

DOMINIO DE INFRAESTRUCTURA DE TI (TO-BE) ESTADO PROPUESTO

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI)
ARQUITECTURA EMPRESARIAL

Bogotá – Colombia
Noviembre de 2020

ÍNDICE DE CONTENIDO

índice de Contenido 2
1. ARQUITECTURA OBJETIVO DEL DOMINIO DE ARQUITECTURA INFRAESTRUCTURA TI 4
1.1. Propósito 4
1.2. Público Objetivo 4
1.3. Insumos 4
1.4. Método 4
1.5. Salidas 4
1.6. Consideraciones 5
2. ELEMENTOS DE LA ARQUITECTURA OBJETIVO 6
3.1. Diagrama BCP – Plan de Continuidad del Negocio 6
3.1.1. En el modelo actual 8
3.1.2. En el modelo propuesto 8
3.2. Virtual Data Center VDC y DRP 8
3.2.1. Internet 10
3.2.2. Ubicación o Sedes 10
3.2.3. Servicios DRP 10
3.2.4. Centro de Datos Virtual – Principal 11
3.2.4.1. Recursos On-Demand 13
3.2.4.1.1. Servicios de Monitoreo 13
3.2.4.1.2. Servicios de Seguridad 13
3.2.4.1.3. VDC - Aplicaciones y/o Servicios 16
3.2.4.1.4. VDC - SO 16
3.2.4.1.5. VDC - Virtualización 17
3.2.4.1.6. VDC - Infraestructura Física 17
3.2.4.1.7. VDC - Infraestructura de Transporte (RED) 17
3.2.4.1.8. VDC - Almacenamiento 17
3.2.5. Servicios Cloud 17

TABLA DE ILUSTRACIONES

Ilustración 1 - Distribución Diagramas en el repositorio 7
Ilustración 2 - Diagrama BCP Propuesto 8
Ilustración 3 - Virtual Data Center VDC y DRP 10
Ilustración 4 - VDC - Centro de Datos Virtual – Principal 12
Ilustración 5 - Servicios de Seguridad 14

1. ARQUITECTURA OBJETIVO DEL DOMINIO DE ARQUITECTURA INFRAESTRUCTURA TI

1.1. Propósito

Presentar el estado objetivo propuesto para el dominio de Arquitectura Infraestructura TI basados en las necesidades, requerimientos, lineamientos normativos y mejores prácticas; soportado en el análisis del estado actual de dicho dominio en la Honorable Cámara De Representantes - HCR, con el objetivo de poder identificar nuevos componentes, actualizar o modificar los existentes de su Infraestructura Tecnológica, así mismo, la relación o relaciones entre ellos y otras con elementos de otros dominios de arquitectura. Este análisis se soporta en las recomendaciones de MAE y prácticas como TOGAF y APM.

1.2. Público Objetivo

Este documento está dirigido a las personas que designe la institución dentro o fuera de ella, especialmente a líderes de estrategia de tecnología y los equipos que buscan determinar qué cambios se deben realizar en la HCR para responder a las necesidades y requerimientos de Infraestructura de TI tanto de las áreas misionales como de apoyo.

1.3. Insumos

Toda la información suministrada por el personal de TI de la entidad, documentos internos de la entidad, reuniones con los usuarios, información ubicada en portales institucionales, catálogos, contratos y entrevistas con proveedores, así mismo, marcos de referencia y mejores prácticas, lineamientos normativos, experiencia en arquitectura por parte del equipo consultor.

1.4. Método

Marco de referencia de arquitectura v2.0, The Open Group Architecture Framework – TOGAF 9.2, lineamientos Application Portfolio Management – APM.

1.5. Salidas

Acorde con las prácticas que soportan el ejercicio de arquitectura empresarial y las obligaciones contractuales se entregan las siguientes salidas: Elementos de la arquitectura objetivo relacionados con el dominio de infraestructura, que incluya: Arquitectura de servicios tecnológicos, Gestión

de la continuidad, Gestión de la disponibilidad, Acuerdos de nivel del Servicio, Monitoreo de la calidad del servicio, Mesa de servicio, Proceso de mantenimiento, Servicios Tecnológicos vs Sistemas de Información.

1.6. **Consideraciones**

Dentro de las consideraciones se debe tener en cuenta el informe de gestión de las TIC[1] presentado por el ingeniero Jefferson Pinzón Hernández, anterior jefe de la división de planeación y sistemas, del cual se resalta el conato de incendio presentado al interior de las instalaciones del Centro de Datos de la entidad, el día 4 de octubre de 2019, que ocasionó graves daños en el sistema de UPS (respaldo de energía), el sistema de almacenamiento de información, la solución de Backup (Storage One), el chasis de servidores, equipos de control de la red inalámbrica (WIFI), el Switch de Core, el sistema de telefonía local, el sistema de aire acondicionado, quedando inhabilitado y descargado el sistema de control de incendio.

Los efectos de esta situación han derivado en la ausencia de distintos sistemas de información, al igual que la pérdida parcial o en algunos casos total de información de la gestión de la HCR de los últimos años. Esta situación se agrava a partir del mes de Marzo de 2020 debido a la obligatoriedad de aislamiento a causa de la pandemia mundial y en consecuencia a la obligación de realizar trabajos por canales digitales o virtuales.

[1] Documento: INFORME GESTION DE LAS TIC CÁMARA DE REPRESENTANTES - 20 JULIO 2019 A 20 JULIO 2020.docx

2. ELEMENTOS DE LA ARQUITECTURA OBJETIVO

Como parte del ejercicio de arquitectura empresarial para la Honorable Cámara de Representantes y teniendo en cuenta lo identificado en las sesiones de trabajo con todos los usuarios de la entidad, la información recibida por parte del equipo de tecnología y la recopilada en las diferentes sesiones, para el caso de la propuesta de la Arquitectura Objetivo para la organización, se ha podido establecer los siguientes componentes en el proceso de modelado, dichos modelos residen en el repositorio designado para tal fin y se obtuvieron, entre otras, usando la herramienta BiZZdesign:

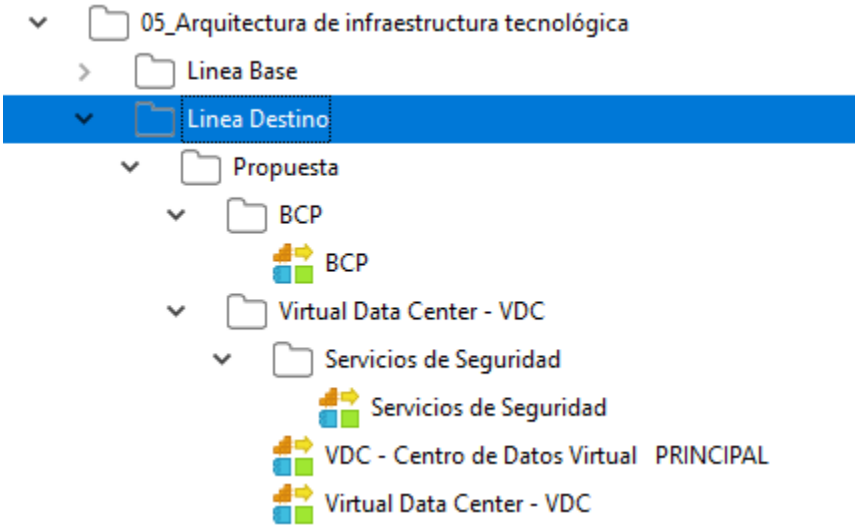


Ilustración 1 - Distribución Diagramas en el repositorio

3.1. Diagrama BCP – Plan de Continuidad del Negocio

Teniendo en cuenta que un BCP (Plan de Continuidad del Negocio o sus siglas en inglés Business Continuity Plan) es un plan logístico que permite a una organización recuperar y restaurar sus funciones críticas (parcial o totalmente) interrumpidas dentro de un tiempo predeterminado luego de una interrupción no deseada a causa de una eventualidad o desastre; se plantea para la Honorable Cámara de Representantes un modelo que permita la recuperación de la operación teniendo en cuenta los siguientes aspectos:

- Un sitio de recuperación: Es un sitio físico diferente a las sedes, donde se recuperará la operación en caso de una emergencia, este sitio debe contar y ser adecuado con: comunicaciones, puestos de trabajo, equipos de cómputo etc.
- Canales de comunicación alternos para comunicación entre el sitio de recuperación y los

centros de datos.

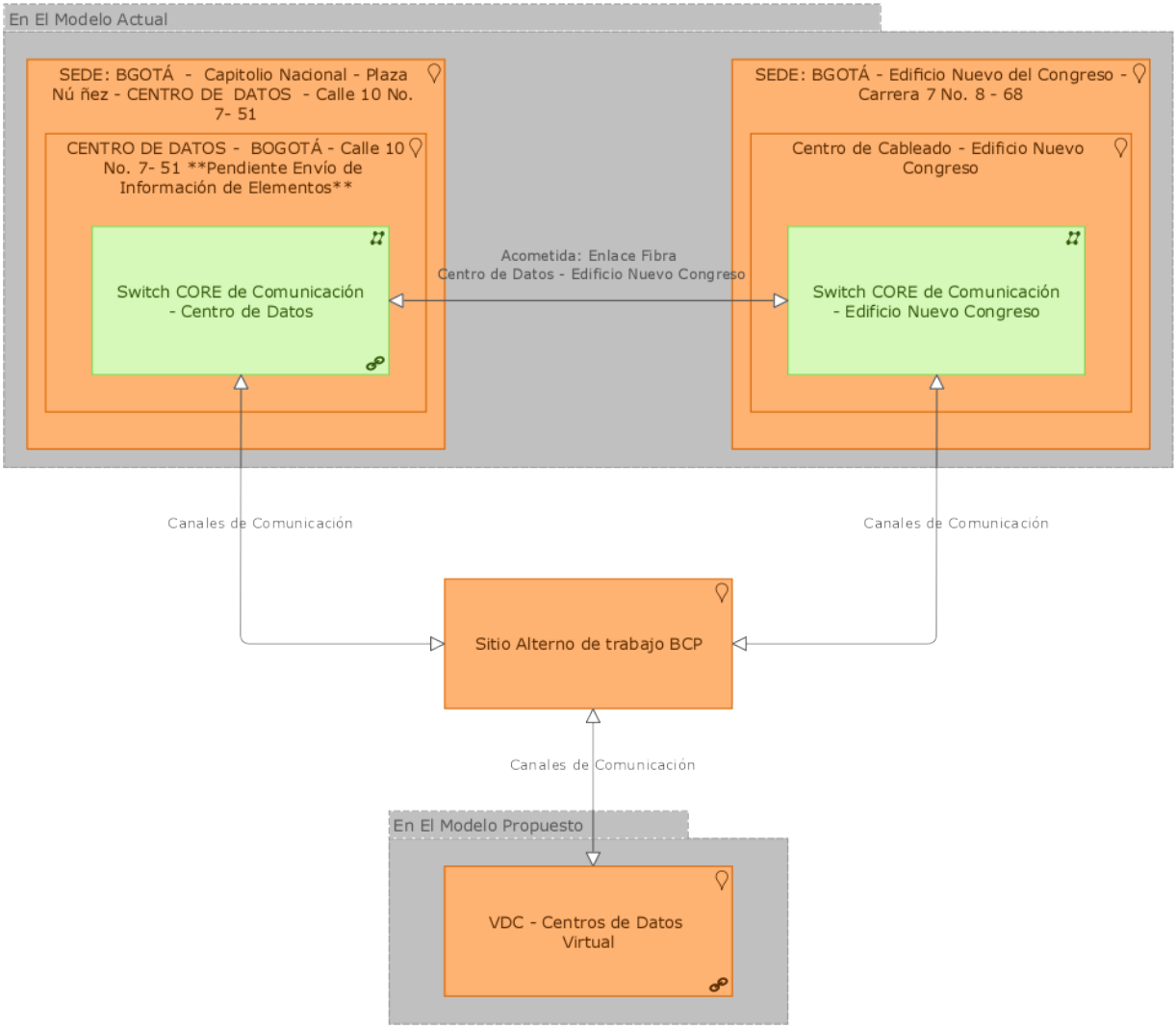


Ilustración 2 - Diagrama BCP Propuesto

Es importante tener en cuenta que, luego de establecer un plan de continuidad del negocio, este debe ser probado por lo menos una vez por año.

El modelo permite establecer las relaciones entre cada componente, a continuación, se muestran dichas relaciones para cada uno de los elementos que hacen parte del BCP:

3.1.1. En el modelo actual

Se deben conectar por medio de canales la arquitectura de comunicación del Switch Core entre la sede BOGOTÁ - Capitolio Nacional - Plaza Núñez - CENTRO DE DATOS - Calle 10 No. 7- 51 y la sede BOGOTÁ - Edificio Nuevo del Congreso - Carrera 7 No. 8 – 68 con el sitio de recuperación definido por la Honorable Cámara de Representantes.

3.1.2. En el modelo propuesto

Se debe conectar por medio de canales de comunicación por medio de fibra la arquitectura de comunicación del sitio de recuperación definido por la Honorable Cámara de Representantes con los VDC - Centros de Datos Virtual.

3.2. Virtual Data Center VDC y DRP

La propuesta Virtual Data Center VDC y DRP establece el modelo propuesto para la Honorable Cámara de Representantes incluyendo componentes existentes y nuevos, representa la manera de acceder a los servicios desde diferentes escenarios y se adentra hacia cada uno de ellos para describirlos en detalle posteriormente.

Los componentes que hacen parte de este modelo son:

Componentes existentes:

- Sedes Honorable Cámara de Representantes
- Canales de comunicación.
- Usuarios Honorable Cámara de Representantes Sin Canal de Comunicación

Componentes nuevos:

- Servicios DRP.
- Centro de Datos Virtual Principal.
- Centro de Datos Virtual Alterno.
- Nuevos canales de comunicación.

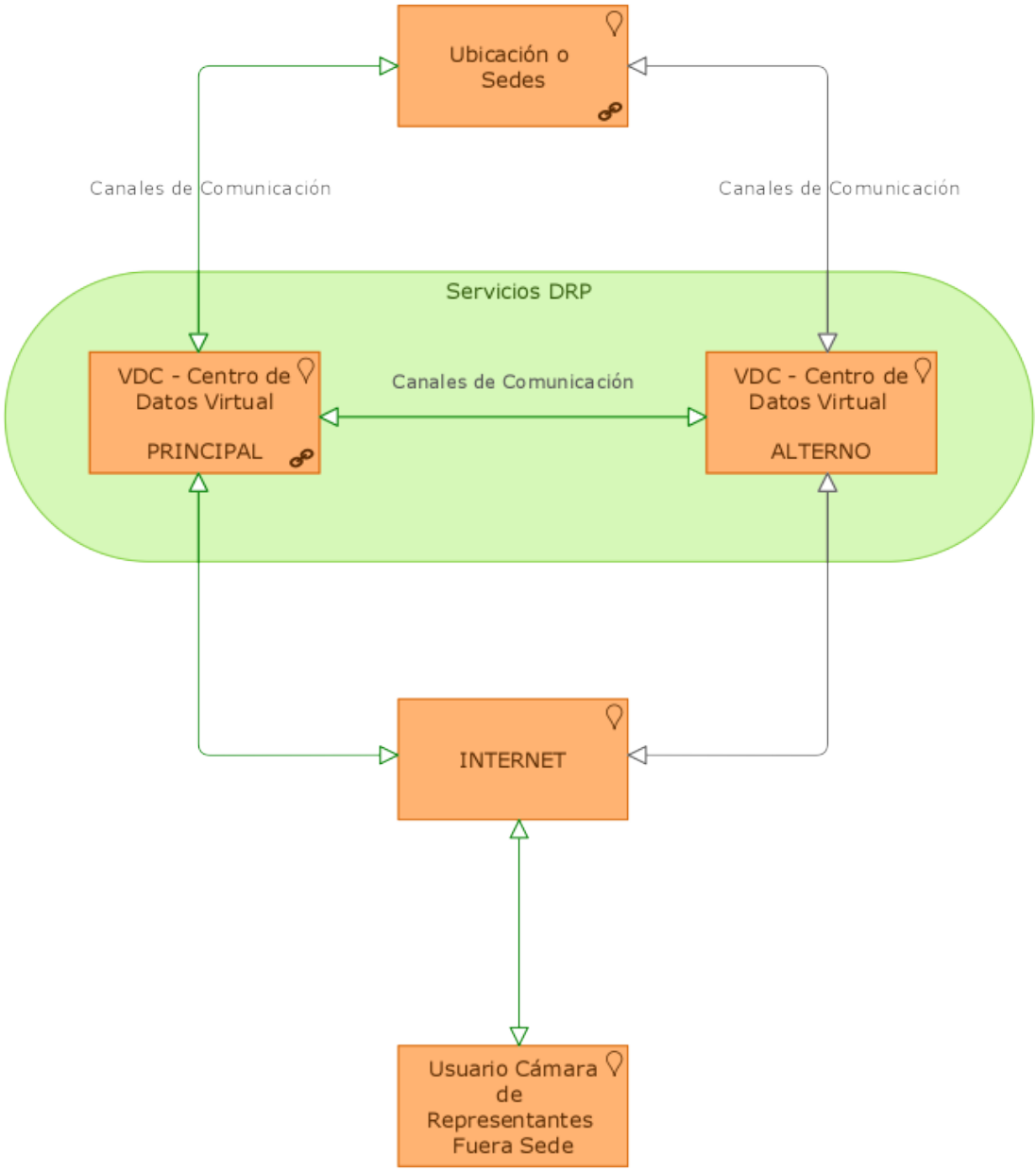


Ilustración 3 - Virtual Data Center VDC y DRP

El modelo permite establecer las relaciones entre cada componente, a continuación, se muestran dichas relaciones y se hace una breve descripción para cada uno de los elementos que hacen parte del modelo Virtual Data Center VDC y DRP:

3.2.1. Internet

Este elemento representa los servicios de Internet para usuarios en Unidad de Víctimas que consumen servicios corporativos ubicados en los centros de datos y no cuentan con un canal de comunicación.

3.2.2. Ubicación o Sedes

Elemento en el diagrama que representa todas las sedes o ubicaciones en la Honorable Cámara de Representantes interconectadas por medio de los canales de comunicación hacia los centros de datos.

3.2.3. Servicios DRP

Este componente representa los servicios de recuperación ante desastres, estableciendo las relaciones entre los centros de datos principal y de recuperación por medio de canales de comunicación, servicios de replicación y demás servicios necesarios para mantener la continuidad de la operación ante una posible eventualidad.

Un plan de recuperación ante desastres - DRP (Disaster Recovery Plan) es un proceso de recuperación que cubre hardware, software y datos críticos, para que un negocio pueda mantener las operaciones en caso de un desastre o eventualidad. Es recomendable también incluir proyectos para enfrentarse a la pérdida repentina o inesperada de personal clave u otros aspectos de la operación. Es indispensable tener en cuenta que hace parte del BCP (Business Continuity Plan).

Principales Actividades	Descripción
Definir una política de continuidad de negocio.	Se debe desarrollar la política de continuidad del negocio para la Honorable Cámara de Representantes.
Identificar y ordenar las amenazas.	Crear una lista de los incidentes de interrupción de la actividad que constituyan las amenazas más probables para la Honorable Cámara de Representantes.
Realizar un análisis del impacto en la empresa.	Se debe determinar qué partes de la Honorable Cámara de Representantes son las más críticas para que sobreviva. Determinarás la cantidad de “días de supervivencia” de la organización para cada función.
Crear un plan de respuesta y recuperación.	Catalogar los datos clave sobre los sistemas de TI, personal, proveedores y clientes. Incluir, acuerdos de licencia, alquiler, garantías, detalles de contactos, etc.

	Determinar la matriz de comunicación en cada categoría de incidente y crear un árbol con los números de contacto para que se hagan las llamadas correctas en el orden correcto. Determinar la matriz de decisiones “quién puede decir qué cosa” para controlar la interacción con los medios durante un incidente (considerar una comunicación con una estrategia de “sólo el CEO” si se trata de un incidente delicado). Ordenar los principales pasos de recuperación de la operación en una secuencia donde queden explícitas las interdependencias funcionales. Capacitar a los líderes de cada área sobre los detalles relevantes, así como la importancia del plan general para sobrevivir a un incidente.
Probar el plan y depurar el análisis	Luego de elaborado, es recomendable probar el plan al menos una vez al año, con ejercicios, análisis paso a paso o simulaciones.

3.2.4. Centro de Datos Virtual – Principal

El Diagrama Virtual Data Center VDC – Principal, representa el modelo general de los servicios que debe prestar el centro de datos para mantener una adecuada y estable operación. Así mismo, el modelo de acceso de un usuario a dichos servicios utilizando diferentes medios de comunicación.

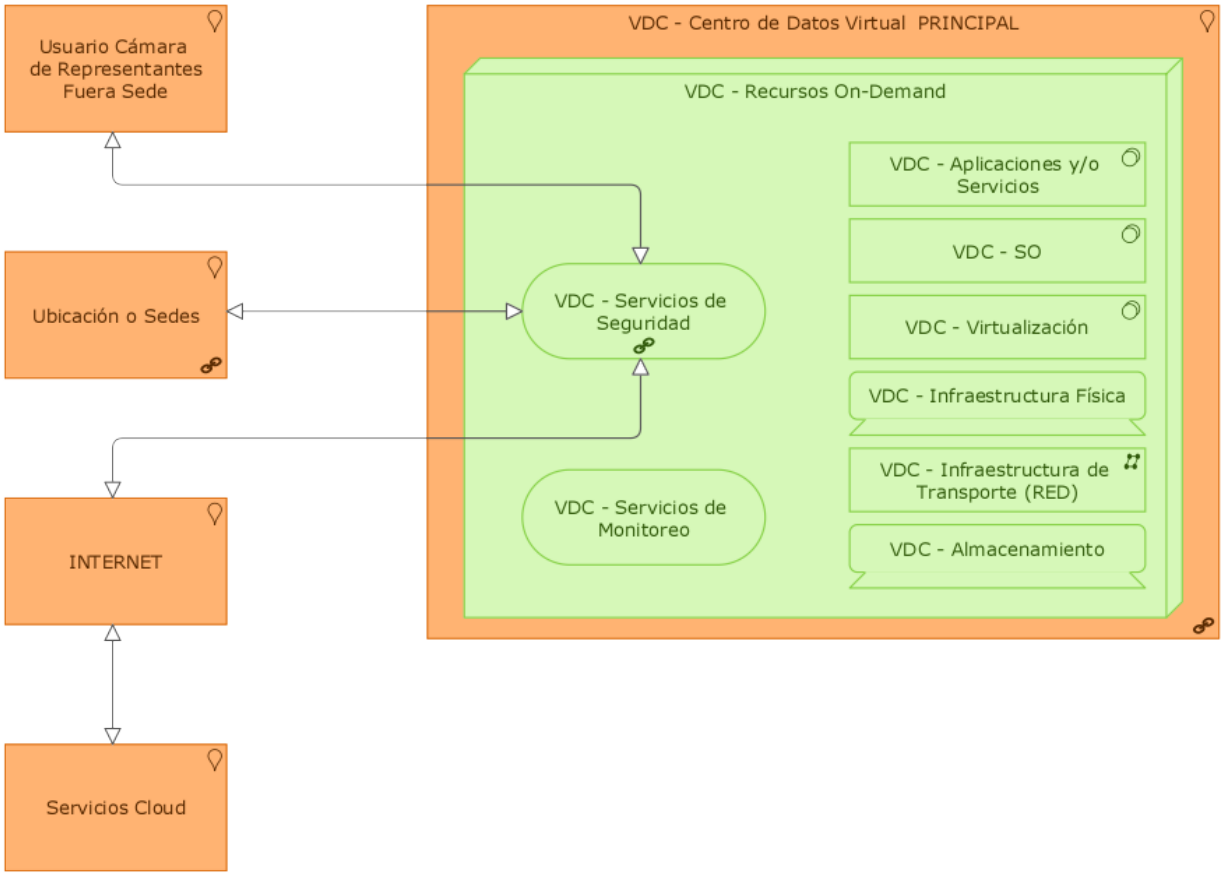


Ilustración 4 - VDC - Centro de Datos Virtual – Principal

Los componentes que hacen parte de este modelo son:

Componentes existentes:

- Sedes Unidad de la Honorable Cámara de Representantes
- Canales de comunicación.
- Internet
- Servicios Cloud existentes.

Componentes nuevos (Servicios de centro de datos – Recursos on-demand):

- Servicios de seguridad.
- Servicios de monitoreo.

- Servicios de Almacenamiento.
- Servicios de Red.
- Infraestructura física.
- Servicios de Virtualización y SO.
- Aplicaciones y servicios.

El modelo permite establecer las relaciones entre cada componente, a continuación, se muestran dichas relaciones y se realiza una descripción para cada uno de los elementos que hacen parte del modelo TO-BE Virtual Data Center VDC – Principal:

3.2.4.1. RECURSOS ON-DEMAND

Recursos On-Demand representa un pool de recursos disponibles y ofrecidos por el Centro de Datos que Unidad de Víctimas podrá usar o dejar de hacerlo en cualquier momento acorde a las necesidades de la operación, planes de crecimiento, proyectos y demás alternativas que se puedan identificar en su momento.

3.2.4.1.1. SERVICIOS DE MONITOREO

Este elemento representa todos los Servicios de Monitoreo que la Honorable Cámara de Representantes demande y desee activar para realizar los procesos de control de alertar y/o alarmas sobre los servicios del centro de datos y otros que se identifiquen sean necesarios incluir.

3.2.4.1.2. SERVICIOS DE SEGURIDAD

Elemento que representa todas las políticas de seguridad informática existentes en la Honorable Cámara de Representantes y otras que la organización identifique deban ser implementadas.

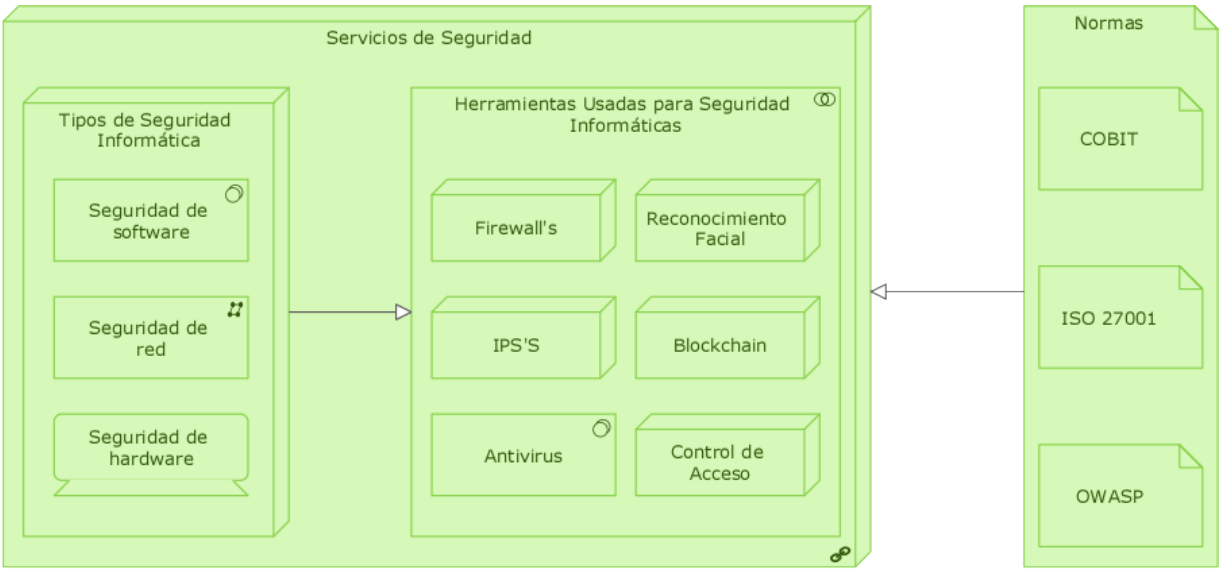


Ilustración 5 - Servicios de Seguridad

En el Diagrama Servicios de Seguridad se propone el modelo de seguridad informática para la Honorable Cámara de Representantes, en él se pueden identificar los elementos de seguridad informática y las normas que deben ser implementadas con el propósito de fortalecer la política de seguridad informática de la institución.

Los componentes que hacen parte de este modelo son:

Herramientas Usadas para Seguridad Informática: Elemento que representa el pool de opciones sobre las herramientas usadas y propuestas para seguridad informática en la Honorable Cámara de Representantes.

- IPS's: Elemento usado en la Honorable Cámara de Representantes que representa en el modelo la implementación de esta tecnología de seguridad IPS (sistema de prevención de intrusos), puede ser un software o dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques.
- Firewall''s: Elemento usado en la Honorable Cámara de Representantes que representa en el modelo la implementación de esta tecnología de seguridad por medio de la cual se puede bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Puede ser un dispositivo, conjunto de dispositivos configurados o componentes lógicos para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios
- Antivirus: Programas usados en la Honorable Cámara de Representantes cuyo objetivo es detectar y eliminar virus informáticos. Así mismo, se hace el uso de programas más avanzados

que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos, también son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, pseudovirus etc.

- Reconocimiento Facial: Elemento propuesto que representa en el modelo la implementación de esta tecnología de seguridad para la identificación de las características faciales de una persona. Así mismo, la aplicación para el acceso a sistemas críticos de la organización, identificación de personal en listas negras, entre otros.
- Blockchain: Elemento propuesto que representa en el modelo la implementación de la tecnología Blockchain (cadena de bloques), que se puede entender como un gran acopio de cuentas o transacciones en los que los registros (los bloques) están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones. De otra manera, se puede definir como una base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones.
- Control de Acceso: El control de acceso informático o control de acceso a sistemas informáticos, en seguridad informática, consiste en la autenticación, autorización de acceso y auditoría.

Tipos de Seguridad Informática: Basados en que, la seguridad informática es la vertiente de la tecnología de la información que se encarga de la protección de datos o información, las comunicaciones y su infraestructura; este componente representa en el modelo propuesto el enfoque sobre los tres tipos de seguridad informática más relevantes:

- Seguridad de hardware: Elemento que representa en el modelo uno de los tipos de seguridad informática el cual hace referencia a la protección de elementos físicos, incluyendo sistemas de alimentación ininterrumpida (SAI), cortafuegos o firewall de hardware, y módulos de seguridad de hardware (HSM).
- Seguridad de software: Elemento que representa en el modelo uno de los tipos de seguridad informática el cual hace referencia a la protección del software contra ataques maliciosos de hackers y otros riesgos, de forma que el software corporativo siga funcionando correctamente. Es necesaria este tipo de seguridad para proporcionar integridad, autenticación y disponibilidad al software corporativo. Es importante tener en cuenta que: los defectos de software tienen diversas ramificaciones de seguridad, tales como errores de implementación, desbordamientos de buffer, defectos de diseño, mal manejo de errores, etc.
- Seguridad de red: Elemento que representa en el modelo uno de los tipos de seguridad informática el cual hace referencia a cualquier actividad diseñadas para proteger (la facilidad de uso, fiabilidad, integridad y seguridad). La seguridad de red efectiva se dirige a una variedad de amenazas y la forma de impedir que entren o se difundan entre los dispositivos de la red. Las amenazas más comunes incluyen:
    - Virus, gusanos y troyanos.

- Software espía y publicitario.
- Ataques de día cero, también conocidos como ataques de hora cero.
- Ataques de hackers.
- Ataques de denegación de servicio.
- Intercepción o robo de datos.
- Robo de identidad.

Normas: Componente que representa las normas que se deben tener en cuenta en la definición o fortalecimiento de las políticas de seguridad en Unidad de Víctimas, las normas propuestas son:

- COBIT**:** (Control Objectives for Information and related Technology, Objetivos de control para la información y tecnologías relacionadas) elemento que representa la metodología publicada en 1996 por el Instituto de Control de TI y la ISACA (Asociación de Auditoría y Control de Sistemas de Información) que se usa para evaluar el departamento de informática de una compañía. Este enfoque se basa en un índice de referencia de procesos, indicadores de objetivos clave (KGl) e indicadores de rendimiento clave (KPI) que se usan para controlar los procesos para recoger datos que la compañía puede usar para alcanzar sus objetivos. El enfoque COBIT propone 34 procesos organizados en 4 áreas funcionales más grandes que abarcan 318 objetivos: entrega y asistencia técnica; control; planeamiento y organización; aprendizaje e implementación.
- OWASP**:** Open Web Application Security Project (Proyecto abierto de seguridad de aplicaciones web), elemento que representa el proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
- ISO 27001**:** Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, así mismo, permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

3.2.4.1.3. VDC - APLICACIONES Y/O SERVICIOS

Elemento que representa en el modelo todas las aplicaciones o servicios ofrecidos por la Honorable Cámara de Representantes a los usuarios finales y que se encuentran ubicadas sobre un sistema operativo en un servidor específico.

3.2.4.1.4. VDC - SO

Elemento que representa en el modelo todos los sistemas operativos; estos pueden estar sobre la capa de virtualización o directamente instalados en un servidor y sobre él las aplicaciones.

3.2.4.1.5. VDC - VIRTUALIZACIÓN

Elemento que representa en el modelo todos los sistemas de virtualización o hipervisores. Los sistemas de virtualización se encuentran directamente sobre la infraestructura o servidor. En otros términos, es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas sobre el mismo componente de hardware.

3.2.4.1.6. VDC - INFRAESTRUCTURA FÍSICA

Elemento que representa en el modelo todos elementos físicos y recursos de cómputo disponibles en el centro de datos (CPU, RAM, Servidores, entre otros) y su disponibilidad.

3.2.4.1.7. VDC - INFRAESTRUCTURA DE TRANSPORTE (RED)

Elemento que representa en el modelo todos los sistemas de comunicación y transporte en el centro de datos, permite la intercomunicación entre todos los componentes.

3.2.4.1.8. VDC - ALMACENAMIENTO

Elemento que representa en el modelo todos los sistemas y tipos de almacenamiento disponibles para albergar la información y datos generados por las aplicaciones, SO, Sistemas de virtualización y demás componentes que generen datos.

3.2.5. Servicios Cloud

Elemento que representa todos los servicios cloud propuestos y existentes en la Honorable Cámara de Representantes. Se trata de la disponibilidad a pedido de los recursos de los sistemas informáticos y usuarios, de capacidades como el almacenamiento de datos y capacidad de cómputo.

El uso de estos servicios a menudo se relaciona con una reducción de costos, disminución de vulnerabilidades y garantía de disponibilidad. Asimismo, se relaciona con un modelo de pago por uso o por demanda.

Es un tipo de prestación de servicios tecnológicos que impacta en diversos aspectos del negocio. El modelo es soportado en infraestructuras tecnológicas dinámicas, caracterizados por la virtualización de recursos, alto grado de automatización, elevada capacidad de adaptación para atender solicitudes variables.

El concepto es muy amplio y cubre casi todos los posibles tipos de servicios en línea, pero cuando una organización promueve el uso de estos servicios, generalmente se refieren a alguna de las siguientes modalidades:

- Software como servicio (SaaS, por sus siglas en inglés): Es un modelo de distribución de software en el que las aplicaciones están alojadas por una compañía o proveedor de servicios y puestas a disposición de los usuarios a través de una red, generalmente internet.
- Plataforma como servicio (PaaS): Es un conjunto de utilitarios para suministrar a los usuarios de los SO (sistemas operativos) y servicios asociados a través de Internet sin necesidad de descargas o instalación alguna.
- Infraestructura como servicio (IaaS): Se refiere a la tercerización de los equipos utilizados para apoyar las operaciones, incluido el almacenamiento, hardware, servidores y componentes de red.

CONTROL DE CAMBIOS

Versión	Fecha	Modificado por	Comentarios	Validado por
1.0	30/11/2020	Afranio Lozano Gómez.	Creación Documento	Sebastián del Toro Álvaro Carreño Ortiz
2.0	18/12/2020	Afranio Lozano Gómez.	Ajuste a comentarios realizados por: Sebastián del Toro Álvaro Carreño Ortiz	