creaciones bajo los mismos términos.

info@ehcgroup.io | www.ehcgroup.io
Panamá, Ciudad de Panamá



www.ehcgroup.io