Unidad de Cómputo y Servicios Informáticos

Anexo Técnico de Requerimientos de la Red e Infraestructura en la Nube

SISCOM-PREP 2023-2024

INSTITUTO ESTATAL ELECTORAL DE BAJA CALIFORNIA SUR

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Contenido

Constitución #415 esquina con la Calle Guillermo Prieto,
Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Presentación.

El presente documento tiene como objetivo plantear los requerimientos necesarios para la implementación de la arquitectura de red y en la nube que soportará tanto al Programa de Resultados Electorales Preliminares (PREP) como al Sistema de Cómputos Distritales y Municipales (SISCOM) en el Proceso Local Electoral 2023-2024 en Baja California Sur..

El Sistema PREP será el encargado de administrar todos los procesos que se describen dentro del Proceso Técnico Operativo del PREP y así mismo en la documentación remitida por el Instituto Nacional Electoral (INE) para efectos de darle puntual cumplimiento.

Así mismo, se debe contemplar lo relativo al SISCOM, el cual comparte similitudes en cuestiones de seguridad, disponibilidad y redundancias con el PREP, y será el encargado de coadyuvar en las actividades desde la Jornada Electoral hasta los Cómputos Oficiales, procesando la información relativa a estas etapas.

Ambas soluciones deben de tener una opción Administrable, es decir, que personal asignado por la Unidad de Cómputo y Servicios Informáticos (UCSI) pueda operarlo y gestionarlo.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Arquitectura de la Solución

La presente propuesta debe contener una Arquitectura N-tier (o multi-tier) con la cual se debe enfocar en el software y aplicativos de la Institución, esta arquitectura manejara diferentes capas representadas por distintos entornos de tecnologías de la Información, llamados (niveles de servicio) bajo una lógica software orientada a la nube, la cual implica una sola instancia de la aplicación, pero sirviendo a múltiples usuarios. La interfaz de usuario será representada por (Nivel de presentación), que se ejecuta en un entorno separado a (Nivel de lógica de negocios) que a su vez también se ejecuta en un entorno distinto del motor de la base de datos y las instancias de información llamada (Nivel de datos). Con esta arquitectura se brindará un panorama general y se creará como componente habilitador en apoyo a la estrategia y visión del Instituto, con base a los requerimientos actuales y futuros de dicho organismo.

El principal entregable corresponde a una Implementación de Arquitectura N-tier para un Centro de Datos Orientado a Servicios en la nube, tomando en consideración las siguientes actividades:

- La descripción y conocimiento de la infraestructura y estructura operativa.
- Las necesidades organizacionales en base a la estrategia.
- Limitaciones, alcance y restricciones.
- Requerimientos de información y estructuración.

Descripción

Hoy en día se requieren Instituciones robustas y flexibles al mismo tiempo, capaces de adaptarse de manera rápida a las exigencias y necesidades del mercado con un sentido innovador en sus productos, procesos y operaciones; en los cuáles la tecnología juega un papel fundamental pues representa un habilitador para el desarrollo y operación de las mismas. Éstas representan una oportunidad para que las Instituciones Gubernamentales puedan impactar en distintos ámbitos que van desde mejoras a sus procesos hasta la creación de nuevas líneas de productos y servicios de valor. De aquí la importancia de la identificación y análisis de las plataformas tecnológicas para cualquier negocio, organización o institución.

La propuesta de implementación de un Centro de Datos Orientado a Servicios para el Instituto, que permita ser un habilitador en la infraestructura y estructura operativa, con el fin de establecer de manera objetiva a los requerimientos y áreas de oportunidad en dicha plataforma para su alineación y transformación en un componente habilitador de valor en apoyo a la estrategia y visión del Instituto.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur. **(612)** 125.0808 y **(612)** 129.4062

Objetivo

El alcance de la propuesta aquí contenida comprende los siguientes puntos:

Desarrollar e implementar una estructura de Centro de Datos orientado a servicios por medio de una nube pública, visto como un solo sistema que proporcione los recursos tecnológicos en el ámbito de aplicativos y servicios críticos para el Instituto, en el Proceso Local Electoral 2023-2024.

Características.

Abierta: Se debe proporcionar un centro de datos completo. Es importante que sea abierta para posibilitar la integración de terceros en todos los proveedores de soluciones.

Integrada y simplificada: Los componentes de TI tradicionales deben integrarse a una sola estructura para asegurar que los recursos informáticos, de almacenamiento y de red puedan optimizarse y mantenerse a medida que cambia el entorno.

Flexible y dinámica: Los entornos de aplicación y virtualización que admite el centro de datos no son estáticos; tampoco puede serlo la estructura. La estructura de un centro de datos controla holísticamente los recursos del mismo. Con ello, se puede ordenar más fácilmente los cambios de configuración necesarios a medida que evoluciona el entorno de aplicación a fin de admitir la automatización y la organización de servicios.

Escalable: No es fácil pronosticar un aumento de los requisitos informáticos, de almacenamiento y de red. Los administradores de TI deben poder ampliar la estructura del centro de datos en tiempo real a fin de asegurar la capacidad suficiente para brindar a trabajadores y clientes una experiencia de alta calidad.

Sólida: Los entornos actuales requieren de operaciones constantes. El tiempo de inactividad significa pérdida de información, de oportunidades y de servicios. Cuando se construye una estructura de centro de datos, se debe tener en cuenta la solidez y la auto reparación a fin de asegurar el máximo tiempo de actividad y el mínimo de interrupciones.

Segura: El centro de datos envía una amplia variedad de información a las aplicaciones y los servicios, incluidos los datos extremadamente confidenciales y críticos para la organización. La seguridad es un área que los arquitectos del centro de datos no pueden comprometer. La estructura del centro de datos proporciona el máximo nivel de seguridad integrada no solo al centro de datos, sino también a los dispositivos del usuario final, incluidos los dispositivos móviles.

Centrada en la aplicación: La estructura del centro de datos proporciona API de control para los recursos informáticos y de red. De esta forma, las aplicaciones pueden conectarse directamente con la infraestructura que la admite. Las API permiten aprovisionar o reconfigurar la infraestructura sobre la marcha, de acuerdo con la política institucional.

Servicios.

Continuidad de servicio. La puesta en servicio de aplicaciones en IEEBCS, obliga a acercarse a un servicio con disponibilidad cercana al 24x7. Esta disponibilidad podría verse comprometida por caída o fallo en alguno de los nodos. El objetivo implica necesariamente

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur. **(612)** 125.0808 y **(612)** 129.4062

que, para los sistemas de información identificados como críticos, haya una garantía de no interrupción del servicio durante el proceso de respaldo y en casos de interrupción de los servicios.

Reducción en la ventana de recuperación de los servicios. En caso de que se produjera una situación que llevará a la recuperación desde copia de seguridad de la información o aplicaciones, es necesario que la ventana temporal de restauración del servicio se reduzca a un intervalo temporal y una posible pérdida de información aceptable por la Unidad de Cómputo y Servicios Informáticos (UCSI) del Instituto.

Consolidación de recursos e índices de utilización más altos. Proporcionar mayores índices de utilización de servidores y almacenamiento a través de virtualización, para establecer eficientemente las cargas de trabajo y procesamiento para la consolidación de la arquitectura del sistema, infraestructura de aplicación, Base de datos, procesos.

Disminución de costos de propiedad. Al optimizar el uso de los recursos, hay menos hardware que adquirir, mantener, alimentar y enfriar. Implementar una estructura de centro de datos orientado a servicio podrá ver una reducción de los gastos operativos y de capital, lo cual disminuirá considerablemente el TCO.

Escalabilidad de servicios: Conforme a las necesidades y capacidad de las demandas en los recursos tecnológicos la solución tiene que ser altamente escalable y que pueda administrarse como una sola entidad entre los sitios o extensiones territoriales.

Mayor dinamismo para respaldar el crecimiento. El diseño modular de la estructura del centro de datos orientado a servicio permite a la UCSI del Instituto Estatal Electoral de Baja California Sur responder más rápidamente a las unidades y políticas de la Institución para aprovisionar los recursos tecnológicos sobre la marcha y de forma simultánea.

Converger todas las operaciones del centro de datos en un solo líder en administración. La convergencia de todas las operaciones del centro de datos en un solo dominio de administración asegura que los equipos de almacenamiento, aplicaciones, servidores y redes estén todos los cambios de configuración estén bien organizados y actualizados.

Automatizar todo lo posible. La capacidad para automatizar y coordinar muchas de las tareas necesarias para operar un centro de datos aumentará considerablemente la disponibilidad y evitará el reducir el tiempo de inactividad por error humano con el objetivo final de permitir a la UCSI responder de manera más rápida y precisa.

Migración Sencilla. Preparar el camino para lograr una transición simple aportando valor en la infraestructura a través de la tecnología y los procesos necesarios que reduzcan los riesgos y costes de planificación, ejecución y mantenimiento.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Seguridad

Función

Plataforma de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios de una red computacional.

En esta Capa están concentrados los dispositivos ofrecen un enfoque unificado de seguridad que es amplio, integrado y automatizado. Controlando la superficie de ataque mediante una amplia visibilidad integrada, deteniendo las amenazas avanzadas con la prevención integrada de amenazas basada en la Inteligencia artificial y reduciendo la complejidad a través de la orquestación y las operaciones automatizadas.

Objetivo

- Establecer una estrategia de seguridad centralizada enfocada en las aplicaciones para la administración del riesgo que incluya la protección adecuada de la confidencialidad, la intimidad y la integridad de la información.
- Diseñar e implementar un esquema de seguridad basado en segmentaciones que supervise continuamente el nivel de confianza de los usuarios, dispositivos y aplicaciones, por medio de un control dinámico con acceso en función de la intención, el comportamiento y el riesgo de la Institución.

Proyecto: Proveer una estrategia de seguridad basada en segmentación para la administración del riesgo por medio de dispositivos centralizados en el Centro de Datos para el IEEBCS

- Crear, Diseñar e implementar una estrategia de seguridad que reduzca drásticamente la superficie de ataque, al hacerla más difícil para la intrusión, vulnerabilidades y explotación de las mismas para evitar su movimiento lateral (este-oeste) a través de la red.
- Se creará un modelo de seguridad en la red, que se extiende desde el centro de datos y los sitios remotos hasta los bordes de la red.
- Implantar una arquitectura SD-WAN ayuda al IEEBCS a lograr una conectividad más rápida, ahorrar costos y mejorar el rendimiento de las aplicaciones en la red en comparación con los entornos WAN.
- Simplificar la complejidad de la seguridad y proporcione visibilidad de las aplicaciones, los usuarios y las redes. Utilizando dispositivos de seguridad especialmente diseñados con servicios de inteligencia de amenazas de terceros, para ofrecer seguridad de primer nivel y protección contra amenazas de alto rendimiento (por ejemplo, prevención de intrusiones, filtrado web, antimalware, control de aplicaciones), creando una serie de respuestas automatizadas basadas en políticas que aceleran el tiempo de resolución.
- Desarrollar la seguridad basada en segmentación permite la integración profunda entre las soluciones basada en la intención de mejorar la postura defensiva del IEEBCS, mitigando los riesgos, respaldandose en el cumplimiento y aumenta la eficiencia operativa.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

- Establecer las herramientas de administración y análisis permitan a los equipos de seguridad hacer más con recursos de seguridad limitados. Las soluciones de gestión y análisis proporcionan una administración eficiente, visibilidad transparente e inteligencia e información en tiempo real en todas las capas de seguridad. Simplificando los flujos de trabajo de administración, acortando los tiempos de implementación y reduciendo las posibilidades de una configuración incorrecta causada por errores humanos.
- Crear un esquema de seguridad para las aplicaciones y prevenirlas de los ataques por medio de protecciones adicionales que un firewall o un sistema de prevención de intrusiones (IPS). El IEEBCS necesita firewalls de aplicaciones web, controladores de entrega de aplicaciones y sandboxing para abordar las últimas amenazas.
- Establecer una operación por medio de una seguridad que se enfoque a Prevenir amenazas cibernéticas, Detección avanzada de amenazas, la automatización de respuestas a incidentes de seguridad que reducen el tiempo de resolución para la detección, protección y remediación, a el soporte del cumplimiento de las normas de seguridad de la institución que incluyan los correspondientes reportes.
- Lograr un soporte y capacitación que incluya al personal del IEEBCS centrados en amenazas, tecnologías de seguridad y soluciones.

Red

Función

Infraestructura para proveer conectividad redundante con rápida convergencia entre todas las capas, de Procesamiento, Almacenamiento, seguridad ubicada al borde de la capa de distribución y acceso.

En esta capa se intercomunican el Núcleo o Core de la red con los usuarios finales, estaciones de trabajo, teléfonos IP y switches de Capa 2 que conectan dispositivos a la capa de distribución y provee agregación.

Objetivo

- El propósito de esta capa es conmutar el tráfico a la más alta velocidad posible por medio de los protocolos LACP entre la infraestructura tecnológica de la institución y los recursos destino.
- Todos los enrutamientos, ACLs y directivas de seguridad estarán especificadas y direccionadas a los equipos Firewall.
- Diseñar y crear la reestructuración de paquetes o datos por medio QoS para reordenamiento entre VLAN.
- Los switches entre cada IDF al MDF mantendrá enlaces redundantes hacia la capa de núcleo por medio del protocolo LACP.
- Se proveerá direccionamiento estático al núcleo de acuerdo con la clasificación de cada puerto por medio de VLAN.
- Activación de protocolos de monitoreo para él envió de alarmas y eventos del dispositivo.

Proyecto: Construcción de su centro de datos unificado-basado en una red centralizada con seguridad integrada bajo estándares en el Centro de Datos para el IEEBCS.

- Implementar una solución de red centralizada con seguridad integrada por medio capas, la cual consistirá en un Núcleo (Core) Enterprise para el centro de datos con administración centralizada e integrado a la capa de seguridad perimetral (Firewall) por medio de interfaces 10Gb y utilizando una arquitectura de alimentación eléctrica vía Ethernet (POE+) a 1Gb para la capa de acceso o dispositivos de acuerdo con los requerimientos y necesidades de la Institución.

Servicios

Función.

Capa destinada a la virtualización del centro de datos para una mejor capacidad de automatización de las Tecnologías de la Información, así como configuración coordinada de servicios de red. De esta manera, las organizaciones pueden beneficiarse de mayor flexibilidad y agilidad, con un suministro más rápido y coordinado de almacenamiento, además de recursos de red, y una mejora en la continuidad de sus productos y servicios.

Objetivo.

Renovar y construir un centro de datos unificados basados en una red convergente que elimine la necesidad de almacenamiento en paralelo y de redes computacionales, así como elevar y eficientar la infraestructura de almacenamiento, conmutación y procesamiento con la suficiente flexibilidad que permita tener los más altos niveles de rendimiento. Para desarrollar un ecosistema interno a fin de aumentar la eficiencia, la simplicidad y el dinamismo operacional conforme a la estrategia digital de la Institución.

Proyecto: Plataforma unificada por medio de una solución de Convergencia enfocada en una nube pública para el IEEBCS.

- Renovación y construcción de su centro de datos unificados basados en una red convergente que elimine la necesidad de almacenamiento en paralelo y de redes computacionales, infraestructura de almacenamiento, conmutación y procesamiento por medio de una nube pública.

Base de datos

Función

Capa de gestión de datos que incluye el almacenamiento y la recuperación de datos, así como la gestión de actualizaciones, permitiendo el acceso simultáneo o simultáneo por parte de más de un proceso, brindando seguridad, asegurando la integridad de la información y brindando servicios de soporte como el respaldo de datos.

Objetivos

- Desarrollar los mecanismos de persistencia de datos (servidores de bases de datos, archivos compartidos, etc.) y con la capa de acceso a datos que encapsule los mecanismos de persistencia y exposición de los datos.
- Debe proporcionar una API para el nivel de aplicación que exponga métodos para administrar los datos almacenados sin exponer o crear dependencias en los mecanismos de almacenamiento de datos.
- Evitar las dependencias en los mecanismos de almacenamiento que permitan actualizaciones o cambios sin que los usuarios se vean afectados o incluso conscientes del cambio.
- Proyecto diseñar y crear una Infraestructura segura para Base de datos con optimización automática de datos para el IEEBCS
- Implementar una infraestructura virtualizada con el cual se pueda conformar una Plataforma de base de datos para entornos en crecimiento, combinando el hardware y software, para proporcionar una función específica, la capa de base de datos.
- Crear un Sistema de base de datos simple, optimizada y asequible, para el procesamiento de transacciones en línea (OLTP) y las cargas de trabajo de almacenamiento de datos.
- Establecer una plataforma de consolidación para bases de datos y aplicaciones, para unificar los sistemas o aplicaciones independientes y ubicarlos en un sistema de base de datos optimizado.
- Diseñar y crear una infraestructura para la optimización automática de datos (ADO), que permite crear políticas para la compresión de datos (Smart Compression) y el movimiento de datos, para implementar y mejorar los niveles de almacenamiento y compresión.
- Aprovisionamiento rápido de entornos de prueba y desarrollo para los programadores que requieran acceso de base de datos.
- Proporcionar una variedad de opciones de implementación de recuperación ante desastres y planes de contingencia para aumentar la disponibilidad y poder cumplir con los niveles de servicio del centro de datos.

Administración y Monitoreo

Función

La capa de administración y monitoreo es la que supervisa y monitorea entornos de redes complejos, telecomunicaciones que requieren alta disponibilidad que pueden requerir atención especial para evitar la degradación del servicio en el centro de datos.

Objetivo

- Infraestructura tecnológica para garantizar la alta disponibilidad de hardware, sistemas operativos, aplicaciones de software y servicios bajo su administración del centro de datos.
- Mantener los sistemas administrados con base en los acuerdos de servicio y niveles de servicio del Centro de datos.
- Configuración de la cuenta del usuario final en la herramienta de administración remota y la solución de automatización de servicios profesionales.

- Implementar una rutina de detección con la herramienta de supervisión y administración remota para identificar todos los dispositivos conectados a la red y sus roles en el entorno.
- Comprobación de las comunicaciones y alertas bidireccionales correctas hacia y desde dispositivos gestionados, sistemas operativos, aplicaciones de software y servicios en la ubicación del usuario final.

Proyecto Creación de un Centro de Operaciones de la red (NOC) del IEEBCS.

Establecer un centro de operaciones en la red de ACE-BCS con el cual se pueda monitorear y gestionar la red incluyendo los siguientes objetivos.

- Herramientas de control y flujo de información para las soluciones de incidencias.
- Información sobre la disponibilidad actual, histórica y planeada de los sistemas.
- Estado de la red y estadísticas de operación
- Gestión de configuraciones/cambios
- Gestión del desempeño/rendimiento
- Gestión de fallas
- Gestión de seguridad

Plan de continuidad operaciones ante desastres

Función

La recuperación ante desastres implica un conjunto de políticas, herramientas y procedimientos para permitir la recuperación o continuación de infraestructura y sistemas de tecnología vital importancia, después de un desastre natural o inducido por el hombre. La recuperación ante desastres se centra en los sistemas de TI o tecnológicos que soportan funciones operativas críticas.

Objetivo

- Planificar la continuidad operativa, en la cual abarque la planificación de recuperación ante desastres de TI.
- Establecer el objetivo de punto de recuperación (RPO-Recovery Point Objetive) y el objetivo de tiempo de recuperación (RTO – Recovery Time Objective).

Proyecto Creación de un Plan de continuidad de operaciones para el IEEBCS.

Establecer un plan de contingencia operativa de los servicios de Tecnología de la información del IEEBCS para establecer los mecanismos de respaldo y de procesos que incluyan los siguientes objetivos.

- Sistema de respaldo y estrategia de recuperación en caso de incidencias en los servicios.

- Establecer un equilibrio entre el RTO y el RPO, teniendo en cuenta el riesgo operacional, junto con todos los demás criterios principales de diseño del sistema, Estado de la red y estadísticas de operación.

Seguridad en redes del IEEBCS

Conforme a los objetivos esenciales se establecerá una arquitectura de servicios en cada uno de los sitios del Instituto Estatal Electoral de Baja California Sur por medio de 3 capas y una red de perímetro que definirán la Red del IEE-BCS bajo estos principios.

Principio 1: Disponibilidad de la red

El sistema será capaz de proporcionar servicios de red de alta disponibilidad.

Motivación:

- Apoyar a los objetivos del Instituto Estatal Electoral de Baja California Sur al proporcionar una red fiable y resistente.
- Flexibilidad, permitiendo al Instituto Estatal Electoral de Baja California Sur a responder a los cambios en los nuevos requerimientos de nivel de servicio, según sea necesario.

Impacto:

- Una red de alta disponibilidad reduce las interrupciones operacionales logrando así una mayor satisfacción y productividad del usuario que se refleja en la atención al ciudadano.

Principio 2: Escalabilidad de la red

La arquitectura de la red debe ser compatible con el crecimiento presentado por las necesidades del Instituto Estatal Electoral de Baja California Sur, tendencias de la industria y de los requerimientos de aplicaciones futuras.

Motivación:

- El Instituto Estatal Electoral de Baja California Sur debe estar preparado para las nuevas aplicaciones de los productos multimedia, voz, video y datos.

Impacto:

- Posicionarse en un ambiente de innovación y escalabilidad de las tecnologías emergentes de acuerdo con las tendencias futuras en la entrega de información.

Principio 3: Administración de la red

La arquitectura de red debe estar gestionada por todos y cada uno de los componentes de la infraestructura. Estos incluyen la disponibilidad de la red, la configuración y el rendimiento.

Motivación:

- Mantener la eficacia y la disponibilidad de la infraestructura tecnológica.
- Proporcionar un entorno proactivo para eliminar o reducir las fallas en la red.
- Gestión de la configuración mejora en el control de los activos para facilitar la planificación y la implementación del sistema.

Impacto:

- Una red manejable se traducirá en la capacidad del Instituto Estatal Electoral de Baja California Sur para realizar movimientos, adiciones y cambios con una interrupción limitada y controlada a la red.

Red de Perímetro.

Proveer una estrategia de administración del riesgo que incluye la protección adecuada de la confidencialidad, la intimidad y la integridad de la información.

Objetivo

- Establecer una estrategia en defensa de profundidad para definir los múltiples niveles de seguridad de acuerdo con el firewall para proteger la red.
- Implantar esquemas de seguridad basados en Host a cada servidor como sea posible.
- Configuración de servicios VPN y accesos remotos.

Capa de Acceso y distribución (Access - Distribution Layer).

Contiene usuarios finales, estaciones de trabajo, teléfonos IP y switches de Capa 2 que conectan dispositivos a la capa de distribución y provee agregación.

Objetivo

- Los switches entre cada IDF al MDF mantendrá enlaces redundantes hacia la capa de núcleo por medio del protocolo LACP.
- Se proveerá direccionamiento estático al núcleo de acuerdo con la clasificación de cada puerto por medio de VLAN.
- Se activarán los protocolos de monitoreo para él envió de alarmas y eventos a un dispositivo central.

Requisitos en Sitio de la Red Segura y en La Nube

Requisitos en Sitio

Para la propuesta de la Red Segura, es necesario contemplar las siguientes oficinas remotas para lograr la comunicación a los servidores en la nube donde se alojarán los aplicativos.

Consejo Distrital/Municipal (total de 21): oficinas de los órganos desconcentrados que se instalan de forma temporal para el Proceso Electoral. Cabe destacar que dichas oficinas son de carácter temporal.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Consejos Distritales Electorales:

MUNICIPIO	DISTRITO ELECTORAL	CABECERA DISTRITAL
LOS CABOS	1	SAN JOSÉ DEL CABO
LA PAZ	2	LA PAZ
LA PAZ	3	LA PAZ
LA PAZ	4	LA PAZ
LA PAZ	5	LA PAZ
LA PAZ	6	TODOS SANTOS
LOS CABOS	7	SAN JOSÉ DEL CABO
LOS CABOS	8	CABO SAN LUCAS
LOS CABOS	9	CABO SAN LUCAS
COMONDÚ	10	CIUDAD CONSTITUCIÓN
LOS CABOS	11	CABO SAN LUCAS
LOS CABOS	12	SAN JOSÉ DEL CABO
LORETO	13	LORETO
MULEGÉ	14	ALBERTO ANDRÉS ALVARADO ARÁMBURO
LA PAZ	15	LA PAZ
LOS CABOS	16	CABO SAN LUCAS

Consejos Municipales Electorales:

MUNICIPIO	CABECERA MUNICIPAL
LOS CABOS	SAN JOSÉ DEL CABO
LA PAZ	LA PAZ
LORETO	LORETO
COMONDÚ	CD. CONSTITUCIÓN
MULEGÉ	SANTA ROSALÍA

Oficinas Centrales, Centros de Captura y Verificación (CCV) del PREP:

OFICINAS CENTRALES / CCV	UBICACIÓN
Oficinas Centrales del Instituto	LA PAZ
Centros de Captura y Verificación (CCV)	LA PAZ

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Tabla Resumen del PREP:

Oficinas	Nodos
19 CATD	38
2 CCV	30 Cada uno
Oficinas Centrales	10
Celulares Android	348
Total de Dispositivos en Red	456

Nota: Respecto a los dos CCV, serán distribuidos en dos lugares diferentes, por lo que es necesario considerar los equipos para la conectividad en cada uno.

Tabla Resumen del SISCOM:

Oficinas	Nodos
21 Consejos Distritales/Municipales	42
1 Oficinas Centrales	10
Total de Dispositivos en Red	52

Para ello, se propone la siguiente solución con los siguientes insumos.

- 1 Fortigate en cada Consejo: con las características necesarias para albergar 4 equipos con redundancias de conexión y posibilidad de tener 2 VPN separadas. Deberá ser en esquema de arrendamiento.
- La posibilidad de agregar una red inalámbrica (access point) con la seguridad del Fortigate para al menos 2 celulares o bien utilizar Forticlient. Los AP se deberán incluir en esquema de arrendamiento.

Para las oficinas del **Centro de Captura y Verificación de Datos (CCV)** se requiere por lo menos:

- 1 Fortigate para soportar 30 equipos en red con redundancia de conexión.
- Los elementos que sean necesarios para llevar a cabo la conexión de los 30 equipos (1 switch de 48 puertos). Deberá ser en esquema de arrendamiento.
- La posibilidad de agregar una red inalámbrica (access point) con la seguridad del Fortigate para al menos 5 dispositivos o bien utilizar Forticlient. Deberá ser en esquema de arrendamiento.

Además de igual forma en esquema de arrendamiento (la totalidad de los insumos señalados a continuación), contemplar los siguientes insumos en la propuesta de red para soportar los equipos:

- Gabinetes (Racks) de Pared para servidores y equipos informáticos

Bajo su definición los racks son un espacio fabricado en metal a modo de armario en el cual se introducen una serie de dispositivos informáticos o de comunicaciones, así como

electrónicos. Estos armarios rack están fabricados con el objetivo de permitir la introducción de equipamiento de diversos estilos y marcas.

Los armarios rack tienen columnas verticales con agujeros colocados de forma regular. Se les denomina unidad rack, o de forma habitual "U", y están siempre reunidos de tres en tres.

En ellos, se busca alojar un equipo Fortigate, los módems de los proveedores de Internet, un regulador de voltaje, una batería tipo UPS, y un ventilador para rack, un Access point, estos 2 últimos en caso de requerirse.

A continuación, se describen algunas opciones de Racks, que debido al funcionamiento y cantidad de equipos que se busca alojar, el tipo de rack que se propone es para pared.

Opción 1:

Servicio: Intellinet Gabinete Mural para Servidor 19", 6U

Características: Tamaño: 48,3 cm (19"), Tipo: Montado en la pared, Dimensiones: 600 x 450 x 351 mm, Capacidad máxima de peso: 60 kg, Color del producto: Negro.

Opción 2:

Servicio: Nexxt Solutions Rack de Pared Cerrado de Aluminio 19", 6U

Características: Tamaño: 48,3 cm (19"), Tipo: Wall mounted rack, Materiales: SPCC, Dimensiones: 600 x 550 x 497 mm, Capacidad máxima de peso: 60 kg, Color del producto: Negro.

Opción 3:

Servicio: Rack de Servidores de 6U para Montaje en Pared, con 16.9”

Características: Tamaño: 16.9”, Modelo: RK616WALM, Tipo: Montado en la pared, Capacidad máxima de peso: 90 kg, Color del producto: Negro.

Opción 4:

Servicio: Gabinete Para Pared Metálico Enson Ens-rkgb6u 600x450mm Características: Dimensiones: 600 x 450 x 368 mm, Capacidad: 6U, Marca: Enson,

- Ventilador para Rack

Un ventilador para Rack es un tipo de ventilador similar al de una computadora, el cual se instala ya sea en la parte superior, o en las paredes del rack, y el cual permite una mejor circulación de aire para los equipos alojados dentro de este.

Los equipos electrónicos por sí solos ya generan calor al estar funcionando por varias horas seguidas, y en un lugar donde la temperatura pueda subir, o bien, no se cuente con un buen sistema de enfriamiento o aire acondicionado, estos ventiladores ayudan a mantener en mejores condiciones los equipos, al mejorar la ventilación de los mismos. Además, normalmente sólo ocupan 1 unidad de rack (1U).

- Regulador de Voltaje

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur. **(612)** 125.0808 y **(612)** 129.4062

Los reguladores de voltaje son dispositivos que adecuan la entrada de electricidad y la estabiliza generando una entrada de corriente constante y regular a los productos. Sirven para que los equipos electrónicos que están recibiendo una corriente variable de energía, donde pueden llegar a contar con picos altos o bajos de voltajes, no afecten el correcto rendimiento de estos.

Este equipo es sumamente importante, ya que otorgará protección a los equipos alojados en el rack, los cuales deben estar en óptimas condiciones para su correcto funcionamiento. Normalmente, los reguladores cuentan con hasta 8 contactos eléctricos, por lo que con un equipo de este tipo en cada oficina será más que suficiente.

El regulador debe soportar los consumos eléctricos de los equipos que se conectarán a este, los cuales se describen a continuación:

- Fortigate: 12Vdc/3A; 100Vac/1.0A; 240Vac/0.6A; 17.2W-18.7W
- Módem: 12Vdc/2A; 4.9-28.7W
- Ventilador para Rack: 110Vac/2.1A;

Descripción de las unidades eléctricas:

- V: Voltio (Voltaje)
- A: Ampere (Amperaje)
- W: Watt (Potencia/ Consumo eléctrico, por hora)
- ac: Corriente Alterna (Corriente recibida por el proveedor del servicio eléctrico)
- dc: Corriente Directa (Corriente recibida en el equipo, a través de un convertidor que incluye cada equipo eléctrico, el cual convierte la AC en DC)
- Vac: Voltaje de corriente alterna
- Vdc: Voltaje de corriente directa
- Sistema de Fuerza Ininterrumpible (UPS)

Un Sistema de Fuerza Ininterrumpible (UPS), es un equipo cuya función principal es evitar una interrupción de voltaje en la carga a proteger, así como la fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo.

Estos sistemas brindan protección de energía garantizada para equipos electrónicos conectados. Cuando se interrumpe el suministro, o cuando éste fluctúa por fuera de niveles seguros, instantáneamente la UPS comienza a proveer un suministro de respaldo limpio a través de baterías y protección contra sobretensiones a los equipos sensibles conectados. Algunos incluso cuentan con una entrada RJ45 para protección de líneas de internet.

Existen distintos tipos y modelos de estos equipos, y de acuerdo al tipo y cantidad de equipos que estarán conectados, y tomando en cuenta el consumo eléctrico de cada uno descrito anteriormente, se requerirá un UPS que soporte dichos consumos.

Se propone entonces un UPS del estilo doméstico, de dimensiones pequeñas, con un diseño parecido a un regulador de voltaje, ya que dichos equipos tienen características suficientes para un óptimo funcionamiento, y un tiempo de autonomía para nuestros equipos de hasta 30 minutos, así como el tamaño ideal para el tipo de rack que se busca instalar. Deberá ser en esquema de arrendamiento.

RESUMEN DE LOS REQUERIMIENTOS DE HARDWARE

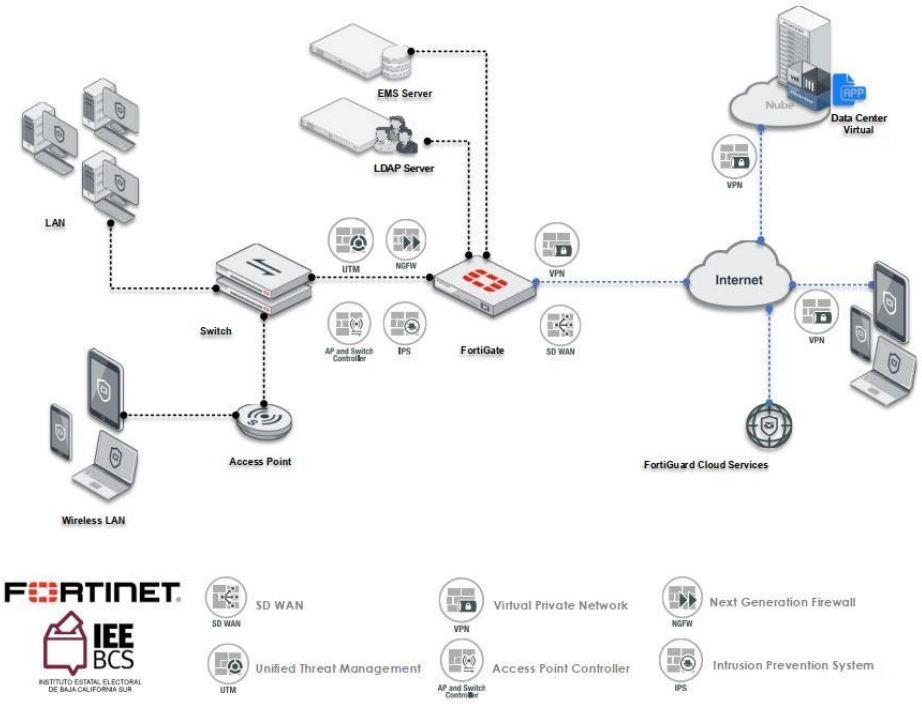
Los Equipos Físicos descritos en el presente Anexo Técnico que son necesarios para la correcta ejecución de los Sistemas PREP y SISCOM se resumen en la siguiente tabla, deben de considerarse bajo un esquema de Arrendamiento por la duración a la que hace referencia el presente documento.

Equipo Tecnológico	Cantidad
Fortigate de los Consejos	21
Fortigate de los CCV	4 (2 en cada CCV)
AP o Medio de conexión inalámbrica con Fortigate	23
Racks	23
UPS	23
Reguladores	23
Ventiladores para Rack	23

*El total hace referencia a 21 OD + 2 CCV.

Aunado a ello, el proveedor deberá de **realizar y contar con la capacidad de efectuar la instalación de dichos Equipos Tecnológicos en los Consejos Distritales y Municipales además de los 2 CCV en un periodo no mayor a 2 meses posterior a su contratación.**

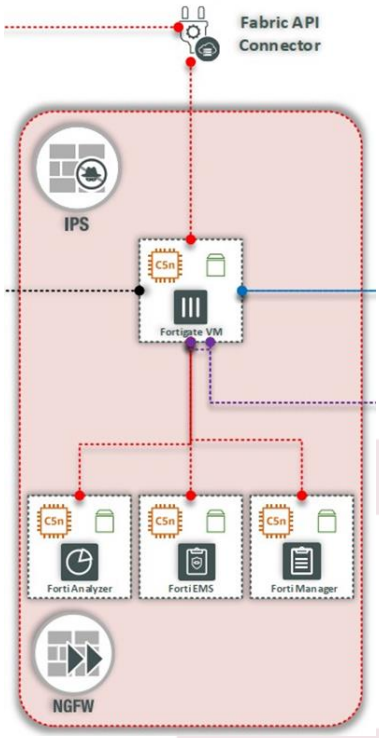
Ejemplo de conexión en Oficinas Remotas (Consejos Distritales y Municipales)



Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Se deberán contemplar los siguientes componentes:

- Fortinet FortiGate Next-Generation Firewall (Fortinet VPN)
- FortiManager Centralized Security Management
- FortiAnalyzer Centralized Logging/Reporting
- Forticlient Enterprise Management Server (Forticlient EMS)
- Fortinet FortiCWP Workload Guardian



Servicios en la Nube

La propuesta debe de considerar al menos una VPC o Red Privada en AWS que permita la conexión de las oficinas a Amazon de forma Segura y Privada. Además debe de considerar al menos 2 VPN separadas para poder garantizar el flujo de la información de manera independiente para los Sistemas PREP y SISCOM.

Se deben de considerar los siguientes elementos en la nube para cumplir con la propuesta de la solución.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur. **(612)** 125.0808 y **(612)** 129.4062

Servicios necesarios para el PREP:

- 4 Amazon Elastic Compute Cloud (Amazon EC2) c6in.xlarge con 4vCPU y 8GB de RAM (3 en Availability Zones Diferentes), 250 GB Storage amount
- 2 Amazon Relational Database Service (Amazon RDS) db.m4.xlarge de 4vCPU y 16GB de RAM 250 GB Storage Amount, 100 %Utilized/Month, Multi-AZ.
- 4 Amazon Simple Storage Services S3
- 2 Amazon Elastic Load Balancer (Amazon ELB)
- Amazon CloudFront. Transferencia de datos a Internet (25 GB por mes), Transferencia de datos a origen (25 GB por mes), Número de solicitudes (HTTPS) (10000000 por mes).
- Amazon CloudWatch
- Amazon GuardDuty
- Amazon Shield Advance
- Amazon Web Application Firewall Services (WAF)

Servicios necesarios para el SISCOM:

- 4 Amazon Elastic Compute Cloud (Amazon EC2) c6in.xlarge con 4vCPU y 8GB de RAM (3 en Availability Zones Diferentes) 250 GB Storage amount.
- 2 Amazon Relational Database Service (Amazon RDS) db.m4.xlarge de 4vCPU y 16GB de RAM 250 GB Storage Amount, 100 %Utilized/Month, Multi-AZ.
- 2 Amazon Elastic Load Balancer (Amazon ELB)
- Amazon CloudFront. Transferencia de datos a Internet (25 GB por mes), Transferencia de datos a origen (25 GB por mes), Número de solicitudes (HTTPS) (10000000 por mes).
- Amazon CloudWatch
- Amazon GuardDuty
- Amazon Shield Advance
- Amazon Web Application Firewall Services (WAF)

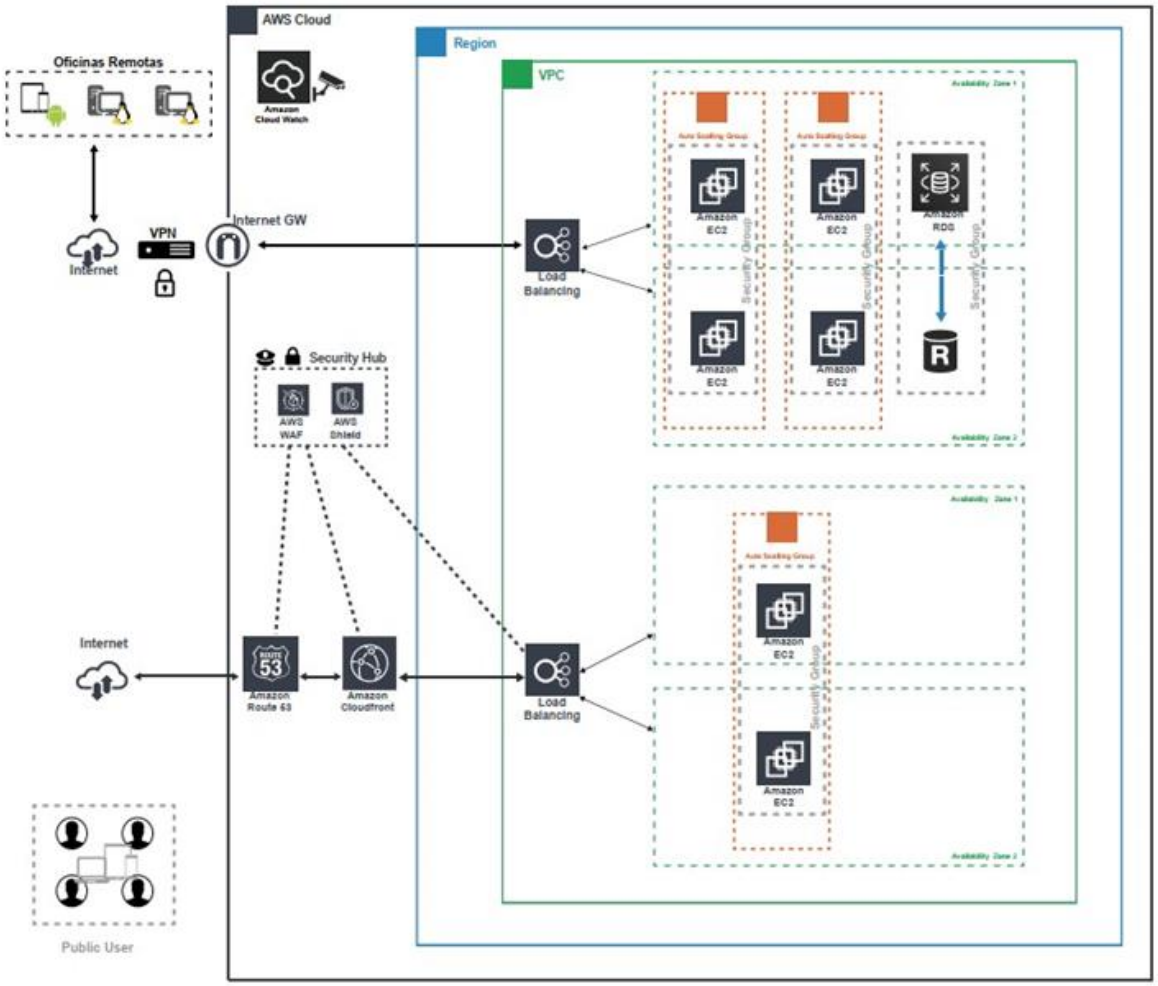
Además de los anteriores, es necesario contemplar un servicio de asistencia y asesoramiento continuo que permita acelerar la solución de incidencias y evitar la interrupción del servicio, por lo que también se debe considerar:

- Amazon Enterprise Support plan

aws

IEE BCS

ISTITUTO ESTATAL ELECTORAL
DE BAJA CALIFORNIA SUR



Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Así mismo, se debe contar con un esquema de redundancias en diferentes Zonas o Regiones como una propuesta adicional.

Detalle de los servicios en la Nube

Conforme a los objetivos esenciales se establecerá una infraestructura de servicios en la nube para el Instituto Estatal Electoral de Baja California Sur para brindarles el servicio a sus 21 oficinas que definirán la Red del IEE-BCS.

Amazon Regions, Availability Zones, and Local Zones

Los servicios de AWS estarán en una región, completamente independiente a las demás dentro de AWS. Cada zona de disponibilidad está aislada con la cual se creará la redundancia, pero estas zonas de disponibilidad en la región están conectadas a través de enlaces de baja latencia para su comunicación. Por medio de esta implementación la infraestructura de IEE-BCS se establecerá los servicios seleccionados.

Amazon Virtual Private Cloud (Amazon VPC)

Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual. Esta red virtual se aprovisiona para operar en su propia infraestructura de servicios escalable de AWS y proveer los servicios de encriptación y especificar un rango de direcciones IP para la VPC, agregar subredes, asociar grupos de seguridad y configurar tablas de rutas en las comunicaciones a sus 21 oficinas del Instituto Estatal Electoral de Baja California Sur.

NAT Gateway (NAT)

Servicio de AWS como puerto de enlace y traducción de direcciones de red (NAT) para permitir que las instancias en una subred privada se conecten a Internet u otros servicios de AWS.

Amazon Elastic Load Balancer (Amazon ELB)

Servicio para el balanceo de cargas de trabajo para direccionar el tráfico entrante de los clientes y dirigir las solicitudes a sus objetivos registrados (como las instancias EC2) en una o más zonas de disponibilidad.

Amazon Web Application Firewall Services (WAF)

Servicio de AWS que es un firewall de aplicaciones web con el cual se protegerán las aplicaciones web o API contra vulnerabilidades de web comunes, que pueden afectar la disponibilidad, comprometer la seguridad o consumir recursos excesivos de la infraestructura del IEE-BCS.

Amazon CloudFront

Servicio de red especializado para la entrega de contenido rápido (CDN) que entrega de forma segura datos, videos, aplicaciones y API a clientes de todo el mundo con baja latencia y altas velocidades de transferencia, todo dentro de un entorno amigable para el IEEBCS.

Amazon CloudWatch

Servicio de monitoreo y rendimiento creado para los servicios de infraestructura en la nube del IEE-BCS. Proporcionará datos e información procesable para el monitoreo de las aplicaciones, responder a los cambios de rendimiento en todo el sistema, optimizando la utilización de los recursos y obtener una visión unificada del estado operativo de la nube privada.

Amazon Shield Advance

AWS Shield Advance es un servicio de protección contra ataques de denegación de servicio distribuidos (DDoS) que protege las aplicaciones ejecutadas en AWS. AWS Shield Advance proporciona una mitigación en línea automática y una detección siempre activa que minimizan el tiempo de inactividad y la latencia de la aplicación, por lo que no es necesario disponer de AWS Support para beneficiarse de la protección contra DDoS. Dicho servicio deberá ser activado solo en los meses de mayo y junio del 2024 con la finalidad de ser utilizado durante la fase de implementación del PREP.

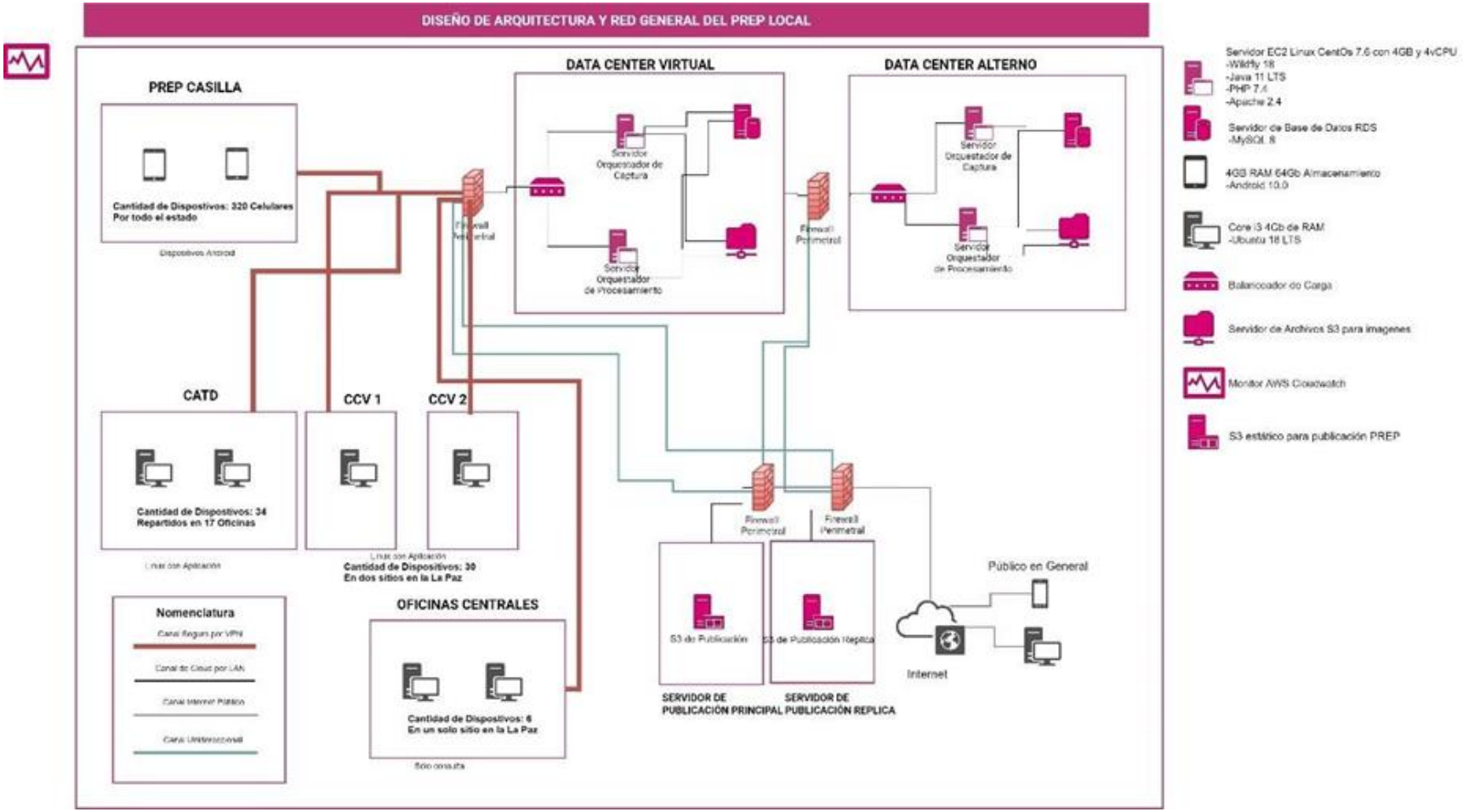
Amazon Enterprise Support Plan

AWS ofrece varios planes de soporte, y uno de ellos es el "Enterprise Support Plan" (Plan de Soporte Empresarial). Este plan está diseñado para satisfacer las necesidades de organizaciones grandes y complejas que dependen críticamente de los servicios de AWS.

- Algunas características clave del plan de soporte empresarial de AWS incluyen:
- Soporte 24/7: Acceso a soporte técnico en cualquier momento del día, los 7 días de la semana, con respuesta a problemas críticos en menos de 15 minutos.
- Gestor de cuenta técnica: Asignación de un gerente de cuenta técnico (TAM, por sus siglas en inglés) que brinda asesoramiento personalizado y trabaja en estrecha colaboración con la organización para optimizar el uso de los servicios de AWS.
- Análisis proactivo: AWS realiza análisis proactivos de la infraestructura del cliente y proporciona recomendaciones para mejorar la eficiencia, la seguridad y la confiabilidad.
- Acceso a la base de conocimientos: Acceso a una amplia base de conocimientos que incluye documentación técnica, tutoriales y recursos exclusivos para clientes del plan de soporte empresarial.
- Entrenamiento técnico: Ofrece acceso a recursos de formación técnica para ayudar a los equipos a aprovechar al máximo los servicios de AWS.

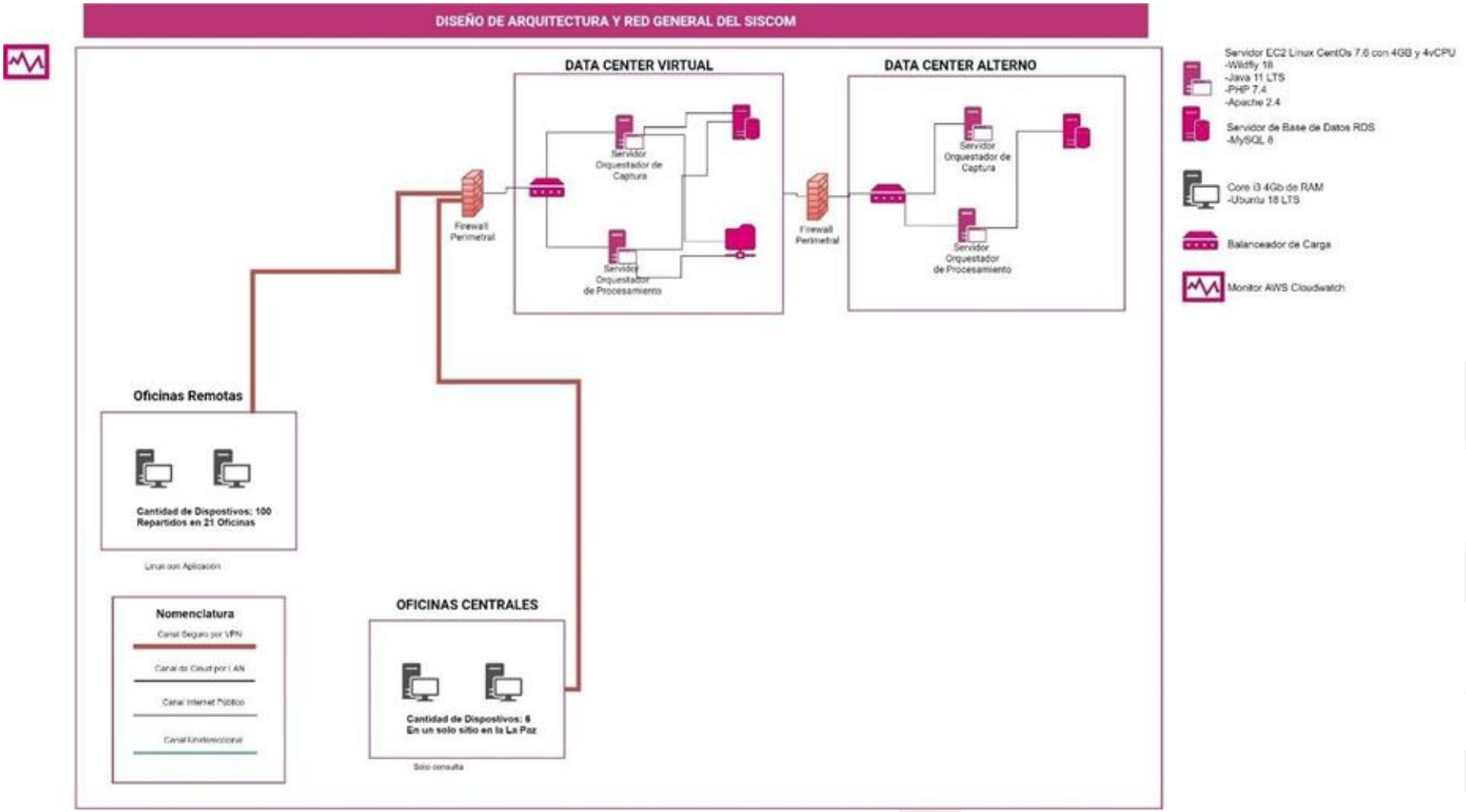
Dicho recurso deberá ser activado en el mes de mayo y junio del 2024 con fin de ser utilizado durante los simulacros y la fase de implementación del PREP, además de los cómputos oficiales en los cuales opera el SISCOM, en la primera semana de junio.

Diagrama de Red de Solución Final PREP



Constitución #415 esquina con la Calle Guillermo Prieto,
Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Diagrama de Red de Solución Final SISCOM



Alcances de Servicios

El servicio, objeto del presente documento quedará bajo el concepto de Servicios de Soporte Especializados y debe incluir lo siguiente:

- Suministro de equipo
- Mantenimiento preventivo y correctivo
- Soporte técnico
- Reconfiguraciones, instalaciones, movimientos, adiciones y cambios
- Mesa de ayuda
- Servicios de implementación
- Entrenamiento
- Gestión de la información
- Niveles del servicio requeridos
- Documentación general requerida

Suministro de equipo y licenciamiento

El proveedor deberá suministrar el equipo, componentes y accesorios de acuerdo con los componentes de la solución.

El equipo para suministrar es nuevo, de la más reciente generación liberada por el fabricante que comprenda la solución propuesta y que cumpla al menos con las características solicitadas de acuerdo a los componentes de la solución.

Mantenimiento preventivo y correctivo

El proveedor deberá mantener en condiciones normales de operación continua el servicio que suministrará, durante la vigencia del servicio, para lo cual se deberán realizar actividades de mantenimiento preventivo y correctivo.

Soporte técnico

El proveedor deberá proporcionar el servicio de soporte técnico de la infraestructura (hardware o software). Este servicio debe proporcionar ayuda y/o asistencia a personal de UCSI del Instituto para resolver determinados problemas mientras hace uso del equipo de la infraestructura, o sobre el software que conforma el servicio, o sobre dudas que se tienen para operar los equipos, software, o servicios que implementen; esto en base a los niveles de escalamiento y soporte requeridos.

Reconfiguraciones, instalaciones, movimientos, adiciones y cambios

El proveedor realizará reconfiguraciones, instalaciones, movimientos, adiciones y cambios de cualquier elemento de configuración que por su naturaleza no puedan ser realizados bajo asistencia remota a solicitud del personal de UCSI y que no sean especificados en cualquiera de los servicios solicitados. Este servicio será solicitado por personal de UCSI, en cualquier momento durante la vigencia del servicio, y éste deberá entregar una calendarización o plan de trabajo, que llevará a cabo para atender la solicitud. Dicho plan deberá ser entregado y aprobado por el personal de UCSI previo a los trabajos a realizarse.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

Mesa de ayuda

El proveedor deberá de contar con una Mesa de Ayuda para poder solventar cualquier problema que se presentase con la solución requerida. Dándole niveles de servicio acorde a la urgencia de la incidencia o requerimiento. Las funciones de la Mesa de Ayuda consistirán en la recepción, clasificación, registro, seguimiento, escalamiento y cierre de los incidentes, así como problemas, peticiones de cambio y solicitudes de servicio reportados por personal de UCSI y puede ser por medio de los siguientes mecanismos:

Portal web

El proveedor deberá contar con un portal WEB especializado para Mesa de Ayuda, en el cuál a través de Internet se levanten los reportes de fallas de los equipos y servicios del servicio, de tal forma que se proporcione al Instituto un folio secuencial de seguimiento por evento.

En este portal se llevará deberá contener una bitácora del estatus del reporte, así como las estadísticas de fallas e historial de incidentes reportados.

El proveedor deberá asegurar que se mantenga actualizada la información del portal garantizando la seguridad, confidencialidad, resguardo y disponibilidad de la información. Solo personal autorizado por el Instituto podrá acceder a los informes.

Por Correo Electrónico

Un correo electrónico especializado para recibir los incidentes o dudas para su atención con un tiempo de respuesta acordé a los niveles de servicio establecidos.

Teléfono de contacto

El proveedor deberá proporcionar un teléfono para la atención personalizada y exclusiva de incidentes y dudas. Así mismo puede ser un canal adicional al correo electrónico y portal web para dar seguimiento a los incidentes.

Servicios de implementación

El proveedor deberá considerar como parte de su propuesta los servicios de implementación, para la instalación, configuración y migración de los servicios a la nueva plataforma propuesta cumpliendo con los requerimientos del Instituto en tiempo y forma.

Planeación

Definir la metodología estratégica más adecuada para el desarrollo del proyecto, las actividades a realizar son:

- Reunión de arranque del proyecto.
- Definición de roles y responsabilidades.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

- Asignación de actividades y fechas.
- Confirmación de sitios y logística.
- Asignación de recursos para el proyecto.
- Comunicar la visión y entregables.
- Identificar y administrar el alcance del proyecto.
- Definir los controles de cambios y procesos de escalamiento.
- Esquema de firmas, entrega y criterios para liberación de pago.

Diseño

En este apartado se elaborará el diseño de la propuesta técnica de acuerdo a las mejores prácticas, además de asegurar que el diseño propuesto cumple con los requerimientos necesarios para la implementación y óptimo desempeño para la operación de los componentes que serán parte del presente proyecto.

Las actividades que desempeñar son las siguientes:

- Levantamiento físico.
- Levantamiento lógico de los equipos y sistemas que intervienen en la implementación del proyecto, configuraciones, protocolos, etc.
- Obtención de diagrama de red a detalle de topología actual.
- Documento con propuesta de diseño de la solución.
- Aceptación de la propuesta de diseño por parte del Instituto.

Implementación

En la fase implementación se integrarán los componentes afectando lo menos posible la operación de la red del Instituto, esto con base en lo documentado en la fase de diseño, para lo cual se permite contemplar lo siguiente:

- Definir el plan de migración de los componentes del Instituto Estatal Electoral de Baja California Sur. La integración de la solución permitirá cumplir con el seguimiento de buenas prácticas en el proceso de instalación, configuración y puesta en operación del sistema de acuerdo con la metodología de ITIL Ver3 actualización 2011.
- El proyecto de la Red Segura del PREP y SISCOM será del 13 de marzo al 30 de junio de 2024 a excepción del servicio de AWS Enterprise Support Plan que será del 1 de mayo al 30 de junio del 2024 y el servicio de AWS Shield Advance que será del 1 de mayo al 30 de junio del 2024.
- Realizar la configuración de los componentes en un ambiente de laboratorio.
- Validación de configuraciones y funcionalidades en ambiente de laboratorio.
- Establecer las fechas y horas de las ventanas de mantenimiento requeridas para la implementación de las soluciones.
- Ejecutar el plan de migración.
- Al día siguiente de la implementación se deberá de dar soporte para lograr la estabilización temprana del servicio.

Constitución #415 esquina con la Calle Guillermo Prieto, Colonia Centro, C.P. 23000. La Paz, Baja California Sur.
(612) 125.0808 y **(612)** 129.4062

- Realizar pruebas de funcionalidad de los componentes del Instituto Estatal Electoral de Baja California Sur.
- Revisar que se cumpla con los requerimientos del Instituto mediante pruebas de funcionalidad del flujo de procesos y administración de la red documentada en la fase de diseño.
- Pruebas de validación conjuntas entre el proveedor y el Instituto Estatal Electoral de Baja California Sur.
- Aceptación del funcionamiento de la implementación por parte del Instituto Estatal Electoral de Baja California Sur.
- Captura de línea base (Base Line) de funcionamiento, desempeño y configuración de los sistemas para comparaciones futuras.

Transferencia de Conocimientos

La fase de transferencia de conocimientos tiene como objetivo preparar y/o incrementar la habilidad del recurso humano definido por el Instituto para poder administrar las altas, bajas y cambios del sistema implementado:

- Descripción de la arquitectura propuesta
- Descripción de los módulos/licencias/suscripciones adquiridas
- Modo de implementación en la arquitectura, así como los beneficios adicionales que brinda
- Descripción de configuración del equipo para realizar altas, bajas y cambios cotidianos.
- Proceso de resolución de problemas básico que incluya la guía para levantar casos de soporte ante el fabricante.
- La duración del entrenamiento no podrá ser menor a 8 horas

Cierre del Proyecto

Para el cierre del proyecto se realizarán las siguientes actividades.

- Memoria Técnica que contiene la siguiente información:
- Respaldo de la Configuración de los equipos, indicando las versiones de software instaladas.
- Diagrama esquemático de la solución.
- Inventario del equipo instalado.
- Reporte de entrega de los equipos en ambiente productivo.
- Firma de carta de aceptación del proyecto por ambas partes.