IEE BCS

INSTITUTO ESTATAL ELECTORAL DE BAJA CALIFORNIA SUR

COMITÉ TÉCNICO ASESOR DEL **SISTEMA DE CÓMPUTOS DISTRITALES Y MUNICIPALES (COTASISCOM)**

ANÁLISIS Y DISEÑO DEL SISTEMA DE CÓMPUTOS DISTRITALES Y MUNICIPALES (SISCOM) PROCESO LOCAL ELECTORAL 2017-2018

Contenido

Introducción.

El presente documento comprende el análisis del **Sistema de Cómputos Municipales y Distritales (SISCOM)**, y en él se deriva la introducción a las metodologías de trabajo a utilizar desde un enfoque de Administración de Proyectos para organizar la labor documental y elementos de SCRUM para llevar a cabo de manera eficaz y efectiva los procesos de análisis, desarrollo y despliegue de la aplicación con calendarización y entregables definidos y una alta participación de las áreas involucradas para concluir en un producto de calidad y en forma.

Dentro de la etapa de análisis se establecerán las prácticas que se aplicarán a lo largo de todo el proceso del ciclo de vida, resaltando que se estará utilizando el ciclo recomendado por la metodología de **Desarrollo de Software Seguro (SDL)**, el cual implica introducir diversos conceptos dentro de las etapas de desarrollo relacionados con la seguridad e integridad de la información, esto para crear un producto mucho más robusto en éste tema, minimizando posibles fallas o vulnerabilidades que comprometan la información y el mismo proceso.

El SISCOM será el sistema que se utilice en el Proceso Local Electoral 2017-2018 para llevar a cabo los cómputos distritales y municipales, el cuál será enteramente desarrollado por la Unidad de Cómputo y Servicios Informáticos (UCSI) y deberá ser capaz de realizar las siguientes actividades: administración de los usuarios que lo operarán, actividades previas, durante y obviamente posterior a la jornada electoral, tales como la captura del estado de los paquetes electorales, cómputos por distrito o municipio (según corresponda) o bien la captura de los cómputos generados en los grupos de trabajos que en su caso se determinen. Así mismo debe ser capaz de generar informes y reportes con fecha de corte tanto a nivel administrativo (registros de operaciones, conexiones, estado de la base de datos) como a nivel operativo (estado de los cómputos, informe de estado de paquetes electorales, entre otros.) Por lo tanto gran parte de la labor se debe centrar en la seguridad, confiabilidad, disponibilidad e integridad de los datos y del propio sistema en particular.

Por último se contempla una serie de Planes de Contingencia y el modelado del sistema en su diagrama lógico para su evaluación previa aprovechando el contexto del documento.

Metodología Ágil: SCRUM.

Una metodología de desarrollo de software consiste principalmente en hacer uso de diversas herramientas, técnicas, métodos y modelos para el desarrollo. Son documentadas y utilizadas para poner en enfoque al equipo que participa en el desarrollo de software, comúnmente para saber los pasos a seguir o donde está el proyecto actualmente (1).

Y esto es particularmente importante en una metodología SCRUM (Ilustración 1) donde los equipos de trabajo son autorganizados y proactivos. Es importante definir que SCRUM es un modelo ágil de trabajo donde se requiere un equipo regularmente pequeño, auto-organizado, con diversos conocimientos y con mucha iniciativa, donde la comunicación es fundamental no solo entre el equipo de trabajo, sino con los interesados para llevar a cabo los objetivos en un menor tiempo posible con una excelente calidad. Además la calendarización se realiza de manera "solapada" (actividades concurrentes o simultáneas) entre actividades y no secuencial como se realizaba en metodologías enfocadas al desarrollo de software tales como: Cascada, Incremental, Espiral, lo que permite el avance simultaneo de diversas tareas. Permite llevar un seguimiento muy puntual del objetivo final (el sistema), partiéndolo en objetivos más cortos en tiempo y dimensión (hitos), dándole la importancia en calidad para formar un cierre del proyecto con excelentes resultados, por medio de juntas semanales cortas que ayuden a poner al tanto al equipo y el líder de trabajo, así como a los interesados (1).

El utilizar en particular SCRUM para el desarrollo del SISCOM permite realizar un trabajo organizado en un tiempo menor con una muy buena calidad. Esto derivado que los tiempos suelen ser cortos con múltiples ajustes en objetivos. Hay que recalcar que el área a cargo del desarrollo (UCSI) atiende diversos temas y no es

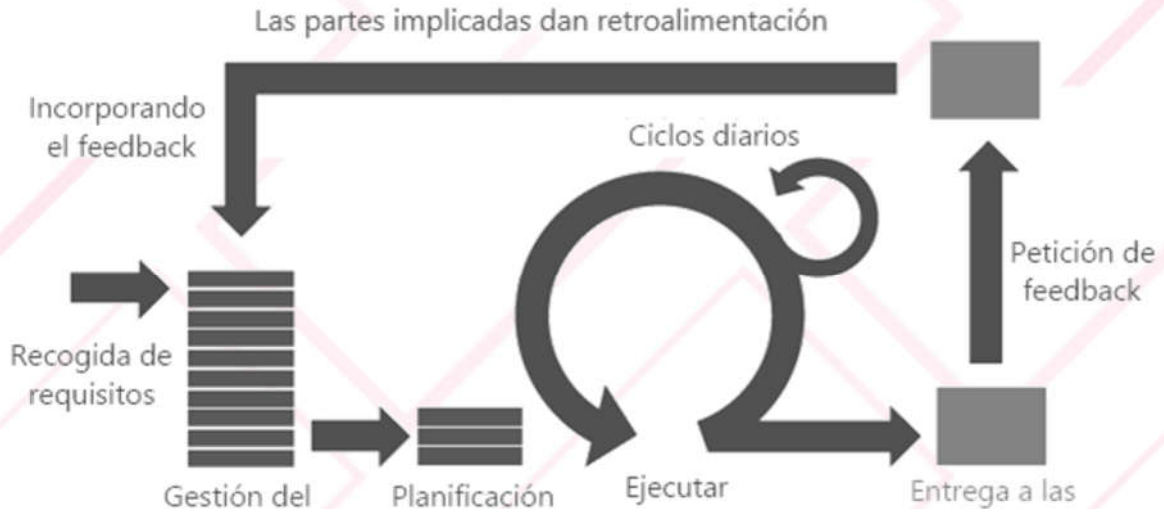

Ilustración 1.-Diagrama del Proceso SCRUM.

una fábrica de software como tal, por lo cual se considera que en vista de que el objetivo de la Unidad es darle la debida importancia a este tema, se considera factible y viable utilizar dicha metodología, ya que permitirá ajustarse a los objetivos para desarrollar un sistema en tiempo y forma y con las mejores prácticas posibles. SCRUM permite realizar cambios en las iteraciones (denominadas "Sprint's"), ajustando tiempos y objetivos por lo que será de gran valor para los posibles cambios o ajustes que surjan en el ambiente o dominio del proyecto como son las leyes o cambios en la organización.

Ciclo de Vida del Desarrollo de Software Seguro (SDL).

El Ciclo de Vida de Desarrollo de Software Seguro (SDL) es un proceso que ayuda a los desarrolladores a crear software más seguro y cumplir los requisitos de seguridad, reduciendo al mismo tiempo los costes de desarrollo *(3)*.

Para ello se apoya de 17 prácticas agrupadas en 7 fases que se pueden describir con el siguiente diagrama (Ilustración 2):

Ilustración 2.- Etapas de Ciclo de Vida de Software Seguro.

Se define la inclusión de mecanismos para controlar la seguridad de un sistema a través de las etapas de desarrollo del software. Esto ayuda a mitigar las posibles vulnerabilidades de un sistema planeando desde la definición de requerimientos funcionales incluyendo aquellos requisitos de seguridad, por ejemplo la arquitectura de la aplicación, lo cual desprende la puntualización de diferentes estándares de seguridad, nivel de acceso, administración de usuarios, sistemas en línea y disponibilidad. Así hasta la liberación y seguimiento del sistema por medio de planes de respuestas a incidentes, archivos de registros de liberación, entre otros.

De las etapas podemos decir lo siguiente:

- Al **inicio**: el equipo, tanto el líder de proyecto como los desarrolladores deben conocer que existen amenazas y empezar con el proceso teniendo éstas en cuenta.
- En **análisis de requerimientos**: establecer que requisitos de seguridad existen en el proyecto, para ello puede necesitarse la participación de un asesor de seguridad en la implementación del SDL. Se utilizará la figura del asesor como guía a través de los procedimientos del SDL. En este punto cada equipo de desarrollo debe tener en cuenta como requisitos las características de seguridad para cada fase.
- En **diseño**: los requisitos de diseño con sus necesidades de seguridad quedarán definidos. Se realizará documentación sobre los elementos que se encuentren en la superficie de un ataque al software, y por último, se realizará un modelo de amenazas, dónde pueden descubrirse nuevos requisitos de seguridad.
- En **implementación**: aplicación de los estándares de desarrollo y de pruebas. Posteriormente se aplicará software que compruebe la seguridad. Además, se realizarán pruebas de **code review**.
- **Validación y despliegue**: análisis dinámico sobre la aplicación, revisiones de código desde el punto de vista de la seguridad y pruebas centradas en la seguridad del software.
- Al **final** se necesita generar un plan de incidentes al terminar cada proceso, una revisión final de toda la seguridad del proceso y crear un plan ejecutivo de respuesta ante incidentes, dónde se obtendrá una retroalimentación de todo lo que ocurre en la liberación del software.

Esto apoya a la metodología seleccionada para llevar a cabo: SCRUM, permitiendo incluir en cada Sprint cambios o ajustes que en previos ciclos se pudieran considerar como vulnerabilidades en el sistema.

A lo largo del presente documento y de la definición de las etapas de desarrollo del sistema, se presentará la inclusión del proceso de SDL puntualizando que mecanismos se incluirán como medida de seguridad en cada una.

Diseño Orientado a Servicios: SOA.

SOA o **Service Oriented Architecture** por su siglas en inglés, es una arquitectura que se centra en ver los procesos de negocio como un conjunto de servicios que operan entre sí, permitiendo que una organización sea más eficiente y colaborativa. Esto permite que los datos, antes aislados en “silos” (denominados así por el concepto en las empresas de la dificultad de trabajar de manera eficiente entre las áreas) se puedan conectar, intercambiar, procesar entre la misma organización o bien con terceros. Se logra exponiendo una capa que será la encargada de ofrecer los

servicios y por medio de otras capas más internas se llevan a la lógica de negocios y los procesos internos (2).

Los fundamentos que rigen a SOA son básicamente 4:

- **Operación**: es una unidad de trabajo fundamental.
- **Servicio**: es un contenedor lógico que se compone a su vez de un conjunto de operaciones, los cuales se ofrecen al usuario.
- **Mensaje**: conjunto de datos de entrada que viajan hacía el servicio.
- **Proceso de Negocio**: un conjunto de operaciones que tienen como objetivo realizar una tarea en específico.

Ilustración 3.-Elementos de la Arquitectura SOA.

La arquitectura permite crea un diseño donde los servicios serán expuestos a la red interna de los órganos descentralizados del instituto, permitiendo ser consumidos por ellos y transportar datos de manera segura. Si se requiere habilitar clientes extras es muy sencillo habilitarlo por medio de este esquema. Los servicios por su naturaleza son débilmente acoplados y de alta reusabilidad, lo que dará pie para manejar las actualizaciones, mejoras y cambios de manera muy efectiva, sobre las unidades de trabajo, permitiendo también reutilizar operaciones ya creadas.

Con la elección de esta arquitectura permitirá:

- Manejo de actualización de versiones, solo se actualiza una sola versión en un solo sitio.
- Centralización de servicios.
- Control total de acceso.
- Monitoreo de una misma aplicación.
- Distribución de tráfico.
- Distribución de peso/memoria de la aplicación.
- Se puede crear sólo la lógica de negocios, y dejar los servicios en un servidor aparte.
- Escalable tanto horizontal como vertical. Es decir a nivel de hardware (ya sea virtual o físico) cómo de software.
- Acceso por parte de múltiples usuarios a una misma aplicación con diferentes privilegios de diferentes puntos, controlado por medio de una **matriz de seguridad** dichos accesos.
- Bitácora registrada tanto a nivel de servidor (logs) como operativo por usuario.

Además apoyará a crear un modelo para futuras referencias, que permita compartir información con otras instituciones, tales como el Instituto Nacional Electoral (INE) o inclusive otros organismos públicos locales (OPLES) por medio de un canal seguro, controlado y monitoreado.

Definición de la Arquitectura: Cliente/Servidor.

En el esquema propuesto se establece una arquitectura *Cliente/Servidor* cuyo objetivo es mejorar la seguridad y limitar aún más el acceso tanto al SISCOM como a los servidores que alojan. El resultado es un esquema hibrido entre SOA y Cliente/Servidor utilizando principios para encontrar una solución adaptable al problema.

La arquitectura de *Cliente/Servidor* se basa en principio en un cliente o clientes que realizan peticiones a un servidor y éste le da respuesta. Pueden estar conectado en la misma red local o por otros medios.

El **contenedor de Servicios** (cómo se define en el esquema SOA), se encontrará en el servidor principal dentro del Data Center Virtual, conectado por medio de la RPV (Red Privada Virtual) de Triara, los túneles de la RPV llegarán a los **Órganos Desconcentrados o clientes**, mismos que ejecutarán una aplicación elaborada en C#, con Visual Studio 2012 con Framework 4.5 de .NET.

Si bien parece una **solución** algo **atípica**, se ajusta perfectamente al objetivo que se ha definido. Los Órganos Desconcentrados tendrán la aplicación para Microsoft

Windows previamente instalada en sus equipos de cómputo (que son propiedad del Instituto y estrictamente configurados por la UCSI) sin dejar código fuente ni elementos que puedan comprometer la seguridad. Esta aplicación tendrá dentro de su funcionamiento los elementos necesarios para conectarse de manera segura y única (por Órgano Desconcentrado) al servidor donde realizará las peticiones y llamadas a los servicios. Estas llamadas tienen cabeceras distintivas que permitirán realizar la trazabilidad de cada una de ellas y el seguimiento, **por lo que podremos saber quién, cuándo y con qué datos realizó la conexión/petición**.

Si por alguna razón se vulnera la seguridad de nuestra RPV, podremos localizar de manera eficiente aquellos datos apócrifos, además de que garantizará la conexión directa ya que será el único mecanismo permitido de conexión.

ESQUEMA SOA, CLIENTE/SERVIDOR DEL SISTEMA DE CÓMPUTOS

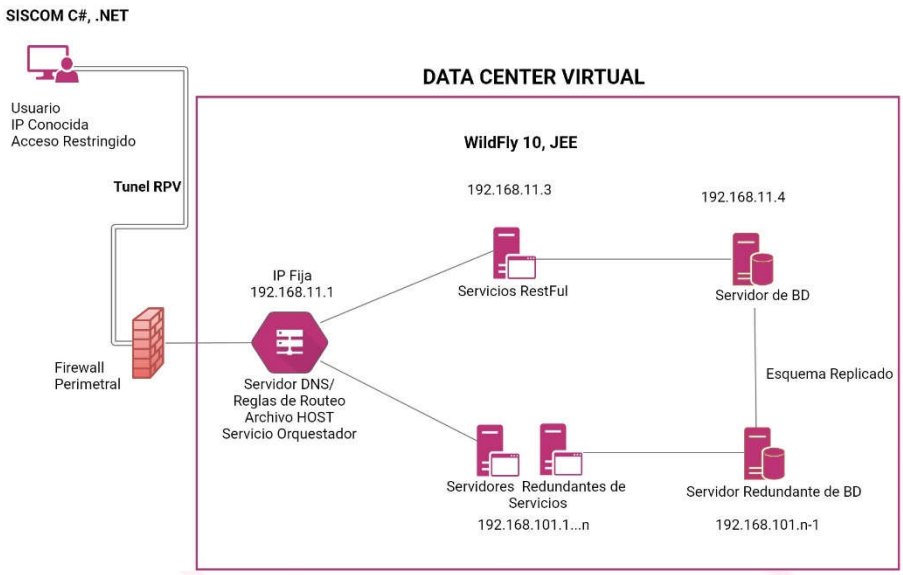

Ilustración 4.-Esquema SOA y Cliente Servidor propuesto.

Si por un supuesto, el ejecutable pudiese copiarse a otra máquina o bien, vulnerarse para ser ejecutado desde una red externa a la RPV, éste no tendría los medios para realizar la conexión por dos motivos especiales:

1- La aplicación SISCOM de Microsoft Windows, tendrá una configuración que nos permitirá leer los datos del equipo origen, los cuales estarán trazados en la Matriz de Seguridad.
2- Si esos datos pudieran suplantarse, junto con la copia de la aplicación, no tendrá manera de conectarse directamente al servidor puesto que solo será visible desde la red RPV.

Por otro lado, el **Servidor** central correrá una aplicación **Wildfly** 10 cómo contenedor de servicios del JEE con Java 1.8, que permiten la interoperabilidad puesto que expone los servicios en **RestFul**, al no necesitar un contrato será sencillo, rápido y eficaz la comunicación, mientras que la parte de seguridad será contemplada a nivel de software por diferentes capas.

Definición de los Stakeholders

Los interesados del proyecto o los Stakeholders, son aquellas personas que tienen un impacto en el desarrollo de un proyecto y por ello también en el éxito del mismo. Identificarlos es importante, ya que crea vías de comunicaciones eficaces y efectivas, saber qué, cómo y cuándo comunicar los avances del desarrollo de proyecto nos permite evitar retrasos en el calendario, que todas las partes involucradas conozcan el estado del proyecto y mantener un nivel de interés en el mismo.

Por ello, es importante agrupar a los Stakeholders en los siguientes grupos:

Ilustración 5.- Matriz de Interesados agrupados en niveles de poder e interés.

No hay que categorizar de manera equívoca dentro de estos grupos, ya que no definen el nivel de importancia de las personas involucradas, sino el nivel de interés en el proyecto a nivel de ejecución, por lo que hay que verlo de la siguiente manera:

Una persona con **alto poder,** es aquella que tiene una influencia sumamente relevante en el proyecto, por ejemplo, la Dirección Ejecutiva de Organización Electoral (DEOE), que tiene la función de velar por el cumplimiento de los Lineamientos y de cómo se llevarán los cómputos, y es por ello que es importante

mantenerlos al tanto con datos e información relevante para mantener un nivel de interés satisfecho.

Por otro lado, las y los Consejeros Electorales del órgano desconcentrado, son figuras importantes, pero que con **mantenerlos informados** es suficiente, para no entrar a detalles muy operativos, puesto que tienen responsabilidades a nivel institucional.

Otro ejemplo es el INE, ya que un Stakeholder no sólo son personas sino también pueden ser instituciones, ésta institución se le debe notificar para **mantener cerca** ya que tiene un alto poder pero el interés es menor por el nivel tan grande operación.

En conclusión, es importante establecer quienes y con qué nivel participan en el proyecto, puesto que ayuda a una mejor comunicación y definición de los objetivos, recordando las bases de SCRUM, son fundamentales para llevar a cabo con éxito el proyecto.

Información general sobre el SISCOM.

El planteamiento original para que el Instituto cuente con una herramienta informática que coadyuve en la importante actividad de los cómputos oficiales de las elecciones que en su ámbito realizan los órganos desconcentrados del mismo, parte principalmente de la aprobación de los **Lineamientos para el Desarrollo de las Sesiones de Cómputos de las Elecciones Locales**, que fueron ratificados mediante acuerdo CG-0029-AGOSTO-2017. En dichos lineamientos se establece toda la logística y operación respecto de dicha tarea, por lo que resulta viable que al contar ya con dicha planeación y definición de actividades se pueda diseñar y desarrollar un sistema informático de apoyo para dichas tareas.

Es necesario destacar que en el pasado Proceso Local Electoral 2014-2015, la UCSI desarrolló e implementó el Sistema de Cómputos Distritales y Municipales, denominado “SISCOM”, por lo que dicho sistema se estará mejorando y ampliando en funcionalidades con miras en cumplir en su totalidad con los requerimientos técnicos y operativos delimitados en los mencionados lineamientos.

El SISCOM será un sistema en línea (Internet) en el cual personal operativo de los órganos desconcentrados podrá capturar los cómputos de cada casilla electoral y tipo de elección correspondiente a su ámbito de competencia, para ello el sistema contará con mecanismos de autenticación de usuarios y contraseñas para acceso al mismo, además de diversos privilegios de operación. El sistema contará también con usuarios de tipo consulta para efectos de que en oficinas centrales del IEEBCS se pueda monitorear y generar reportes del avance de dichos cómputos, como por

ejemplo durante la Sesión permanente de Cómputos del Consejo General del Instituto.

El SISCOM utilizará como bases de datos de insumo, las correspondientes a la distritación electoral estatal vigente, la relación de las casillas aprobadas para el Proceso Local Electoral 2017-2018, así mismo la lista de los partidos políticos, coaliciones, candidaturas comunes que se hayan registrado en dicho proceso electoral, así como la distribución de votos que se hayan acordado en los respectivos convenios de coalición o candidatura común.

Como parte de las mejoras al SISCOM utilizado en el último Proceso Local Electoral (2014-2015), será la habilitación de módulos operativos para auxiliar a los órganos desconcentrados en el manejo de la información relacionada del estado en que llegan los paquetes electorales así como también lo relativo a los grupos de trabajo y puntos de recuento que en su caso se determinen implementar durante la sesión de cómputos.

Al ser el SISCOM un sistema cuya información es tan sensible y que además de alguna manera viaja por internet, es necesario incorporar diversos mecanismos de seguridad y disponibilidad para la correcta ejecución del mismo, los cuales se describen en el presente documento.

Requisitos del Sistema.

De la definición de requisitos del sistema, se establecen los módulos necesarios para su operación así como la descripción de sus funcionalidades. Cabe destacar que se sentarán principios de la metodología de SDL para establecer los mecanismos de seguridad propias de esta etapa.

Para establecer las etapas de los requisitos del sistema es necesario definir las funcionalidades propuestas para el mismo, por ello se describen a continuación los módulos del mismo, pudiendo contener funciones adicionales a medida de que se lleven a cabo los “Sprint’s”. En un análisis inicial, se contempla lo que se presenta a continuación.

Módulos del Sistema.

1.- Administrador del sistema.

Es un módulo enteramente operativo del nivel 0, es decir, el más alto puesto que contiene todo el control del mismo: desde los usuarios, bitácoras, la matriz de seguridad para los controles de accesos seguros, entre otros mecanismos. Además permite monitorear a nivel técnico el sistema.

Control de Usuarios.
El control de usuarios permite la gestión de todos aquellos actores que interactúan sobre el sistema a manera tanto operativa (Órganos Desconcentrados) como administrativa (UCSI). Contendrá un log de cambios o bitácora para conocer qué y quién realizó un cambio de permisos, tipo de usuario, nombres y demás datos que contenga la estructura de los mismos.

Reportes de Bitácoras de operación e información de salud del sistema.
Es necesario incluir la funcionalidad de generar bitácoras tanto en línea o históricas para poder realizar trazabilidad de las operaciones. Así mismo poder encontrar errores de estancamiento de información con los mismos datos.

La información deberá poder ser filtrada por datos específicos si así se requiera, para poder encontrar algún problema con alguna captura o situación atípica. Si se requiere podrá buscarse en bitácoras específicas, es decir, la idea inicial es tener una bitácora operativa global (bitácora de bitácoras), donde se canalicen todas las operaciones del sistema, así mismo será necesario tener las siguientes bitácoras (que se describirán en la sección relacionada explícitamente de la seguridad)

- Bitácora de administrador: Se registrarán todos los cambios realizados en el módulo de administrador como son los cambios de usuarios, permisos, y accesos.
- Bitácora de la Jornada Electoral: Se guardaran todas las operaciones con relación a la Jornada Electoral, esto es: altas de paquetes y estado de los mismos, incidentes, elementos generales de las AEC entre otras operaciones.
- Bitácora de los Cómputos Distritales y Municipales: Es una bitácora de operaciones muy importante para el proceso actual. Contendrá las operaciones que se realicen en todo el módulo de Cómputos Distritales y Municipales, desde operaciones erróneas, hasta la trazabilidad de una operación de cómputo de casilla. Así mismo puede ser utilizada para poder generar operaciones fuera de línea para luego cuando haya conexión puedan ser enviadas al Servidor de Servicios Principal.
- Bitácora de Grupos de Trabajo y Puntos de Reencuentro: Se registrará las operaciones relacionadas con los grupos de trabajo y puntos de reencuentro, quienes lo dan de alta, modificaciones y bajas, así como las operaciones relacionadas con estos: recuento de casillas.
- Bitácora de RFL y REL: La bitácora de RFL o Reportes Fuera de Línea contemplará los reportes que sean concentrados en base de datos de respaldo o no en línea, es decir, aquella información que por su índole no requiera actualización crítica, por ejemplo, casillas, totales de paquetes, entre otros. Mientras que los REL o Reportes En Línea son aquellos críticos que contienen abstracción en tiempo de real de información importante, como lo

es el desarrollo o avance de los cómputos. La idea es poder tener la relación de quienes, que y cuando consultan la información para poder tener registro de cómo se maneja éstos datos.

Matriz de seguridad.

El esquema de seguridad sería el punto más crítico en el tema, puesto que los servicios siempre están expuestos en internet, existiendo la posibilidad de ataques y peligros de intrusos para captura/daño de información.

El uso de https puede apoyar al esquema cifrado pero se debería reforzar con encriptación de dos puntos, utilizando un algoritmo eficiente y eficaz tanto para garantizar la integridad como la velocidad de respuesta.

Una herramienta posible es una "Matriz de Seguridad" que permita la manipulación y control total de la aplicación por medio de un panel de administrador en tiempo real. Dicha matriz puede contener los privilegios de acceso así como toda información necesaria para realizar el "match" o emparejamiento de operaciones.

Por ejemplo que permita cruzar la relación usuario/máquina/ip/hora/fecha de acceso.

En una situación práctica la matriz funcionaría de la siguiente manera:

- Conexión de un distrito en La Paz:
- IP: 192.168.11.4
- Usuario de acceso: DISII
- Máquina: mac:x:x:x:x
- Hora de acceso: 8:23am.
- Operación: Cómputo de Acta.

En la matriz de seguridad deberá existir la combinación de factores:

Matriz=*idUsuario and idAcceso and idMaquinaUsuario and horaFechaAccesoPermitido and idOperacion*.

Si se cumplen los requisitos, la operación puede ser realizada.

La Matriz es un herramienta muy eficaz, pero se debe diseñar correctamente para la cuestión de eficiencia en relación de transacciones (#de operaciones, usuarios operando, cantidad soportada por servidor) X minuto.

Gestión de insumos de la Base de Datos.

Módulo funcional que permite el manejo de los datos que servirán de insumo para que el SISCOM pueda funcionar de acuerdo a los lineamientos y correcta operación. Dichas base de datos podrán ser actualizadas, modificadas y consultadas, esto para

poder replicar la información necesaria de manera directa. Al ser un módulo totalmente de insumos del sistema, deberá ser accedido únicamente por los administradores del sistema. Entre las bases de datos se encuentran las siguientes:

- Distritos, Secciones y Casillas Electorales del PLE 2017-2018
- Listado de Candidatas y Candidatos del PLE 2017-2018

Generación de tokens dinámicos.
Es un módulo especial, ligado con el módulo de Captura de Cómputos, permitirá generar un token único para habilitar la recaptura de un cómputo que haya sido capturado por error. El módulo deberá tener su propia bitácora para ver incidencias, reincidencias y posibles casos de análisis.

Su funcionamiento radica en seleccionar un usuario, casilla computada y motivo de recaptura. Una vez validado los datos, el Sistema enviará ya sea por SMS o Correo Electrónico un token de uso exclusivo y único, así como con una duración de máximo 5 minutos. Una vez pasados los 5 minutos, el token será inhabilitado y no podrá usarse (si esté expira). Igual será el caso si el token fue utilizado en una ocasión.

Además deberá de registrar las excepciones que ocurran, por ejemplo, si el token se usó en otro usuario u otra casilla; si el token se intentó utilizar más de una vez o cualquier intento de cambio sin token.

El token no podrá ser en texto plano, deberá ser encriptado y codificado y así comparado en la base de datos, aunque el usuario final únicamente verá e ingresará 4 dígitos.

2.- Jornada Electoral.

Estado de los paquetes electorales.
Para poder dar seguimiento y monitorear los Paquetes Electorales que lleguen a los distritos será necesario un módulo que permite gestionar lo relacionado con ello. El objetivo principal es poder almacenar información de los paquetes en el SISCOM una vez recibidos, estos datos permitirán generar reportes para conocer la situación de los mismos, así como incidentes, paquetes extraviados, en mal estado o bien donde las actas no se encuentren en la ubicación adecuada.

1. Se deberá registrar en el sistema el ingreso de los paquetes al Órgano Desconcentrado.
2. Se llenará información como la siguiente:
   - Hora.
   - Día.
   - Persona que entrega.

- Persona que recibe.
- Tipo de casilla.
- Sección.
- Ubicación.
- Estado del paquete.

3. Marcar si el sobre PREP está por fuera junto con la copia de las actas de escrutinio y cómputo.

Resultados Preliminares

Para el día de la jornada se deberá de realizar un conteo para los Resultados Preliminares. Estos se llevan a cabo por medio de la copia del acta que se encontrará anexada.

Para ingresarlo al sistema será muy similar al Cómputo oficial al miércoles posterior a la Jornada Electoral.

El usuario del SISCOM tendrá un módulo de Resultados Preliminares, donde ingresará casilla por casilla los datos de las actas. Si un Acta no se encuentra, o bien está dentro del paquete, deberá ser marcada para ser abierto el día de los cómputos.

Al igual que los cómputos será de doble captura para minimizar errores y en caso de requerir una modificación se realizará la notificación mediante oficio a la UCSI o con una notificación. Esto puesto la naturaleza del proceso que deberá ser más ágil que los cómputos oficiales.

Elementos Generales de las Actas de Escrutinio y Cómputo.

Es un módulo sencillo que permitirá capturar elementos adicionales de las Actas de Escrutinio y Cómputo. Como posiblemente comentarios al respecto de las actas que permita identificarlas para posible recuento, o bien para otros fines por definir.

3.- Grupos de Trabajo (GT) y Puntos de reencuentro (PR).

Cálculo de GT y PR.

El presente módulo podrá realizar los cálculos necesarios por Distrito y Municipio para poder generar, de acuerdo al número de casillas que serán motivo de recuento, los Grupos de Trabajo y Puntos de reencuentro necesarios para llevar dicha labor. Esto de acuerdo al Distrito o Municipio en cuestión que este realizado la operación, por ejemplo:

1. Se deberá seleccionar y confirmar las casillas cuyos resultados serán objeto de Recuento.

2. Número de Grupos de Trabajo, existiendo 1 por Distrito o bien 2 por Municipio por defecto.
3. Número de segmentos Disponibles, cada segmento se considera como un lapso de 30 minutos, y se calcularán a partir del tiempo restante comprendido entre la hora en que se integren y comiencen sus actividades los Grupos de Trabajo y 48 horas posteriores, pudiendo variar de acuerdo a las necesidades de cada Órgano Desconcentrado.
4. Puntos de Reencuentro, puede haber uno más puntos de recuento.

Por ejemplo:

El número de casillas instaladas en un distrito es de 64, de los cuales, 34 actas de escrutinio y cómputo de casilla serán cotejadas en el Pleno del Órgano Desconcentrado, los 30 paquetes electorales
*restantes serán objeto de recuento (**NCR**).*

*Cálculo de **S:** Considerando que el tiempo restante para realizar el cotejo es de 48 horas (de las 08:00 horas del día miércoles de los cómputos, a las 08:00 horas del día viernes); por lo que el número de segmentos de media hora (**S**) es igual a 96; por lo tanto: **PR** = (30/1)/96 = 0.31 = 1 Punto de Recuento por Grupo de Trabajo (Se redondea la cifra). Como se señaló, el redondeo será hacia arriba a partir de una fracción igual o superior a 0.30, o hacia abajo cuando no alcance esta cifra; en este caso, el Grupo de Trabajo necesitaría 1 Punto de Recuento para recontar un total de 30 paquetes electorales en el tiempo disponible.*

4.- Captura de Cómputos.

Cómputo Distrital o Municipal.

En relación a todo el proceso del cómputo de las actas se realizará en el módulo de Cómputo Distrital o Municipal el cual visualmente y operativamente será muy sencillo de manipular.

1. Contendrá un acceso por token único que será enviado previo a los Órganos Desconcentrados, con un usuario y contraseña: el token es de uso único para el día de inicio (recordemos que los cómputos deben ser ininterrumpidos y sin recesos), para el Órgano, para el usuario y para esa contraseña, esto para restringir el acceso aún más al SISCOM.
2. Tras el login de estos tres elementos, contendrá una pantalla siguiente, donde se cargarán las Casillas pertenecientes al Distrito o bien al Municipio a computar. Al seleccionar una Casilla, se mostrarán los recuadros correspondientes al Acta de Escrutinio y Cómputo con las candidaturas y candidatos aprobados. Este proceso será de doble verificación para minimizar los errores de captura: con una primera captura normal y una

segunda con la primera bloqueada y oculta. Si no coinciden ambos recuadros se deberá repetir el proceso y registrar el error en la bitácora de los Cómputos.

3. Cada casilla computada desaparecerá de la lista una vez finalizada y confirmada.
4. Luego regresará a la lista de Casillas nuevamente donde se esperará la siguiente Casilla.
5. Una vez terminado el cómputo de todas las Casillas, el sistema se cerrara y no permitirá más el acceso a ese token, usuario y contraseña para el cómputo de las casillas, pero si para posiblemente hacer solicitudes de correcciones.
6. Si es necesario realizar una modificación a una casilla computada, deberá realizarse desde la opción de "Solicitud de **token de corrección de Casilla**" el cual es un token diferente al de acceso único de la aplicación. Donde el usuario deberá ingresar la casilla, el motivo de la corrección y su confirmación por medio de su contraseña, esto notificará a la UCSI para habilitar la recaptura, lo que a nivel técnico el SISCOM hará lo siguiente:
    a. Registrar el incidente del usuario con el motivo de la recaptura de la casilla computada.
    b. Registrar en la bitácora de los Cómputos la solicitud.
    c. Notificar vía correo a la UCSI sobre la solicitud.
    d. Por medio del módulo de administrador de "Generación de tokens dinámicos", se visualizará la solicitud. De acuerdo al motivo, y con previa autorización del Encargado del SISCOM en turno, se aprobará o negará la recaptura, pudiendo registrar el motivo de dicha negación. Esta autorización también generará un registro en la Bitácora de Administrador.
    e. En caso de aprobación, se enviará un correo o SMS al usuario que lo solicitó con el token dinámico, el cual deberá ingresar en los próximos 5 minutos al apartado de "Corrección de casilla con token dinámico", donde únicamente deberá ingresar el token y el sistema automáticamente leerá la Casilla a computar para minimizar los errores. El usuario únicamente deberá recapturar todo con los datos correctos y guardar, mismo proceso que la captura normal.
    f. En caso de negación de la corrección, se le notificará el motivo por el cual se denegó la corrección.
7. En caso de no tener conexión por algún motivo con el servidor principal ver "Plan de Contingencia para los Cómputos".

Cómputo en Grupo de Trabajo.

El proceso de cómputo en Grupo de Trabajo será muy similar al de los cómputos normales. Lo que podrá variar es que únicamente saldrán las casillas con motivo de

recuento, los usuarios podrán ingresarlas desde el módulo de “Grupos de trabajo y puntos de reencuentro”. Al entrar a ésta dinámica el sistema únicamente cargarán estas casillas para ser recapturadas. En las demás operaciones será exactamente igual a los cómputos distritales y municipales, pero sus bitácoras tendrán un identificador distintivo para saber que se trató de un recuento.

5.-Reportes.

Dentro de los reportes necesarios en el SISCOM se encontrarán en 2 rubros, RFL (Reportes Fuera de Línea) y los reportes REL (Reportes En Línea). Lo importante de ésta separación es definir aquellos que se conectarán a base de datos críticas o de constante cambio y delicadas, para obtener la información y que tienen un alto grado de concurrencia de inserciones o actualizaciones y aquellas que son más estáticas por decirlo de alguna manera, o que tienen cambios poco significativos y que además su concurrencia es menor en relación a inserciones o actualizaciones.

Entre los reportes se encuentran los siguientes:

Informe de estado de paquetes electorales.
Es un reporte diseñado para poder conocer el estado de los paquetes electorales del día de la Jornada Electoral, contendrá información sobre fecha, hora, quien recibe, como se encuentra el paquete, si el sobre destinado para el Programa de Resultados Electorales Preliminares (PREP) está en su sitio, entre otra información que podrá ser ajustada en el desarrollo.

Cómputos Distritales y/o Municipales.
Esta información será de un reporte en línea que hará consultas directas a la base de datos de los cómputos, la idea será hacerlas de manera eficiente y en tiempo real, ya que serán utilizadas para conocer el estado actual del avance de los cómputos. Será posible saber total de casillas computadas, por computar, total todo esto por distrito y municipio. Se graficará la información para poder ser proyectada en la sesión permanente del Consejo General del Instituto.

Entre otros.
Se podrán definir nuevos reportes si así se requieren a medida que avance el desarrollo.

Seguridad e Integridad de la Información.

Principios de operación.

Garantizar que la seguridad sea lo más efectiva posible es un arduo trabajo. Es un área tan delicada como definir los requisitos funcionales de un sistema, si falta uno o uno queda incompleto nos vemos envueltos en modificaciones que retrasan el

despliegue o bien el sistema no cumple con lo requerido en su liberación para ser operado.

El principio de “whitelist” (lista blanca) o de permitir lo mínimo indispensable siempre viene bien para la seguridad, siempre y cuando se haga de manera metódica y cuidando los detalles.

Definir lo que sólo estará permitido ayuda a evitar dejar huecos de seguridad que nos podría suceder en su contraparte, denegar todo lo que no está permitido. En un ejemplo práctico: una “blacklist” o lista negra nos permite denegar a toda una lista de IP o bien de usuarios, pero si olvidásemos una en particular podríamos dejar una vulnerabilidad que permita un fallo crítico. Por el otro lado, sí solo permitimos aquello que deseamos, por ejemplo una sola IP o un solo usuario, automáticamente lo demás queda descartado. Si bien no garantiza la seguridad en un 100% nos da un margen de error mínimo, evitando así “olvidar” aquellas cosas que no queremos permitir.

Red Privada Virtual (RPV).

Una solución a lo mínimo permitido son las Redes Privadas, dónde únicamente estarán conectados por medio de un canal seguro los 21 Órganos Desconcentrados Distritales y Municipales. Está solución es por medio de una tecnología de Telmex denominada RPV, donde por medio de un dispositivo (adicional al módem de Infinitum) se conecta el Órgano Desconcentrado directo a un túnel privado con nuestro servidor donde se alojará la aplicación del SISCOM.

Dichos canales garantizan su seguridad, ya que no son visibles en internet y son enlaces directos con el destino central. En este caso, el destino central es un servidor en un Data Center Virtual, mismo que está detrás de un Firewall perimetral. Los enlaces al ser directos, no tiene salida a internet, disminuyendo los riesgos de ataques. Además el servidor no estará expuesto a Internet, lo que impide un posible ataque de DDoS o de modificación de datos.

Se resumen en el siguiente esquema (Ilustración 6):

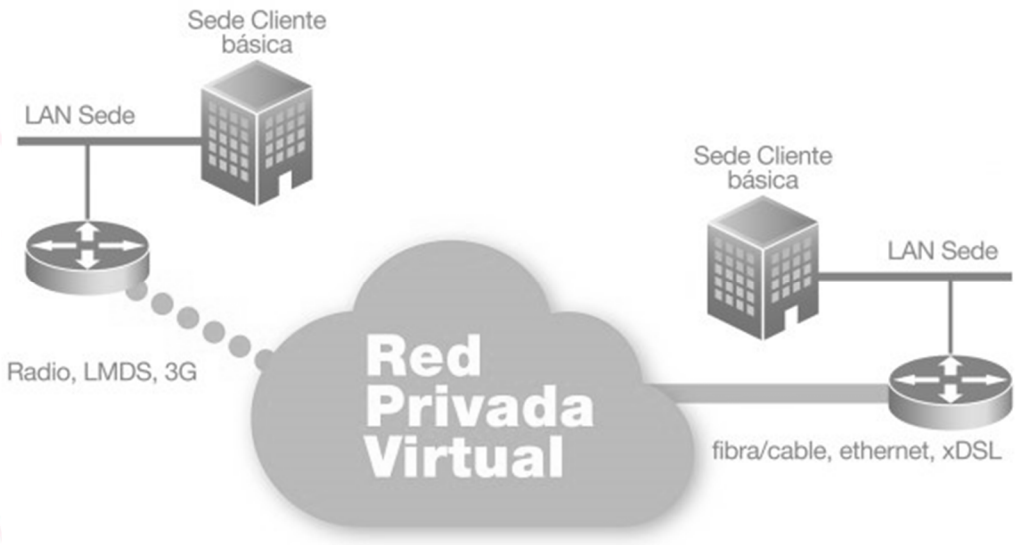

Ilustración 6.- Esquema de Red Privada Virtual propuesto.

Además nos apoyaremos de otras técnicas de seguridad para brindar mayor certeza y confiabilidad al sistema por lo delicado del tema. Entre ellos la Matriz de Seguridad y Bitácoras.

Capital Humano: reconocimiento la importancia de la personas en el ambiente del sistema.

El hombre es el factor principal en un sistema informático, él lo diseña, lo pone en práctica, lo explota y lo mantiene, tanto desde el punto de vista tecnológico como informativo.

Es un elemento susceptible a las influencias, tanto positivas como negativas del mundo circundante, que puede provocar reacciones muy disímiles ante situaciones dadas; de ahí que constituya un objetivo de trabajo de todos aquellos que pretendan desestabilizar el buen funcionamiento del sistema informático en sentido general.

Por eso debemos estar conscientes que inducido o fortuitamente el hombre ante causas y condiciones que lo propicien se convierte en la principal amenaza de un sistema informático, al estar en capacidad de desencadenar acciones riesgosas contra el mismo.

La ingeniería social es la práctica de manipular psicológicamente a las personas para que compartan información confidencial o hagan acciones inseguras.

De la misma forma si es capaz de concientizar su responsabilidad dentro del sistema de medidas de Seguridad Informática, hará de este una coraza infranqueable en la defensa de la confidencialidad, integridad y disponibilidad de la

información y la adecuada utilización de las tecnologías informáticas y de comunicaciones.

Entre las causas que pueden provocar conductas de amenazas a un sistema informático por las personas, podemos citar las siguientes:

- Impulsos mezquinos o codiciosos que pueden provocar fraudes, robos y contaminación de información entre otras.
- Descontento por la falta de reconocimiento al trabajo que realiza, condiciones inadecuadas para ejecutar sus funciones o desacuerdo con las políticas de dirección de la entidad.
- Jóvenes experimentadores y ávidos de hacer público y centrar atención sobre sus conocimientos en materia informática y de comunicaciones.
- Existencia de profesionales de espionaje electrónico que cobran fuerza con el alto grado de conectividad en redes de computadoras en el mundo.
- Personal sin la calificación necesaria ocupando funciones vinculadas a la explotación de sistemas informáticos o sobre calificación para puestos de trabajos que no lo requieren.

Todo esto alerta sobre la importancia de la selección del personal, con la preparación profesional y confiabilidad que se ajuste con los puestos de trabajo dentro del sistema informático, así como realizar un programa de concientización que contribuya a educar a los hombres en el conocimiento de las obligaciones legales y medidas de protección que incluye la seguridad informática.

Capacitación del Personal con enfoque de seguridad.
Como se vio anteriormente la parte más vulnerable de un sistema es el personal que opere o que participe en algún punto del proceso. Es por ello que es necesario concientizarlos de que los riesgos y amanezcas que conllevan la operación de un sistema son reales y que son consecuencias en muchas ocasiones por acciones que ellos mismos realizan ya que el 97% de los ataques son por este medio (6).

Desarrollar una cultura de seguridad dentro de la Institución es darles a conocer al personal que los riesgos son reales y más importante aún instruirlos en cómo deben actuar para salvaguardar todos los activos de la misma (como la información, equipo de informática, dispositivos electrónicos, entre otros) y a sí mismos.

Por ello se realiza un plan de concientización y capacitación del SISCOM donde se verán, entre otros, los siguientes temas:

TEMARIO DE CAPACITACIÓN SOBRE LA SEGURIDAD INFORMÁTICA

- **Concientizando sobre la Seguridad.**
  - Buenas prácticas de seguridad en el entorno laboral.
- **Ingeniería Social ¿Qué es?**
  - Objetivo de la Ingeniería Social.
  - Técnicas de Ingeniería Social.
- **Sencillos tips para defenderse**.
- **Guía de apoyo ante situaciones de riesgo y amenaza.**

Hay que recalcar que el objetivo es puntual y es crear conciencia sobre la seguridad informática por ello es importante que la profundización no sea tan intensa y extensa, recordemos que nuestros órganos desconcentrados están en una labor compleja por sí misma y por ello la UCSI tiene que realizar la capacitación de forma sencilla, eficaz y rápida.

Elementos que componen un Sistema Informático.

La identificación de los elementos que componen un sistema informático es sumamente importante para poder determinar las amenazas, riesgos y vulnerabilidades que puedan afectar. Entre los elementos que lo contemplan son los siguientes:

- **Equipo tecnológico**: Computadora con todos los componentes que la integran así son: teclado, mouse, regulador, monitor, bocinas, impresoras, usb, cables, bafle, modem, router.
- **Programa**: SISCOM y programas complementarios que apoyen a su desarrollo; Chrome, Microsoft Excel, lector PDF.
- **Datos**: toda información que sea parte del proceso, incluyen datos de las casillas, actas, candidaturas, etc.
- **Procedimientos**: Lineamientos para los Cómputos.
- **Personas**: Operadores del SISCOM, personal de apoyo, y aquellos que se determinen.
- **Comunicación**: Canal Infinitum, RPV y Banda Ancha Telcel.

Cada elemento debe ser perfectamente ubicable, además de conocer sus posibles fallos y soluciones para poder determinar un modelado de amenazas y plan de riesgos que los soporten.

Modelado de Amenazas.

El análisis de modelo de amenazas (TMA) es un análisis que ayuda a determinar los riesgos de seguridad que pueden acaecer en un producto, aplicación, red o entorno, así como la forma en la que se aparecen los ataques. El objetivo consiste en determinar cuáles son las amenazas que requieren mitigación y los modos de hacerlo (5).

Los pasos de nivel alto para llevar a cabo un TMA son los siguientes:

- Paso 1. Recopilar información básica
- Paso 2. Crear y analizar el modelo de amenazas
- Paso 3. Analizar las amenazas
- Paso 4. Identificar las tecnologías y técnicas de mitigación
- Paso 5. Modelo de seguridad de documento y las consideraciones de implementación
- Paso 6. Implementar y probar las mitigaciones
- Paso 7. Mantener el modelo de amenazas sincronizado con el diseño

El modelado de amenazas se aplica mejor de forma continua a lo largo de un proyecto de desarrollo de software. El proceso es esencialmente el mismo pero en diferentes niveles de abstracción, aunque la información se vuelve más y más granular durante todo el ciclo de vida. Lo ideal es que un modelo de amenazas de alto nivel debe estar definido en la fase de planificación, y luego refinado a lo largo del ciclo de vida. A medida que se agregan más detalles al sistema, se crean y se exponen a nuevos vectores de ataque. El proceso de modelado de riesgos en curso debe examinar, diagnosticar y tratar estas amenazas (8).

Análisis de riesgos: ISO27005.

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001 (7).

Identificación de riegos

Un evento solo es un riesgo si existe un grado de incertidumbre asociado con él.

- Correr aplicaciones en condiciones vulnerables.
- Sistemas operativos, vulnerables y sin actualizaciones
- Diseñar aplicaciones inapropiadas, incompletas, con bugs y errores recurrentes
- Tecnologías obsoletas
- Mal rendimiento de la infraestructura IT

SISCOM:

Los riesgos Identificados hasta el momento son los siguientes:

- Personal vulnerable ante la ingeniería social.
- Dependencia de Triara y sus enlaces.

- Servidores Virtuales en un solo sitio.
- Equipo con falta de alguna actualización faltante que comprometa al Sistema Operativo en pleno proceso.
- Ataques a los servidores de Triara que comprometan la respuesta y velocidad de procesamiento de los servicios.

Evaluación de riesgos.

Es necesario establecer un vínculo entre los escenarios de riesgos en el sistema y el impacto institucional que estos generarían, para así comprender el efecto de los eventos negativos que puedan generar.

La evaluación de riesgos se realiza a menudo en más de una iteración, la primera es una evaluación de alto nivel para identificar los riesgos altos, mientras que las iteraciones posteriores detallan en el análisis de los riesgos principales y tolerables.

Adicionalmente la evaluación de riesgos requiere los siguientes puntos:

- Un estudio de vulnerabilidades, amenazas, probabilidad, pérdidas o impacto, y la supuesta eficiencia de las medidas de seguridad.
- El proceso de evaluación de amenazas y vulnerabilidades, conocidas y postuladas para estimar el efecto producido en caso de pérdidas y establecer el grado de aceptación y aplicabilidad en las operaciones del negocio.
- Identificación de los activos y facilidades que pueden ser afectados por amenazas y vulnerabilidades.

El propósito de una evaluación del riesgo es determinar si las contramedidas son adecuadas para reducir la probabilidad de la pérdida o el impacto de la pérdida a un nivel aceptable.

SISCOM:

Riegos con alto impacto:

- Fallo en ambos equipos de los Órganos Desconcentrados que impida computar en el sistema.
- Personal que comprometa los cómputos por medio de intereses por la aplicación de la ingeniería social.

Riesgos controlados o medios.

- Perdida de conectividad RPV.
- Fallo en un equipo del Órgano.

Riesgos bajos.

- Perdida de corriente en el local.

Análisis de Riesgo

Este es el paso principal en el marco de la norma ISO/IEC 27005. La mayor parte de las actividades primarias se prevé que cumplan con el primer proceso o paso de evaluación de riesgos. Este paso implica la adquisición de toda la información pertinente sobre la organización y la determinación de los criterios básicos, finalidad, alcance, límites y organización de las actividades de gestión de riesgos. El objetivo es por lo general el cumplimiento de los requisitos legales y proporcionar la prueba de la debida diligencia el apoyo de algún sistema de gestión de seguridad de la información (SGSI) que pueda ser certificado. El alcance puede llegar a hacer un plan de notificación de incidentes o un plan de continuidad del negocio.

SISCOM:

Es necesario establecer un plan específico que permita dar pie a la identificación de los riesgos, análisis, procesamiento, notificación, continuidad y solución. En el presente documento al ser de análisis se enfatizan en la identificación, pero a lo largo del desarrollo y en los Sprint's del Ciclo de Vida se irán generando documentos que apoyen a la norma ISO 27005.

Escenarios de riesgo

Escenarios de riesgo es el corazón del proceso de evaluación de riesgos. Los escenarios pueden derivarse de dos maneras diferentes y complementarias:

- Enfoque de arriba hacia abajo de los objetivos generales de la empresa a los escenarios de riesgo más probable es que puede tener un impacto.
- Enfoque de abajo hacia arriba, donde se aplica una lista de escenarios de riesgo genéricos a la situación

SISCOM:

Por medio de los Simulacros se pueden presentar los Escenarios de riesgo, entre los ubicados se encuentran los siguientes:

Pérdida del RPV: no solo es perder el enlace si no la capacitación del personal del SISCOM para saber cómo reaccionar ante la situación.

Qué hacer cuando la ingeniería social comprometa la seguridad del sistema: es una situación altamente riesgosa, ya que desde identificarla podría ser compleja, por eso es sumamente necesario establecer y conocer patrones del personal, por medio de

los escenarios y estudio de los mismos quizás podemos establecer medidas de detección que posiblemente comprometan al sistema.

Respuesta a los Riesgos

El propósito de definir una respuesta al riesgo es llevar el riesgo a un nivel que se pueda tolerar. Es decir, el riesgo residual debe ser dentro de los límites de tolerancia al riesgo. El riesgo puede ser manejado de acuerdo cuatro estrategias principales (o una combinación de ellos):

- Evitar el riesgo aislando las actividades que dan lugar al riesgo
- Mitigar el riesgo adoptando medidas que detectan y reducen el impacto del riesgo
- Transferir riesgos a otras áreas menos susceptibles o a otras entidades con más experiencia.
- Aceptar riesgos que se corren deliberadamente y que no se pueden evitar, sin embargo es necesario identificarlos, documentarlos y medirlos

SISCOM:

La respuesta antes los riesgos presentados así como dentro de las amenazas, se contemplan en los planes de contingencia en el final del documento. Gracias a la metodología seleccionada podremos mejorar a medida que los Sprint's se lleven a cabo, para darle robustez toda la parte de la seguridad.

Sobre la Bitácora.

Registrar toda operación en una tabla o logs es sumamente relevante, tiene finalidades de auditoria, trazabilidad de operaciones, sustento y de depuración. A su vez esto puede servir para registrar acciones fuera de línea (FL) esto si llegase a perder enlace de conexión con el servidor principal y así poder registrarlas una vez que el sistema éste de nuevo conectado. Es importante también registrar intentos fallidos o de operaciones que no cuadren con la Matriz de Seguridad. Además de tener la trazabilidad de las operaciones pudiendo obtener el inicio y fin de una operación, esto para poder saber si una operación se realizó de manera inconclusa o con anomalías y poder detectar exactamente donde ocurrió el problema.

Pueden haber dos registros de Bitácoras, uno totalmente operativo, donde se registren operaciones realizadas por los usuarios como ingreso al sistema, inserción de un valor, actualización de un registro o generación de un reporte, así mismo otra de seguridad dónde se contemplen registros por usuario de operaciones relevantes como: login (números de accesos exitosos y fallidos), inserción de datos fuera del horario de matriz o de intento de manipulación por algún agente externo, es decir, una llamada a un WebServices fuera de los servidores permitidos.

Tipos de bitácoras.
Deberían existir dos tipos de bitácoras:

Bitácora de operaciones: para registrar todas las acciones que realizan los usuarios y administradores del SISCOM, que entren en la siguiente lista:

- Modificación de información.
- Agregar información.
- Eliminar información.
- Ingresos al sistema.
- Consulta de reportes/datos.

Dentro de estas Bitácoras se encontrarán:

- Bitácora de Administrador.
- Bitácora de la Jornada Electoral.
- Bitácora de Cómputos Distritales y Municipales.
- Bitácora de Grupos de Trabajo y Puntos de Reencuentro.
- Bitácora de RFL y REL.

Bitácora del servidor: para registrar y trazar las peticiones y respuestas del servidor, tanto a nivel lógico (IP, meta-data) como nivel de servicio (tiempos de respuesta, errores en procesos o lógica de programación).

Está ultima bitácora es enteramente técnica, por medio de un servicio intermedio que interpreta la seguridad podrá registrar en nuestro entorno JEE las peticiones a todos los servicios en un log únicamente accesible el personal de la UCSI.

Plan de Contingencia para los Cómputos.

Dada la naturaleza del proceso, de lo delicado de la información y además de que se debe ofrece una disponibilidad del 100% para que los Cómputos no se detengan bajo ninguna circunstancia, puesto que por disposiciones legales los cómputos deben ser ininterrumpidos y sin recesos, se debe tener diversos planes de contingencia que puedan solventar diferentes situaciones que competan a la solución tecnológica.

Caso de pérdida de energía eléctrica.
Se contempla la renta o adquisición de una planta eléctrica que permita conectar los dispositivos informáticos que sea prioritarios para continuar con el cómputo como lo son:

- CPU.
- Monitor.
- Enlace RPV.

Se deberá regresar a las conexiones de la red eléctrica principal una vez que se haya restablecido el servicio.

Caso sin enlace con el Servidor de Triara que ejecuta los servicios.
Si nuestra RPV llegase a tener una interrupción el día de los Cómputos, se optará por los siguientes pasos:

1. Al notar el usuario que no puede realizar operaciones que requieran enlace con el servicio, esto por medio de un mensaje que le notificará el SISCOM de Escritorio sobre que existe un fallo de comunicación con el servidor, deberá notificar inmediatamente a la UCSI.
2. La UCSI notificará al soporte técnico de Triara de manera inmediata.
3. Para evitar el retraso de los cómputos se deberá habilitar en la aplicación un modo denominada "SISCOM FL" Sistema de Cómputos Fuera de Línea. Éste modo funciona de manera sencilla, si al intentar realizar una petición al Servidor, la aplicación de Escritorio no obtiene una respuesta, ésta notificará al usuario en operación informándole de dos posibles acciones:
    a. Entrar en modo SISCOM FL o bien; Intentar de nuevo la Operación.
4. Entrar en modo SISCOM FL: El modo fuera de línea solicitará un token, el cual es único para cada Órgano Distrital y Municipal, además estará "amarrado" (es decir, información única para cada computadora que permite relacionarse al sistema disminuyendo la suplantación o robo de identidad) a la máquina que previamente será configurada para que ligue el token con el Órgano Desconcentrado y la información única del Hardware del equipo.
5. El SISCOM FL guardará en un array cifrado los cómputos que se realicen en el modo Fuera de línea.
6. La UCSI en cuanto tenga respuesta o se dé solución al Enlace de RPV llamará al Órgano Desconcentrado para notificarle que ejecute la aplicación del SISCOM normal, el cual será activable con un icono en la parte superior de la aplicación.
7. El modo SISCOM con operación normal pedirá nuevamente las credenciales del usuario, intentará ingresar al usuario nuevamente y si tiene éxito informará visualmente cuales casillas faltan por sincronizar con el servidor.
8. Por último el usuario aceptará la sincronización y una vez finalizada el sistema regresará a la ventana de Selección de Casillas.

Caso de contingencia donde se requiera subir la información antes del término de los cómputos.
Si se estipula que los cómputos en el SISCOM deben estar divulgados a nivel institucional al término del plazo de los cómputos distritales y municipales, se podrá requerir a los siguientes supuestos:

- Si el órgano desconcentrado sin RPV se encuentra en un rango considerable (de 2 a 3 horas máximas de distancia) de algún otro órgano que si cuente con RPV, se procederá al traslado y configuración en la Matriz de Seguridad de la nueva ubicación y continuará con la sincronización y en su caso captura.
- Si el órgano desconcentrado sin RPV está en termino del tiempo y además la distancia del próximo órgano con RPV es mayor al tiempo restante, se permitirá la sincronización con la parte pública del Servidor de Servicios, misma que des encriptará el array del SISCOM FL y lo sincronizará con el servidor principal.

Caso donde el servidor que ejecuta los Servicios de Triara falle.
Si el servidor de Triara falla, se tendrá un respaldo de los servicios y Base de datos para contingencia donde se le solicitará a Triara que redirija el tráfico en el RPV.

Caso donde el equipo de cómputo que ejecuta la aplicación C# falle.
Si la computadora donde está la aplicación de C# de SISCOM falla, se deberá habilitar una segunda (ambas computadoras de los Órganos Desconcentrados tendrán configurada la aplicación pero solamente una tendrá el acceso concurrente).

La UCSI deberá:

1. Habilitar en la Matriz de Seguridad los datos necesarios para el acceso al equipo de respaldo del Órgano Desconcentrado.
2. Se deshabilita el acceso de la computadora del Órgano Desconcentrado que falló.

Endurecimiento del servidor principal

El *hardening* o endurecimiento del servidor principal consiste en aplicar políticas y funciones para que la seguridad sea más robusta en el sentido de estabilidad y confiabilidad.

Entre los elementos que se contemplan para el endurecimiento del servidor principal están los siguientes:

- Ocultar de los errores (fallos seguros por el concepto de si algo fallará que sea controlado) de páginas no encontradas las versiones del servidor: apache, Centos y MySql. No garantiza que no se ubiquen estos datos, pero si nos da un margen de tolerancia en la seguridad.
- Los puertos expuestos (abiertos) en el servidor serán única y exclusivamente los estrictos necesarios y además serán para accesos restringidos.
- El usuario ssh no será root. Se deberá ingresar dentro de la terminal (con credenciales distintas) si se requiere operaciones root.

- El usuario root no existe como tal, tiene otro nombre para evitar ataques de diccionarios.
- El usuario ftp exclusivamente sube en la parte pública y es por sftp.
- Las contraseñas serán reseteadas cada 15 días y nunca almacenadas ni escritas.

Dentro del WildFly se habilitan las siguientes opciones:

- Tiempos de espera cortos para evitar que los hilos se queden colgados.
- Límites de peticiones pequeños para evitar DDoS.
- Restricciones de peticiones solamente de DNS e IP's Conocidas.
- Número máximo de clientes conectados limitados a 23: 16 Distritos, 5 Municipales y 1 Consulta concurrente y 1 Administrador, pensando en operaciones concurrentes.
- Se habilita el Log a nivel de peticiones y de errores en la configuración del WildFly.
- Usuario y contraseña en las peticiones a los servicios.
- El acceso, monitoreo, cambios, altas y bajas del servicio se hace con un usuario diferente y único para el servicio que sólo es conocido por el personal que lo opera.

Se establecerán las presentes medidas más sin embargo no son limitativas pudiendo mejorarse a medida que se vean vulnerabilidades o situaciones que se pudieran corregir.

Referencias.

1. Project Management Institute (PMI) (2008) Guía PMBOK. 4ta Edición en español. EUA: PMI.
2. Erl, Thomas. SOA Principles of Service Design. Prentice Hall, 2007
3. TechNet de Microsoft, Ciclo de Vida de Desarrollo Seguro SDL. https://social.technet.microsoft.com/wiki/contents/articles/36676.ciclo-de-vida-de-desarrollo-seguro-de-software-es-es.aspx#B
4. Ian Sommerville, Ingeniería del software Pearson Educación, 2005 ISBN 8478290745, 9788478290741
5. BizTalk Server, Modelado de Amenazas, https://docs.microsoft.com/es-es/biztalk/core/threat-model-analysis
6. Ingeniería Social, https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
7. Análisis de riesgos, http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/
8. Modelado de amenazas, https://www.owasp.org/index.php/Modelado_de_Amenazas

OBSERVACIONES ENVIADAS POR EL MSC. JAVIER CARMONA (PENDIENTES)

COTASISCOM

Presentes

Por medio de la presente, les hago llegar las siguientes recomendaciones acerca del documento de análisis con el objetivo de construir un sistema integro del cual no se tenga duda alguna acerca de la seguridad del mismo.

1. Con respecto al modelado de amenazas. Esta es una actividad la cual se lleva a cabo tomando en cuenta todos los activos que tienen que ver con el sistema. En el documento se plasma la metodología que se utilizará para el modelado de amenazas. Se recomienda la utilización del Threat Modeling Tools de Microsoft.
2. El análisis de riesgo de un sistema es una auditoria que se lleva a cabo sobre una parte de una organización. Se recomienda establecer el contexto según lo marca iso27005. Lo analizado cumple.
3. En el ciclo de vida de software seguro. Hay que tomar en cuenta las actividades de seguridad que se van a implementar en cada etapa, para así asegurarnos que se esta llevando a cabo dicha metodología.
4. Sobre la prevención de desastres y recuperación se cumple.
5. Hardening al servidor principal, se cumple en el análisis. Tomar en cuenta las pruebas de penetración al mismo desde cualquier punto de la red interna, así mismo, establecer en una etapa posterior los ataques por medio de fuzzer.
6. Dentro del diseño de software seguro, tomar en cuenta el top ten de owasp 2017 en la etapa de análisis de vulnerabilidades.

   Todo lo anterior son lluvias de ideas que se me ocurren para el fortalecimiento del sistema.

Sin más por el momento.

MSC. Javier Alberto Carmona Troyo

Partidos
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
nombre
siglas
tipo
estatus
+crear()

Empleado:Usuarios
...
+crear()

Operaciones
id
idUsuario
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
operacion
estatus
+crear()

MatrizSeguridad
id
idEmpleado
usuario
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idUsuario
idEquipo
idOperacion
idHorario
+crear()

Equipo
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
MAC
IP
nombre
estatus
+crear()

Horario
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
cron
detalle
estatus
+crear()

Tokens
id
fechaCreacion
usuarioCreacion
fechaUso
usuarioUso
token
estatus
+crear()

VotosNulos
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
tipoEleccion
estatus
+crear()

Usuario
id
IdEmpleado
usuario
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
IdEquipo
password
ambito
tipo
estatus
+crear()

BitAdmin
id
fechaCreacion
usuarioCreacion
IdUsuario
idEquipo
idOperacion
datos:json
+crear()

BitJE
id
fechaCreacion
usuarioCreacion
idUsuario
idEquipo
idOperacion
datos:json
+crear()

BitComputos
id
fechaCreacion
usuarioCreacion
IdUsuario
idEquipo
idOperacion
datos:json
+crear()

Acta
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
folio
comentarios
estatus
+crear()

CandidatosNoReg
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
tipoEleccion
estatus
+crear()

CandidaturasComunes
INFORMACIÓN DE OTRO SISTEMA
+crear()

BitGTPT
id
fechaCreacion
usuarioCreacion
idUsuario
idEquipo
idOperacion
datos:json
+crear()

BitReportes
id
fechaCreacion
usuarioCreacion
IdUsuario
idEquipo
idOperacion
datos:json
+crear()

GTPT
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idGrupo
idCasilla
horaInicio
horaFin
estatus
+crear()

Grupos
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idUsuarios
idPartido
estatus
+crear()

Candidaturas
INFORMACIÓN DE OTRO SISTEMA
+crear()

ComputosAyun
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
idCandidatura
estatus
+crear()

ComputosAyun:RPAyun
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
idCandidatura
estatus
+crear()

PaquetesElectorales
id
fechaCreacion
usuarioCreacion
usuariosModificacion
fechaModificacion
hora
dia
idPersonaRecibe
idPersonaEntrega
idCasilla
idEstadoPaquete
token
estatus
+crear()

estatusPaquetes
id
fechaCreacion
usuarioCreacion
descripcion
estatus
+crear()

Casillas
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
idCandidatura
estatus
+crear()

ComputosDipu
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
idCandidatura
estatus
+crear()

ComputosDipu:RPDipu
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
idCandidatura
estatus
+crear()

ComputosAyun:GTPR
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
idCasillas
votos
idCandidatura
estatus
+crear()

ComputosDipu:GTPR
id
fechaCreacion
usuarioCreacion
fechaModificacion
usuariosModificacion
IdCasillas
votos
IdCandIdatura
estatus

UCSI
UNIDAD DE CÓMPUTO
Y SERVICIOS INFORMÁTICOS

SISTEMA DE CÓMPUTOS DISTRITALES Y MUNICIPALES (SISCOM) PARA EL PRÓXIMO PROCESO LOCAL ELECTORAL 2017-2018

IEE BCS
INSTITUTO ESTATAL ELECTORAL
DE BAJA CALIFORNIA SUR

Tareas	Fecha Inicio	Fecha Fin	Duración	Dias Completados	Días por completar	Porcentaje de Avance
Módulo del Sistema	02/01/2018	02/01/2018	0	0.00	0.00	0%
Administrador del Sistema	02/01/2018	02/01/2018	0	0.00	0.00	0%
Control de Usuarios	02/01/2018	08/01/2018	6	0.00	6.00	0%
Reportes de Bitácoras	02/01/2018	08/01/2018	6	0.00	6.00	0%
Matríz de Seguridad	08/01/2018	14/01/2018	6	0.00	6.00	0%
Gestión de Insumos	08/01/2018	14/01/2018	6	0.00	6.00	0%
Generación de tokens	14/01/2018	20/01/2018	6	0.00	6.00	0%
Jornada Electoral	20/01/2018	20/01/2018	0	0.00	0.00	0%
Estado de Paquetes Electorales	20/01/2018	28/01/2018	8	0.00	8.00	0%
Resultados Preliminares	20/01/2018	28/01/2018	8	0.00	8.00	0%
Elementos Generales de las AEC	28/01/2018	03/02/2018	6	0.00	6.00	0%
Grupos de Trabajo	03/02/2018	03/02/2018	0	0.00	0.00	0%
Cálculo de GT y PR	03/02/2018	09/02/2018	6	0.00	6.00	0%
Captura de Cómputos	09/02/2018	09/02/2018	0	0.00	0.00	0%
Cómputo Distrital/Municipal	09/02/2018	27/02/2018	18	0.00	18.00	0%
Cómputo den GT	09/02/2018	15/02/2018	6	0.00	6.00	0%
Reportes	15/02/2018	27/02/2018	12	0.00	12.00	0%
Fin o Cierre	27/02/2018	27/02/2018	0	0.00	0.00	0%

Inicio (númerico)	43102.00