Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Curso de adaptación al Grado de Ingeniería Informática

Transformación digital y nube híbrida de la Diputación de Guadalajara.

Trabajo fin de estudio presentado por:	Carlos-Fernando Quintas Riego
Línea de investigación:	Seguridad redes comunicaciones
Director/a:	Francisco José Soltero Domingo
Fecha:	14/03/2021
GITHUB: https://github.com/capialvi/TFG_ADDS	

Resumen

El presente trabajo pretende ser un punto de partida para aquellos servicios de informática y nuevas tecnologías de las administraciones públicas y más concretamente, en el caso de una administración de carácter local como la Diputación Provincial, que necesitan acometer un plan de adecuación de sus sistemas de información a las nuevas normativas de seguridad y a los nuevos tiempos digitales, en los que, las amenazas que se ciernen sobre los, cada vez más utilizados, sistemas telemáticos en el envío de datos de carácter personal son cada vez más y más avanzadas.

El plan para establecer los niveles óptimos de seguridad es muy amplio y abarca muchas áreas de las nuevas tecnologías, y no podrá ser tratado en su totalidad en el presente trabajo. No obstante, se intentará sentar unas bases sólidas de los puntos críticos que se tendrán que abordar para conseguir los objetivos planteados por la nueva sociedad y su forma de procesar la información. Se hará hincapié, como aportación, al establecimiento de una nube hibrida, utilizando Directorio Activo y Azure Directorio Activo ambos de Microsoft, en lo que concierne al ámbito de la identificación de los usuarios ante los sistemas de información y del acceso a la red, a los recursos y servicios que se ofrecen en una organización a nivel telemático.

Palabras clave: Transformación digital, seguridad comunicaciones, ciberseguridad, nube hibrida.

Abstract

This paper aims to be a starting point for those IT and new technologies services of public administrations and more specifically, in the case of a local administration such as the Provincial Council, which need to undertake a plan to adapt their information systems to the new security regulations and the new digital times, in which the threats that loom over the increasingly used telematic systems in the sending of personal data are becoming more and more advanced.

The plan for establishing optimum levels of security is very broad and covers many areas of the new technologies and cannot be dealt with in its entirety in this paper. However, an attempt will be made to lay a solid foundation for the critical points that will have to be addressed to achieve the objectives set by the new society and its way of processing information. As a contribution, emphasis will be placed on the establishment of a hybrid cloud, using Active Directory and Azure Active Directory, both from Microsoft, regarding the identification of users before the information systems and access to the network, resources and services offered in an organization at the telematic level.

Índice de contenidos

Índice de figuras

1. INTRODUCCIÓN

Con la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (Ley 39/2015, 2015) y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (Ley 40/2015, 2015), se ha iniciado un proceso de transformación digital del Sector Público, incluyendo a las entidades provinciales y locales. Esto supone una evolución muy importante en la mejora de la eficacia y eficiencia de la Administración Pública, que permitirá mejorar la experiencia de usuario de la ciudadanía en el uso de los servicios ofrecidos por todas las Administraciones. Esta mejora, implica la necesidad de proporcionar entornos digitales de calidad y seguros para todos los participantes, garantizando aspectos como la confidencialidad, la autentificación, la veracidad, la integridad, la disponibilidad y la copia de seguridad.

En los últimos años, todos los Gobiernos de España han ido adoptando medidas y programas para permitir el crecimiento digital de nuestro país, tanto en los que refiere a la ciudadanía, al tejido empresarial, como a las administraciones públicas y los servicios que estas ofrecen. Estos avances han ido en consonancia con las distintas agendas digitales europeas y se han reflejado en distintos programas y planes en nuestro Estado, como pueden ser: el Plan Info XXI, el Programa España.es, el Plan Avanza, la Agenda Digital 2013 y actualmente la Agenda España Digital 2025, (MINECO_Agenda_2025, 2020), presentada el 23 de julio de 2020. Con el mismo enfoque se presentó y publicó el 14 de abril de 2019 la Estrategia Nacional para la Ciberseguridad 2019, (CCNCERT_Estrategia2019, 2019).

España Digital 2025, (MINECO_Agenda_2025, 2020) focalizará sus objetivos en el impulso de la transformación digital del país para poder relanzar el crecimiento económico, reducir la desigualdad, aumentar la productividad y aprovechar todas las oportunidades que las nuevas tecnologías nos brindan para avanzar y prosperar con eficacia, eficiencia y seguridad,

permitiendo, al mismo tiempo, hacer esto con el merecido respeto a los valores constitucionales y europeos así como, a la protección de los derechos individuales y colectivos.

España Digital establece 50 medidas que se desarrollan en base a diez ejes estratégicos:

1. Conectividad digital.
2. Liderar el despliegue 5G en Europa.
3. Reforzar las competencias digitales de los trabajadores y de la ciudadanía.
4. Reforzar la ciberseguridad.
5. Impulsar la digitalización de las Administraciones Publicas, actualizando sus infraestructuras tecnológicas.
6. Acelerar la digitalización de las empresas.
7. Acelerar la digitalización del modelo productivo.
8. Mejorar el atractivo de España como plataforma audiovisual para generar negocio y puestos de trabajo.
9. Transitar hacia la economía del dato, garantizando la seguridad y privacidad.
10. Garantizar los derechos en el nuevo entorno digital, y en particular, los derechos laborales, de los consumidores, de los ciudadanos y de las empresas.

Tal y como dijo el presidente del Gobierno en la presentación de la estrategia Nacional de Ciberseguridad, (Pedro Sánchez, 2019): "*En plena era de trasformaciones y de incertidumbres. Hemos de ofrecer un horizonte moral y material sólido, y para ello es cada día más imprescindible una ciberseguridad acorde a los nuevos tiempos y amenazas. Capaz de atender los distintos retos y hacerlo desde la cooperación público-privada y con el apoyo de una ciudadanía consciente de la realidad cambiante y comprometida con las soluciones a los desafíos.*"

En este entorno nos encontramos con unas administraciones locales, en concreto en las Diputaciones Provinciales, con un nivel de madurez, en relación con la administración digital, muy bajo. Concretamente y según el estudio realizado por Ernst & Young, S.L. (EY) en marzo de 2019, (Ernst & Young, 2019), donde se analiza el nivel de cumplimiento de la legislación vigente, así

como las mejoras que se tendrán que poner en marcha en un futuro próximo con el objetivo de ofrecer una experiencia positiva al ciudadano en su relación con las Administraciones Públicas.

1.1. Justificación.

Los ejes estratégicos, mencionados en la introducción, cuarto: reforzar la ciberseguridad y décimo: garantizar los derechos en el nuevo entorno digital, y en particular, los derechos laborales, de los consumidores, de los ciudadanos y de las empresas, de la Agenda Digital 2025, (MINECO_Agenda_2025, 2020), obligan a establecer los mecanismos necesarios para garantizar la confianza de nuestros usuarios (ciudadanos, empresas, e incluso, otras administraciones) en los sistemas de información que se usan en las administraciones públicas, en este caso concreto, en la Diputación de Guadalajara. Es por ello por lo que, como parte de un plan más amplio, que abarca todo lo concerniente a la ciberseguridad y seguridad física, surge la necesidad de realizar este trabajo.

Desde el punto de vista de la ciberseguridad, se tiene que trabajar con fuerza para que toda información que se introduce o genera en los sistemas de información goce de las pertinentes y necesarias medidas de seguridad. Es en este sentido donde la madurez de la Diputación de Guadalajara se encuentra un poco más verde, como veremos más adelante en el estado del arte y este nivel de madurez tan bajo ha provocado que el servicio de informática y nuevas tecnologías junto a la alta dirección de la empresa hayan decidido realizar un plan de adecuación de los sistemas de información de la empresa, dentro del cual se contempla lo expuesto en este trabajo.

2. ESTADO DEL ARTE.

Actualmente la información en las empresas y organismos públicos se ha convertido en uno de los activos más importantes de las mismas, de sobra es conocida la importancia que el análisis de dicha información tiene para la toma de decisiones y la planificación estratégica de la alta dirección. Así mismo, cada vez se está haciendo más hincapié en la protección de los datos de carácter personal y de la información que los sistemas de información de las organizaciones emplean en el desempeño de sus funciones.

No se puede realizar este trabajo sin entrar y estudiar las tendencias actuales de la ciberseguridad, tal y como establece el informe del Instituto Nacional de Ciberseguridad (INCIBE), en su Informe sobre tendencias en el mercado de la ciberseguridad, (INCIBE, Tendencias en el mercado de la Ciberseguridad, 2016) en el cual mediante el uso de:

- Estudios de mercados de referencia, como: Forrester, Gartner, Deloitte, Forbes, EY.
- Catálogos de productos de grandes empresas, como: MCAFEE, Kaspersky, Cisco, Symantec, etc.
- Informes de incidentes y amenazas de organismos públicos, como: ENISA, OCDDE, CNI, CCN CERT, etc.

Se puede llegar a la conclusión, y así se explica en dicho informe, (INCIBE, Tendencias en el mercado de la Ciberseguridad, 2016) que la ciberseguridad permite:

- Ser un mecanismo para la toma de decisiones para el modelo de negocio y la estrategia de las empresas.
- Permite la definición de nuevos segmentos de desarrollo y oportunidades para las empresas.

El mismo informe, (INCIBE, Tendencias en el mercado de la Ciberseguridad, 2016), se establecen 20 tendencias globales en ciberseguridad catalogadas en base a 6 sectores de actividad. El que nos afecta en cuestión es el Sector TIC, con las siguientes tendencias:

- Servicios de seguridad en la nube, "Security As A Service (SaaS)"
- Cifrado en tiempo real, como mecanismo de protección para la seguridad de los datos en las transacciones electrónicas.
- Cifrado homomórfico, que nos permite que la información se codifique para que pueda ser compartida por terceras partes.
- Hacking ético, buscando vulnerabilidades mediante la realización de pruebas de penetración o "pentest".
- Certificado de confianza digital, mediante la utilización y emisión de sellos de confianza digital.

En el mundo que nos movemos donde todo se encuentra conectado, se genera y se generará cada vez mayor cantidad de datos, con cuyo tratamiento se consigue cada vez mayor cantidad de información. En la mayoría de los casos, parte de esta información es de carácter personal, lo que permitirá que en un futuro no muy lejano uno de los bienes con los que se tratará en los mercados sean los "datos", que los consumidores podrán recopilar y vender u ofrecer a las empresas como un producto más.

Actualmente la pandemia COVID-19 ha cambiado y está cambiando no sólo la forma, sino también el dónde, los empleados, los ciudadanos y las empresas gestionan sus servicios con las administraciones, haciendo de la localización algo que tiene que estar soportado por la tecnología para dar soporte a esta nueva forma de relacionarse. (Gartner, Top Strategic Technology Trends for 2021, 2020). El "Anywhere, anytime and on any device", (En cualquier sitio, a cualquier hora y con cualquier dispositivo), que incluye el uso de la nube digital y por supuesto la necesidad de mejorar la privacidad en la computación forma parte de la base que ayuda a crear ese entorno de confianza y resiliencia.

La creación del clima necesario para la **confianza digital** que permita mejorar la protección de los Organismos Públicos y que permita a los ciudadanos y empresas el uso e implicación del entorno digital, necesita de la ciberseguridad como factor clave. Al tiempo se puede observar como la Agenda digital para España, (MINECO_Agenda_2025, 2020), se centra en conseguir los avances tecnológicos y adecuar las infraestructuras de las administraciones públicas, guiando a las mismas en la consecución del objetivo antes citado: conseguir la tan necesaria "confianza digital" mediante la **transformación digital**.

Pero se puede seguir hablando sin antes dejar claro el concepto de "transformación digital" y sus objetivos. Como ya se indica en la introducción, las nuevas normativas referentes a tratamiento digital de información, procedimiento común electrónico, carpeta ciudadana, servicios electrónicos, etc. Todos ellos incluidos y reglamentados en las nuevas leyes de transformación digital, obligan a las administraciones públicas a mostrar un nivel de madurez, en lo que respecta a la ciberseguridad, capaz de ofrecer la confianza necesaria a los ciudadanos y empresas para que se relacionen de manera electrónica con ellas y lo hagan con todas las garantías posibles que se puedan ofrecer.

Tal y como se comenta en el trabajo sobre transformación digital de Sergio Jiménez, (Jiménez, 2019) se puede decir que la transformación digital está definida en sí misma como un cambio y además un cambio continuo. Ya que la evolución de las tecnologías impide que esa transformación llegue a ser temporal, con un final concreto en el tiempo. Por lo tanto, se podría definir la transformación digital, y cito textualmente a Sergio Jiménez, como: "el conjunto de cambios que permiten a una organización aprovechar la tecnología para crear valor diferencial y suficiente a las personas y organizaciones que se relacionan con ella".

Este cambio constante y evolutivo se puede ver muy gráficamente en la siguiente ilustración:

Ilustración 1. La cuarta revolución industrial. Fuente: (Jose Manuel Riveroll, Robert Beltrán López, Erwin Adame Gómez, Erwin Adame Gómez, 2019)

Pero ¿cómo se puede evaluar el estado de madurez de las administraciones públicas en el ámbito de la transformación digital? Esto se verá en el siguiente apartado: "Madurez de las Administraciones Públicas".

2.1. Análisis de las TI y las comunicaciones en la Administración Pública.

2.1.1. Madurez de las administraciones públicas.

Para poder responder a la pregunta planteada en el apartado anterior, ¿cómo se puede evaluar el estado de madurez de las administraciones públicas en el ámbito de la transformación digital?, primero se tiene que establecer una serie de atributos y niveles de ponderación para poder evaluar el estado de estas administraciones con el objetivo de poder crear proyectos y establecer objetivos que permitan evolucionar a lo que los nuevos tiempos tecnológicos requieren. En estos términos se realiza el estudio sobre la Administración Digital en España, (Ernst & Young, 2019),

en el que se refleja la situación tanto de Administración General del Estado (AGE), como de las administraciones de las entidades locales (EELL) y en el caso concreto de este trabajo: las Diputaciones Provinciales.

En este estudio se han tenido en cuenta las siguientes temáticas:

- El portal web.
- La sede electrónica.
- La asistencia al ciudadano y empresa.
- La identidad digital y firma electrónica.
- La representación y registro electrónico.
- El expediente, documento y archivo electrónico.
- Las comunicaciones y notificaciones al ciudadano.
- La interoperabilidad.
- La reutilización.

Y los resultados alcanzados son los siguientes:

- Portal web, sólo el 48% de las diputaciones cumple con todos los requisitos.
- Sede electrónica, sólo el 27% de las diputaciones cumple la totalidad de los requisitos.
- Identidad digital y firma electrónica, un bajo 9,5% de las diputaciones cumple todos los objetivos.
- Representación y registro electrónico, solo 1 diputación cumple el 100% de los requisitos.
- Asistencia al ciudadano y empresas, el 42% de las diputaciones lo gestionan de manera adecuada.
- Comunicaciones y notificaciones al ciudadano, sólo el 23% de las diputaciones lo cumplen.

En concreto dicho estudio refleja que el nivel de madurez de la Diputación de Guadalajara, que es el caso que nos interesa en este trabajo, se encuentra en el penúltimo puesto del ranking con un 18.1% de índice de madurez. Dejando clara constancia de la necesidad de realizar este trabajo y de implementar técnicas que permitan avanzar a esta institución en el camino correcto para la generación de un clima de confianza y resiliencia que permita a todos los participantes de sus servicios actuar de forma segura y confiada.

Es por esto por lo que se ha considerado necesario desde el Servicio de Informática y Nuevas Tecnologías, del cual estoy al frente, y de mutuo acuerdo con la Dirección de la empresa, de afrontar este reto que consiste en modernizar y asegurar el funcionamiento de los sistemas de información que se utilizan actualmente. Tal y como se cita en dicho estudio: "*Por otra parte,*

entre las diputaciones que presentan un mayor margen de mejora se encuentran La Gomera, Guadalajara y Cuenca, las cuales no superan el 30% del índice y cuyas actuaciones e inversiones deberán ir dirigidas a reforzar su relación con la ciudadanía y empresas a través de la administración digital." (Ernst & Young, 2019, p. 21).

2.1.2. Informe IRIA 2018.

Con la incorporación de la gobernanza TIC y la creación de la Comisión de Estrategia TIC, en el Real Decreto 806/2014, de 26 de septiembre, (Real Decreto 806/2014, 2014, p. 75263 a 75278), a la que le corresponde como principal la función de "actuar como Observatorio de la Administración Electrónica y Transformación Digital". Dicha comisión se encarga de realizar el estudio de la encuesta de la Integración de la Recogida de Información y su Administración (IRIA), realizada por el Instituto Nacional de Estadística (INE), que se divide en siete apartados y ha tenido en cuenta los objetivos generales del Plan de Acción sobre Administración Electrónica de la UE 2016-2020.

El informe IRIA 2018, (Comisión Estratégica TIC, IRIA 2018, 2018), se basa en la información recogida a Diputaciones Provinciales y Forales, Cabildos y Consejos Insulares y Municipios de más de 500 habitantes a fecha de 01 de enero de 2018.

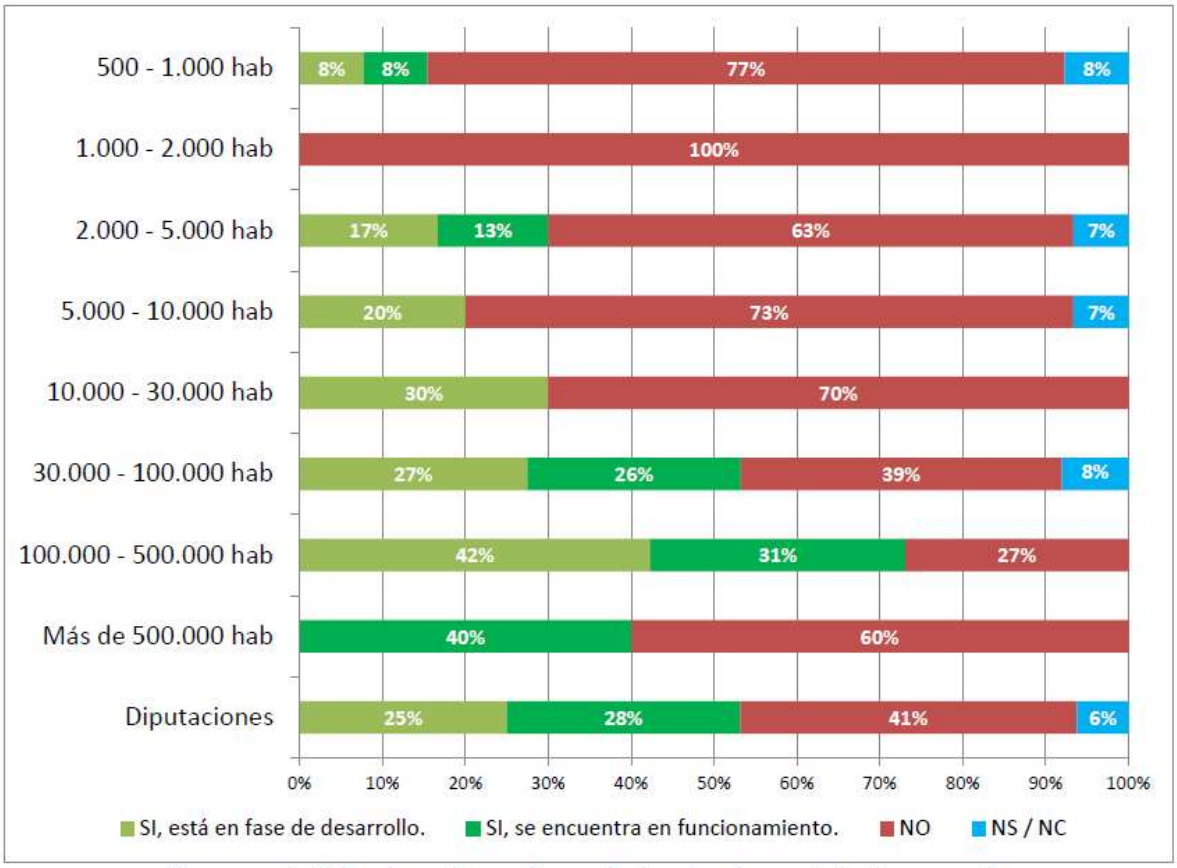

Ilustración 2.Estado de los Planes de transformación digital en las entidades (porcentaje).

Gracias a este estudio se puede observar, ilustración 2, las entidades que han puesto en marcha algún plan para iniciar el camino a la Transformación Digital poniendo el foco en el caso de las Diputaciones, donde el 41% no lo ha iniciado y el 6% no sabe o no contesta.

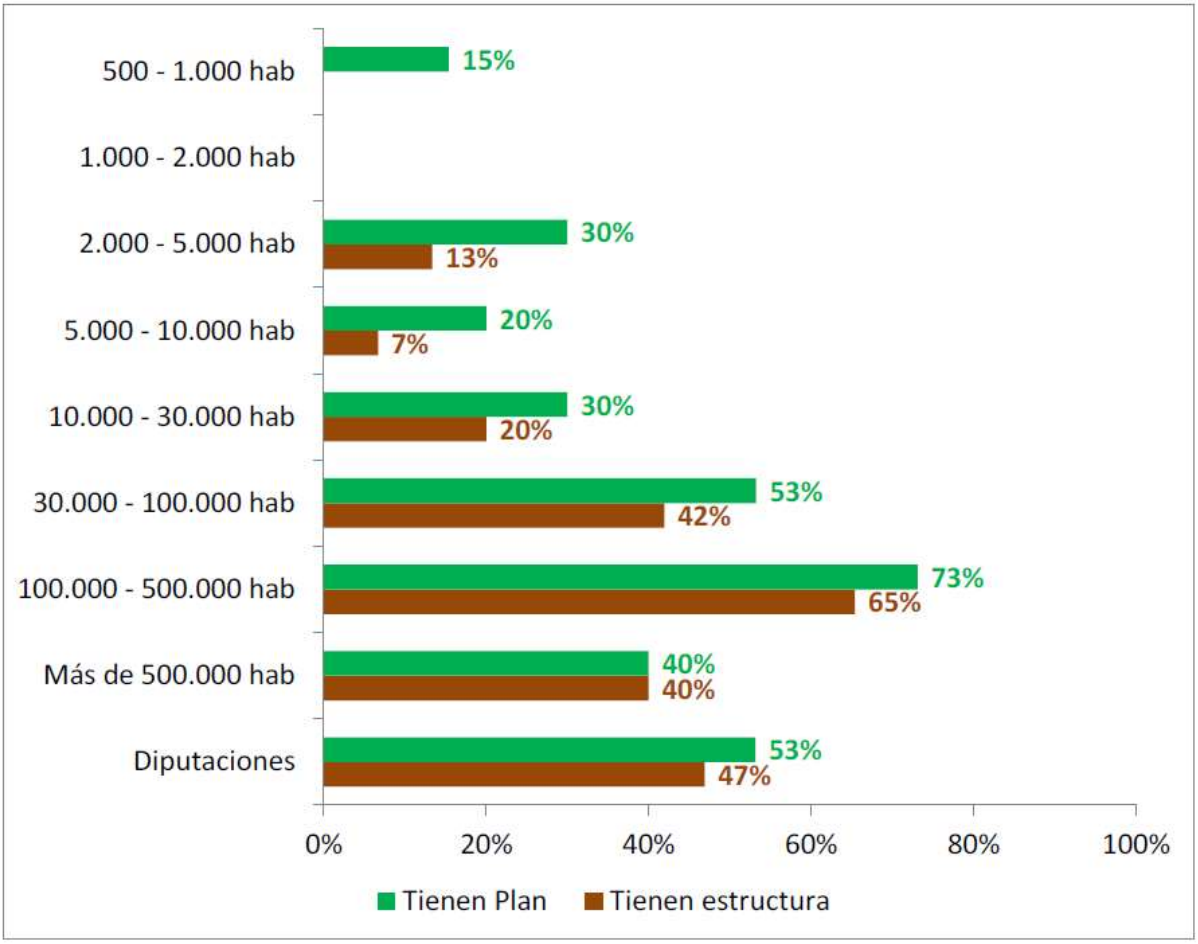

Ilustración 3.Entidades que han creado alguna estructura organizativa con el objetivo de impulsar la transformación digital (porcentaje).

En la ilustración 3 se ven las entidades locales, que, habiendo establecido o iniciado el Plan de Transformación Digital, han establecido la estructura organizativa necesaria para llevar a cabo ese impulso digital. Una vez más se detecta que, en el caso de las Diputaciones, el porcentaje de las que tienen un plan es del 53% y que las que tienen la estructura organizativa necesaria para poder desarrollarlo es del 47%.

2.1.3. Plan de digitalización de España 2025.

El Plan de Digitalización de España 2025, (Agenda 2030, 2020) establece tres ejes fundamentales en la planificación para estructurar las administraciones públicas:

- Eje 1. Transformación digital de la Administración General del Estado (AGE).
- Eje 2. Proyectos de alto impacto en la digitalización del Sector Público.
- Eje 3. Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública, Comunidades Autónomas y Entidades Locales.

Dentro del Eje 3, se establece la medida número 16 que establece la "Transformación Digital de las Comunidades Autónomas y de las Entidades Locales". Afectando de lleno a la Diputación Provincial de Guadalajara, como entidad local que es.

Ilustración 4. Objetivos finales eje 3 Plan digitalización 2025.

Como uno de los objetivos finales del eje3, que se muestran en la ilustración 4, se puede ver que las Entidades Locales se encuentran incluidas en dicho plan de digitalización

En el mismo trabajo se puede observar que esta transformación digital, no sólo conlleva un cambio en las TIC, sino también una reforma y actualización normativa que afectará al Esquema Nacional de Seguridad, que una vez reformado, permita una correcta evolución de la política de seguridad de todas las entidades del Sector Público, (incluidas las Diputaciones), estableciendo unos nuevos principios y requisitos mínimos que garanticen de una manera adecuada la

ciberseguridad y una actualización de las normas técnicas de seguridad que logren una adecuada y coherente implantación de dichos requisitos y medidas de seguridad.

Para dicha actualización se deberán tener en consideración las siguientes regulaciones:

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, transpuesta por medio del Real Decreto-ley 12/2018, de 7 de septiembre, que señala la necesidad de tener en cuenta el Esquema Nacional de Seguridad.
- El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) N.º 526/2013 («Reglamento sobre la Ciberseguridad»).
- El Real Decreto-Ley Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

En estas reformas participará la Comisión Sectorial de Administración Electrónica (CSAE).

2.2. Computación en la nube (Cloud Computing).

A estas alturas del trabajo seguro que en algún momento se ha podido leer y comentar algo sobre el término de la "Computación en la NUBE", cierto es que es un concepto que en los últimos años está tomando mucha relevancia por todo lo que ha avanzado y por todo lo que ofrece. Pero ¿qué significa en realidad este concepto? Tal y como explica Rafael Castillo, en su documento "Computación en la nube y Microsoft como proveedor" (Castillo, 2013) se puede obtener una definición del término, ofrecida por el NIST: "*Es un modelo que habilita de manera conveniente, el acceso por redes, bajo demanda, de un conjunto de recursos computacionales compartidos (por ejemplo, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente configurables y habilitados, con un mínimo esfuerzo administrativo o de interacción con el proveedor del servicio."*

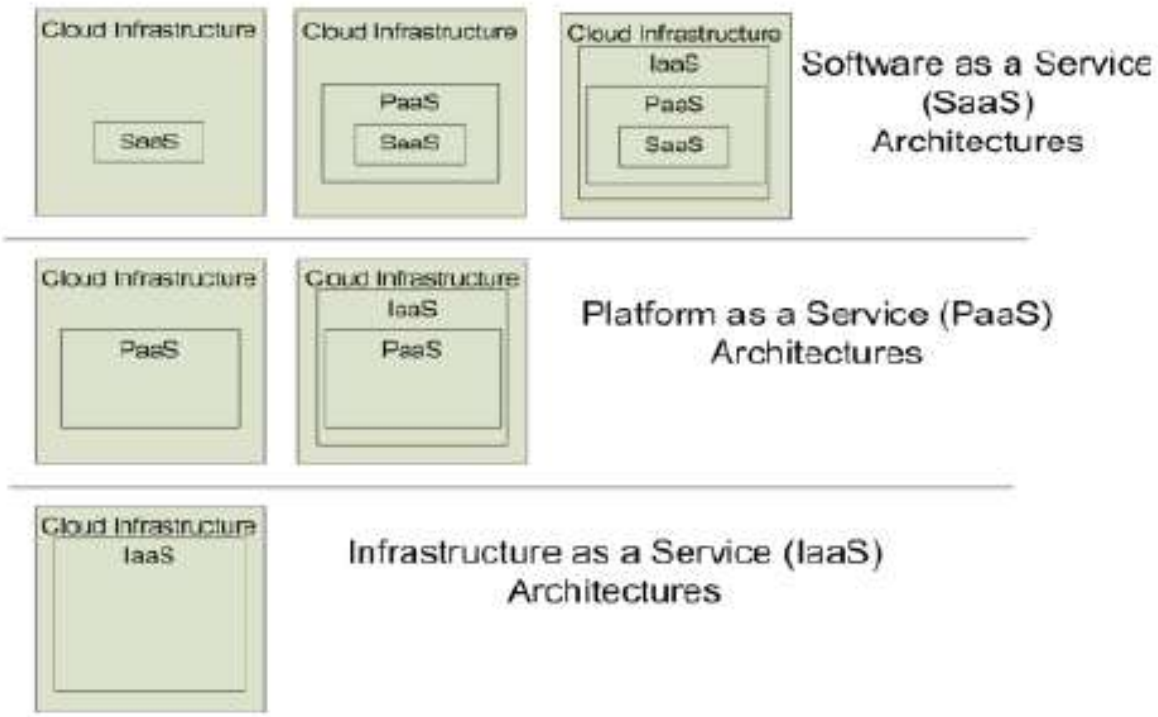

Ilustración 5. Arquitectura de los modelos de servicio de la computación en la nube

Además, ¿que ofrece el Cloud Computing en términos de seguridad y resiliencia?, pues básicamente tres Modelos de servicio, (véase Ilustración 5): SaaS (Software as a Service), PaaS (Platform as a Service) y IaaS (Infrastructure as a Service).

Si se echa la vista atrás, se puede observar que no hace mucho tiempo el tener algo en la nube era sólo posible para las grandes corporaciones con un alto nivel de inversión/gasto en este tipo de infraestructuras. Actualmente los costes han bajado mucho. Según Lenildo Morais, maestro en Ciencias de la Computación y Gerente de Proyectos de Ustore, empresa del Puerto Digital de Pernambuco (Brasil), dice en un artículo escrito en "Computing", (Morais, 2020): "*Cada vez más empresas se plantean hacer un traslado de todo o parte de su TI a la nube"*. Y como muy bien define Lenildo en su artículo, esto no es una decisión banal, al contrario, se deben medir no solo los costos sino la calidad y el rendimiento que se busca.

Dentro de estas nuevas formas de implantación se dispone de muchas opciones y en la mayoría de los casos es algo que queda como decisión del equipo TIC y de la dirección de la empresa.

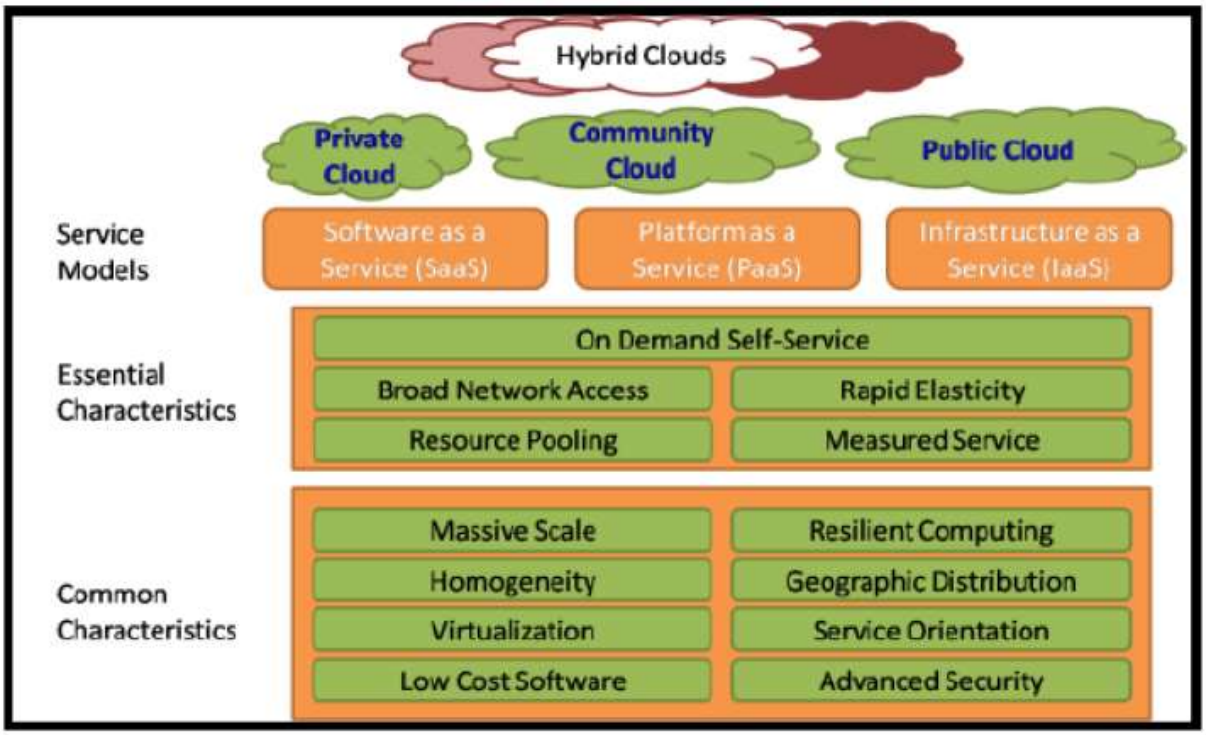

Ilustración 6. Marcos de trabajo según el NIST.

Viendo la ilustración 6, marcos de trabajo según el NIST, se pueden obtener las siguientes opciones:

- Nubes públicas. En este modelo los servicios y los recursos son públicos, pero mantienen un nivel de seguridad adecuado.
- Nubes privadas. Es un modelo en el que la organización adquiere su propia infraestructura e implanta sus servicios y aplicaciones en ella. Puede ser arrendada o propia.
- Nubes hibridas. Es una combinación de los dos modelos anteriores, ofreciendo la posibilidad de establecer servicios y aplicaciones a nivel público o a nivel privado según las necesidades. Permiten además una gran movilidad y migración entre ambas plataformas. Actualmente es una muy buena opción para aquellas organizaciones que

quieren seguir manteniendo parte de privacidad sin renunciar a la utilización de la nube pública y sus ventajas.

En general se puede hablar de que el mantenimiento de la seguridad de las redes informáticas, el hecho de que las empresas pequeñas y medianas busquen constantemente las soluciones más económicas para sus balances en cuestión de almacenamiento y aplicaciones, la falta de una estructura organizacional TIC o la existencia de personal con falta de los conocimientos necesarios, todo esto sumado a la necesidad actual de movilidad por parte de los empleados hace que la computación en la nube pública o la computación mediante nube híbrida sea una de las mejores opciones. Tal y como se indica en el informe sobre tendencias en ciberseguridad del INCIBE, y más concretamente en su informe sobre Servicios de seguridad en la nube, (INCIBE, Servicios de seguridad en la nube SaaS), se observa el impacto que esta tendencia tiene sobre los distintos sectores en el siguiente gráfico:

Ilustración 7. Impacto tendencia SaaS. fuente INCIBE.

Sin embargo, el ir a un modelo de nube pública no es tan fácil como puede parecer en un primer momento. Se deben tener en cuenta los costos, el rendimiento, la disposición del personal, el conocimiento y la estructura del personal TIC. Mientras que las infraestructuras “on premise” requieren una inversión inicial, los servicios en la nube, aunque más asequibles, requieren un coste periódico anual. Es decir, con la nube pública los costos fijos se convierten en variables, todo dependerá de las necesidades que en cada momento sean requeridas por el volumen de información, operaciones que se realicen en nuestros sistemas, lo que permite a las

organizaciones ser más flexibles y adaptables a los cambios de tendencias en el uso de nuestros servicios.

En nuestro caso y el de este trabajo, se ha optado por dar un primer paso, e ir hacia un modelo de **nube hibrida**, haciendo outsourcing de aquellos servicios que permiten ofrecer las suficientes garantías de seguridad y de gestión con la estructura de TI que poseemos en la actualidad. Pero manteniendo el control interno de otra parte de estos.

2.3. Directorio Activo en las organizaciones.

Directorio Activo, (AD – de sus siglas en inglés Active Directory), es un servicio de directorio propietario de Microsoft para ser usado en entornos Windows Server. Apareció con la versión de Windows 2000 Server hace ahora más de 15 años. En todo este tiempo han ido sacando distintas versiones al mismo tiempo que evolucionada el propio sistema operativo Windows Server desde su versión inicial a la actual 2019.

Aunque la versión que se implanta en la actualidad, y que será la que se implante para la infraestructura de este proyecto, es la de Windows Server 2019, los libros de consulta que se han encontrado hacen referencia a la versión del 2016. Las diferencias entre las versiones de AD implementadas en ambas versiones no son muchas, enfocándose el AD más hacia un concepto de nube hibrida mediante la introducción y conexión del AD local con Microsoft Azure Active Directory Domain Server. Que es, en última instancia, el objetivo principal del presente trabajo. No obstante, y para que sirva de referencia se detallan a continuación algunas de las novedades de AD en su versión con Windows Server 2016, (Microsoft AD DS, 2017):

- Privileged Access Management (PAM). Permite suavizar los problemas en cuanto a seguridad causados por robos de credenciales y otros ataques similares.
- Azure AD Join. Permite inicio de sesión único (SSO – Single Sign On) en los recursos de la organización: aplicaciones, Office 365, sitios web, etc.

- Posibilidad de crear cuentas empresariales en dispositivos Bring Your Own Device (BYOD), además de permitir la integración con aplicaciones Mobile Device Management (MDM).

Según un estudio del ESJ (Enterprise Systems Journal), (Gohstand, 2010), en el que se dice que: "*un 95% de las empresas que pertenecen al "1000 fortune" tienen implantado el DA"*. Se puede observar claramente el nivel de implantación de este tipo de servicio de directorio en la mayoría de las empresas mundiales más importantes.

Si bien es cierto, y se tendrá que prestar especial atención, que sobre esta infraestructura de directorio han surgido en los últimos años diversos y variados tipos de ataques, como, por ejemplo (Miguel-Tomás, 2019):

- WannaCry, aprovechando las debilidades del protocolo SMB V1.
- Debilidades del protocolo RDP (Remote Desktop Protocol). Contra los servidores Windows Server y el puerto 3389
- Vulnerabilidades por una política incorrecta o incompleta de parcheado del software base.

Se debe, por tanto, planificar muy bien la infraestructura de DA, para que se encuentre protegida tanto frente a los antiguos ataques ya desarrollados con éxito, como para los nuevos que puedan aparecer.

En este sentido Microsoft ha evolucionado hacia lo que actualmente se conoce como "**identificación en la nube**", con la implantación del "**Microsoft Azure Active Directory**" (MAAD), (Microsoft Azure AD, 2021), como un sistema de identidad empresarial que ofrece la posibilidad de un inicio de sesión único (SSO – Single Sign On, en inglés) y autentificación multifactor. Lo que permitirá defenderse de un amplio abanico de ataques a la ciberseguridad. Como así lo demuestra el reconocimiento como uno de los mejores sistemas de autentificación del "Magic Quadrant for Access Management" de Gartner, publicado el 17 de noviembre de 2020, (Gartner, Magic Quadrant for Access Management, 2020). Del cual se extrae la siguiente gráfica:

Ilustración 8. Magic Quadrant for Access Management

MAAD ofrece:

- Inicio de sesión único.
- Acceso condicional con autentificación multifactor.
- Una única plataforma de identidades.
- Integrar las identidades con aplicaciones y servicios.
- Permite a los trabajadores trabajar a distancia, cualquier sitio a cualquier hora.
- Utilizar cientos y cientos de aplicaciones SaaS.

Pero, además, si se integra y conecta MAAD con AD "On Premise", se consigue lo mejor de ambos mundos:

1. Tener un servicio local que no necesita utilizar ningún servicio exterior para identificar a los usuarios, lo cual ofrece una actuación rápida y sin necesidad de enviar datos al exterior.
2. Apoyarse en el servicio de autentificación en la nube, que permitirá que los trabajadores puedan identificarse desde cualquier sitio y a cualquier hora.
3. Tener una solución de alta disponibilidad en cuanto a la identificación, ya que, en caso de caída de alguno de los dos sistemas, siempre se podrá seguir utilizando el otro.

Aprovechando la metodología definida por Ruiz-Ibáñez, Miguel-Tomás en su documento de "Metodología técnica de revisión de directorio activo", (Miguel-Tomás, 2019) en el que se establecen los 5 pasos necesarios para completar la documentación de implantación de DA, véase:

1. Búsqueda y revisión bibliográfica de las fuentes. Adicionalmente, recopilación de información y clasificación de estas, adquirida mediante la experiencia laboral.
2. Despliegue de la infraestructura de laboratorio para realizar las pruebas descritas en el documento, así como las medidas defensivas.
3. Documentación organizada de las pruebas elaboradas sobre la infraestructura de laboratorio.
4. Estimación de costes y tiempos.
5. Conclusiones generales.

Este trabajo se iniciará con la fase de obtención de información. Esta fase se apoyará en la estructura e información obtenida de la documentación de Microsoft sobre AD DS, (Microsoft AD DS, 2017) que en su capítulo titulado "Planeación y diseño de AD DS", se puede obtener una guía con recomendaciones para desarrollar la estrategia de implementación de AD DS basándose en los requisitos de cada organización. Aunque la información que puede verse en esa guía hace referencia al sistema operativo Windows Server 2008, 2012 y 2016, se podrá ver en este

documento que el sistema operativo de base que se va a montar en este caso es la versión 2019 Datacenter, ya que toda la información que hace referencia a AD DS en Windows Server 2016 puede igualmente aplicarse a la versión 2019.

2.4. Alternativas a Microsoft AD

Como aportación para futuras investigaciones, a continuación, se enumeran algunas de las alternativas al Microsoft AD:

- **Apache Directory Server**, (Apache, s.f.). Soportado por la Apache Software Foundation, como parte del proyecto Vision. También conocido como ApacheDS, es un servidor de directorio escrito en Java, que no solo permite objetos de directorio, sino que también admite disparadores y procedimientos almacenados. Características principales:
  - Compatible con el protocolo LDAPv3, certificado por la Open Group.
  - Totalmente adaptado a los esquemas de la X.500.
  - Con un servidor Kerberos integrado. Que soporta KDC (Key Distribution Centre), TGS (Ticket Granting Server) y AS (Authentication Server).
  - Replicación multi-maestro mediante la RFC 4533 que lo hace compatible con OpenLDAP.
  - Multiplataforma, Linux, Max OS y Windows.
- **Open LDAP**, (LDAP, s.f.). Se trata de un software Open Source que implementa el Lightweight Directory Access Protocol (LDAP). Incluye:
  - Demonio servidor LDAP.
  - Librerías de implementación del protocolo LDAP.
  - Utilidades y herramientas.
- **FreeIPA**, (FreeIPA, s.f.). Es una solución para Linux que combina:
  - Sistema Linux Fedora.
  - 389 Directory Server.
  - MIT Kerberos.
  - NTP, DNS.

- **eDirectory**, (eDirectory, s.f.). Es el servidor de directorio de la marca Novell que ahora forma parte de la empresa Micro Focus. Permite utilizar el eDirectory como un servicio Web mediante SOAP y publicarlo mediante UDDI. Tambien admite multiplataforma: Windows, Linux, Solaris, Netware.

2.5. Como funciona AD DS.

Antes de entrar por completo en el diseño de la solución propuesta en este trabajo, es conveniente tener una buena comprensión del funcionamiento del AD DS y de sus conceptos y terminología básicos.

AD DS es un servicio de directorio que se utiliza en entornos de Windows Server. En definitiva, se trata de una base de datos distribuida y jerárquica que permite proteger, localizar, organizar y administrar todos los recursos del equipo y la red: archivos, usuarios, grupos, periféricos y otros dispositivos. Una de sus principales funciones es la de autenticación y autorización. Pero en general cuando nos referimos a AD, normalmente nos estamos refiriendo a los servicios de dominio (DS – Domain Services), que son en realidad los que proporcionan los servicios de autenticación y autorización.

Lógicamente, como cualquier otro producto, AD DS ha ido mejorando con el tiempo y Microsoft ha ido incluyendo más servicios adicionales.

2.5.1. Servicios adicionales de AD DS.

- **Active Directory Lightweight Directory Services. (AD LDS)**. Se trata de una versión ligera de los servicios de dominio que aporta simplicidad y unas funcionalidades básicas sin necesidad de controladores de dominio. Muy práctico en caso de empresas o entornos pequeños.
- **Active Directory Certificate Services. (AD CS)**. Son los servicios que nos permiten el uso de los certificados digitales y que además admiten la infraestructura de clave pública o (PKI – Public Key Infrastructure) en inglés. Este servicio nos habilita para gestionar las

credenciales de clave pública para conseguir el cifrado, en vez de tener que recurrir a opciones externas.

- **Active Directory Federation Services. (AD FS)**. Aporta un servicio de inicio de sesión único en la web, de tal manera que una empresa puede autenticarse en su propia red y tener autorización al mismo tiempo para accedes a la red de otra empresa si así lo tiene permitido.
- **Active Directory Rights Management Services. (AD RMS)**. En este caso nos encontramos con un avance muy importante en la gestión de permisos y autorizaciones en lo que a archivos o documentos se refiere, ya que los permisos y restricciones se adjuntan al documento y no al usuario.

2.5.2. Estructura AD DS.

- **Bosque**. Se trata del nivel más alto de la jerarquía dentro de la organización y también se trata del límite de seguridad. El bosque permite la delegación de autoridad frente a los administradores, de tal forma que se pueden delegar las tareas de administración a un administrador con acceso total pero solo a un grupo de recursos del bosque. Es muy importante tener en cuenta que toda la información del bosque se almacena en todos los controladores de dominio de todos los dominios del bosque. Cuando se realiza por primera vez la implantación de un AD DS el primer servidor en ser instalado es el "dominio raíz" y su nombre se asignará automáticamente al bosque.
- **Árbol**. Es un conjunto de dominios que comparten el mismo espacio de nombre raíz. Es decir, son aquellos nombres de dominio que se van creando según las necesidades de la organización y que pueden tener, o una relación de padre/hijo con otro dominio de la organización, o ser un árbol distinto dentro del bosque. Importante, no son límites de seguridad o replicación.
- **Dominio**. Como ya se ha comentado anteriormente, cada bosque posee un dominio raíz y se pueden crear dominios adicionales que permiten particionar el bosque. El dominio limita la replicación de AD DS sólo a los controladores que están en su interior. Este es el

principal objetivo de dividir en dominios, controlar la replicación. Esto permite ahorrar y controlar el ancho de banda y limitar la probabilidad de ataques en la información compartida.

Cada controlador de dominio contiene una copia idéntica de la base de datos de AD DS de su dominio.

- **Unidad Organizativa (OU – Organizational Unit)**. Permiten agrupar la autoridad sobre un subconjunto de recursos de un dominio, proporcionando un límite de seguridad para los privilegios y autorización elevados, pero es importante saber que no limita la replicación de objetos de AD DS como en el caso de los dominios.

  Se usan para delegar el control dentro de agrupaciones funcionales, implementar y limitar la seguridad y los roles entre los grupos.

2.5.3. Controladores de dominio.

Debido a la importancia de este concepto es preferible tratarlo de manera autónoma y específica, sacándolo de la estructura de AD DS para explicarlo un poco más en profundidad. En definitiva, los controladores de dominio, en el caso de AD DS, son servidores de Windows que poseen la base de datos de AD DS y ejecutan las funciones y servicios relacionados con AD DS.

Es importante entender que el controlador de dominio almacena una copia de la base de datos de AD DS que contiene toda la información sobre los objetos dentro del mismo dominio junto con un esquema de todo el bosque al que pertenece el dominio del que es controlador. En ningún caso, un controlador de dominio puede almacenar información perteneciente a otro bosque diferente, aunque se encuentren en la misma red.

Funciones de los controladores de dominio:

- Funciones especiales de controlador de dominio. Son funciones que no estarán disponibles para todos los controladores del dominio, sino que se establecen normalmente en el primer controlador de dominio que se instala y que realizará funciones de maestro.

- Maestro de esquema. Existe uno por bosque y contiene el esquema del bosque que usaran el resto de los controladores de dominio.
- Maestro de nombres de dominio. Existe uno por bosque, de esta forma se garantiza que los nombres de todos los objetos sean únicos, algo muy importante dentro de la organización del dominio a la hora de poder identificar unívocamente a todos los recursos que contiene.
- Maestro de infraestructura. Existe uno por dominio, su función principal es almacenar los objetos eliminados y permitir el rastreo de objetos de otros dominios.
- Maestro del identificador relativo. Uno por dominio, gestiona los identificadores de seguridad únicos (SID – Security IDentifier) en todo el dominio.
- Emulador de controlador de dominio primario (PDC – Primary Domain Controller). En versiones anteriores de AD DS existía la función de PDC que era realizada por un único controlador de dominio en todo el dominio. Se ha mantenido esta emulación para garantizar la compatibilidad con versiones anteriores.
- Almacén de datos. Se encarga del almacenamiento de la información en cualquier controlador de dominio. Se compone de tres capas:
    - Capa inferior. La propia base de datos.
    - Capa media. Formada por:
        - Componentes de servicio.
        - Agente del sistema de directorio.
        - Capa de base de datos.
        - Motor de almacenamiento.
    - Capa superior. Formada por:
        - Servicio de almacenamiento del directorio.
        - El LDAP (Lightweight Directory Access Protocol).
        - Interfaz de replicación.
        - El API de mensajería.
        - Administrador de cuentas (SAM – Security Account Manager).

2.5.4. Replicación en AD DS.

La replicación es uno de los conceptos más importantes a la hora de hacer un diseño de un sistema de AD DS, ya que tendrá un impacto muy grande en las comunicaciones y su ancho de banda, por lo que se debe tener muy bien dimensionado y meditado en que ubicaciones de la organización se colocan los controladores de dominio.

Si se parte de la base de que, tener varios controladores de dominio en nuestro dominio es necesario si se quiere tener asegurado que nuestro dominio funcione correctamente, que sea seguro y tolerante a fallos. Pero que, para conseguir esto, todos los controladores de dominio tienen que poseer una copia de la base de datos del dominio, se puede decir que la replicación es la que se encarga de que cada controlador tenga una copia completa y exacta de la base de datos del dominio. Esta es, en definitiva, la función principal del proceso de replicación. Este proceso de replicación utiliza un sistema de extracción, es decir, no es que los controladores envíen los datos a otros controladores, sino que son los controladores que se quieren actualizar los que extraen la información del resto de controladores. Esto se hace de forma predeterminada cada 15 segundos. Y solo entre los controladores del mismo dominio.

Si por circunstancias, en alguna sede disponemos de conexiones lentas y rápidas, podemos planificar un "coste" para cada conexión de tal forma que se intente siempre replicar por la más rápida. Es por eso, que es importante tener en cuenta nuestras infraestructuras de comunicaciones entre sedes a la hora de colocar controladores de dominio repartidos por las sedes planificando con cuidado su ubicación en función del ancho de banda disponible y del que se va a usar en el proceso de replicación y su efecto en el rendimiento de las comunicaciones para el resto de los servicios que se utilizan en las sedes y que afectarán directamente al rendimiento de los trabajadores.

2.5.5. Sistema de nombres de dominio. (DNS – Domain Name System).

Se debe tener en cuenta que existe una relación muy estrecha entre los servicios de directorio y el Sistema de Nombres de Dominio o (DNS – Domain Name System), ya que el AD DS se integra directamente con el DNS de tal forma que se podría decir, tal y como explica Javier Olivares

Serrano en su libro (Serrano, 2017), que: "cualquier dominio de AD DS es por fuerza un dominio DNS, pero todo dominio DNS no es por necesidad un dominio AD DS". Aunque se sale del ámbito de este trabajo, debido a la importancia del DNS en la infraestructura de AD DS, a continuación, se expondrá una breve explicación sobre algunos de los conceptos que nos serán útiles para comprender el desarrollo de este trabajo.

DNS fue definido por el IETF (Internet Engineering Task Force) como un protocolo estándar de resolución de nombres. Actualmente descrito por Paul Mockapetris en las RFC 1034 (RFC-1034 (IETF) Paul Mockapetris, 1987) y 1035 (RFC-1035 (IETF) Paul Mockapetris, 1987) que se basaron en las RFC's 882 y 883 escritas por el mismo y en las que propuso los fundamentos de los servicios de nombres de dominio. Y que de una manera sencilla podemos definir como un servicio que permite resolver los nombres de los equipos pertenecientes a dominios DNS.

En realidad, se trata de una base de datos distribuida y jerárquica, concebida y distribuida entre los distintos servidores DNS que componen la instalación. Por defecto contiene un nivel raíz (.) y los dominios de primer nivel (com, gov, org, etc), estos últimos gestionados por el ICANN (Internet Corporation for Assigned Names and Numbers). El resto de los niveles son gestionados por las empresas a las que son asignados, pero siempre estarán asociados a un dominio de primer nivel.

Arquitectura básica:

- Espacio de nombres de dominio (DN – Domain Namespace). Se compone de registros de recursos (RR – Resource Records) y son los que permiten identificar cada recurso del dominio con sus tipos y datos asociados, normalmente un nombre relacionado con una dirección IP. Existen distintos tipos de registros en función del objeto al que describen.
- Servidores de nombres DNS (DNS Name Servers). Son los equipos que ofrecen el servicio DNS y ejecutan y resuelven las consultas recibidas de otros equipos. En caso de no poder resolver, reenvían la solicitud a otros servidores de más nivel para que la resuelvan. Contienen todo o parte del espacio de nombres y utilizan los Nombres de Dominio totalmente Cualificados (FQDN – Fully Qualified Domain Names), en lo que a nombres se

refiere se recomienda respetar la RFC-1123 (IETF - RFC-1123) sobre convecciones de nombre de hosts.

- Clientes DNS (DNS Resolvers o DNR). Son los clientes que realizan las consultas a los servidores DNS.

Tal y como se comentó con anterioridad, AD DS contiene información de todos los objetos del dominio en su base de datos, y en el caso concreto de los controladores de dominio, se utiliza el sistema de nombres de dominio (DNS) para situarlos, de ahí su importancia. Como se ha explicado, dentro de AD DS, cada dominio tiene un nombre de dominio DNS y cada equipo, (pc, portátil, Tablet, etc.), que se conecta al dominio cuenta con su propio nombre DNS dentro del mismo.

Cuando se hace referencia a un objeto dentro de un dominio se hace normalmente usando su FQDN, por lo hay que identificar ese nombre (FQDN) con una dirección IP que pueda ser utilizada por el resto de los protocolos de comunicaciones para localizar el equipo al que se quiere hacer referencia.

2.6. Integración de AD DS con Azure.

La parte correspondiente a la solución en la nube, ya se tiene implantada en nuestra organización, por lo que no vamos a entrar en detalles de cómo implantar este tipo de sistema. Pero, lo que si interesa de verdad es cómo se puede conectar el servicio AD DS que se implantará nuevo, con el actual Azure AD para que, en conjunto, se obtenga el sistema de “autentificación hibrida”, que como se recordará, es uno de los objetivos principales del presente trabajo.

Afortunadamente, el trabajo se sustenta sobre la base de usar dos servicios proporcionados por el mismo desarrollador, Microsoft, por lo que la integración y la comunicación están de sobra garantizadas, disponiendo de todas las herramientas necesarias para que ambos entornos funcionen a la perfección como uno solo y que ese funcionamiento sea totalmente transparente para el usuario final.

Además, los administradores contarán con las suficientes herramientas y asistentes que les ayudarán en su operación diaria una vez que los sistemas se encuentren conectados y funcionando.

Pero ¿qué es en realidad Azure Active Directory (Azure AD) ?, pues simplemente se trata de un servicio de autenticación con la misma filosofía que el ya tratado AD DS, pero en esta ocasión ubicado en la nube. Aunque se puede obtener información completa en (Microsoft Azure AD, 2021), se enumeran a continuación los elementos básicos que necesita la arquitectura para implementar esta conexión entre los dos servicios:

- **Servicio de Azure AD**, que no es otra cosa que nuestro Azure AD instalado y configurado en la nube y que actúa como nuestro servicio de autenticación en la nube. Esta instancia tendrá una copia de los objetos de nuestro AD DS local.
- **Servidor local de AD DS**. Es el servicio AD DS local que se configura on-premise en nuestro data center y que permitirá la autenticación de nuestros usuarios de forma local.
- **Servidor de Azure AD Connect Sync**, (Microsoft Azure AD Connect, 2020). Será un equipo local en el que se deberá instalar el servicio de sincronización de Azure AD connect. En realidad, este será el servicio que se encargue de mantener sincronizada la información de nuestros objetos de AD DS local con el Azure AD en la nube, propagando los cambios entre uno y otro servicio.

De una manera gráfica y sencilla se puede reflejar esta arquitectura con la siguiente imagen:

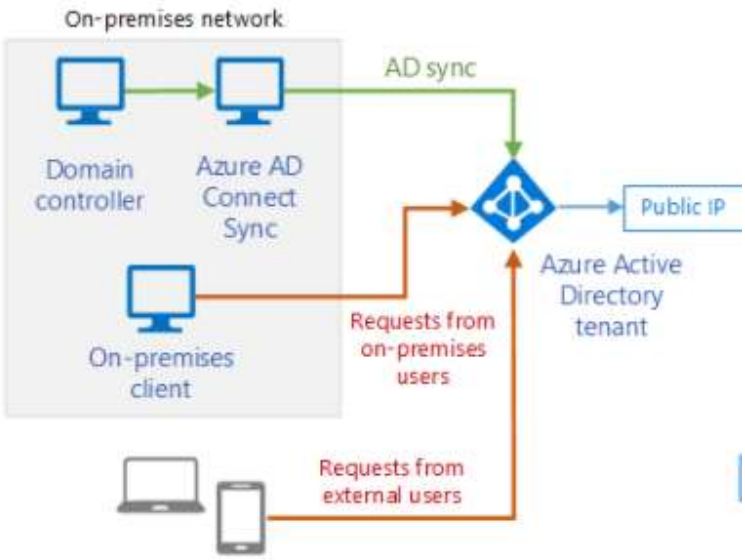

Ilustración 9. Arquitectura Azure. Fuente Microsoft.

De igual manera que en el caso de AD DS, con Azure AD Connect se dispone de la posibilidad de utilizar distintas topologías, a continuación, hacemos un resumen de las que se pueden implantar:

- Un único bosque, un único directorio de Azure AD.
- Varios bosques, un único directorio de Azure AD.
- Varios bosques: topologías independientes.
- Varios directorios de Azure AD.

El hecho de usar un tipo de topología u otro dependerá en gran medida del tamaño de la organización, tanto a nivel de número de usuarios como de ubicaciones geográficas. En nuestro caso, y en lo que se refiere a este trabajo, se utilizará la topología de único bosque con un único directorio de Azure AD, por ser el que mejor se adapta a nuestra estructura y el que ofrece una manera más sencilla de mantenimiento y administración.

2.6.1. Azure AD Connect.

Para conseguir el objetivo de este trabajo, autenticación hibrida con Microsoft AD DS y Azure AD, se hace necesario conectar con alguna herramienta nuestro AD DS local con el Azure AD ubicado en la nube, esa herramienta es el **Azure AD Connect**, que ofrece las siguientes características:

- Sincronización de hash de contraseñas. Proporciona un método de inicio de sesión que sincroniza el hash de la contraseña de un usuario de AD local con Azure AD.
- Autenticación de paso a través. Permite a los usuarios el uso de la misma contraseña de forma local y en la nube sin necesidad de un entorno federado.
- Integración de federación. La federación es una parte opcional de Azure AD Connect que puede utilizarse para configurar un entorno hibrido.
- Sincronización. Es el proceso responsable de la creación de usuarios, grupos y otros objetos. También se asegura de que la información de todos los objetos del entorno local coincida con la de la nube.
- Seguimiento de estado. Conocido como Azure AD Connect Health, proporciona la herramienta necesaria para realizar la supervisión desde una ubicación central.

Azure AD Connect ofrece tres opciones para configurar la autenticación hibrida:

- **Sincronización de hash de contraseñas de Azure AD**. (PHS – Password Hash Synchronization). Este método sincroniza el hash de contraseña de un usuario local de AD DS con una instancia de Azure AD en la nube. Permite reducir el número de contraseñas que tienen que recordar los usuarios.
- **Autenticación de paso a través de Azure AD**. (PTA – Pass-Through Authentication). Como en el caso anterior, también permite a los usuarios el uso de la misma contraseña en la nube y en local. Cuando un usuario inicia sesión paso a través valida sus contraseñas directamente con el AD DS local. Pero además de permitir el uso de una única contraseña, en este caso, nos permitirá aplicar directivas locales de seguridad y contraseñas a nuestros usuarios.

Otro aspecto para tener en cuenta es que permitirá usar la característica de inicio de sesión único de conexión directa (SSO – Single Sign On). Para que cuando los usuarios accedan a las aplicaciones es sus máquinas corporativas dentro de la red de la empresa, no tengan que escribir su contraseña para iniciar sesión.

- **Autenticación federada**. (AD FS – Active Directory Federation Services). Consiste en una colección de dominios entre los que se han establecido relaciones de confianza. Se puede federar nuestro entorno local con Azure AD y usar esta federación para la autenticación. Con este método toda la autenticación se realiza de forma local y permite a los administradores aplicar medidas de seguridad y niveles de control de acceso más rigurosos.

➢ Funcionamiento del PHS.

Como se verá más adelante en este trabajo, la solución adoptada estará basada en PHS, de ahí que se haya considerado necesario profundizar un poco más en su funcionamiento para entender

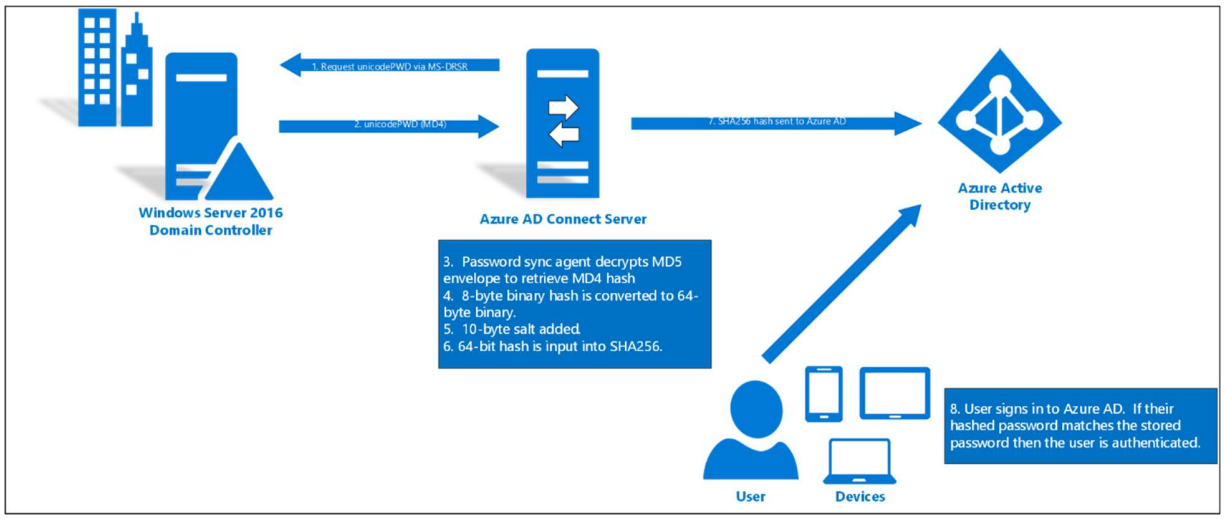

Ilustración 10. PHS authentication. Fuente Microsoft.

cómo actúa este tipo de autenticación:

1. Cada cierto tiempo (dos minutos), el agente de sincronización en AD Connect solicita los hashes de contraseña almacenados en el controlador de dominio AD. Utilizando el

protocolo de replicación MS-DRSR (MicroSoft Directory Replication Service Remote protocol), (DRSR, 2021). Esta replicación se realiza con una cuenta que posee los permisos necesarios para replicar cambios en todos los AD.

2. Cuando el controlador de dominio recibe la petición, cifra el hash de contraseña MD4, (IETF RFC-1320, 1992), mediante un hash de MD5, (IETF RFC-1321, 1992), de la clave de sesión RPC y un valor secreto. A continuación, envía la información al agente mediante RPC (Remote Procedure Call). El controlador también envía el valor secreto utilizando MS-DRSR para que el agente pueda abrir el sobre MD5.
3. El agente de sincronización recibe el sobre cifrado y el valor secreto, con este último descifra los datos y obtiene el hash MD4.
4. El agente de sincronización de hash amplía el hash de 16 bytes a 64 bytes.
5. El agente de sincronización agrega un valor secreto por cada usuario de 10 bytes al de 64 bytes.
6. El agente combina el hash MD4 con el generado en el punto anterior y lo pasa por la función PBKDF2, establecida en el RFC-2898 (IETF RFC-2898, 2000). Utilizando 1000 interacciones del HMAC-SHA256, (HMAC – Hashed Message Authentication Code) y (SHA – Secure Hash Algorithm), como algoritmo de hashing.
7. El agente obtiene un hash de 32 bytes combinando el valor secreto del usuario (paso 5) y el número de las interacciones de SHA256 del paso 6 y lo transmite para su uso al Azure AD mediante TLS (Transport Layer Security).
8. Cuando el usuario intenta identificarse utiliza el mismo proceso: MD4+valor secreto+PNKDF2+HMAC-SHA256. Si el resultado coincide con lo que tiene almacenado Azure AD, el usuario ha introducido la contraseña correcta y es autenticado.

- Ventajas de uso de PHS con Azure AD Connect.

Las principales ventajas que presenta este método son:

- Mayor seguridad.
- Posibilidad de recibir alertas de problemas críticos de AD.

- Fácil de implementar y administrar.
- Métricas de rendimiento avanzadas.
- Mejora de la experiencia de usuario (UX- User eXperience)
- Incluido en la licencia de suscripción de Azure.

3. DISEÑO DE LA PROPUESTA

3.1. Fundamentos jurídicos.

La base normativa que afecta al desarrollo de las actividades y competencias de la Diputación Provincial de Guadalajara, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. (Ley 39/2015, 2015)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. (Ley 40/2015, 2015)
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado por Real Decreto 951/2015, de 23 de octubre. (ENS 3/2010, 2010)
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. (Resolución de 13 de octubre de 2016, 2016)
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. (Resolución de 7 de octubre de 2016, 2016)
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. (Resolución de 27 de marzo de 2018, 2018)

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad. (Resolución de 13 de abril de 2018, 2018)
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. (Real Decreto 4/2010, 2010)
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. (Real Decreto 1671/2009, 2009)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (Ley Orgánica 3/2018, 2018)
- Artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (Ley Orgánica 15/1999, 1999)
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD). (• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (Ley 34/2002, 2002)
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. (Ley 37/2007, 2007)
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. (Ley 19/2013, 2013)
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. (Ley 25/2007, 2007)
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. (Ley 56/2007, 2007)

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. (Ley 9/2014, 2014)
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril. (Ley 11/1999, 1999)

Las referencias más importantes que motivan la realización de este trabajo son:

- La "*Disposición transitoria. Adecuación de sistemas*" del Real Decreto 3/2010, de 8 de enero, (ENS 3/2010, 2010), por el que se regula el Esquena Nacional de Seguridad (ENS) en el ámbito de la Administración Pública, que establece:

  1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

  2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

  El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

  3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.

  Este plazo venció en enero de 2014.

- Posteriormente, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, estableció un nuevo plazo para la implantación

de las nuevas medidas, recogido también en su "*Disposición transitoria única. Adecuación de sistemas*":

Las entidades incluidas dentro en el ámbito de aplicación del presente real decreto dispondrán de un plazo de veinticuatro meses contados a partir de la fecha de la entrada en vigor del presente real decreto, para la adecuación de sus sistemas a lo dispuesto en el mismo.

Este plazo venció en noviembre de 2017.

3.2. Objetivos

El presente trabajo se enmarca en un proyecto mucho más grande que intenta adaptar el entorno de las nuevas tecnologías y desarrollar un **Plan de transformación digital** dentro de la Diputación de Guadalajara (DG), en cumplimiento de la normativa actual y sobre todo del ENS en lo que a seguridad de los sistemas de información se refiere.

Dentro de este Plan se ven involucrados, no solo sistemas de información relacionados con las tecnologías de la información, sino que abarca al total de la organización, contando con el compromiso aceptado y confirmado de la Alta Dirección, en lo que se refiere a nuevos modelos de procesos, tratamiento de la información escrita, archivado de documentos físicos, utilización de los espacios comunes y protección de la información que se encuentra en papel, etc.

Como parte importante de este plan de transformación digital se hace necesario crear el entorno de confianza y confiabilidad necesario y adecuar nuestros sistemas de información a lo establecido en el ENS. **Por lo que el objetivo principal** de este trabajo es **implementar un entorno basado en Microsoft Windows Server 2019 Datacenter** y con una arquitectura de **nube híbrida conectando con Azure AD**, que permita la correcta autenticación de usuarios internos y externos a la vez que ofrezca todos los niveles de seguridad tal y como se establecen en el ENS y más concretamente en la guía del CCN-STIC 870A Implementación del ENS en Windows Server 2012 R2, (CCN-STIC-870A, 2020).

Dentro de las tareas que se deben plantear como organización pública, y aunque ya se ha dicho que abarca otras partes de la organización, como base importante del proyecto se encuentra todo lo relacionado con los Sistemas de Información y las Nuevas Tecnologías que se emplean en la DG, y entre otras se pueden destacar las siguientes tareas a realizar:

- TAREAS PREVIAS.
    - Generar un mapa lógico de la red de la Diputación Provincial de Guadalajara que incluya todos sus centros. Inventariando toda la electrónica de red que da sustento a nuestras comunicaciones.
    - Estudio y rediseño del direccionamiento de red aplicando los criterios establecidos en la normativa establecida en el Plan de direccionamiento e interconexión de redes en la Administración, (CTT - Plan direccionamiento AAPP, 2021).
- TAREAS DEL PROYECTO.
    - Diseño e implantación de Directorio Activo.
    - Implantar la conexión con Azure AD en la nube, utilizando Microsoft Acure AD Connect que permita establecer un modelo de autenticación hibrida.
    - Establecer los pasos necesarios, a desarrollar con posterioridad al proyecto, para dejar configurado un entorno con todos los servicios funcionando y que permitan la creación de un entorno totalmente seguro y confiable además de, fácilmente administrable.

En resumen, se trata de un Plan de Adecuación enmarcado en la normativa vigente y que obliga a implantar las medidas preventivas y reactivas en nuestra organización, que consigan proteger y preservar la confidencialidad, la disponibilidad, e integridad de la información. Dichas medidas deberán ser acordes a la importancia que la información contenida en los distintos sistemas de información de la DG y su relevancia e importancia tanto para la propia organización como para los usuarios que depositan su información en nuestros sistemas por el simple hecho de utilizar nuestros servicios y procedimientos.

Ilustración 11. Control de acceso y copias. Fuente INCIBE.

Ilustración 12. Seguridad empleados. Fuente INCIBE.

En términos de seguridad, de sobra es conocida la frase: **«El usuario es el eslabón más IMPORTANTE de la cadena de la seguridad»**

Estos son los protagonistas reales de este trabajo, dotar a los usuarios de una herramienta confiable que les permita utilizar sus equipos de procesos de información con las garantías adecuadas y que a su vez esta confianza propia se extienda al exterior y a los usuarios

externos, generando el entorno de confianza necesario.

3.3. Justificación solución propuesta.

Un directorio es una base de datos jerárquica que contiene información relativa a los objetos a los que hace referencia. En este caso se hace referencia a todos los objetos que intervienen en nuestra red de comunicaciones, usuarios, equipos, grupos, políticas de seguridad, recursos de red, impresoras, etc. Todos estos objetos, que en un momento dado están disponibles en nuestro entorno de red, pueden ser requeridos por un usuario que necesita, por ejemplo: imprimir por una impresora de red o acceder a un repositorio de ficheros. Sería lógico pensar que ese usuario necesita de una herramienta que les proporcione un acceso sencillo y rápido a todos los recursos/objetos a los que, según sus permisos o privilegios, tiene acceso. En este punto es donde entra en funcionamiento un Servicio de Directorio, como el que se va a implantar en este trabajo.

Como ya se indicó en el estado del arte, en el mercado existen muchos servicios de directorio, algunos gratuitos y otros no, pero que cumplen a la perfección sus funciones. La siguiente pregunta que hay que hacerse es: ¿En base a qué se puede realizar la elección? Pues bien, esta elección puede basarse en muchos aspectos distintos, pero los más importantes, y los que se han tenido en cuenta en el presente trabajo son:

- Arquitectura actual.
    - Costes de implantación y reutilización de lo existente.
    - Posibilidad de conexión con la infraestructura actualmente usada.
    - Beneficios que aporta a la situación actual.
    - Licencias ya en uso compatibles con la solución.
- Conocimiento del servicio de directorio y no necesidad de formación de los técnicos.
- Facilidad de adaptación de los usuarios a las nuevas capacidades.
- Entorno amigable para los usuarios.
- Ofrecer una UX adecuada, que permita a los usuarios involucrarse en el uso de los nuevos servicios implantados.

Por todo ello, la solución elegida para implantar en este trabajo es el **Servicio de Dominio de Directorio Activo de Microsoft, (AD DS, en inglés Active Directory Domain Services)**, en un entorno de base con el sistema operativo Microsoft Windows Server 2019, conectado mediante **Microsoft Azure AD Connect**, con el servicio de **Microsoft Azure AD**, para ofrecer autenticación y autorización hibrida en la nube.

Este servicio de directorio ofrece, entre otras, las siguientes funcionalidades:

- Publicar a nivel empresarial todos los servicios necesarios para el buen funcionamiento de la organización.
- Permite a los administradores tener un servicio de seguridad global, que permite de una manera muy sencilla, garantizar un alto nivel de seguridad de acceso y de confidencialidad de los datos sensibles.
- En la situación de aumento del teletrabajo, permite utilizar listas de control de acceso a un firewall en función de la autenticación del usuario a través de una conexión VPN. Permitiendo o no al usuario acceder de forma remota a los recursos de red privados.
- El directorio permite la distribución de forma global, lo que garantiza que todos los usuarios de la red podrán utilizar todos los servicios de seguridad y búsqueda de AD DS.
- Tolerancia a fallos, permitiendo la replicación de las bases de datos de directorio en distintos servidores distribuidos geográficamente en distintos sitios. Lo que permite que, ante la desaparición de un determinado servidor de directorio, otro en la red, pueda ocupar sus funciones y seguir dando soporte a los usuarios.
- Tener una única directiva de contraseñas y bloqueo de cuentas de usuario del dominio. Complejidad, caducidad de las contraseñas, etc.

En resumen, gracias a la implantación del directorio activo como servicio de autenticación, el control de los accesos a los equipos informáticos, (inicios de sesión), el acceso a los distintos recursos de red, (servidores on-premise y en la nube), el acceso a las distintas aplicaciones corporativas, (RRHH, obras, presupuestos, etc.), se dispondrá de la herramienta necesaria para

saber en todo momento quién, cuando, desde donde y como accede a los sistemas de información y recursos de la organización. En definitiva, asegurar la:

- Autenticidad. Se refiere al hecho de que la información sea auténtica.
- Confidencialidad. Que personas no autorizadas no conozcan la información.
- Integridad. Que la información no ha sido modificada o alterada.
- Disponibilidad. Que la información esté disponible cuando realmente se necesita.
- Trazabilidad. Que el tratamiento de la información es rastreable a posteriori.

En la actualidad, el uso de teletrabajo y acceso remoto a aplicaciones se ha hecho más necesario que nunca, las empresas y las administraciones públicas han de implementar aquellas herramientas y canales de uso más seguros de estas nuevas formas de comunicarnos, trabajar y relacionarnos electrónicamente.

Es por ello por lo que se necesita un sistema de autenticación y asignación de permisos de acceso a recursos y aplicaciones remotas, que sea capaz de aportar fluidez y rapidez, al mismo tiempo que debe tratarse de una infraestructura segura. Para no sobrecargar de peticiones externas los servidores “on-premise”, es recomendable que, en este entorno, se cuente con una autenticación en la nube, además de la característica “on-premise”. De esta forma, cuando un usuario requiera autenticarse, si está dentro del entorno de la organización podrá hacerlo rápida y eficientemente dentro de su red interna. Pero, cuando ese mismo usuario se encuentre en su domicilio o en la sede de algún cliente o proveedor, tendrá a su disposición el sistema de autenticación en la nube, de igual manera rápido y eficaz. De ahí que la solución propuesta en este trabajo incluya la implantación de un sistema de nube híbrida.

3.4. Metodología.

Confiando claramente en la experiencia de los técnicos de la DG y del conocimiento que posee el propio proveedor de las soluciones: Microsoft. Se ha decidido que la mejor metodología para llevar a buen término este proyecto es la propia creada por Microsoft en su capítulo “Planeación y diseño de AD DS” dentro de su documento de Servicios de Dominio de Active Directory,

(Microsoft AD DS, 2017). Adecuando en lo que sea necesario dicha metodología a la infraestructura, servicios y tamaño que se presentan en la Diputación de Guadalajara.

En ese documento de Microsoft se plantea que todo proyecto de implementación de AD DS debería constar, mínimo, de tres fases importantes:

- Fase de diseño. En esta fase el equipo de diseño recopilará los requisitos y creará el diseño de AD DS que mejor se adapta a la organización y sus necesidades.
- Fase de implementación. En esta fase el equipo de implementación desplegará el diseño anteriormente probado en un entorno de laboratorio y una vez constatado el correcto y deseado funcionamiento se desplegará en el entorno de producción.
- Fase de operaciones. Esta fase consiste en que el equipo de operaciones se haga responsable del mantenimiento del AD DS y de su correcto funcionamiento.

En este caso, y debido al tamaño de los recursos del Servicio de TI, los equipos de diseño, de implementación y de operaciones estarán formados por los mismos integrantes. Una parte correspondiente a personal de TI de la propia Diputación y otra parte formada por 2 técnicos de la empresa adjudicataria del contrato de suministro de la infraestructura y licencias necesarias para la implantación de este trabajo. Que estarán en posesión de las necesarias certificaciones a nivel de Microsoft que aseguren un conocimiento detallado de los servicios a implantar, así como de la experiencia certificada en la resolución de implantaciones acordes con el ámbito de este trabajo.

Además, y añadiéndolo como parte final, se incluirá en este trabajo una última fase de formación al personal de TI de la Diputación, con el objeto de mejorar y actualizar sus conocimientos en lo que a estos servicios se refiere. Dicha fase de formación quedará como parte de los futuros trabajos a corto plazo y se ejecutará a la finalización de la fase de operaciones.

3.4.1. Fase de diseño.

Como en casi todos los proyectos, la fase de diseño suele ser la más importante y de la que depende el buen desenlace del resto de fases del proyecto. Un buen diseño lógico del dominio

va a permitir sacar el máximo provecho de nuestro AD DS, de sus servicios y de sus características, pero lo más importante es que se tendrá una herramienta centralizada óptima y sencilla que facilitará la gestión de nuestros objetos de AD DS.

Este diseño permitirá también, optimizar la fase de implementación e integrar de manera sencilla nuestro AD DS con otras aplicaciones ya sean de Microsoft o no.

- Diseño de la estructura lógica de AD DS.
  - Determinar participantes: 1_1_DiseñoLogico_Participantes.doc
    - Arquitecto de proyecto. Este perfil administrará la toma de decisiones de diseño e implementación de AD DS, proporcionando conocimientos técnicos necesarios para el correcto diseño e implementación. Ajustará el diseño del AD DS a las necesidades de la organización y actuará como punto de unión y consenso entre los equipos de diseño, implementación y operaciones.
    - Jefe de proyecto. Perfil muy ligado también a la organización y conocimiento de las necesidades de esta. Se encargará de que todo el proyecto se vaya cumpliendo, tanto a nivel de presupuesto, como de ejecución. Garantizando que, en cada momento o fase de este, todos los participantes que deben actuar se encuentran haciéndolo. Sirve también para establecer la comunicación entre los equipos del proyecto y la parte de Gobierno de la organización.
    - Propietarios y administradores de los datos. Dos perfiles que en organizaciones no muy grandes pueden desempeñar la misma persona. Se trata de que, como administradores, garanticen el correcto funcionamiento y evolución del AD DS en la organización una vez desplegado y, como propietarios de los datos, tendrán que hacerse cargo del mantenimiento de la información almacenada en el AD DS, cuentas de usuario y equipo, recursos locales, etc. Velando porque toda esta información se encuentre actualizada y al día y coincida con los requerimientos de funcionamiento de la organización.

- Propietario del bosque. Responsable de implementar el dominio raíz de cada bosque, así como del primer controlador de dominio. Delegar la autoridad administrativa dentro del AD DS. Autorizar y comprobar cambios del esquema. Implementar y valorar todas aquellas políticas de grupo que se apliquen a nivel de dominio.
- Propietario de AD DS. Deberá tener un conocimiento profundo de la infraestructura de DNS de la organización, ya que participará activamente en el diseño y creación del espacio de nombres de AD. Administrará por tanto toda la infraestructura del DNS incluido es servidor DNS y los datos.
- Propietario del sitio. En esta ocasión se trata de una persona que debe tener un conocimiento profundo del diseño de la red de comunicaciones de la organización. Permitiéndole tomar decisiones de diseño del sitio en lo que a comunicaciones y actualizaciones entre sedes se refiere.
- Propietario de la Unidad Organizativa. Se encargará de administrar los datos de la unidad o unidades organizativas (OU) que le correspondan.
- Equipo de diseño y equipo de implementación. Son las personas que participarán activamente tanto en la obtención de datos para el diseño como para la posterior implementación.

En resumen, se trata de definir claramente los participantes en la totalidad del proceso de implantación del AD DS, de tal forma que todos ellos tengas claras sus responsabilidades y nivel de participación, tanto a nivel de diseño, implementación como posterior mantenimiento del servicio y los datos.

❖ Diseño del bosque. 1.2_DiseñoBosque.doc

Este punto, que puede parecer sencillo, necesita de una planeación y obtención de requisitos muy importantes, porque de este punto van a depender el resto de las fases del proyecto y de su correcta adaptación a nuestra organización. En realidad, se trata de dos pasos:

- Identificar requisitos del bosque. 1.2.1_RequisitosBosque.doc

  Tanto los requisitos de la estructura organizativa como operativos, aplicaciones para unidades de negocio específicas. Deberemos tener en cuenta dos criterios importantes: Qué ámbito de autoridad de administración necesitamos y si deseamos autonomía frente aislamiento.

  Conceptos muy importantes:

  Autonomía. Implica independencia, pero no el control exclusivo sobre un recurso. Existen administradores con más privilegios que pueden controlar estos recursos.

  Aislamiento. Implica independencia, pero también control exclusivo de los recursos. Ningún otro administrador puede acceder ni cambiar nada que afecte a los recursos aislados.

- Determinar el número de bosques necesarios. Este punto dependerá de los requisitos anteriormente analizados, ya que los requisitos de aislamiento limitan mucho las posibilidades de diseño y sobre todo en cuanto al número de bosques. También se deberá tener en cuenta que el modelo más sencillo es el de bosque único, tanto por ser el más rentable como por ser el más fácil de implementar y mantener.

Llegados a este punto sería conveniente explicar brevemente los modelos de diseño de bosque:

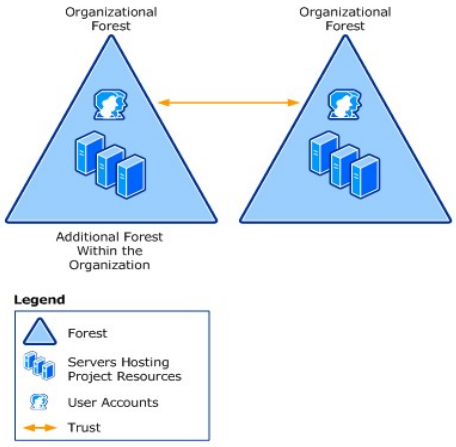

Ilustración 13.Mod.Organizacional (fuente Microsoft Docs).

Modelo Organizacional. En este modelo existirá uno o varios bosques cada uno de ellos conteniendo tanto usuarios como recursos, en este caso podemos obtener autonomía de servicio, aislamiento de servicio o aislamiendo de datos. Se pueden establecer relaciones de confianza entre distintos bosques si fuera necesario acceder a recursos en otros bosques.

Cada AD requiere al menos UN bosque organizacional.

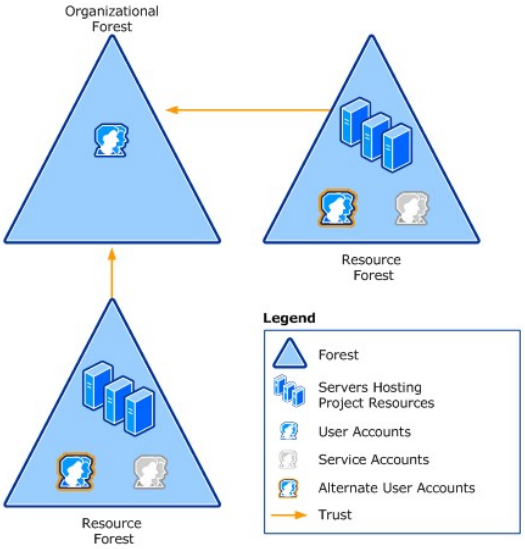

Ilustración 14. Mod.Recursos (fuente Microsoft Docs).

Modelo de Recursos. Este modelo se compone de un bosque que almacenará los recursos y solo los recursos. Únicamente podrá contener los usuarios necesarios para realizar la administración. Y por otro lado estarán el resto de los bosques con usuarios y recursos propios. Entre todos será necesario establecer las relaciones de confianza necesarias para el correcto acceso entre bosques.

Este modelo proporciona aislamiento y protege ciertas áreas de nuestra red que necesitan de mayor protección.

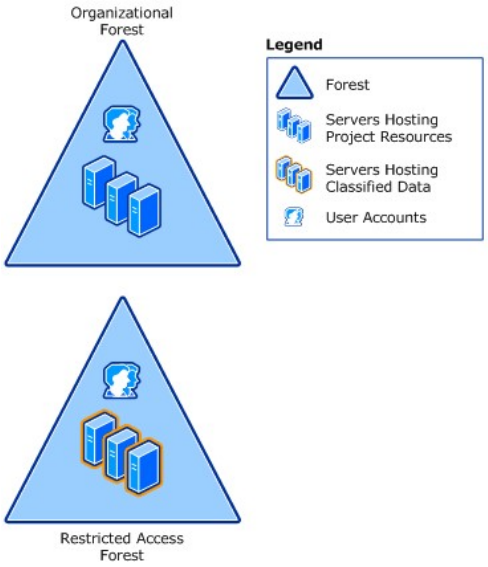

Ilustración 15. Mod. Acceso restringido. (fuente Microsoft Docs).

Modelo de Acceso restringido. Al menos tendrá como mínimo dos bosques, el bosque organizacional con su funcionamiento normal y por otro lado el bosque de acceso restringido. No existe relación de confianza entre ellos por lo que los usuarios deben tener dos cuentas y dos equipos, repartidos en cada uno de los bosques.

Es el modelo que mayor aislamiento y seguridad ofrece, pero por supuesto no falto de inconvenientes para los administradores y para los usuarios.

- Diseño del dominio. 1.3_DiseñoModeloDominio.doc.

  Para poder hacer un correcto diseño del dominio se deberán tener cuenta dos factores muy importantes:

  - La capacidad del ancho de banda de nuestra red a la hora de planificar la replicación.
  - El número de usuarios de nuestra organización.

  En esta ocasión se dispone de dos tipos de modelo:

  Modelo de dominio único. Esta es la forma más sencilla de administrar un dominio, con un dominio único de raíz con un solo dominio que contendrá a todos los usuarios y recursos de la organización. En este caso cualquier controlador podrá autenticar a los usuarios y todos los controladores pueden ser configurados como catalogo global.

  Modelo de dominio regional. Este modelo permite organizar nuestros dominios por regiones o sedes, lo que nos permitirá optimizar aquellas sedes que se conectan por WAN

a la sede principal y que, o bien por bajo ancho de banda, o bien porque implique un alto coste, queramos reducir la cantidad de tráfico entre sedes, aprovechando así el ancho de banda para los datos de uso de los usuarios.

También se puede dar el caso de empezar con un modelo de dominio único y que el crecimiento de nuestra organización requiera en un futuro la instalación de sedes remotas con no muy altas especificaciones de comunicaciones, se podrá en ese momento migrar un **modelo hibrido** en la que parte de nuestros objetos de Directorio se encuentren localizados en aquellas sedes con peores comunicaciones.

Una vez determinado el modelo a implantar, se tendrá que decidir el número de dominios que se necesitan crear. En el enlace https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/determining-the-number-of-domains-required,

se puede consultar una tabla con los cálculos aproximados que hay que tener en cuenta a la hora de decidir el número de dominios.

❖ Diseño de infraestructura DNS.

Como ya se indicó en el punto 2.5.5, la importancia del DNS cuando se implementa un AD es muy relevante. Queda fuera del alcance de este trabajo profundizar en el funcionamiento del DSN y sus características, no obstante, y debido a la repercusión que este punto tendrá sobre nuestro AD DS se considera conveniente aportar las decisiones más importantes que se tendrán que tomar en esta fase, así como una serie de documentos que podrán servir de ayuda.

- Que espacio de nombres se va a utilizar.
- Donde ubicar los controladores de dominio.
- Organizar las Zonas DNS integradas con AD.
- Como nombrar a los equipos que se unirán al dominio AD DS.

Se pueden utilizar como apoyo de los siguientes documentos:

- 1_4_1_DiseñoLogico_PlanificacónDominio.doc

- 1_4_2_DiseñoLogico_InventarioDNS

❖ Diseño de Unidades Organizativas (OU). 1_5_DiseñoLogico_UnidadesOrganizativas.doc

Las unidades organizativas (OU), permitirán delegar el control y la responsabilidad del mantenimiento de los objetos que contendrá nuestro AD DS. En esta primera aproximación se deberá pensar en aquellos grupos de objetos que van a necesitar un tratamiento independiente dentro de nuestro AD DS. Posteriormente a este primer boceto, se tendrá que ir diseñando y añadiendo otras OU's necesarias, por ejemplo, para la aplicación de políticas de grupos específicas, asignación de permisos específicos, etc.

Dependiendo de nuestra organización, se podrá asignar un rol de "propietario de OU", cuya función principal será controlar los objetos que se encuentren dentro de la OU de su responsabilidad. O bien, se podrá asignar inicialmente esa tarea a un administrador del servicio del dominio, que siempre tendrá el control.

Las OU's permiten obtener autonomía administrativa y aislamiento de los datos de otros administradores.

❖ Diseño de la topología de sitio de AD DS.

La topología de sitio de AD DS no es otra cosa sino una representación lógica de nuestra red física. Este diseño consistirá en planificar la ubicación de los controladores de dominio, los enlaces entre sitios, las subredes y subsedes. Y ayudará a utilizar de una manera mucho más eficiente las rutas que los equipos clientes usaran para hacer las consultas a nuestro AD DS. Un buen diseño de sitio aportará, entre otros, los siguientes beneficios:

- Optimizar que los equipos cliente encuentren recursos cercanos a su ubicación.
- Agendar y planificar la replicación para aquellas sedes que posean un ancho de banda limitado.
- Minimizar las tareas administrativas que se requieren para llevar a cabo el mantenimiento del sitio.

- Minimizar el coste de replicación, ahorrando en costes de comunicaciones y aprovechando al máximo el ancho de banda de nuestras conexiones WAN para tareas más productivas para los usuarios.

❖ Recopilar información de la red.

- Crear un mapa que represente la infraestructura física de nuestra red y centros a integrar en nuestro AD DS.
- Preparar un listado con nuestros enlaces y sus características de ancho de banda.
- Preparar un listado con las distintas subredes de cada uno de los centros.
- Hacer un listado de los dominios que vamos a necesitar junto con el número de usuarios de cada localización.

Se pueden utilizar los siguientes documentos:

- 1_6_1_DiseñoSitio_SitiosyEnlaces.doc
- 1_6_2_DiseñoSitio_SubredesyLocalizaciones.doc
- 1_6_3_DiseñoSitio_DominiosyUsuariosenLocalizaciones.doc

❖ Planear la ubicación del controlador de dominio.

Una vez recopilada la información del punto anterior, se dispondrá de la información necesaria para tomar las decisiones de ubicación de nuestros controladores de dominio. Es necesario que se piense adecuada y concienzudamente en la ubicación de, al menos, los siguientes servicios o roles:

- Controlador de dominio de bosque raíz. 1_7_DiseñoSitio_UbicacionControladores.doc. Sería aconsejable que este controlador se encontrara en una ubicación lo más céntrica posible en el diseño de nuestro sitio. Suele ser conveniente que se encuentre en nuestro data center principal.
- Controladores de dominio regionales. En el caso de que así lo hayamos planificado en el punto anterior, se debe considerar colocar un controlador de dominio regional en cada uno de los dominios que tenemos creados en las sedes externas.

- Servidor de catálogo global. Esto no sería necesario si se hubiera decidido implantar una organización con un único dominio, ya que como se vio en puntos anteriores, en un modelo de único dominio todos los controladores poseen una copia del catálogo global. En caso de tener sedes con más de 100 usuarios se hace aconsejable incluir en esa sede un servidor con este rol.

❖ Crear un diseño del sitio. 1_8_DiseñoSitio_AsociarSubredesControladores.doc

Es ahora cuando se tiene que decidir qué sedes o ubicaciones se van a convertir en sitios. Se proponen dos razones fundamentales que nos ayudaran a tomar esta decisión:

- Cuando la ubicación vaya a tener un controlador de dominio.
- Cuando la ubicación tenga que poseer servidores de aplicaciones que requieran de un sitio para su correcto funcionamiento como por ejemplo un DFSN – Distributed File System Namespaces).

En caso de que nuestra ubicación no requiera de un sitio se tendrá que incluir la subred de esa ubicación en el sitio con más ancho de banda disponible.

❖ Planear la capacidad del controlador de dominio.

Cuando se piensa en implementar un AD DS, siempre se tendrá que utilizar como mínimo un servidor, que podrá ser físico o virtual. Pero uno de los aspectos más importantes de cara al rendimiento y funcionamiento de nuestro AD DS es tener en cuenta algunos puntos para dimensionar las características de este servidor de manera adecuada. Para ello se deberán tener en cuenta los siguientes puntos:

- Memoria.
- Red.
- Almacenamiento.
- Procesador.

Se puede visitar el siguiente enlace, donde se encontrarán los parámetros actualizados a tener en cuenta para realizar nuestros cálculos: https://docs.microsoft.com/es-

es/windows-server/administration/performance-tuning/role/active-directory-server/capacity-planning-for-active-directory-domain-services

3.4.2. Fase de implementación.

En esta fase se llevará a cabo la implantación de nuestro AD DS en los servidores seleccionados, haciendo que el grupo de trabajo de implementación lleve a buen término las especificaciones y recomendaciones obtenidas en la fase de diseño. Es en este punto, muy importante, la coordinación con el arquitecto de AD DS y el jefe de Proyecto. La implantación se realiza siguiendo y respondiendo a las preguntas que Microsoft Windows Server nos hace cuando iniciamos el asistente para la configuración del Servicio de AD DS. No es alcance de este trabajo el representar en este documento todas las ventanas y opciones que nos proponen los tutoriales de instalación.

3.4.3. Fase de operaciones.

En este punto, ya se tiene el servicio de AD DS instalado, configurado y funcionando. Ha llegado pues el turno para el equipo de operaciones y los dueños de las unidades organizativas, para mantener el correcto funcionamiento de nuestro AD DS. Por supuesto que uno de los puntos más importantes de esta fase es la de mantener toda la información de los objetos de nuestro AD DS lo más actualizada posible. De manera que la administración sea sencilla y que el acceso a los distintos recursos y autenticación esté garantizado para todos los usuarios.

Este proceso puede ser llevado a cabo, bien a través de las consolas de administración incluidas con nuestro servicio de AD DS, o bien, mediante el uso de procedimientos o scripts desarrollados con el lenguaje PowerShell que también viene incluido con nuestro Windows Server.

3.4.4. Integración de AD DS con Azure. Identidad hibrida.

La identidad hibrida, (Microsoft Hybrid Identity, 2019), supone una solución para la cada vez más utilizada combinación de aplicaciones locales y en la nube, en la que los usuarios deben tener la posibilidad de acceso tanto en local como en la nube. Este escenario, supone tener usuarios en la nube y en local, lo que complica las tareas de administración de los entornos de AD. En nuestro

caso, y de acuerdo con las necesidades y tamaño de nuestra organización, se hace aconsejable aplicar el escenario de **PHS – Password Hash Synchronization o Sincronización de Hash de Contraseña**, en español.

La PHS utiliza Azure AD Connect para sincronizar un hash de la contraseña de un usuario desde la instalación de AD en local hacia la instalación de Azure AD de la nube. En realidad, se trata de una replicación tal y como funciona la replicación en AD, salvo que en este caso la replicación se produce con el entorno en la nube, permitiéndonos iniciar sesión con la misma contraseña en ambos entornos.

Para utilizar este escenario se necesita:

- Instalar Azure AD Connect.
- Configurar la sincronización entre AD local y Azure AD.
- Habilitar la sincronización de hash de contraseñas.

Los pasos para la instalación rápida se pueden encontrar en: https://docs.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-install-express.

3.5. Caso de estudio.

3.5.1. Diseño lógico de la red.

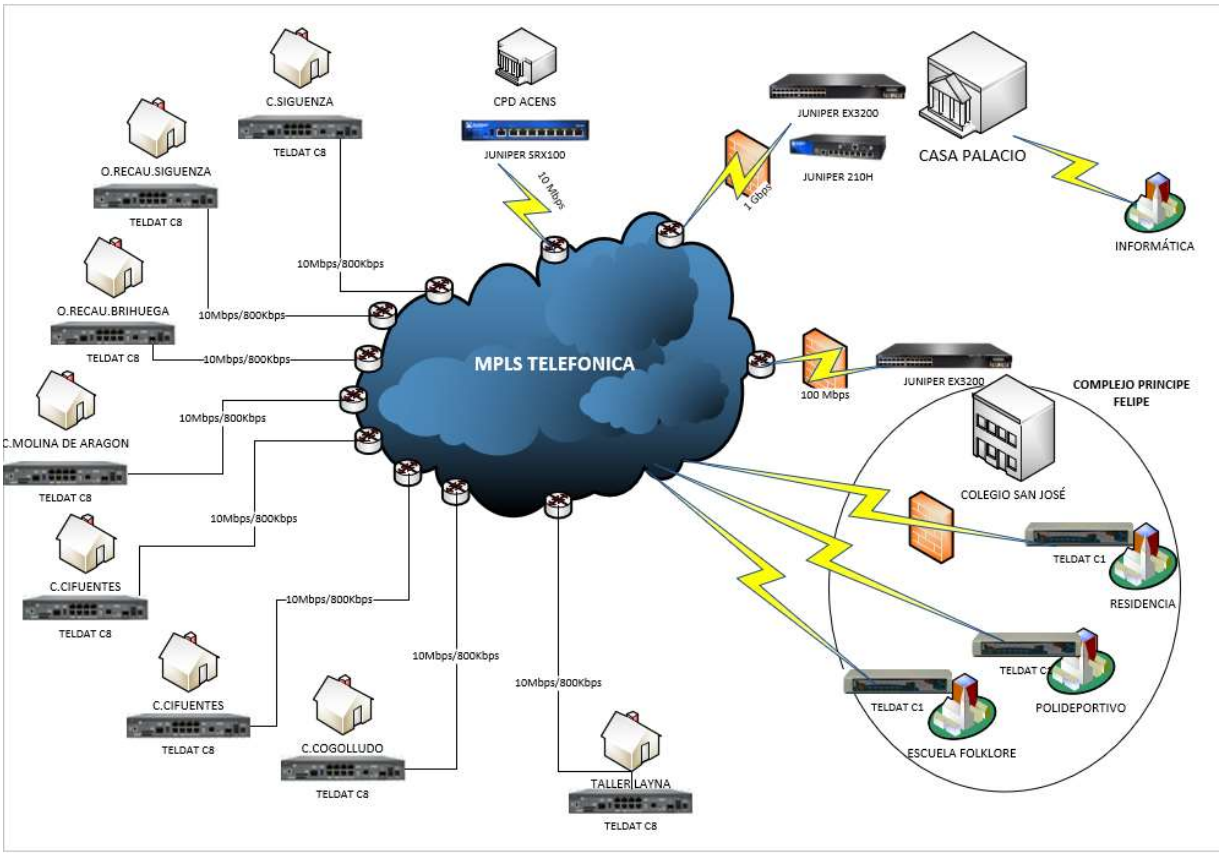

Ilustración 16. Diseño lógico red actual. Fuente propia.

Basada en una solución MPLS de Telefónica, todas las sedes y subsedes se encuentran conectadas mediante macrolan, bien de fibra o bien de ADSL.

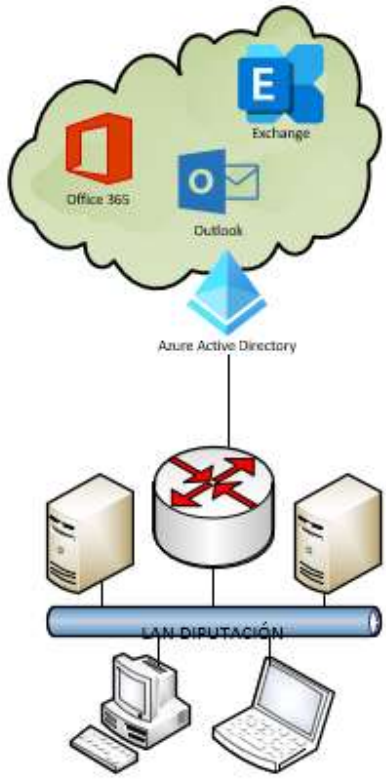

Ilustración 17. Entorno actual. Fuente propia

Actualmente la DG tiene una configuración en la nube mediante la utilización de la plataforma de Microsoft Office 365 y correo de Exchange, que utiliza una base de datos de directorio de Azure. Esta infraestructura permite la autenticación a nivel de servicios de Office 365 y de lo que en su entorno se encuentra contratado. Sin embargo, no se dispone de ningún sistema de autenticación que permita mantener el control de usuarios y accesos dentro de nuestra red local y a los recursos que se puedan publicar, tanto en la nube, como en los servidores on-premise.

Esto plantea una situación en la que, de una forma automática y sin control, toda la información recogida por nuestros equipos informáticos, (PC's, portátiles, Tabletas, etc.), se encuentra del todo desprotegida y a la merced de lo que los hackers, piratas informáticos o personas con malas intenciones, quieran hacer, sin dejar de tener en cuenta incluso a los propios usuarios que por error o accidentes puedan provocar desastres. No solo desde el entorno de las redes, cableadas y wifis, sino también desde el entorno propio de los PC's y portátiles. Ya que no disponen de ningún sistema de autenticación fuerte y seguro, que mantenga la información que contienen a salvo de miradas y de amigos de la información ajena.

3.5.2. Solución propuesta.

Tal y como se ha ido recogiendo a lo largo de este trabajo, se hace necesaria, ahora más que nunca, la implantación de un sistema de autenticación que dote a nuestros sistemas de información de los niveles de seguridad requeridos por toda la normativa actual y futura. Generando un sistema de confianza tanto para los usuarios internos como para los externos, que depositan en nosotros sus datos con la creencia de que se encuentran protegidos y a salvo de piratas informáticos y otros usos indebidos.

Desde el servicio de informática y nuevas tecnologías, conmigo a la cabeza y contando con el apoyo incondicional de la alta dirección de nuestra institución, dado que en la actualidad se dispone de un sistema implantado con Azure AD en la nube, para poder aprovechar esta infraestructura, se ha optado por instalar un servidor on-premise con Microsoft AD DS que permita la autenticación local de los usuarios y la aplicación de políticas de seguridad a los todos los objetos del AD. Integrando a todos los equipos dentro del AD DS y conectado el mismo con un sistema de sincronización de hash de contraseñas a través de Azure Connect que permita un sistema de autenticación hibrido tanto para aplicaciones locales como para aquellas que se vayan implantando en la nube.

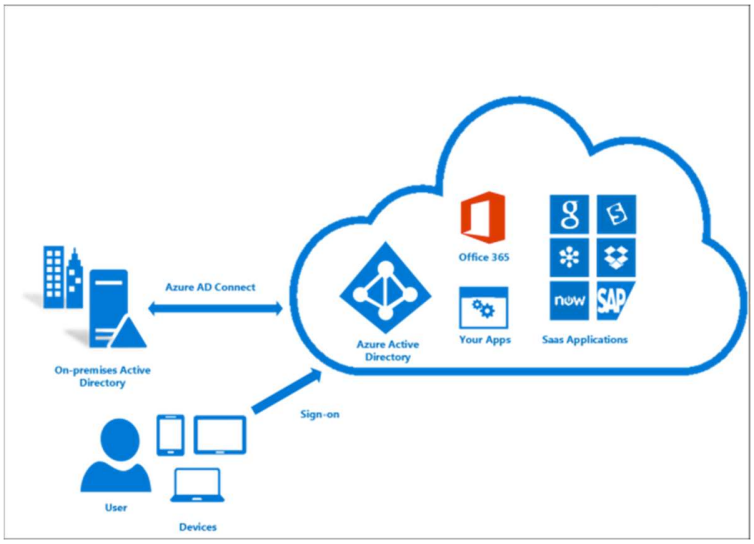

Ilustración 18. Entorno deseado. Fuente Microsoft.

También se va a aprovechar para hacer una adecuación de nuestro direccionamiento IP interno para adecuarlo a la normativa, no vinculante, pero si aconsejable, establecida por la

Administración General del Estado (AGE) y que así se encuentra publicado en el Centro de Transferencia de Tecnología del Gobierno de España, (CTT - Plan direccionamiento AAPP, 2021).

Se realizará, además, una ampliación de nuestros servicios de macrolan para pasar aquellas subsedes que se encontraban con ADSL a fibra y mejorar la conexión con dichas subsedes, de manera que tengan un ancho de banda adecuado para soportar los nuevos servicios de replicación y de autenticación de directorio.

3.5.3. Arquitectura.

- Solución On-Premise.

Los requerimientos técnicos de la infraestructura a instalar tanto hardware como software en las instalaciones de la DG será:

- Características principales y generales

  - Se deberá proponer la redundancia en los componentes para asegurar una disponibilidad del 99,9% en la producción.
  - No deberá haber puntos singulares de fallos.
  - Los enlaces redundantes deberán plantearse como activos para optimizar el ancho de banda.
  - Para la conectividad de los servidores físicos de virtualización y el almacenamiento se deberán proveer todas las interfaces necesarias para su conexionado sin contar con los explicitados en los puntos siguientes de servidores y almacenamiento. Estos interfaces se suministrarán por duplicado en cada uno de los servidores y el almacenamiento por redundancia en las conexiones.
  - La conectividad entre los servidores físicos (host) de virtualización y el almacenamiento deberá realizarse por iSCSI, FCoE, NFS con conexiones de al menos 10Gbps o por Fibre Channel (FC) de, al menos, 16 Gbps.

- Se instalará una arquitectura modular, permitiendo realizar ampliaciones de manera independiente en el futuro para ajustarse a las necesidades y al crecimiento futuro de la Diputación Provincial de Guadalajara.
- Todo el equipamiento ofertado deberá ser en formato rack normalizado de 19".

❖ Clúster de servidores.

Dos servidores físicos configurados en alta disponibilidad, (clúster), con las siguientes características y requisitos mínimos:

- 2 procesadores de última generación con, al menos, 16 núcleos por procesador y con una frecuencia de CPU de 2,1GHz. Pudiendo llegar a soportar hasta 28 núcleos.
- 256 GB de memoria DDR4, como mínimo. El servidor debe tener al menos 12 sockets por procesador. Que permita trabajar con DRAM para proveer rapidez y alta capacidad. Además de soportar NVDIMMs.
- Dos puertos Fibre Channel de 16 Gbps por servidor
- 4 puertos de red de 1 Gbps
- Doble fuente de alimentación de al menos 600W.
- Han de tener al menos un conector de video VGA
- Han de tener, al menos, tres puertos USB 3.0 de los que uno debe estar en su parte frontal.
- Han de tener, al menos, 3 PCIe 3.0 slots.
- Los servidores han de ser compatibles con el sistema de almacenamiento para que pueda albergar su sistema operativo que será al menos de 2 discos de al menos 200GB en RAID-1
- Soporte para crecimiento en almacenamiento que permita unidades SFF, LFF y NVMe, incluso mezclando los distintos tipos de unidades en el mismo chasis para alcanzar un almacenamiento inteligente.

❖ Almacenamiento.

- El almacenamiento será cubierto por una cabina de discos, en formato rack, ubicada en el CPD de Casa Palacio. Que deberá suministrar almacenamiento tanto a los servidores físicos indicados el punto anterior con el objeto de contener las máquinas virtuales, así como suministrar repositorios de red compartidos.
- Deberá soportar distintas tecnologías de discos de alto (SSD y/o Flash) y bajo rendimiento (SAS). Poderse configurar de manera hibrida y permitir el almacenamiento por niveles (tiering) automático.
- La capacidad neta del almacenamiento será al menos de 10 TB netos para uso tanto como servidor de ficheros como uso por el entorno de virtualización. De estos 10 TB se ofertará un mínimo de 2,4 TB netos en alto rendimiento SSD, el resto podrá ser en SAS. Los dos tipos de almacenamiento se instalarán en configuración de RAID 5 + 1 disco de HotSpare.
- Esta capacidad neta se considerará disponible en su totalidad para datos de la Diputación Provincial de Guadalajara, no teniéndose en cuenta el espacio de formateo, seguridad RAID, ni discos de HotSpare o cualquier otro espacio necesario para el de funcionamiento del entorno.
- Con conectividad Fibre Channel que deberá ser configurado con un mínimo de dos puertos FC16Gbps por controladora.
- Con Controladora RAID dual activo-activo con un mínimo de 24 GB de caché por controlador
- Se realizará una copia de seguridad de la caché (ya sea mediante batería, condensadores o cualquier otra tecnología equivalente).
- Debe admitir la expansión y el reemplazo en caliente de discos duros, controladores redundantes, ventiladores y fuentes de alimentación y Raid 1, Raid 1 + 0, Raid 5 y Raid 6.
- Admitirá un mínimo de 512 unidades lógicas con un tamaño de LUN que admita más de 100 TB a nivel de controlador de almacenamiento. También admitirá al menos unidades

SAS Enterprise de 600GB, 1.2TB, 1.8TB, 2.4TB, SSD de 960GB, 1.92TB, 3.84TB y unidades NL de 6TB, 8TB, 10TB, 12TB, 14TB, 16TB.

- Posibilidades de expansión máxima de al menos 3 receptáculos de unidades (ya sea LFF y / o SFF) con al menos 96 unidades SFF o 36 LFF para un total de 368,64 TB SFF / 668,16 TB LFF+SFF de capacidad. Podrá configurarse con capacidad de thin provisioning. Así como, con la organización en niveles de datos en Sub-Lun en tiempo real en diferentes tipos de unidades dentro de un grupo determinado como SSD, SAS, NL-SAS, etc.
- Existirá un software de gestión de rendimiento incorporado y el panel de configuración mostrará el rendimiento general de IOPS y MB/s. El subsistema de almacenamiento tendrá soporte para instantáneas y clones basados en el controlador y se instalará con la licencia de al menos 512 instantáneas de licencia a partir del día 1.
- El sistema debe tener la capacidad de configurar discos intercambiables en caliente y discos de Spare globales y discos de Spare para sets de raids.

❖ Copias de seguridad.

Para la copia de seguridad se implantará un NAS Backup de rack que será instalado en el CPD de la sede Príncipe Felipe. Con las siguientes características:

- Capacidad neta de al menos el doble de la capacidad ofertada en servidores (200 GB) y la cabina (10 TB). Configurado en RAID 5.
- Posibilidad de futuras expansiones/ampliaciones, bien con la instalación de más discos o añadiendo más chasis de expansión.
- Conectividad redundante de Gigabit Ethernet y/o 10 Gigabit Ethernet.

Se instalará el software de backup que cubra los sockets ofertados con las siguientes características:

- Opciones de backup y recuperación cloud, virtual y físico.
- Replicación de máquinas virtuales (VM) basadas en imagen desde una VM o backup.
- Gestión y despliegue de Agentes de backups para Linux y Microsoft Windows.
- Storage Snapshots e integración avanzada de almacenamiento.

❖ Licencias software necesarias para la infraestructura.

Se necesitarán al menos las siguientes licencias de software:

- Licencia o licencias de Windows Server 2019 Datacenter, necesarias para cubrir los núcleos de los servidores, con, al menos, 350 licencias User CAL en total.
- Al menos 3 licencias de Windows Server 2019 Estándar para 16 núcleos.
- Adquisición de la licencia del software necesaria para la solución de backup.

➢ Hardware propuesto para la implantación.

- Servidores: **Servidor HPE ProLiant DL360 Gen10**
- Almacenamiento: **Cabina almacenamiento HPE MSA 1060.**
- Copia de seguridad: **Cabina NAS Synology RackStation RS8218RP+.**

(Ver especificaciones técnicas del hardware propuesto en el ANEXO I.)

➢ Solución direccionamiento IP.

La solución propuesta para el direccionamiento IP es utilizar una subred 10.0.0.0/16 utilizando subredes /24 para cada una de las subsedes. Implantando la utilización de Virtual Local Area Network (VLAN), con el fin de independizar y poder configurar QoS para los distintos servicios de la red.

No se especifican más detalles por mantener la discreción de los datos internos de la red de la DG.

➢ Solución AD DS.

Se creará un árbol con un dominio único y un solo sitio. Este dominio local será un subdominio de nuestro actual dominio público dguadalajara.es y estará soportado por los servidores descritos en la sección de servidores. Al igual que en el caso del direccionamiento IP, por discreción, no podemos ofrecer más datos sobre la solución final propuesta.

Se muestra a continuación un diseño lógico de la nueva red:

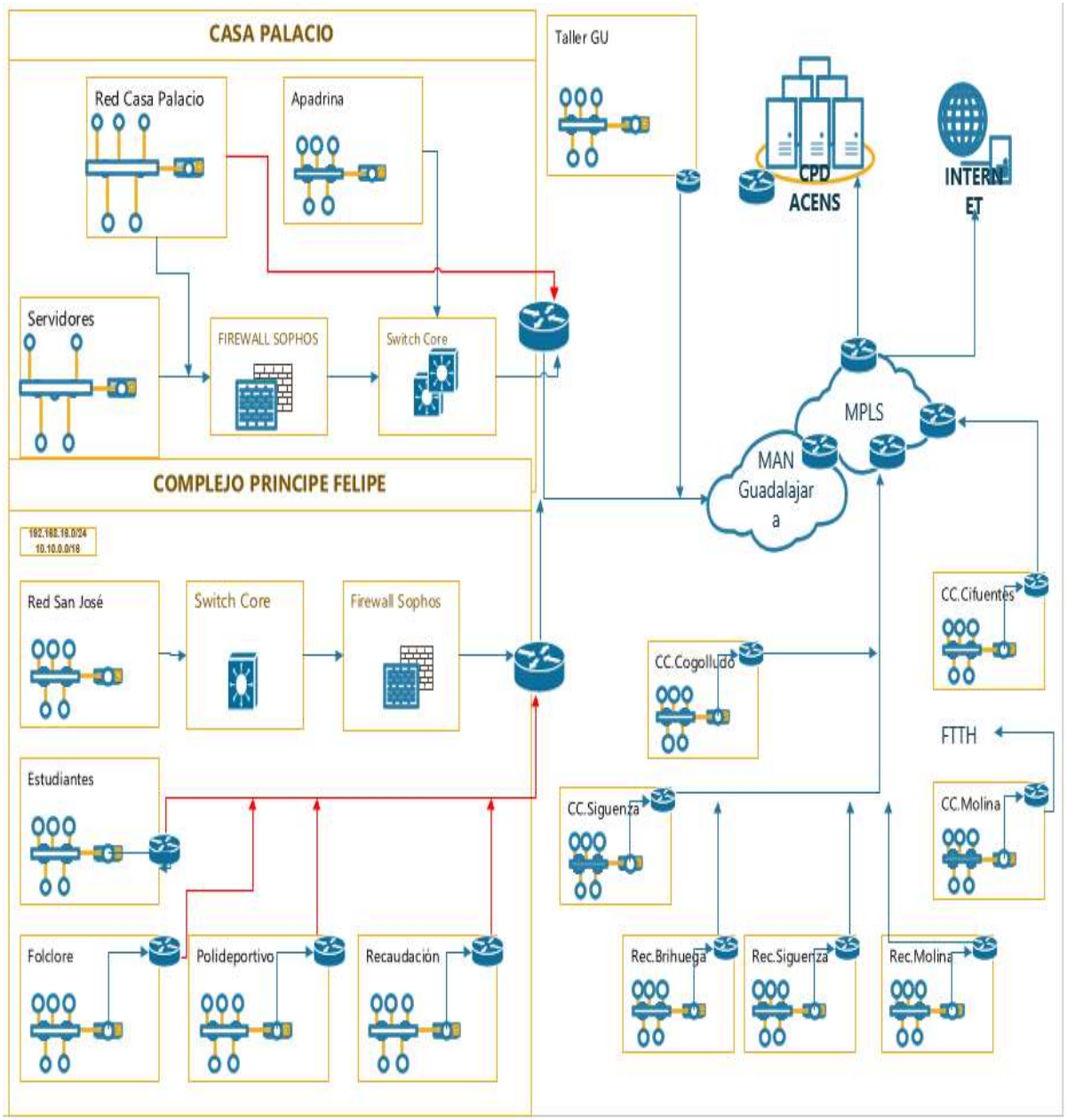

Ilustración 19. Diagrama lógico Red Propuesto. Fuente propia.

3.5.4. Evaluación solución propuesta

Basándose en la solución propuesta se puede realizar un balance de las principales ventajas que nos ofrece esta implantación y que anteriormente no existían o eran insuficientes:

- Seguridad.
    - Protección de los equipos servidores. Gracias a la arquitectura en clúster, el sistema está preparado para soportar la caída de uno de los servidores sin interrumpir el servicio suministrador.
    - Protección de los equipos locales. Al establecer cuentas de dominio para cada uno de los usuarios, con una política de contraseñas restrictiva y que obligue al cambio de esta periódicamente, protegemos la información que pueda encontrarse de manera local en los equipos de usuario.
    - Bloqueo de los puestos de trabajo, cuando el usuario de ausenta de supuesto de trabajo, impidiendo el acceso no autorizado.
    - Protección de las comunicaciones, mediante la aplicación de redes privadas virtuales entre los distintos departamentos.
    - Configuración de los equipos servidores con políticas de seguridad restrictivas, aplicando el criterio de “aplicar por defecto la seguridad más restrictiva”.
    - Aplicación de políticas de seguridad en los equipos locales que impidan su manipulación y la instalación de software no autorizado.
    - Aplicación de actualizaciones automáticas y forzosas de los equipos locales y de los servidores, en este último caso planificadas por el departamento de TI, que mantengan los sistemas operativos protegidos de las vulnerabilidades.
    - Mantenimiento de la información de empresa en recursos centralizados, auditados y asegurados, con registro de auditorías y de trazabilidad.
    - Realización periódica y automática de backups en una sede externa, permitiendo la recuperación de información ante accidentes y/o intentos de intrusión por parte de terceros.
- Administración.

- Facilitar al servicio de TI la administración de los sistemas, ayudándose de las herramientas administrativas proporcionadas por Microsoft para sus sistemas operativos de servidor.
- Reducir el número y complejidad de las incidencias a resolver en los puestos de trabajo, al tratarse de un entorno mucho más controlado y definido y al impedir al usuario hacer lo que quiera en sus equipos.
- Auditar y monitorear el estado y prestaciones de los servicios ofrecidos por la solución, permitiendo realizar un mantenimiento preventivo y proactivo, anticipándose a la aparición de problemas que puedan provocar una pérdida de disponibilidad.
- Actualizar los procesos y flujos de trabajo del personal de TI, aumentando la eficiencia y la eficacia de sus actuaciones.

- Organización.
  - Poseer un repositorio común donde poder compartir la información entre departamento, evitando duplicidades y mantenimientos de bases de datos duplicadas y facilitando que la información sea única, aunque provenga de distintas fuentes de la organización.
  - La alta dirección dispondrá de los recursos necesarios para obtener aquella información relevante que le permita ser más eficaz en la toma de decisiones y en el establecimiento de los objetivos de la organización.
  - Ofrecer al exterior un entorno de seguridad y confianza que muestren a nuestra organización como una organización adaptada a los nuevos tiempos y las nuevas tecnologías, que facilita y garantiza la seguridad de sus relaciones electrónicas tanto con los ciudadanos como con otras administraciones.

4. CONCLUSIÓN Y TRABAJO FUTURO

4.1. Conclusión.

Aunque todavía el proyecto se encuentra en la fase de implantación, los actuales hitos conseguidos:

- Propagación subredes nuevas y VLAN's por electrónica de red. 60%
- Configuración de Azure Connect con AD local. 100%
- Creación de Unidades organizativas en el AD DS. 25%
- Creación de algunos usuarios dentro de sus OU's correspondientes. 10%
- Creación de políticas de contraseñas aplicables al dominio. 10%
- Unión de equipos al AD DS. 10%
- Ampliación de subsedes a FTTH. 90%
- Creación de recursos de red compartidos en cabina de almacenamiento. 15%
- Creación de políticas de copias de seguridad de máquinas virtuales. 10%
- Creación de políticas de copias de seguridad de recursos compartidos. 5%

De los equipos y usuarios implantados y adaptados a la nueva infraestructura de autenticación y compartición, se puede destacar la total colaboración de los trabajadores de la Diputación, incidiendo mucho en el concepto y en la facilidad que les supone la utilización de una sola clave de acceso a las infraestructuras, aplicaciones locales y aplicaciones en la nube, facilitándoles enormemente su trabajo diario al no tener que recordar una contraseña para cada aplicación que utilizan.

Los usuarios también han transmitido al servicio de TI, el gran nivel de comodidad y confiabilidad que para ellos supone tener toda la información de trabajo en los recursos de red, sabiendo que

existe una política de copias adecuada y que en cualquier momento se garantiza la recuperación de la información.

La facilidad de administración que para el servicio de informática y nuevas tecnologías supone la nueva infraestructura, permitiendo autenticación de técnico como administrador en los equipos locales y permitiendo que los usuarios no sean administradores y por tanto se pueda tener controlado el software y las aplicaciones que se encuentran instaladas en los equipos.

La autenticación hibrida, permite conciliar de una manera práctica y sencilla el actual uso que se está haciendo del teletrabajo, no solo por motivos de la pandemia lo que ha supuesto un empuje muy fuerte para este tipo conexión, sino porque el teletrabajo es una herramienta de conciliación familiar que hace de los trabajadores personas más felices y a gusto con su entorno, lo que sin lugar a duda redunda en un beneficio para la empresa, en este caso la DG, y en última instancia redunda en una mejor atención a nuestros usuarios, que no son otros sino los ciudadanos y las entidades locales menores de la provincia de Guadalajara.

4.2. Trabajo futuro.

Tal y como se ha mostrado en la conclusión, el proceso de implantación de este trabajo no ha terminado todavía y por supuesto que este trabajo se enmarca en un proyecto mucho más grande que abarca otro tipo de intervenciones, como pueden ser:

- TAREAS CORTO PLAZO.
    - Realizar un inventario y comprobación del estado de Servidores y Servicios actuales. Para ir realizando su migración a la nueva infraestructura.
    - Realizar un inventario de los recursos de red, actualmente disponibles. Planificar junto a los responsables de cada servicio que necesidades actuales y futuras se deben considerar y adecuarlas a la nueva infraestructura.

- Realizar un inventario de las redes Wifi. Así como el tipo de acceso y quienes acceden a través de qué y cuando. Implantar algún sistema de gestión y control de accesos y redes WIFI.

- TAREAS CORTO/MEDIO PLAZO.
  - Configuración del entorno de los servidores bajo las indicaciones de la guía CCN-STIC 870A, (CCN-STIC-870A, 2020)
  - Implantación del sistema de administración de la red, OMNIVISTA (Alcatel). Actualmente en proceso de implantación.
  - Implantación de algún sistema de inventario/descubrimiento de equipos, por ejemplo, OCS.
  - Implantación de un sistema de asignación dinámica de direcciones de red (IP's). mediante el uso del servicio DHCP (Dynamic Host Control Protocol), administrado mediante la herramienta IPAM (IP Address Management), (IPAM, 2020).
- TAREAS MEDIO/LARGO PLAZO.
  - Realizar un **Plan de Copias de Seguridad** dimensionado en función de los recursos de red ofrecidos. Este Plan de Copias de Seguridad debería incluir la comprobación de su funcionamiento periódico realizando pruebas de recuperación aleatorias.
  - Implantación de servicios centralizados de control de software en equipos cliente, antes conocido por el nombre de SCCM (System Centre Configuration Manager) y ahora a partir de la versión 1910 sustituida por Microsoft Endpoint Configuration Manager (CM – Configuration Manager), (CM, 2019).
  - Software de gestión centralizado de impresión, para el uso de equipos multifunción de alto rendimiento y centralizado.
  - Centralización de las bases de datos de aplicaciones en servidores de bases de datos virtuales, on-premise, que soporten Microsoft SQL y Maria DB.

- Establecer el Plan de Recuperación de Desastres (DRP – Disaster Recovery Plan), estableciendo los parámetros de:
  - RPO – Recovery Point Objective. Cantidad de datos que podemos perder y que permite la continuidad de negocio.
  - RTO – Recovery Time Objective. Tiempo que se necesita para la recuperación del negocio ante un desastre.
- Crear un plan de formación en seguridad a usuarios finales. Paso muy importante porque "el punto débil de una cadena es su eslabón más débil", y en este caso son los usuarios y sus malos hábitos a la hora de trabajar con tecnología e información digitalizada.
- Crear un Plan de Adecuación de los Sistemas, que incluya:
  - Política de seguridad de la empresa.
  - Plan de mejora de la Seguridad.
  - Categorización de los sistemas.
  - Análisis de riesgos.

5. BIBLIOGRAFÍA

• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, d. 2. (27 de abril de 2016).

• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga. • *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga*. UE: BOE. Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Agenda 2030. (2020). *Plan de Digitalización de las AAPP 2021-2025.* Madrid. Obtenido de https://administracionelectronica.gob.es/pae_Home/dam/jcr:ae43f87a-9cdb-4ed9-9d78-d665a5d8491a/20210127_Plan_Digitalizacion_AP_2021-2025.pdf

Alvaro Mello, A. M. (2020). *A Master CIO in Government.* Obtenido de https://www.gartner.com/en/documents/3861181/a-master-cio-in-government0

Apache. (s.f.). *Apache Directory*. Obtenido de https://directory.apache.org/apacheds/

Castillo, R. (23 de Jun de 2013). *Computación en la nube (Cloud Computing) y Microsoft como proveedor.*

CCNCERT. (2019). *Decálogo de ciberseguridad.* Madrid. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1153-decalogo-de-ciberseguridad/file.html

CCNCERT_Estrategia2019. (2019). *Estrategia de Ciberseguridad Nacional 2019.* Madrid. Obtenido de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/7970-espana-cuenta-con-una-nueva-estrategia-de-ciberseguridad-nacional.html

CCN-STIC-870A. (Julio de 2020). *CCN-CERT.* Obtenido de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/982-870a-implementacion-ens-windows-server-2012-r2-jul15.html?path=

CISCO Benchmark 2020. (2020). *CISCO Benchmark Report 2020.* CISCO. Obtenido de www.cisco.com/go/securityreports

CISCO mejores prácticas redes. (s.f.). *Politicas de seguridad de la red, mejores prácticas.*

CM, M. (Noviembre de 2019). *Microsoft Endpoint Configuration Manager*. Obtenido de https://docs.microsoft.com/es-es/mem/configmgr/core/understand/introduction

Comisión Estratégica TIC, IRIA 2018. (2018). *Informe IRIA 2018.* Madrid. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Informes/pae_InformeIRIA/pae_InfDescripcion.html?urlMagnolia=/pae_Home/pae_OBSAE/pae_Informes/pae_InformeIRIA.html

Conejo, A. M. (2019). *Windows Server 2016. Las bases imprescindibles para administrar y configurar su servidor.* (Segunda ed.). Barcelona: ENI.

CTT - Plan direccionamiento AAPP. (Abril de 2021). *Centro de Transferencia Tecnológica*. Obtenido de https://administracionelectronica.gob.es/ctt/plandira#.YLsq1KgzaUk

Directiva (UE) 2016/1148 de 6 de Julio de 2016, r. a. (2016). *Directiva (UE) 2016/1148 de 6 de Julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel de seguridad de las redes y sistemas de información de la Unión.* DOUE.

DRSR, M. (Abril de 2021). *Technical Documents.* Obtenido de https://docs.microsoft.com/es-es/openspecs/windows_protocols/ms-drsr/f977faaa-673e-4f66-b9bf-48c640241d47

eDirectory. (s.f.). *eDirectory*. Obtenido de Micro Focus: https://www.novell.com/developer/develop_to_edirectory.html

ENS 3/2010. (29 de Enero de 2010). Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. España:

Ministerio de Presidencia. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

Ernst & Young, S. (2019). *La administración Diogital en España.* España: 2019 Ernst & Young, S.L. Obtenido de https://www.ey.com/es_es

Estrategia Nacional de Ciberseguridad. (2019). *Estrategia Nacional de Ciberseguridad.* Author and editor. Obtenido de www.cisco.com/go/securityreports

FreeIPA. (s.f.). *Free IPA*. Obtenido de https://www.freeipa.org/page/About

Gartner. (2020). *Magic Quadrant for Access Management.* Obtenido de https://www.gartner.com/en/documents/3993219/magic-quadrant-for-access-management

Gartner. (2020). *Meet Gartner IT Score for Security & Risk Management.* Gartner.

Gartner. (2020). *The IT Roadmap for Digital Business Transformation.* Obtenido de https://www.gartner.com/en/publications/gb-the-it-roadmap-for-digital-business-transformation

Gartner. (2020). *Top 10 Emerging risks of 4Q20.* Gartner.

Gartner. (2020). *Top Strategic Technology Trends for 2021.* Brian Burke, Research Vice President, Gartner. Obtenido de https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/

Gartner, B. B. (2020). *The Top Strategic Technology Trends for 2021.* Obtenido de https://www.gartner.com/en/webinars/3996485/the-top-2021-gartner-strategic-technology-trends

Gartner, T. S. (2019). *Shift from managing risk and security to enable value creation.* Gartner. Obtenido de https://www.gartner.com/en/documents/3913561-shift-from-managing-risk-and-security-to-enabling-value-

Gartner, T. S. (2021). *Rethink the security & risk strategy.* Obtenido de https://www.gartner.com/en/publications/rethink-security-risk-strategy-ebook

Gohstand, J. (15 de 06 de 2010). Getting the Most from Active Directory in the Enterprise. Obtenido de https://esj.com/articles/2010/06/15/active-directory-in-the-enterprise.aspx

IECISA El Corte Inglés. (2017). *Ciberseguridad en el sector público.*

IETF - RFC-1123. (s.f.). *IETF Datatracker.* Obtenido de https://datatracker.ietf.org/doc/html/rfc1123

IETF RFC-1320. (Abril de 1992). Obtenido de https://www.ietf.org/rfc/rfc1320.txt

IETF RFC-1321. (Abril de 1992). Obtenido de https://datatracker.ietf.org/doc/html/rfc1321

IETF RFC-2898. (September de 2000). Obtenido de https://www.ietf.org/rfc/rfc2898.txt

INCIBE. (2016). *Tendencias en el mercado de la Ciberseguridad.* Madrid. Obtenido de http://www.incibe.es

INCIBE. (s.f.). *Ciberseguridad en el teletrabajo.* Obtenido de https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INCIBE. (s.f.). *Concienciación y formación.* Obtenido de https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INCIBE. (s.f.). *Políticas de seguridad para la pyme: almacenamiento en la red corporativa.* Obtenido de https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INCIBE. (s.f.). *Servicios de seguridad en la nube SaaS.* Obtenido de https://www.incibe.es/polo-tecnologico/estudios-informes

INE. (2018). *Encuesta equipamiento y uso de teconologías y comunicación en los hogares.*

IPAM, M. (Julio de 2020). *IP Address Management*. Obtenido de https://docs.microsoft.com/en-us/windows-server/networking/technologies/ipam/ipam-top

ITU. (2015). *Global cibersecutity index & cyberwellness profiles.*

Jiménez, S. (2019). *Transformación digital para Administraciones Públicas.* INAP. Obtenido de http://publicacionesoficiales.boe.es

Jose Manuel Riveroll, Robert Beltrán López, Erwin Adame Gómez, Erwin Adame Gómez. (2019). *Liderazgo Generacional y su papel en la Industria 4.0.* Universidad Tecnologica de Chetumal, Chetumal. Obtenido de https://www.researchgate.net/publication/333561453_Liderazgo_Generacional_y_su_papel_en_la_Industria_40

LDAP, O. (s.f.). *OpenLDAP*. Obtenido de https://www.openldap.org/

Ley 11/1999, d. 2. (21 de abril de 1999). Ley 11/1999, de 21 de abril, de modificación de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. *Ley 11/1999, de 21 de abril, de modificación de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local*. España: BOE. Obtenido de https://www.boe.es/buscar/doc.php?id=BOE-A-1999-8932

Ley 19/2013, d. 9. (9 de diciembre de 2013). Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.* España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887

Ley 25/2007, d. 1. (18 de octubre de 2007). Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.* España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

Ley 34/2002, d. 1. (11 de julio de 2002). Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *Ley 34/2002, de 11 de julio, de servicios de*

la sociedad de la información y de comercio electrónico. España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley 37/2007, d. 1. (16 de noviembre de 2007). Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.* España: BOE. Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-19814

Ley 39/2015, d. 1. (02 de 10 de 2015). Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565

Ley 40/2015, d. 1. (02 de 10 de 2015). Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566

Ley 56/2007, d. 2. (28 de diciembre de 2007). Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. *Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.* España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2007-22440

Ley 9/2014, d. 9. (9 de mayo de 2014). Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.* España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950

Ley Orgánica 15/1999, d. 1. (13 de diciembre de 1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Ley Orgánica 3/2018, d. 5. (5 de diciembre de 2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Ley Orgánica 3/2018,*

de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. España: BOE. Obtenido de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Microsoft AD DS. (31 de 05 de 2017). *Servicios de dominio de Active Directory.* Obtenido de https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/active-directory-domain-services

Microsoft Azure AD. (2021). *Microsoft Azure AD DS*. Obtenido de https://azure.microsoft.com/es-es/services/active-directory/

Microsoft Azure AD Connect. (2020). *Azure AD Connect*. Obtenido de https://docs.microsoft.com/es-es/azure/active-directory/hybrid/whatis-azure-ad-connect

Microsoft Hybrid Identity. (Mayo de 2019). *What is hybrid identity*. Obtenido de https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

Miguel-Tomás, R.-I. (05 de Septiembre de 2019). Metodología técnica de revisión de Directorio Activo. Jaén, España. Obtenido de https://hdl.handle.net/10953.1/11910

Millás, V. M. (2017). *Aspectos incorporación de la Directiva NIS al ordenamiento jurídico español.*

MINECO_Agenda_2025. (2020). *Agenda España Digital 2025.* Madrid. Obtenido de https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

Morais, L. (2020). *Computación en la Nube: Inversión y Valor Agregado.* Pernambuco. Obtenido de https://www.computing.es/cloud/opinion/1115963046301/computacion-nube-inversion-y-valor-agregado.1.html

Pedro Sánchez. (26 de Abril de 2019). *Sitio oficial del Departamento de Seguridad Nacional.* Obtenido de https://www.dsn.gob.es/documento/estrategia-nacional-ciberseguridad-2019

Real Decreto 1671/2009, d. 6. (6 de noviembre de 2009). Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. *Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.* España: BOE. Obtenido de https://boe.es/buscar/act.php?id=BOE-A-2009-18358

Real Decreto 4/2010, d. 8. (8 de enero de 2010). Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. *Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.* España: BOE. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2010-1331

Real Decreto 806/2014, d. 1. (2014). *Sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos.* Madrid: BOE. Obtenido de https://www.boe.es/buscar/doc.php?id=BOE-A-2014-9741

Resolución de 13 de abril de 2018, d. l. (13 de abril de 2018). Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad. *Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.* España: BOE. Obtenido de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-5370

Resolución de 13 de octubre de 2016, d. l. (13 de Octubre de 2016). Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. *Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de*

conformidad con el Esquema Nacional de Seguridad. España: BOE. Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-10109

Resolución de 27 de marzo de 2018, d. l. (27 de marzo de 2018). Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. *Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.* España: BOE. Obtenido de Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

Resolución de 7 de octubre de 2016, d. l. (7 de Octubre de 2016). Resolución de 7 de octubre de 2016, de la Secretaría de Estado de. *Resolución de 7 de octubre de 2016, de la Secretaría de Estado de*. España: BOE. Obtenido de Resolución de 7 de octubre de 2016, de la Secretaría de Estado de

RFC-1034 (IETF) Paul Mockapetris. (11 de 1987). *NOMBRES DE DOMINIO - CONCEPTOS E INSTALACIÓN.* Obtenido de https://www.rfc-es.org/rfc/rfc1034-es.txt

RFC-1035 (IETF) Paul Mockapetris. (11 de 1987). *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION.* Obtenido de https://datatracker.ietf.org/doc/html/rfc1035

Seguridad, G. I. (2020). *Informe de ciberseguridad COVID 19. Aprovechando el pánico.* Obtenido de https://www.grupoica.com/documents/20562/81835/INFORME+CIBERSEGURIDAD+COVID-19/b4e57756-c9a9-4ebe-923f-981601bdb118

Serrano, J. O. (2017). *Windows Server 2016. Arquitectura y administración de los servicios de dominio (AD DS).* Barcelona: ENI.

Torrijos, J. V. (2014). De la digitalización a la innovación teconologica: valoración jurídica del proceso de modernización de las administraciones públicas españolas en la última década. *IDP*.

ANEXO I

Especificaciones técnicas del hardware utilizado en la solución.

Servidores:

Servidor HPE ProLiant DL360 Gen10

- Familia del procesador Intel® Xeon® Scalable de la serie 8100 Intel® Xeon® Scalable de la serie 6100 Intel® Xeon® Scalable de la
- serie 5100 Intel® Xeon® Scalable de la serie 4100 Intel® Xeon® Scalable de la serie 3100
- Número de procesadores 2, máximo según modelo
- Núcleo de procesador disponible 28, 26, 24, 22, 20, 18, 16, 14, 12, 10, 8, 6 o 4, según el modelo
- Caché de procesador 8,25MB L3 11MB L3 13,75MB L3 16,50MB L3 19,25MB L3 22MB L3 24,75MB L3 27,50MB L3
- 30,25MB L3 33MB L3 35,75MB L3 38,50MB L3
- Velocidad del procesador 3,6 GHz
- Tipo de fuente de alimentación 2 Ranuras flexibles
- Ranuras de expansión 3, para obtener una descripción detallada, consulte las QuickSpecs
- Memoria, máximo 3 TB con 128 GB DDR4
- Ranuras de memoria 24 ranuras DIMM
- Tipo de memoria HPE DDR4 Smart Memory
- Características de los ventiladores del sistema Conexión en caliente redundante estándar
- Controlador de red Adaptador Ethernet HPE 331i de 1Gb y 4 puertos por controladora o HPE FlexibleLOM opcional, según
- el modelo
- Controlador de almacenamiento 1 de los siguientes, según el modelo de controladora HPE Smart Array P408i-a SR Gen10 o controladora
- HPE Smart Array P816i-a SR Gen10 o controladora HPE Smart Array E208i-a SR Gen10
- Dimensiones mínimas (alto x ancho x fondo) 43,46 x 70,70 x 4,29 cm
- Peso 13,04kg mínimo 16,27kg máximo

- Gestión de infraestructura HPE iLO Standard con aprovisionamiento inteligente (integrado), HPE OneView Standard (requiere
- descarga), HPE iLO Advanced, edición de seguridad HPE iLO Advanced Premium y HPE OneView
- Advanced (requiere licencias)

Almacenamiento:

Cabina almacenamiento HPE MSA 1060.

- Capacity 368 TB
- Host interface Fibre Channel, iSCSI, or SAS
- depending on model
- Storage expansion options 24 drive bay SFF disk enclosure or 12 drive bay LFF disk enclosure
- Clustering support No
- SAN backup support Yes
- Storage mirroring support Yes
- Systems Insight Manager support No
- Compatible operating systems Windows Server 2019
- Windows Server 2016
- VMWare vSphere 6.7
- Red Hat Linux 8
- SuSE SLES 15
- Form factor 2U
- Energy efficiency Energy Star Compliant
- Minimum dimensions (H x W x D) 8.9 x 44.5 x 50.8 cm
- Weight 5 kg

Copia de seguridad:

Cabina NAS Synology RackStation RS8218RP+.

- CPU Intel Atom C3538 quad-core 2.1GHz
- Hardware encryption engine Yes (AES-NI)
- Memory 4 GB DDR4 Non-ECC UDIMM (expandable up to 64 GB with 16 GB ECC UDIMM x 4)

- Compatible drive type 16 x 3.5" or 2.5" SATA SSD/HDD (drives not included)
- External port
    - 2 x USB 3.0 port
    - 1 x Expansion port
- Size (H x W x D)
    - 132.3 x 430.5 x 624.5 mm
    - 132.3 x 482 x 656.5 mm (with server ears)
- Weight 17.4 kg
- LAN 4 x 1GbE (RJ-45)
- PCIe 3.0 slot
    - x8 slot x 1 (4-lane)
    - High-performance network interface card support
- Wake on LAN/WAN Yes
- Scheduled power on/off Yes.
- System fan 3 (80 x 80 x 32 mm)
- AC input power voltage 100V to 240V AC
- Power frequency 50/60Hz, single phase
- Operating temperature 5°C to 35°C (40°F to 95°F)
- Storage temperature -20°C to 60°C (-5°F to 140°F)
- Relative humidity 5% to 95% RH
- Maximum operating altitude 5,000 m (16,400 ft)
- General DSM Specification
- Networking protocol SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN ™, L2TP)
- File system
    - Internal: Btrfs, ext4
    - External: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT6
- Supported RAID type Synology Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
- Storage management

- Maximum internal volumes: 512
- Maximum iSCSI targets: 32
- Maximum iSCSI LUNs: 256
- iSCSI LUN clone/snapshot support

- SSD cache SSD read-write cache support.