ANÁLISIS DE BRECHAS DE LA SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA TI BASADO EN ISO/IEC 27005

SERVICIUDAD E.S.P

DOSQUEBRADAS, AÑO 2021

TABLA DE CONTENIDO

INTRODUCCIÓN

Las Entidades y organizaciones a nivel mundial deben ser conscientes de los riesgos a los que está sometida su infraestructura tecnológica, debido a las múltiples vulnerabilidades que existen por canales y herramientas como la conectividad y el deterioro por obsolescencia tecnológica. Los activos de información han tomado un lugar muy alto en las cadenas de valor de las organizaciones, por lo que se hace prioritario establecer protocolos y modelos de seguridad y privacidad de la información y buenas prácticas de infraestructura para proteger dichos activos.

Mediante este documento se realiza y presenta el informe diagnóstico de la situación actual de la infraestructura tecnológica, sus debilidades, vulnerabilidades y las recomendaciones para actualizar y mantener la infraestructura de SERVICIUDAD E.S.P en óptimas condiciones.

1. OBJETIVOS

- Analizar el manejo de la información en el proceso de TI, desde el punto de vista de políticas y prácticas orientadas a la seguridad de la información.
- Determinar los riesgos asociados a los activos de información en el proceso de TI, basados en el estándar ISO/IEC 27005.
- Sugerir prácticas de seguridad tomadas de la guía GTC ISO/IEC 27002, que pueden llegar a mitigar los riesgos asociados a los activos de información en el proceso de TI.

2. ALCANCE

En el siguiente documento se presenta un diagnóstico de la red actual e infraestructura de la Entidad SERVICIUDAD E.S.P; con el fin de brindar un conjunto de recomendaciones basado en las mejores prácticas de TI para los diferentes servicios bajo análisis, en aras de mitigar ataques de tipo interno y externo, fortalecer la infraestructura de TI actual y mitigar los fallos en servicios de misión crítica.

3. MARCO CONCEPTUAL

La International Organization for Standardization (ISO, 2013) define; la seguridad de la información, según ISO/IEC 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar los siguientes.

- **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC5411 1:2006].

La información, junto a los procesos y sistemas que la utilizan, son activos fundamentales de una Entidad, esta y sus sistemas de información se encuentran expuestos a un número elevado de amenazas que, siendo aprovechadas cualquiera de las vulnerabilidades existentes, pueden enfrentar a activos críticos de información a formas diversas de fraude, sabotaje, espionaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio, son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde la propia Entidad o aquellos provocados accidentalmente por catástrofes naturales o fallos técnicos

IMAGEN Nª1. ENFOQUE DE RIESGOS ISO 27000

Figura 1. Riesgos
Tomada de: www.ISO27000.es.

Fuente: Tomada de www.ISO27000

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la Entidad, con la Alta Dirección al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

En esta sección se identifican los componentes de la línea base de la arquitectura tecnológica en servicios de infraestructura a evaluar, correspondientes a:

1. Nube
2. Redes de comunicaciones LAN y WAN
3. Servidores
4. Servicio de almacenamiento
5. Sistema de impresión y equipos de computo
6. Seguridad perimetral
7. Usuarios

4. DESCRIPCIÓN DE COMPONENTES

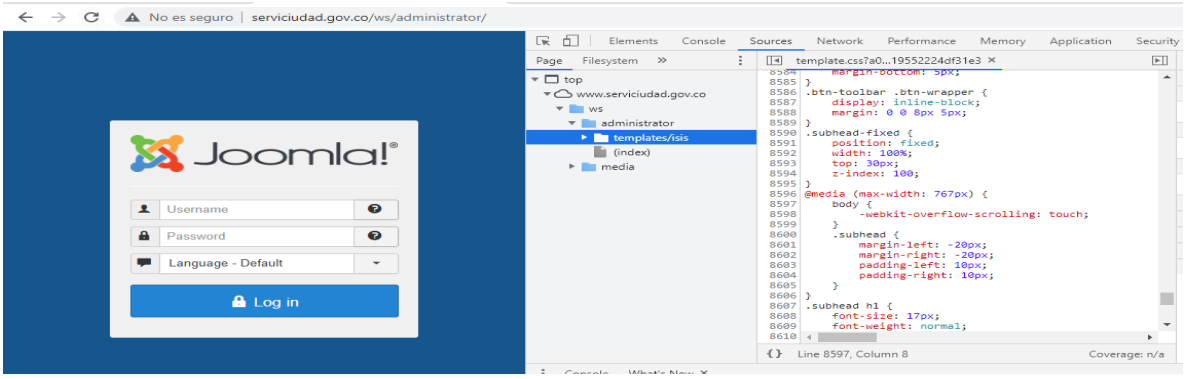
4.1 COMPONENTE SERVICIOS DE NUBE

SERVICIUDAD E.S.P cuenta con un sitio web institucional bajo el dominio http://www.serviciudad.gov.co y el desarrollo se encuentra bajo el gestor de contenidos Joomla Content Management System (CMS)

IMAGEN Nª2. SITIO WEB DE LA ENTIDAD

Fuente: Elaboración Propia

IMAGEN Nª3. GESTOR DE CONTENIDO SITIO WEB DE LA ENTIDAD



Fuente: Elaboración Propia

4.1.1. EXPLORACIÓN DE CONTENIDOS

IMAGEN Nª4. EXPLORACIÓN DE CONTENIDOS

Al validar el rendimiento del sitio web se recomienda instalar y configurar la funcionalidad PageSpeed, este es un módulo de código abierto para Apache desarrollado por Google, que automatiza muchas de las optimizaciones y buenas prácticas que recomienda Google PageSpeed para mejorar la velocidad del sitio web.

Funciona aplicando diversos filtros de salida, es decir, haciendo cambios en el contenido antes de que este salga del servidor hacia el cliente.

Hay más de 40 filtros de optimización disponibles, algunos de los cuales son:

- Optimización de imágenes y compresión.
- Concatenación y minificación de recursos CSS y JavaScript.
- Extensión de caché.
- Carga aplazada de JavaScript y recursos gráficos.

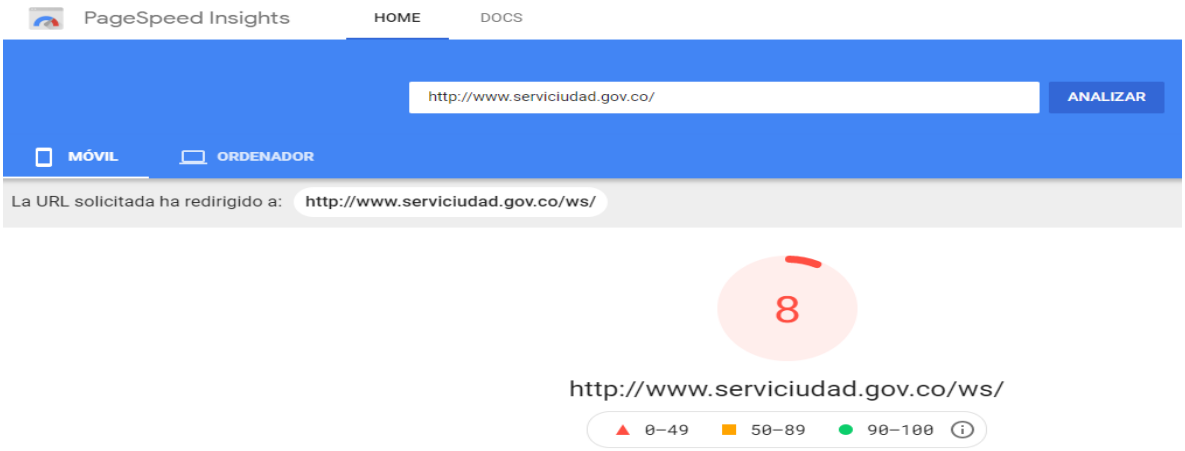
El rendimiento actual acorde a las métricas descritas anteriormente para la versión móvil y ordenador es el siguiente:

TABLA Nª1. RENDIMIENTO ACTUAL SITIO WEB

Versión	Porcentaje	Estado
Móvil	8%	BAJO
Ordenador	69%	MODERADO

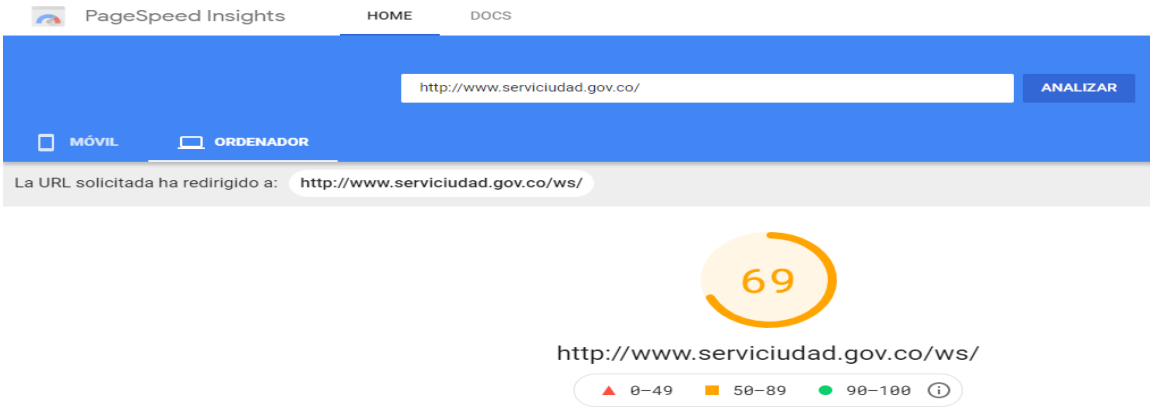
Fuente: Elaboración Propia

IMAGEN Nª5. RENDIMIENTO ACTUAL VERSIÓN MÓVIL



Fuente: Elaboración Propia

IMAGEN Nª6. RENDIMIENTO ACTUAL VERSIÓN ORDENADOR



Fuente: Elaboración Propia

4.1.2 DESCRIPCIÓN Y RECOMENDACIONES

TABLA Nª2. DESCRIPCIÓN Y RECOMENDACIONES DE SERVICIOS EN LA NUBE.

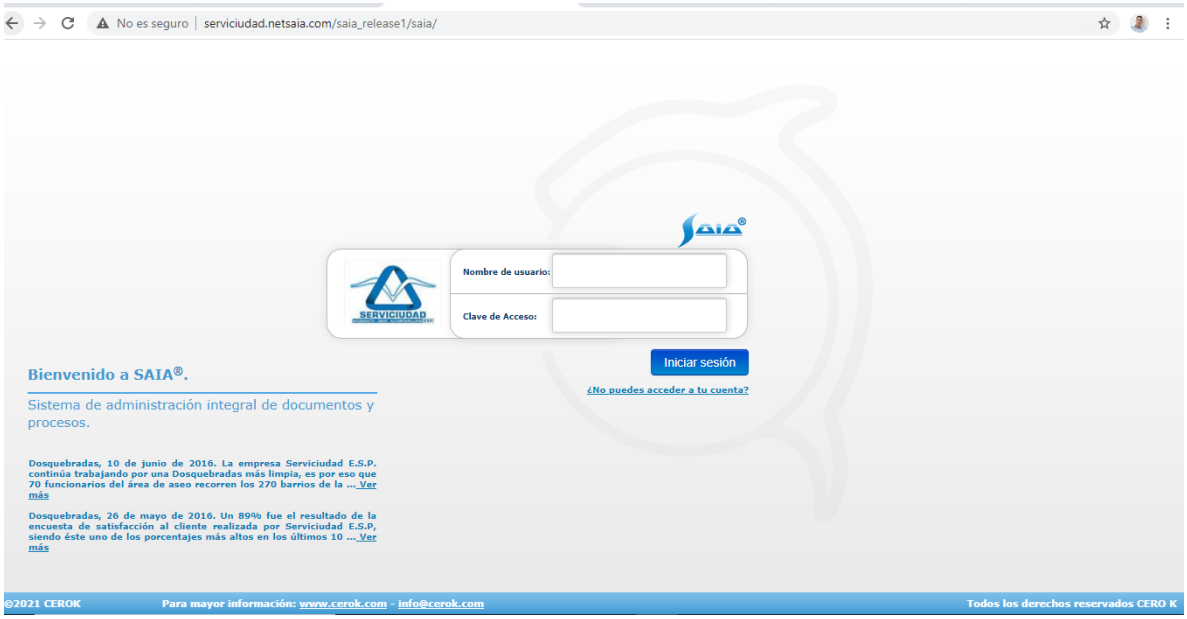
Componente	Descripción	Recomendación
Sitio web	Sitio web institucional - componentes LAMP CMS Joomla	Actualización de la versión de joomla acorde a los plugins instalados con el fin de corregir vulnerabilidades identificadas
	HTTPS	Implementación de certificado SSL emitido por una Entidad de confianza
	FAVICON	Modificar con el fin de ocultar a los usuarios información del CMS
	Administración del sitio	Enmascarar la url de administración /administrator bajo la implementación de plugin – ocultar esta con el fin de prevenir ataques orientados a joomla
	Exploración de contenidos	Realizar configuraciones en apache para ocultar la exploración de información sensible
	LAMP (LINUX, APACHE, MYSQL, PHP)	Actualización acorde a las versiones estables y servicios publicados
	Validación de plugins y componentes	Instalar componentes y templates licenciados

Fuente: Elaboración Propia

4.1.3. COMPONENTE SAI: SISTEMA DE GESTIÓN DOCUMENTAL SAIA: http://serviciudad.netsaia.com/saia_release1/saia/

Al ser un aplicativo de terceros, este alcance no comprende las validaciones técnicas y remediaciones requeridas a nivel de seguridad para la plataforma

IMAGEN Nª7. PLATAFORMA SAIA



Fuente: Elaboración Propia

TABLA Nª3.DESCRIPCIÓN Y RECOMENDACIONES SAIA

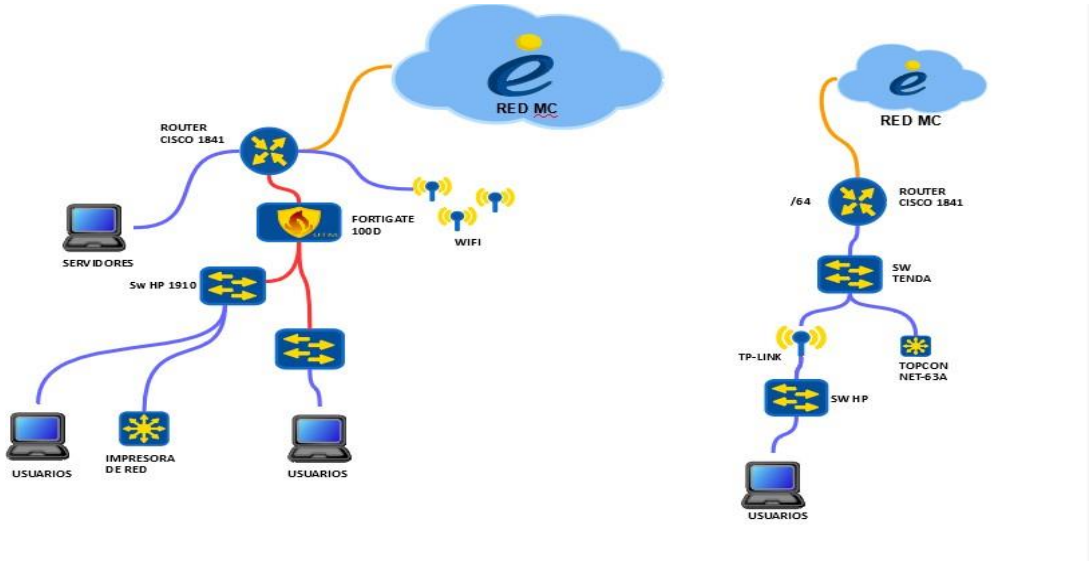
Componente	Descripción	Recomendación
SAIA	HTTPS	Implementación de certificado SSL, emitido por Entidad de confianza

Fuente: Elaboración Propia

4.2. COMPONENTE REDES DE COMUNICACIONES LAN Y WAN

La Entidad SERVICIUDAD E.S.P cuenta con dos sedes las cuales cuentan con un canal de internet, cada una bajo el ISP Media Commerce.

IMAGEN Nª8. REDES DE COMUNICACIONES LAN Y WAN



Fuente: Elaboración Propia

Con el fin de aportar a la continuidad del negocio, se propone implementar un canal secundario de internet el cual funcione como contingencia ante una afectación en el principal, este canal debe ser adquirido con un proveedor ISP diferente al actual.

Se debe realizar configuración de comunicación mediante una VPN LAN-2-LAN entre las sedes por ambos canales, para garantizar una alta disponibilidad e implementar mecanismos de cifrado de información en el túnel.

4.2.1. RED FÍSICA

Actualmente la red de la Entidad SERVICIUDAD E.S.P no cuenta con subredes definidas, ocasionando que todo se encuentre bajo el mismo dominio de broadcast lo cual la hace susceptible a ataques informáticos tipo man-in-the-middle, IP spoofing y network sniffing.

Por lo anterior, se recomienda segmentar la red no solo a nivel físico, sino también a nivel lógico y por tanto es necesario definir VLANs para cada uno de los diferentes segmentos a utilizar.

Dado que cada segmento tiene su propio direccionamiento IP, es necesario

disponer de un dispositivo que haga la función de enrutamiento entre estas subredes. Esta función capa tres se le puede asignar al firewall perimetral cuando el número de redes y el tráfico entre estas no son muy grandes.

Cuando el tráfico interno sea considerable, será recomendable que la función sea asignada a un switch capa tres, que se encargue del enrutamiento entre redes internas.

Dentro de las VLAN's antes mencionadas, se debe definir una para gestión a través de la cual acceder a la configuración de los dispositivos de red que lo permitan. Esta VLAN debería ser de acceso restringido en el firewall y solo otorgarles acceso a las subredes o IPs de los administradores. Esta misma red debería utilizarse para despacho de mensajes de syslog a un servidor centralizado lo cual puede ayudar en el diagnóstico de fallos de red cuando estos se presenten.

Por último, la red de almacenamiento por naturaleza que es mover bloques de I/O entre los hosts físicos, se recomienda que sea un switch GigaEthernet independiente y aislado del tráfico de usuarios.

4.2.2. ACCESO REMOTO

Las configuraciones gestionadas a nivel de firewall permiten la comunicación de los usuarios mediante la herramienta forticlient; para la cual solo se cuenta con un perfil y configuración de acceso a la red, se deben crear perfiles de acceso SSL acorde a las funciones de cada área y restringir sus privilegios sobre toda la red.

En resumen, estas son las recomendaciones que se deben aplicar:

- Segmentar o crear VLANs
- Implementar un router (o switch L3 GE)
- Implementar VLAN de gestión y un syslog para centralizar reporte de eventos de red y servidores.
- Implementar un Switch aislado para storage.

4.2.3 DIRECCIONAMIENTO

El direccionamiento interno debe cumplir con el RFC-918, que establece los rangos de direcciones privados para utilizar en redes internas. Dado que existe

la posibilidad de que aparezca la necesidad de hacer VPN LAN-2-LAN contra otras redes privadas en el futuro, es recomendable evitar el uso del direccionamiento al inicio o al final de los pools privados y escoger direcciones de red más menos intermedias en los pools, para minimizar la probabilidad de colisión con el direccionamiento de futuros partners de red.

El servicio DHCP debe brindar direcciones en todos los scopes de usuarios, pero por seguridad se debe deshabilitar en las subredes de Data Center, se deben crear varios scopes acorde a la segmentación de red.

En resumen, estas son las recomendaciones que se deben aplicar:

- Direccionamiento privado en todos los segmentos de LAN.
- Implementar un DHCP con scopes para cada segmento.
- Crear VPN LAN-2-LAN para garantizar la comunicación entre las sedes

4.2.4 SEGMENTOS

Para garantizar la seguridad de la red, se debe separar en segmentos lógicos de acuerdo a una clasificación por niveles de acceso requeridos.

4.2.4.1 La DMZ

Es la red que albergará a todos aquellos servidores que requieran ser accedidos desde Internet. La razón de esto se debe a que la exposición de estos a Internet aumenta la probabilidad de que alguno de ellos esté comprometido en el futuro y este sea utilizado como bastión de ataque a los demás servidores en la misma subred. Al tener la DMZ aislada de la red interna, el ataque queda confinado únicamente a un segmento menor. De ahí el nombre de zona desmilitarizada pues esta es una con cierta laxitud en las medidas de seguridad al estar parcialmente expuesta a Internet.

Dado que los Windows Terminal Server (WTS) se suelen utilizar como puntos de entrada a la red interna y que estos son inherentemente inseguros, la recomendación es que, si se van a ubicar WTS en DMZ, se deben crear dos redes

DMZ y ubicar en una de ellas únicamente los WTS dada su alta probabilidad de ser usado como vector de ataque.

Si bien la anterior recomendación mitiga la probabilidad de que se comprometan otros servidores, la mejor recomendación es no ofrecer WTS expuestos a Internet y en su lugar hacer uso de una sola DMZ ubicando los WTS en la red interna. Para acceder a tales servidores se requerirá una conexión VPN la cual debe estar disponible para las sedes remotas, así como para los usuarios móviles.

En conclusión, las recomendaciones para la DMZ son:

- Una sola DMZ y acceso VPN para sedes y usuarios.
- Usar WTS desde equipos internos.

4.2.4.2 Red De Servicios

Es la red donde están conectados todos los servidores que ofrecen servicio a la red de usuarios. Esta red también se le conoce como la red de Data Center. Esta red solo debe albergar servidores y ninguna estación de trabajo de usuarios. En esta red no debe habilitar el servicio DHCP ya que los servidores deben tener IP estática así buscando dificultar la conexión furtiva de equipos no autorizados. El Data Center debe estar protegido por firewall para otorgar solo acceso a los puertos de servicios que se quieran ofrecer a la red interna.

4.2.4.3. Red de usuarios

Esta es la red donde se encuentran todos los usuarios de la red alambrada. El direccionamiento debe ser dinámico; Lo ideal es que entre redes de usuario no haya firewall, pero se debe segmentar en varias subredes buscando disminuir el tráfico de los Switchs debido al broadcast inherente a las estaciones Windows. Una buena práctica es nunca sobrepasar más de 60 estaciones por segmento. Para el caso de SERVICIUDAD E.S.P en principio solo se requieren dos subredes de usuarios, pero se pasarán por el firewall por motivos de escalamiento. Esta red también se le conoce como la red de endpoints donde se deben aplicar políticas de seguridad, de las cuales la mínima es la de tener control antivirus en cada escritorio lo cual se mencionará más adelante con mayor detalle.

4.2.4.4. Red Wifi Interna

Esta es la red inalámbrica para colaboradores y desde esta se puede acceder a los servicios corporativos. Por lo anterior, se deben tener medidas de seguridad adecuadas para la conexión a esta red. Tener una sola clave compartida es bastante inseguro y se aconseja el control de acceso con portal cautivo, usuario y contraseña o en su defecto registrar las direcciones MAC de las estaciones que se conectarán a esta red. Por lo tanto, se recomienda generar autenticación vía Mac address.

4.2.4.5. Red Wifi Invitados

Esta red es esencialmente para ofrecer acceso a Internet. Por lo tanto, no se debe dar conectividad a la red corporativa desde la red de invitados. La autenticación de esta red debería hacerse con portal cautivo y usuarios efímeros, es decir usuarios que se crean desde una cuenta de lobby y se les asigna una caducidad que una vez sea alcanzada, la cuenta desaparezca automáticamente.

4.2.4.6. Red De Gestión

Esta red debe ser restringida y a través de esta se acceden a las gestiones de los servidores y equipos de misión crítica, así como la gestión de las NAS y equipos de comunicaciones Switchs y Routers, que sean gestionables. El acceso a esta red también debería ser controlado por firewall y solo usuarios administradores de TI.

4.3. COMPONENTE SERVIDORES

Con el fin de proteger los servidores es indispensable prestar un mantenimiento continuo lógico y físico sobre los mismos, este debe comprender las siguientes actividades:

- Realizar actualizaciones periódicas denominadas críticas.
- Proteger mediante copias de seguridad acorde a las políticas de TI.
- Definir políticas de backup automatizado.
- Realizar validación de usuarios con privilegios de administrador.
- Control de versiones.
- Realizar Mantenimiento físico.
- Permitir puertos conocidos en el firewall acorde a las aplicaciones y versión de sistema operativo.
- Publicar servicios bajo HTTPS.
- Restringir la navegación o salida a internet del segmento de servidores.
- Cifrar información.
- Implementar Windows Server Update Services.

En la siguiente tabla se proporcionan las características de los servidores alojados en el Data Center y sus recomendaciones.

TABLA Nª4 RECOMENDACIONES DE LOS SERVIDORES ALOJADOS EN EL DATA CENTER

COMPONENTE	DESCRIPCIÓN	ROL	SISTEMA OPERATIVO	RECOMENDACIÓN
Servidor de dominio	Hp proliant dl320 gen.8 v.2	Directorio activo – DNS - DHCP	Windows server 2012 r2	• Gestionar actualizaciones críticas de seguridad • Generar plan de backup sobre cada rol • Verificar y validar la vigencia del licenciamiento del sistema operativo. • Activar firewall y permitir puertos conocidos • Depurar usuarios con perfiles administrador.

COMPONENTE	DESCRIPCIÓN	ROL	SISTEMA OPERATIVO	RECOMENDACIÓN
Servidor de aplicaciones	Hp modelo: 590638-001 serie: proliant dl180 g6 server.	Bases de datos	Windows server 2008	• Gestionar actualizaciones críticas de seguridad. • Migrar sistema operativo mínimo Windows server 2012 R2 por obsolescencia. • sistema operativo actual sin soporte. • Genera plan de backup. • Verificar y validar la vigencia del licenciamiento del sistema operativo. • Activar firewall y permitir puertos conocidos. • Depurar usuarios con perfiles administrador.

COMPONENTE	DESCRIPCIÓN	ROL	SISTEMA OPERATIVO	RECOMENDACIÓN
Hypervisor	Dell power edge 2950	Host de virtualización	Linux debían	• Virtualizar con plataforma VMware Esxi • Licenciar HOST. • No permitir autenticación como usuario root. • Enmascarar puerto de acceso ssh. • Tener sistema activo con todos los features de vmware.
Webservice	Hp proliant ml 310 gen.8	Servidor de transacciones	Windows server 2012	• Gestionar actualizaciones críticas de seguridad. • Genera plan de backup. • Verificar y validar la vigencia del licenciamiento del sistema operativo. • Activar firewall y permitir puertos conocidos. • Depurar usuarios con perfiles administrador.

Fuente: Elaboración Propia

4.3.1. RECOMENDACIONES COMPONTE SERVIDORES

Las recomendaciones en este aspecto están orientadas a mejorar la gestión de la infraestructura y para esto lo primero es la necesidad de iniciar el plan de consolidación y virtualización de servidores; logrando estabilizar el servicio y aportar a la mejora continua, prestando un óptimo desempeño.

La implementación de licenciamiento válido para el sistema de virtualización habilita una característica de vSphere llamada Data Recovery, la cual ofrece una API para que se pueda usar software de terceros, para la implementación de sistemas de backup automatizados y desatendidos de las VMs que no requieren el apagado de las máquinas.

Esta característica de Data Recovery, ofrece un servicio llamado Changed Block Tracking o CBT, que permite al software de terceros la elaboración de backups incrementales que minimizan el uso del espacio en el repositorio de backup, cuando se guardan varios puntos de retención.

En conclusión, las recomendaciones para la plataforma de virtualización son:

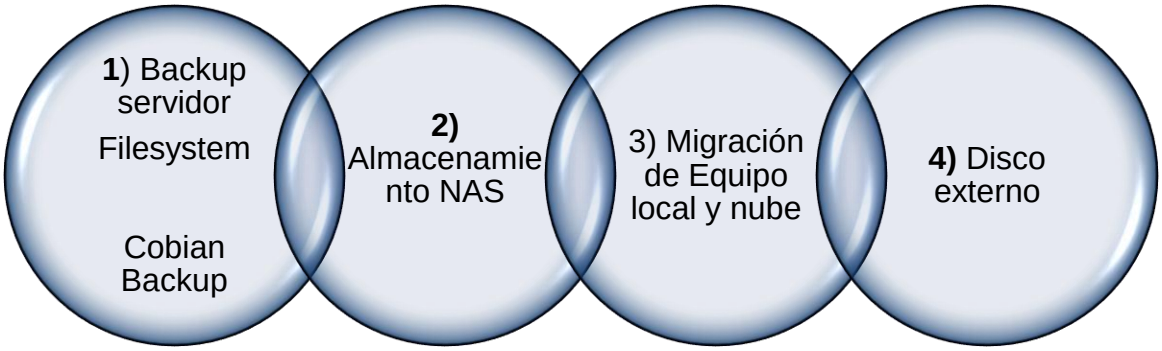
- Licencias de VMware y vSphere.
- Licenciar e implementar un vCenter.
- Configurar gestión en red aparte.

4.3.2. COMPONENTE BACKUP SERVIDORES

Actualmente la Entidad cuenta con un modelo de Backup bajo la herramienta Cobián Backup por servidor, allí se respalda información considerada crítica acorde a una política diaria y completa, la cual es alojada en una unidad NAS de manera temporal para su posterior migración a Disco externo en custodia del área TI, el modelo implementado con sus respectivas debilidades se puede visualizar a continuación:

4.3.2.1 Modelo actual implementado de backup servidores

IMAGEN Nª9. MODELO ACTUAL IMPLEMENTADO DE BACKUP



Fuente: Elaboración Propia

TABLA Nª5 DEBILIDADES DEL MODELO BACKUP SERVIDORES

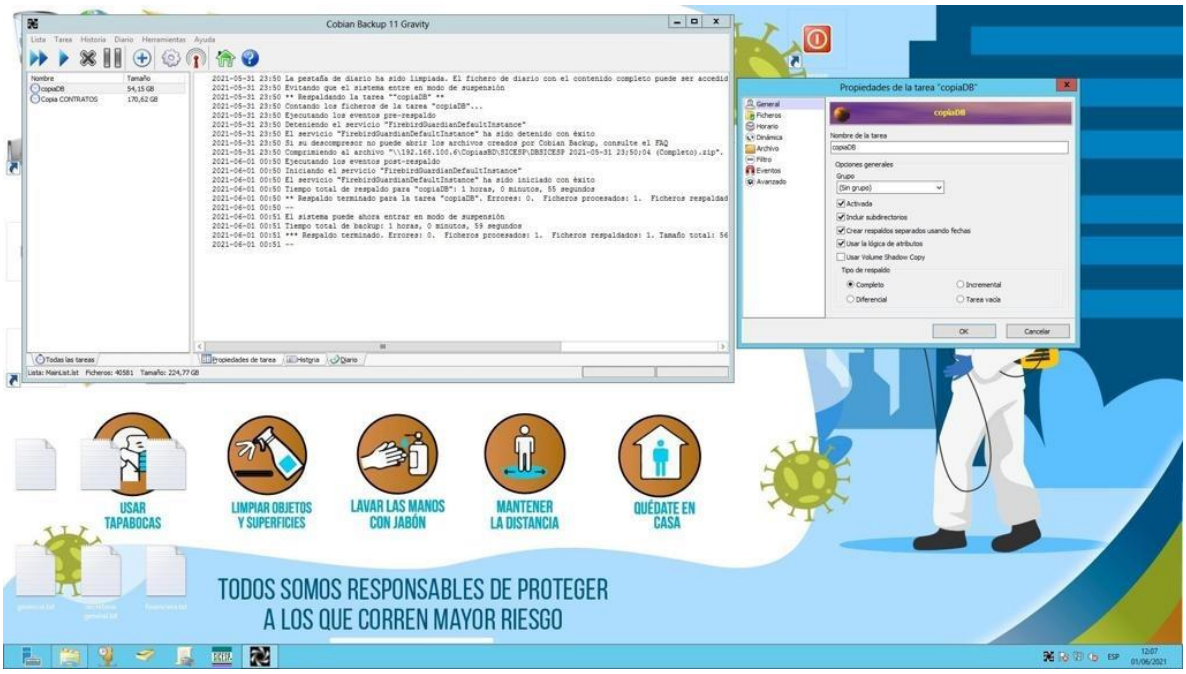
No	ETAPA	DEBILIDADES
1	Backup servidor Filesystem	a. Herramienta Cobian Backup no licenciada. b. La tarea de backup permite gestión del servidor completo a nivel de sistema operativo y solo se realiza backup a unos cuantos archivos de algunos programas y no al servidor completo. c. Requiere auditoria y monitoreo diario de manera manual.
2	Almacenamiento NAS	a. El recurso Nas debe permitir la sincronización automática y continua de los backups hacia la nube. b. Se debe mantener el firmware actualizado.
3	Migración de Equipo local y nube	a. La ejecución de la tarea de migración a nube se encuentra limitada a un equipo de cómputo personal.

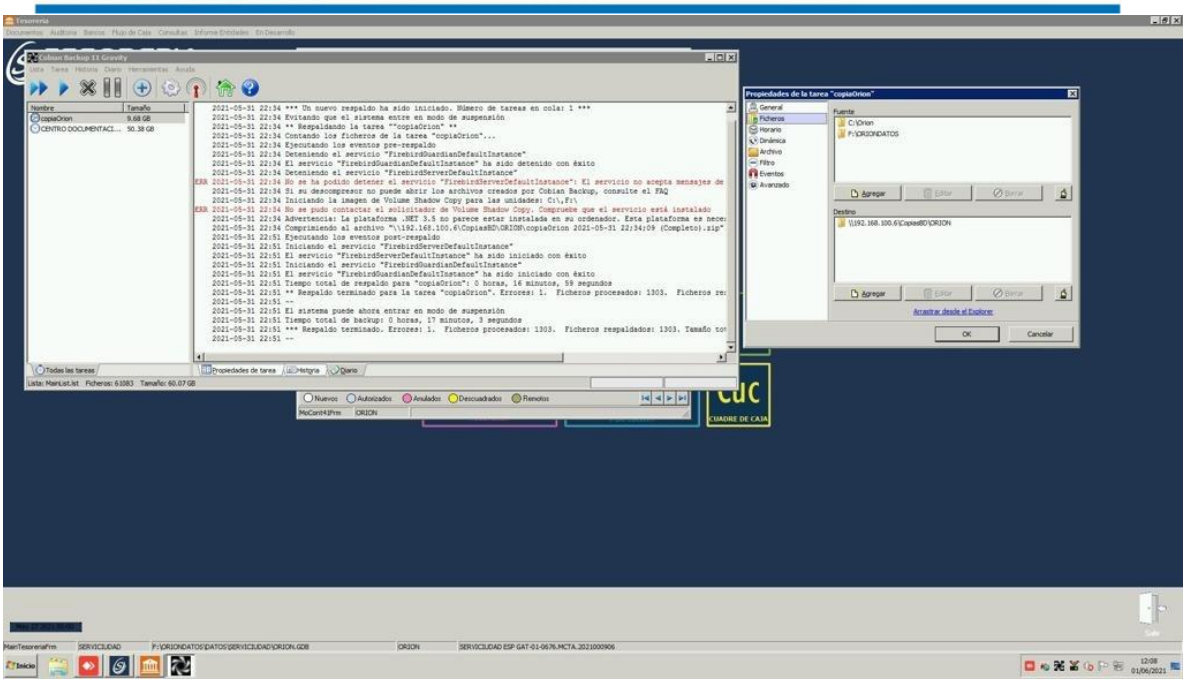
		b. Se debe garantizar el suministro de energía y validación de políticas GPO (Directorio activo o dominio de Windows) para validar que el equipo no se inactive mientras se está realizando el proceso de copias de seguridad. c. Se encuentra expuesto a posibles incidentes físicos. d. Este equipo de cómputo es utilizado para tareas diarias y cotidianas del Jefe de Sistemas y por ser portátil es constantemente trasladado de ubicación, lo que genera un riesgo adicional por daño de sus componentes en los traslados o pérdida por hurto y ocasionar interrupciones en el proceso de backup.
4	Disco externo	a. El disco externo se encuentra expuesto a posibles incidentes físicos. b. Se debe garantizar su custodia y encriptación de los datos. c. Se debe proteger con contraseña el acceso. d. El disco duro se encuentra alojado en un entorno que no cumple con ninguna recomendación ni norma técnica para custodia de información de copias de seguridad.
	Todo el Modelo	a. La selección de los archivos para ser copiados en el proceso de respaldo no obedece un proceso técnico ni estandarizado de copias de seguridad. b. No se tiene documentado un protocolo para realizar este proceso. c. No se ha verificado la validez del proceso de respaldo actual, realizando un proceso de simulacro de restauración de las copias de seguridad realizadas en otra máquina o servidor por lo que no se tiene certeza si las copias actuales son funcionales o no. d. Al analizar el repositorio de copias de seguridad solo se pudieron visualizar unas

		cuantas copias recientes del proceso actual, lo que no permite validar la trazabilidad de las copias de seguridad, ni el cumplimiento formal de manera diaria de la realización de este proceso.

Fuente: Elaboración Propia

IMAGEN Nª10. EVIDENCIAS TAREAS BACKUP POR SERVIDOR HERRAMIENTA COBIAN BACKUP





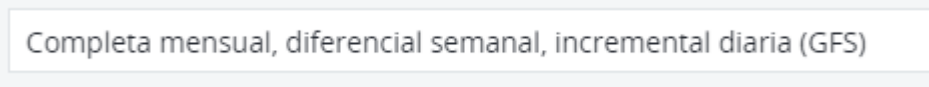
4.3.2.2 Modelo sugerido de backup servidores

- Se debe elaborar una política de respaldo, custodia y recuperación de la información para la entidad; teniendo en cuenta la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que esté adaptada a las condiciones específicas y particulares de cada servicio de TI.
- Esta política debe ajustarse y estar orientada en las buenas prácticas, leyes y normas relacionadas con la seguridad de la información: Ley 1273 de 2009 – De La Protección de la Información y de los datos, ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27002:2005 – Código Para la Práctica de la Gestión de la Seguridad de la Información, ISO 22301:2012 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO 9001:2015.
- Es responsabilidad de los líderes de procesos y jefes de dependencias garantizar que la información institucional catalogada como critica “aquella necesaria para mantener operativos los procesos de la entidad”, sea almacenada en los servidores de la entidad ubicados en el centro de datos

- El software de respaldo y restauración de información debe estar instalado en los servidores para los cuales se haya hecho solicitud de backup. Se debe contar con las licencias necesarias que garanticen el cumplimiento de dicha solicitud.
- Se debe garantizar la custodia y almacenamiento de los medios magnéticos (Discos Externos) con una empresa externa especializada.

ESQUEMA DE COPIAS DE SEGURIDAD PROPUESTO

Se debe contemplar el modelo de backup de todos los servidores bajo la siguiente recomendación:



1. Una Copia Completa mensual
2. Una Copia diferencial a la semana
3. Copias incrementales diarias

El almacenamiento del recuso debe ser externo y permitir la posterior migración al servicio de nube aprovisionado por la entidad con frecuencia diaria en horario no

laboral, con el fin de no afectar el rendimiento y saturación del canal destinado para tal fin.

Las copias de seguridad deben ser restauradas de manera aleatoria acorde a la política de seguridad, con el fin de garantizar su ejecución y confirmar su estado saludable.

4.4. COMPONENTE ALMACENAMIENTO

La Entidad SERVICIUDAD E.S.P cuenta con un repositorio de almacenamiento tipo NAS; este servidor NAS es susceptible a los ataques de malware, también pueden aprovecharse de vulnerabilidades presentes a nivel del firmware, ataques DDoS o ransomware, para todo ello, se debe proteger adecuadamente. Es importante evitar la entrada de intrusos que puedan dañar la seguridad.

TABLA Nª6 RECOMENDACIONES DEL COMPONENTE ALMACENAMIENTO

Rol y servicios	Físico	Marca y modelo	Recomendaciones
Almacenamiento en red	SI	LENOVO PX12	Renovar equipo NAS por obsolescencia tecnológica.

Fuente: Elaboración Propia

4.4.1. RECOMENDACIONES

- Utilizar contraseñas robustas
- Habilitar la doble autenticación
- Actualizar el firmware
- Activar la protección contra DoS
- Optar por el acceso solo a nivel local
- Generar configuración en RAID
- Generar backup de la información en repositorio externo

4.5. SISTEMA DE IMPRESIÓN Y EQUIPOS DE CÓMPUTO

La Entidad cuenta con variedad en las impresoras, se recomienda implementar un sistema de impresión centralizado que arroje estadísticas de usuarios, archivos impresos, cantidad de impresiones, entre otros, que al final logren la aplicación de controles, la reducción de costos y optimización del proceso.

4.5.1. EQUIPOS DE CÓMPUTO

La Entidad cuenta con equipos de cómputo asignados a los usuarios, para los cuales se requiere fomentar el buen uso y garantizar su optimo desempeño.

Las computadoras requieren condiciones ambientales óptimas para funcionar correctamente. Éstas son algunas de las medidas que se pueden tomar para proteger los equipos de las amenazas naturales y ambientales, y minimizar los daños causados por éstas:

- Realizar copias de seguridad de los datos.
- Instalar las computadoras en ubicaciones seguras, buscando lugares donde se disminuya la probabilidad de sufrir daños por factores ambientales. Por ejemplo, evitar instalarlas en salas que estén expuestas a excesos de polvo o humedades.
- Protección contra sobre voltajes y acondicionamiento de la línea.
- Actualizar y licenciar el antivirus.
- No realizar transacciones desde páginas web no confiables.
- No instalar herramientas o programas no licenciados.
- Evitar conectarse desde redes inalámbricas abiertas que no tienen ninguna seguridad.
- No descomprimir archivos de extensión desconocida sin antes verificar en “vista previa” el contenido del mismo.

4.5.1.1. Recomendaciones De Seguridad

- Vincular todos los equipos al dominio *ADDSServiciudad.gov*
- Actualizar de manera constante las políticas del Directorio Activo (GPO).
- Implementar rol de actualizaciones periódicas a nivel de sistema operativo.
- Realizar mantenimientos preventivos.

4.6. COMPONENTE SEGURIDAD PERIMETRAL

La Entidad SERVICIUDAD E.S.P cuenta con un dispositivo de seguridad perimetral Fortinet relacionado a continuación:

TABLA Nª7 COMPONENTE SEGURIDAD PERIMETRAL

Referencia	Observaciones
Fortigate 100D	Se requiere actualización de firmware y afinamiento en seguridad acorde a las buenas prácticas.

Fuente: Elaboración Propia

De acuerdo con Fortinet, compañía destacada en soluciones de ciberseguridad de alto rendimiento, casi un 80% de los incidentes de ciberseguridad industrial que se producen en organizaciones con infraestructuras críticas, están provocados por cuestiones internas como errores humanos involuntarios en la configuración del software o el funcionamiento inadecuado de protocolos de red.

4.6.1. RECOMENDACIONES DE SEGURIDAD

- Activar perfiles de navegación para los usuarios LOCAL, SSL/VPN permitidos.
- Deshabilitar cualquier característica de gestión que no se utilice. Por ejemplo, si no se utiliza HTTPS, SSH o SNMP, conviene deshabilitarlos en los interfaces de red. SSH además habilita la posibilidad de permitir acceso potencial a atacantes.
- Priorizar e implementar las reglas de seguridad que más se utilizan al principio de la política de seguridad.
- Generar logs solo del tráfico necesario. La escritura de logs, especialmente en los discos internos del dispositivo, afecta al rendimiento del sistema.
- Habilitar solo la inspección de aplicaciones necesarias.
- Mantener al mínimo las alertas del sistema. Si se envían a un servidor syslog, podrían no ser necesarias las alertas por email o SNMP, que requerirían un proceso redundante.
- Configurar las actualizaciones desde FortiGuard con una cadencia razonable. Las actualizaciones diarias cada 4 ó 5 horas son suficientes en la mayoría de los casos. programar las actualizaciones en el horario de menor carga/menor tráfico.
- Minimizar los perfiles de seguridad. Si un perfil no es necesario en una regla de firewall, no debería incluirse.
- Mantener los VDOM mínimos necesarios. En modelos muy pequeños, evitar utilizarlos.

- Evitar el uso de Traffic Sharing cuando se necesite el máximo rendimiento. Por definición, Traffic Sharing ralentiza el tráfico.
- Preparar un Plan de Recuperación Operacional. En el desafortunado caso de un desastre, todas las organizaciones necesitan un proceso documentado para evaluar los daños, reparar sistemas y máquinas y reestablecer sus operaciones. Los simulacros regulares de seguridad también ayudan a los operadores a adoptar una recuperación rápida y eficiente cuando más se necesita.

4.7. COMPONENTE USUARIOS

4.7.1 SOCIALIZAR Y SENSIBILIZAR A LOS COLABORADORES

Se recomienda realizar periódicamente capacitaciones sobre las políticas de seguridad de la información de la Entidad y las actualizaciones de las mismas. Además de esto, socializar y sensibilizar a los colaboradores sobre las amenazas a las que están expuestos.

4.7.2. RECOMENDACIONES

- Hacer uso de herramientas de protección del dispositivo como EDR (Endpoint Detection and Response), los cuales permiten una gestión integral y centralizada de la política de seguridad de la Entidad localmente en los dispositivos de los empleados.
- Realizar copias de seguridad de manera periódica haciendo uso de los medios de almacenamiento entregados por la Entidad para tal fin.
- No enviar archivos con información de la Entidad, por medios no oficiales como whatsapp, dropbox, wetransfer, correos de dominio gratuito, etc.
- Mantener actualizado su sistema operativo con los últimos parches
- No instalar programas o extensiones de navegadores de fuentes desconocidas ya que estas suelen traer malware el cual puede afectar sus dispositivos y extraer la información sensible.
- Evitar el uso de aplicaciones de escritorio remoto que no estén verificadas por la Entidad, estas herramientas pueden crear puertas traseras por medio de las cuales podría comprometerse el servicio o las credenciales de

acceso de usuario y por lo tanto permitir el acceso a los equipos corporativo.

CONFIDENCIALIDAD

Este documento es de carácter confidencial y solo podrá ser usado por el personal de TI de la Entidad para adoptar las recomendaciones aquí plasmadas.