Universidad de Alcalá

Escuela Politécnica Superior

MÁSTER EN DIRECCIÓN DE PROYECTOS INFORMÁTICOS

TRABAJO FIN DE MÁSTER

"SEGURIZACIÓN DEL PUESTO DE TRABAJO: ENTORNO NUBE Y CONEXIÓN REMOTA"

AUTOR: Daniel Barreiro Gil

TUTOR: José Javier Martínez Herraiz

Septiembre de 2021

UNIVERSIDAD DE ALCALÁ
Escuela Politécnica Superior

MÁSTER EN DIRECCIÓN DE PROYECTOS INFORMÁTICOS

Trabajo Fin de Máster
"Segurización del puesto de trabajo: entorno nube y conexión remota"

Autor: Daniel Barreiro Gil

Director/es Máster: Dr. José Amelio Medina Merodio

TRIBUNAL:

Presidente: Dr. José Amelio Medina Merodio

Vocal 1º: Dr. José Javier Martínez Herraiz

Vocal 2º: Dra. M. Carmen Pagés Arévalo

CALIFICACIÓN: .....

Alcalá de Henares, a 17 de septiembre de 2021

Agradecimientos

A mis padres, por la educación que me han regalado, en la que siempre ha primado el respeto, la constancia y perseverancia, el compromiso, la capacidad de sacrificio y de trabajo a partes iguales, la objetividad dentro de la subjetividad y el valor del aprendizaje. Sin ella, no sería quien soy ni habría sido capaz de conseguir todos los logros alcanzados.

A mi madre en especial, quien ha entregado tanto tiempo, tesón y energía para salvar a este navío de la zozobra.

No me olvido de Laura y su fantástica contribución artística, que ha conseguido pintar de alegría la seriedad.

Índice

Índice de figuras

Índice de tablas

Introducción

Desde hace varias décadas, los sistemas informáticos se han ido convirtiendo en piezas fundamentales de la gestión y operación de entidades, tanto privadas como públicas, llegando incluso a ser el núcleo del negocio de multitud de ellas. Hoy en día, no se comprende una sociedad mercantil o entidad gubernamental sin un sistema informático que vertebre sus comunicaciones, apoye sus procesos y gobierne sus datos. Son, de hecho, estos mismos sistemas los que han facilitado que, durante el más de año y medio que la sociedad lleva padeciendo la pandemia debida al SARS-CoV-2, la operativa de la mayor parte de las mencionadas entidades se mantuviese activa, en ciertos casos con limitaciones y en otros con un desarrollo incluso mayor al experimentado con anterioridad al albur de la emergencia sanitaria mundial.

Este nuevo paradigma, no obstante, ha venido acompañado no sólo de beneficios y efectos positivos, sino que ha generado un nuevo modelo de delincuencia virtual que entraña una problemática la cual, en muchos casos, llega a tener un impacto tan severo como la delincuencia del mundo físico (o más). Precisamente desde comienzos de 2020 y aprovechando la especial coyuntura, en la que el uso de los sistemas informáticos ha crecido de manera exponencial debido a las múltiples restricciones y limitaciones al movimiento o concentración de personas en un mismo espacio, se ha generado un incremento vertiginoso de los ataques a los sistemas informáticos y a los usuarios de aquellos.

Según los datos aportados en su informe *Cyber Attack Trends: 2021 Mid-Year Report* por el fabricante de seguridad de origen israelí Checkpoint [1], los ciberataques a organizaciones se han incrementado durante la primera mitad de 2021 un 29% a nivel global y, más concretamente, un 36% en la región de EMEA como la más afectada. Estos incrementos se han centrado fundamentalmente en los ataques de tipo *ransomware* (incluyendo la nueva variante denominada “triple extorsión”) y en aquellos dirigidos a la cadena de suministro, que se han visto facilitados debido al auge del teletrabajo y las conexiones remotas con un control más laxo. Los ataques más significativos hasta el momento, como puedan ser el de Kaseya o el de Colonial Pipeline, ejemplifican tanto el *modus operandi* de los atacantes como el catastrófico resultado, con impacto no sólo en las propias compañías, sino en los clientes finales y socios de negocio.

Es importante resaltar que el origen de estos ataques complejos muchas veces se encuentra en otros ataques más sencillos dirigidos a trabajadores, equipos obsoletos o subredes descuidadas de la organización. Precisamente una de las vías de entrada inicial que los ciberdelincuentes más están explotando, ya sea para penetrar en los sistemas de la organización, suplantar la identidad o secuestrar recursos del propio *hardware* con fines maliciosos, es la del usuario final, generalmente inexperto en tecnología y con una función no directamente relacionada con las TI de la organización. Resulta relativamente sencillo aprovecharse de la falta de conocimiento de estos usuarios a través de las técnicas de ingeniería social, muy desarrolladas en la actualidad, especialmente aquellas relacionadas con el uso del correo electrónico. Según el volumen 6 del *Spear Phishing Report* del fabricante de sistemas de ciberseguridad Barracuda Networks [2], a fecha de julio de 2021, una organización media recibe alrededor de 700 ataques de ingeniería social cada año.

Precisamente, resultan de especial interés en lo relativo a este informe los ataques dirigidos al puesto de trabajo, ya que el objeto principal del mismo es el diseño de un puesto de trabajo que garantice un

nivel protección cibernética adecuado para lidiar con los retos que se plantean hoy en día, en un ámbito tecnológico concreto (que se definirá más adelante), centrado en uno de los fabricantes líderes del sector como es Microsoft. La elección de este fabricante se ha basado principalmente en la penetración de su tecnología en el mercado (los sistemas Windows son prácticamente estándares), por lo que resulta un elemento crítico en el apartado tecnológico de muchas organizaciones, lo que le lleva a ser objeto de ataques específicos constantes, tanto hacia sus versiones *on premise* como en las herramientas SaaS en *cloud* que ha desarrollado en los últimos tiempos.

Palabras clave

- *Cloud*
- SaaS
- *On premise*
- Conexión remota
- Ciberseguridad
- Teletrabajo
- Confianza cero

Abstract

Since many decades ago, information systems have become a key piece for organizations, public or private, getting even the status of business core for some of them. Today, each govern or corporate entity has a backbone information system to hold its communications, supporting processes and governing data. In fact, these systems have helped entities to keep business continuity during the difficult period the humankind has (and still is) faced due to the global COVID-19 pandemic and, in some cases, even grow the business.

This brand new paradigm has brought not just benefits and positive effects, but also a huge growth of cybercrime, causing many times a remarkable impact in organizations finances or reputation. Taking the advantage of the restrictions and telecommuting increasing caused by the pandemic, since early 2020, cyberattacks have skyrocketed its numbers and results.

As the security manufacturer Checkpoint highlights on his “Cyber Attack Trends: 2021 Mid-Year Report” [1], cyberattacks addressed to organizations have globally grown in 29% during the first half of 2021, specifically for EMEA as the most affected region (they have grown a 36%). Ransomware and supply chain attacks have registered the highest growth due to the rush in deploying remote non-secured connection for workers. Kaseya and Colonial Pipeline attacks showed the damage these attacks can do, not just to the target organizations but also to clients or partners.

It is important to keep in mind that many of these attacks find their origin in less relevant incident related to individuals, obsolete systems, non-secure passwords or unattended subnets within the organization’s network. One of the most used ways to get access is to get advantage of the rawness or naivety of some users who do not have deep tech knowledge because they do not need it to perform their work. As the vol. 6 of “Spear Phishing Report” from Barracuda Network states, in July 2021 [2], an average organization receives around 700 social engineering attacks per year.

It is the aim of this document to design a properly secured workplace able to face any threat or manage possible attacks successfully that could happen in the current and future telecommuting scenario. The scope of this document is limited to a specific scenario, focused on Microsoft technologies due to its broad market penetration in principal systems like operative systems (Windows and Windows Server) and cloud services (Office 365 and Azure).

Key words

- Cloud
- SaaS
- On Premise
- Remote Connection
- Cybersecurity
- Telecommuting
- Zero trust

1. Contexto

A lo largo de este informe se realizará un análisis de las condiciones tecnológicas actuales (desde un punto de vista genérico), incluyendo los riesgos y amenazas que atañen al puesto de trabajo actual y las herramientas de seguridad disponibles, y se diseñará una solución de seguridad que reduzca los riesgos y permita la gestión de los incidentes en caso de ocurrir.

El entorno tecnológico considerado contempla los estándares actuales a fecha de realización del informe, y se basa en un escenario de tecnología Microsoft tanto en el apartado de computación (portátiles con Windows 10 Enterprise) y *software* de productividad (paquetes ofimáticos Office y Office 365, entornos compartidos Sharepoint y gestor de correo Exchange), como en las aplicaciones de seguridad. Esta asunción se realiza con el objetivo de acotar el alcance del informe, centrándolo en un entorno tecnológico ampliamente difundido a nivel mundial y suficientemente útil para ejemplificar escenarios similares que utilicen tecnologías de otros fabricantes.

2. Objetivos

2.1. Objetivo Principal

El punto central de este informe, en torno al que gira todo su desarrollo y que se traduce en el objeto fundamental del mismo, es el diseño de un entorno de puesto de trabajo remoto, seguro y confiable, adaptado a las condiciones actuales (amenazas, trabajo remoto, etc.), que permita a una organización media garantizar unos mínimos adecuados en el ámbito de la ciberseguridad y el control de sus sistemas para prevenir posibles amenazas y cumplir con la regulación vigente. Dicho escenario estará basado en la premisa de la amplia penetración en el mercado nacional de las tecnologías, tanto nube como *on premise*, del fabricante Microsoft.

Para cumplir con este objetivo se establecen objetivos secundarios que se irán cumpliendo a lo largo del informe. Estos objetivos se resumen en el epígrafe siguiente.

2.2. Objetivos Secundarios

Para llegar al diseño óptimo de una solución segura para el puesto de trabajo, se hace necesario conocer en profundidad el contexto de amenazas y riesgos asociados que afectan al entorno, así como la normativa vigente en cuanto a protección de los datos manejados y las recomendaciones establecidas por los organismos competentes. Serán, por lo tanto, estos dos puntos objetivos secundarios a resolver en este informe.

3. Estado del arte

3.1. Funcionamiento de los sistemas informáticos para el trabajo a distancia

Aunque el origen del concepto de teletrabajo tuvo lugar durante la crisis del petróleo en Estados Unidos, en 1973, acuñado por el ingeniero de la NASA Jack Nilles como medida de ahorro de combustible en un contexto de escasez debido a la guerra, ha sido a lo largo de las dos últimas décadas cuando verdaderamente ha comenzado a tomar forma. El rápido y exponencial desarrollo de la informática, las comunicaciones y la reducción de los costes de acceso a los equipamientos han propiciado que para las organizaciones sea técnica y económicamente viable impulsar el teletrabajo entre sus empleados. Asimismo, la presión social de los últimos tiempos con respecto a la conciliación entre la vida profesional y privada también ha contribuido en este desarrollo.

Pero, sin duda, el elemento que más ha impulsado este modelo ha sido la pandemia mundial originada por el virus de la COVID-19. Ante un panorama de restricciones de aforo y movilidad y de cambios constantes, aquellas empresas para las que ha sido posible han encontrado en el teletrabajo una vía para garantizar la continuidad de su negocio aun en condiciones tan complejas como las vividas.

La Ley 10/2021[1], dedicada a la regulación del trabajo a distancia y teletrabajo, define estos dos términos de la siguiente manera:

> a) «Trabajo a distancia»: forma de organización del trabajo o de realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular.
>
> b) «Teletrabajo»: aquel trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación.

Ilustración 1. Teletrabajo

[1] Ley 10/2021, de 9 de julio, de trabajo a distancia (BOE 164, de 10 de julio de 2021)

Considerando lo anterior, se concluye que el teletrabajo implica la realización del mismo por parte del trabajador estando físicamente alejado de las instalaciones de la organización, pero manteniendo el contacto con la misma a través de medios telemáticos. Inevitablemente, esto implica que el trabajador debe disponer de, al menos, un dispositivo informático con capacidad de conexión a internet (ordenador portátil, sobremesa, teléfono inteligente, etc.), la propia conexión a internet, herramientas (*software*) de comunicación (correo electrónico, mensajería instantánea, red social corporativa, videoconferencia, etc.), herramientas de colaboración y recursos compartidos (Sharepoint, One Drive,…) y herramientas propias del negocio o área de desempeño de la organización que sean necesarias para realizar el trabajo requerido.

Adicionalmente a lo anterior, desde un punto de vista más cercano al de la organización que al del usuario, también será necesario para la misma organización disponer de sistemas y herramientas que garanticen tanto la monitorización y el control remoto puntual de los dispositivos como la seguridad de la propia información manejada por el trabajador y sus conexiones. La privacidad del trabajador es básica, pero es absolutamente necesario que la organización sea capaz de gestionar la seguridad y cumplimiento de sus dispositivos, tanto a nivel de regulación interna como de legislación (por ejemplo, cumplimiento de RGPD).

Aunque, tradicionalmente, el modelo que ha predominado en lo relativo a la propiedad de los dispositivos haya sido aquel en el que estos pertenecen a la organización, en la actualidad la mayor difusión de la tecnología punta entre la población, los requisitos específicos de cada usuario y la inclinación de la balanza CAPEX – OPEX [3], [4] de las organizaciones hacia el lado del gasto operativo (los dispositivos de *hardware* son considerados activos de las organizaciones, por lo que se contabilizan como inversión en lugar de gasto operativo) han propiciado que el modelo *Bring Your Own Device* (BYOD) [6] comience a hacerse un hueco entre las distintas organizaciones.

El modelo BYOD plantea retos y condiciones complejas para una organización que se salen de los estándares habituales y requieren un nivel mayor de particularización. Debido a este motivo, no se contemplará en el alcance de este informe, que se centra en el modelo tradicional de propiedad de los dispositivos por parte de la organización.

Para poder continuar profundizando en los fundamentos del teletrabajo desde un punto de vista técnico, se hace necesario comprender ciertos conceptos que hoy en día se manejan de forma habitual.

El primero de ellos, tal y como lo define el NIST [7] en una de las redacciones más aceptadas internacionalmente, es el *cloud computing* o computación en nube en castellano:

> La computación en nube es un modelo que permite un acceso bajo demanda, conveniente y ubicuo, a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) y que puede ser aprovisionado con rapidez y puesto en marcha con un mínimo esfuerzo de gestión o interacción con el proveedor del servicio.

Se compone de cinco características esenciales (autoservicio bajo demanda, amplio acceso de red, agrupación de recursos, elasticidad y capacidad de medir el servicio), tres modelos de servicio (*Software as a Service* [SaaS], *Platform as a Service* [PaaS] e *Infrastructure as a Service* [IaaS]) y cuatro modelos de implementación (nube privada, nube comunitaria, nube pública y nube híbrida).

Los modelos de servicio determinan qué parte de la infraestructura y *software* gestiona el proveedor del servicio, y de qué parte se encarga la organización usuaria. Así, el NIST [7] define los tres modelos comentados de la siguiente manera:

- ***Software as a Service* (SaaS):** la capacidad ofrecida al consumidor es la de utilizar las aplicaciones del proveedor, que se ejecutan desde una infraestructura de nube. Las aplicaciones son accesibles desde varios dispositivos del cliente a través de una interfaz ligera, como un navegador web o un programa interfaz. El consumidor no gestiona o controla la capa subyacente de la infraestructura en nube, incluyendo red, servidores, sistemas operativos, almacenamiento o incluso capacidades específicas de aplicación, con la posible excepción de ciertas configuraciones específicas de usuario a nivel de aplicación.

- ***Platform as a Service* (PaaS):** la capacidad ofrecida al consumidor es la de implementar en la infraestructura de nube aplicaciones creadas o adquiridas por el consumidor, utilizando lenguajes de programación, librerías, servicios y herramientas compatibles con el proveedor. El consumidor no gestiona o controla la infraestructura en nube subyacente, incluyendo redes, servidores, sistemas operativos o almacenamiento, pero tiene control sobre las aplicaciones implementadas y los posibles ajustes de configuración para el alojamiento de las aplicaciones.

- ***Infrastructure as a Service* (IaaS):** la capacidad ofrecida al consumidor es la de provisionar recursos de procesamiento, almacenamiento, redes y otros recursos fundamentales para la computación, donde el consumidor puede implementar y ejecutar *software* arbitrario que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona o controla la capa de infraestructura en nube subyacente, pero tiene el control sobre los sistemas operativos, el almacenamiento y las aplicaciones desplegadas, así como un control limitado sobre determinados elementos de red (por ejemplo, host firewalls).

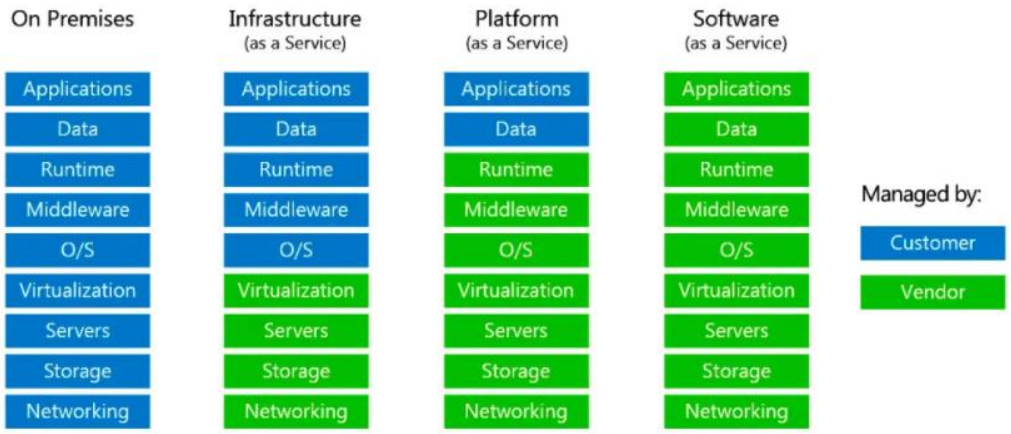

Ilustración 2. Modelos de servicio en nube.

Los diferentes formatos de despliegue o implementación definen el mayor o menor grado de dedicación de los recursos hacia el consumidor. El NIST [7] define cada uno de estos modelos como sigue:

- ***Private cloud* (nube privada):** la infraestructura en nube se provisiona para uso exclusivo de una sola organización que comprende varios consumidores (por ejemplo, unidades de negocio). Puede ser

propiedad, administrada y operada por la organización, un tercero o una combinación de ambos, y puede residir en un entorno local (*on premises*) o externo (*off premises*) a la organización.

- ***Community cloud* (nube comunitaria):** la infraestructura en nube se provisiona para uso exclusivo de una comunidad específica de consumidores de organizaciones que comparten preocupaciones (por ejemplo, misión, requisitos de seguridad, políticas y consideraciones de cumplimiento). Puede ser propiedad, gestionada y operada por una o más de las organizaciones de la comunidad, por un tercero o una combinación de ambos, y puede residir en un entorno local (*on premises*) o externo (*off premises*) a la comunidad.

- ***Public cloud* (nube pública):** la infraestructura en nube se provisiona para uso del público en general. Puede ser propiedad, administrada y operada por una entidad empresarial, académica, gubernamental o una combinación de ellas. Se despliega en las instalaciones del proveedor de la nube.

- ***Hybrid cloud* (nube híbrida):** la infraestructura en nube se compone de dos o más infraestructuras en nube diferentes (privadas, comunitarias o públicas) que continúan siendo entidades únicas, pero que están vinculadas por tecnología estándar o propietaria que permite la portabilidad de datos y aplicaciones (por ejemplo, el *cloud bursting* para equilibrar la carga entre nubes).

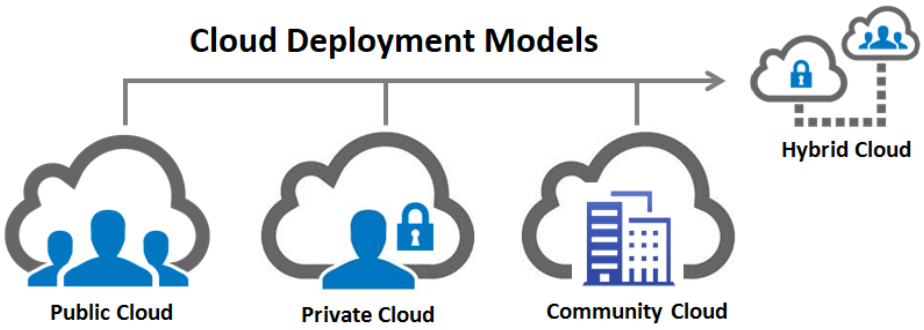

Ilustración 3. Modelos de implementación en nube.

Desde el punto de vista de los sistemas de la organización, también existen diferentes modelos para soportar y dar servicio tanto a las conexiones de los usuarios y a aquellas aplicaciones a las que necesitan acceder. Existen fundamentalmente tres modelos o arquitecturas base con las que trabajar:

- **Infraestructura local (*on premise*):** la infraestructura se despliega de forma completamente local en las instalaciones de la organización. La organización es la propietaria y gestiona y controla toda la infraestructura, desde las redes hasta las aplicaciones. Con respecto a los servicios de acceso remoto que pueda proporcionar a sus usuarios, la organización es la responsable de implementarlos y mantenerlos.

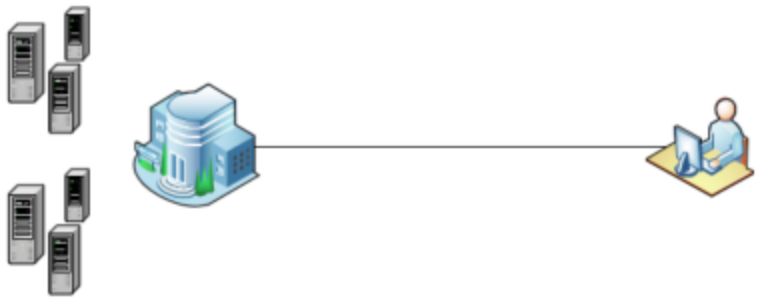

Ilustración 4. Infraestructura local.

- **Infraestructura en nube (*full cloud*):** la infraestructura reside por completo en las instalaciones de un tercero, pudiendo variar el nivel de responsabilidad de cada parte sobre la misma en función del modelo de servicio definido. Esta modalidad no es muy habitual hoy en día, ya que normalmente la organización suele preservar una parte de sus sistemas localmente por diferentes motivos.

Ilustración 5. Infraestructura en nube.

- **Infraestructura híbrida (*hybrid infrastructure*):** en la actualidad, este modelo es uno de los más utilizados, el que más crecimiento está experimentando y el que mayores posibilidades ofrece. Combina una parte de la infraestructura en nube, definiendo el modelo de servicio e implementación con cada proveedor involucrado, y otra parte *on premise*, que la organización continúa teniendo en propiedad y controla y gestiona a su antojo. Este modelo permite aprovechar las bondades de ambos escenarios (nube y local) y define un balanceo de responsabilidades específicas entre la organización y el proveedor o proveedores de servicios, en función del diseño implementado.

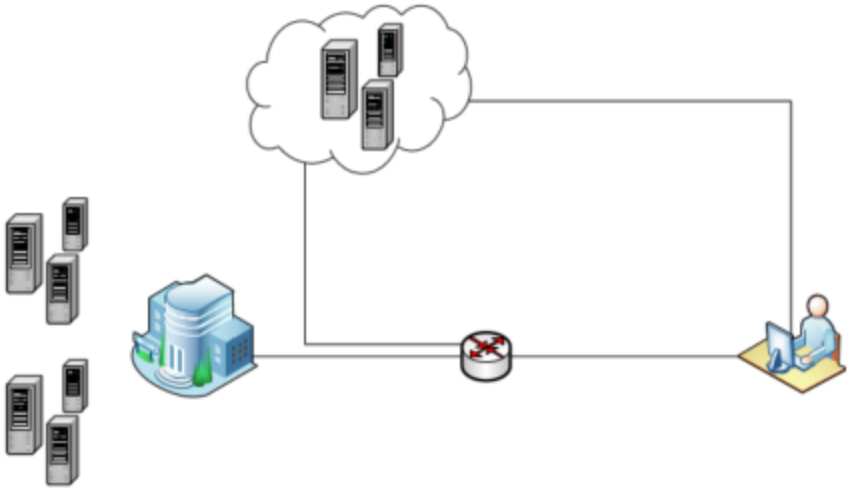

Ilustración 6. Infraestructura híbrida.

Una vez aclarados estos conceptos, es el momento de analizar el esquema básico para una conexión remota a un entorno profesional.

En primer lugar, debe existir un dispositivo desde el que el usuario solicite la conexión e interactúe con el sistema. Dicho dispositivo podría materializarse de formas muy diversas (ordenador portátil, teléfono inteligente, tableta, etc.) pero, para el cometido de este informe, quedará restringido a computadoras sobremesa y portátiles con sistemas operativos Windows 10 Enterprise en adelante (para la definición de este esquema básico no es relevante, pero para desarrollos posteriores de este informe sí lo será).

Para que el dispositivo pueda conectarse con el sistema de destino, se hace necesario disponer de una conexión de red, preferiblemente una conexión FTTH (*Fiber To The Home*) de alta velocidad o – cuando las infraestructuras lo permitan – una conexión aérea 5G. Entre esta conexión y el dispositivo puede disponerse una red Wifi o LAN (*Local Area Network*), garantizando siempre que la velocidad y ancho de banda disponibles cumplan con los requisitos mínimos necesarios para poder interactuar con soltura con los sistemas de destino.

Las conexiones podrán realizarse principalmente a través de seis métodos y sus derivadas específicas, tal y como define el CCN [8] en su documento *Arquitecturas de Acceso Remoto Seguro*.

- VPN (*Virtual Private Network*).
- Portal Web.
- Sistema de escritorios remotos.
- Sistema de escritorios virtuales.
- Acceso directo a aplicaciones.
- Espacio de trabajo digital (*Digital Workspace*).

El uso de uno u otro sistema vendrá determinado fundamentalmente por el tipo de recursos a los que se pretenda acceder, su localización (*on premise* o *cloud*) y los requisitos de la organización. Se profundizará en ellos en el siguiente epígrafe.

Al otro lado de la conexión debe existir, al menos, un recurso de validación de la identidad y de gestión de las conexiones remotas (servidor RDP, gestor VPN, servicio web, etc.) que soporte y se ocupe de controlar todas las peticiones.

3.2. Tecnologías disponibles para la conexión remota

En el epígrafe anterior se mencionan los seis tipos de tecnologías que más se utilizan en entornos profesionales para realizar conexiones a distancia. El cometido de este punto es, precisamente, profundizar en el detalle de cada uno de ellos para comprender mejor su funcionamiento; cuestión necesaria para avanzar en el diseño de la solución final.

Tal y como lo define el CCN [8] en su documento *Arquitecturas de Acceso Remoto Seguro*, una solución de acceso remoto seguro debe cumplir las siguientes condiciones:

- Facilitar la movilidad de forma integrada. La solución debe ser apta para cualquier tipo de dispositivo e independiente de la ubicación del usuario.
- Proporcionar al usuario una experiencia satisfactoria: facilidad de uso y eficiencia.
- Constituir un punto de acceso único. La solución debe constituir un único punto de acceso a todos los servicios, aplicaciones y recursos que el usuario pueda necesitar, independientemente de donde se encuentren.
- Proporcionar seguridad tanto a la información intercambiada con el usuario como a los recursos accedidos, sin poner en riesgo el resto de los recursos de la red interna. Debe permitir la aplicación de las políticas de seguridad de la organización.

Una vez sea posible garantizar el cumplimiento de estas premisas, será necesario definir el objeto de la conexión y, por ende, el punto de destino de dicha conexión. De forma genérica, las conexiones podrán tener los siguientes destinos:

- Toda la red (o varios puntos de la misma no accesibles remotamente de manera individual) de la organización.
- Aplicaciones y servicios publicados a través de un portal web.
- Un equipo específico.
- Aplicaciones o escritorios virtualizados.
- Aplicación concreta.
- Espacio de trabajo digital.

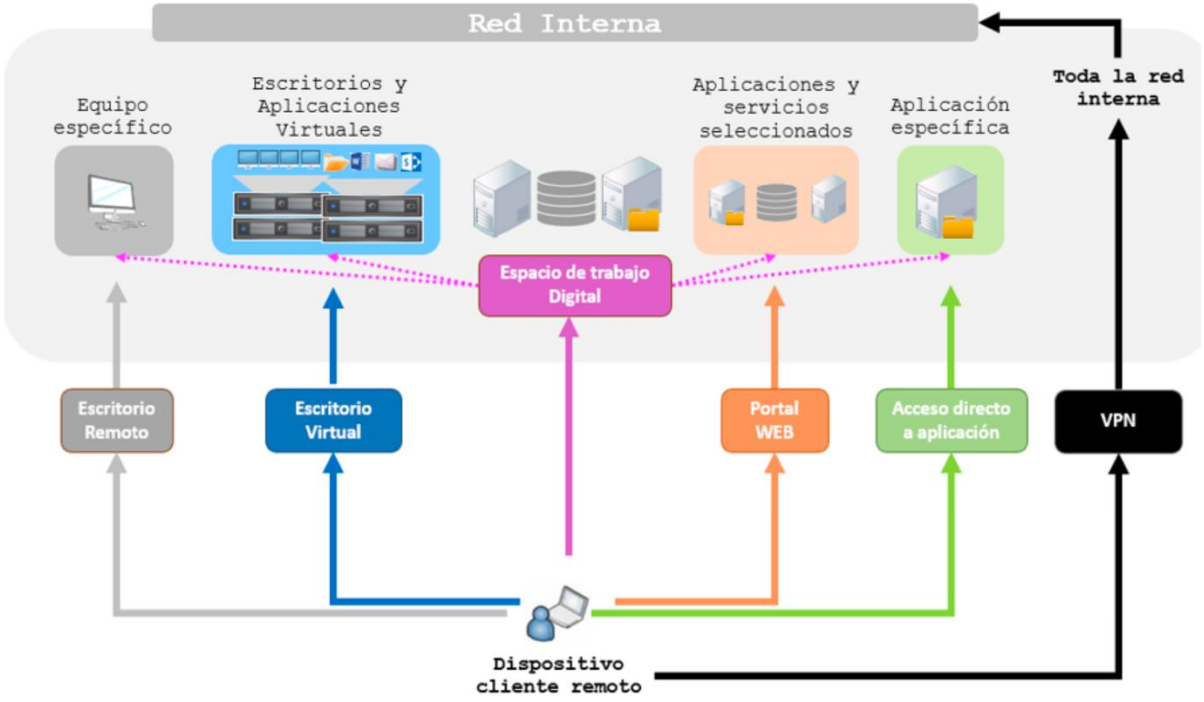

Ilustración 7. Diagrama de arquitecturas de acceso remoto y sus respectivos destinos.

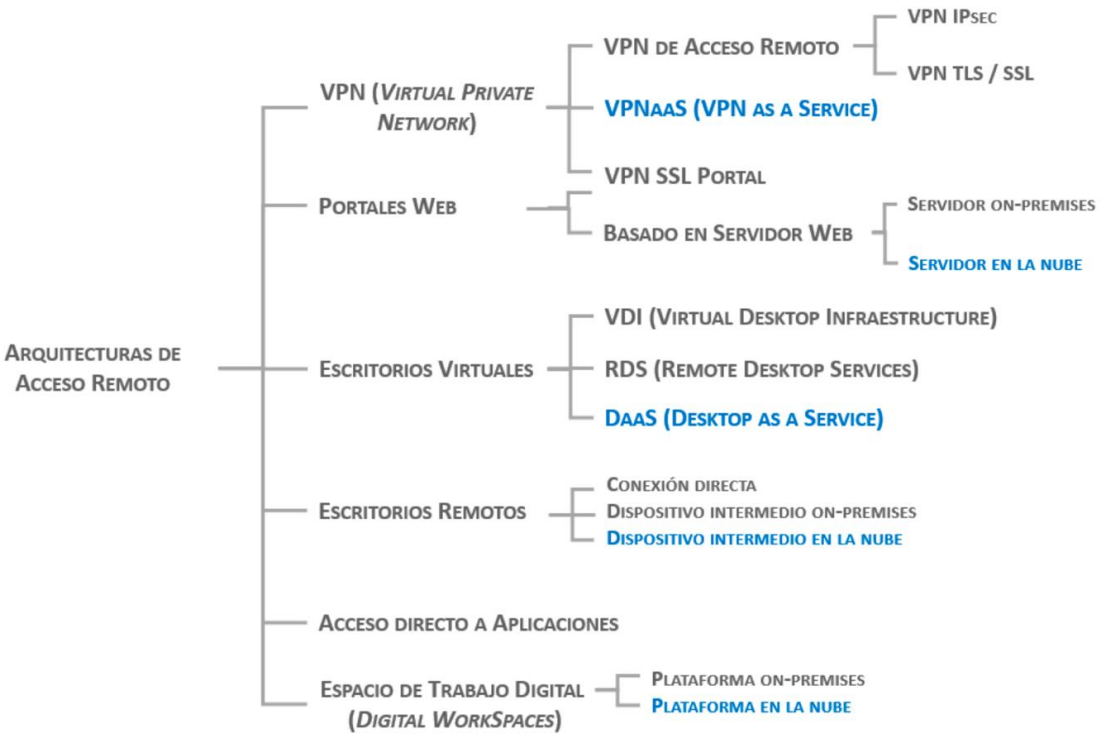

Ilustración 8. Arquitecturas de Acceso Remoto.

Red Privada Virtual (VPN)

Su principio de funcionamiento se basa en generar un "túnel" (VPN *tunneling*) seguro virtual sobre una red abierta como es internet. Este canal virtual establecido se dedica en exclusiva al tráfico de la organización, aportando mecanismos para garantizar la seguridad de las comunicaciones, los accesos y la información transmitida.

En cuanto a los puntos que conecta, para el caso que ocupa a este informe será relevante el tipo de VPN para acceso remoto. Se utiliza para proporcionar una conexión adecuada de aquellos dispositivos clientes que se conecten desde fuera a la red corporativa. Este tipo de VPN utiliza protocolos de comunicación segura (con cifrado de las transmisiones) localizados en el nivel de la capa 3 [9] para proporcionar acceso a la red corporativa. Los más difundidos son TLS (*Transport Layer Security Protocol*) e IPsec (*Internet Protocol Security*), que garantizan la confidencialidad de las comunicaciones a través de algoritmos de cifrado simétrico y la integridad y autenticidad de aquello que se transmite usando valores MAC (*Message Authentication Code*), posibilitan la autenticación del acceso mediante el uso de certificados de clave pública X.509v3, habilitan políticas anti-reenvíos, ofrecen *Forward Secrecy* y confieren control sobre la sesión.

Además de estas características, los elementos que constituyen la infraestructura VPN pueden proporcionar funcionalidades adicionales de seguridad como un control de acceso profundo o granular, evaluación de la seguridad del dispositivo cliente (*host check*) o actuando como *man in the middle* legítimo entre la red pública y la interna. Es decisión de la organización decidir la elección de un equipamiento u otro y sus funcionalidades adicionales, así como implementarlas o centrarlas en otros elementos o dispositivos de la infraestructura. Es habitual que el servidor VPN se localice en una DMZ de la organización.

En cuanto a la infraestructura propia necesaria para el buen funcionamiento de la VPN, se requieren, al menos, los siguientes componentes:

- Servidor o *gateway* VPN: Se encarga de la gestión del tráfico y el establecimiento de las conexiones dentro de la red segura VPN. Puede estar alojado en nube o localmente en un servidor físico o virtual.

- Agente VPN: Es una pieza de *software* que se despliega en el equipo cliente y se encarga de establecer y mantener la conexión VPN con el servidor.

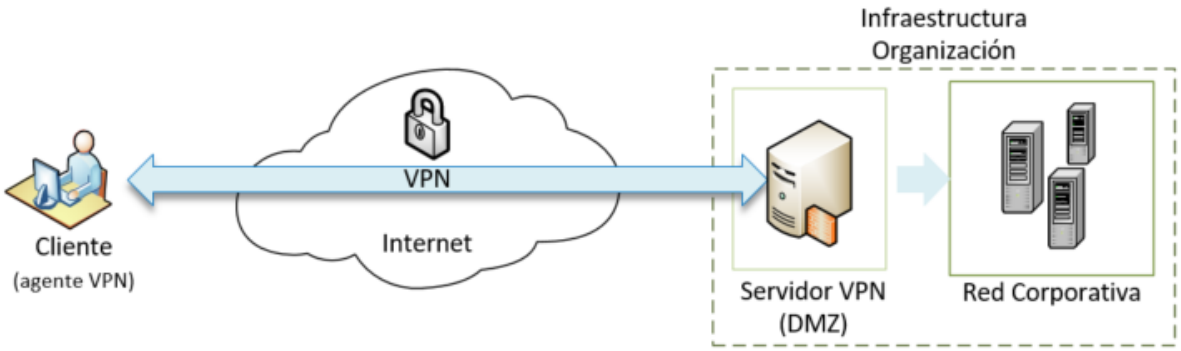

Ilustración 9. Conexión VPN.

En cuanto a los modos de funcionamiento, se aplican fundamentalmente tres:

- Túnel solicitado desde el equipo cliente: el usuario del equipo cliente solicita al servidor una conexión privada para acceder a la red de la organización. Funciona bajo demanda.

- Túnel permanente: la conexión entre el equipo cliente y el servidor VPN se inicia cada vez que el equipo cliente se conecta a internet.

- *Split tunneling* (segmentación de tráfico): se produce una diferenciación del tráfico entrante y saliente del equipo cliente, de tal forma que aquel tráfico designado como "corporativo" (esta característica deberá ser definida por la organización y configurada en el servidor VPN y la pieza de *software* del equipo cliente) se selecciona y redirige a través del túnel VPN, mientras que el resto fluye a través de internet como cualquier conexión doméstica sin dispositivos o configuraciones específicas.

-

Existe una alternativa, también válida para entornos corporativos y profesionales, que no requiere del despliegue de ningún agente en el equipo cliente para proporcionar un servicio de conexión VPN segura. Se trata de redes VPN SSL, que emplean los denominados **VPN SSL Portal**. Esta tecnología emplea portales web, actuando como un *proxy* inverso, para facilitar el acceso de los usuarios a las aplicaciones corporativas publicadas. El portal permite el acceso a aquellos usuarios autorizados, y sólo a las aplicaciones para las que tienen derechos. Está enfocado fundamentalmente hacia aplicaciones de tipo cliente/servidor.

Todo lo comentado hasta el momento hace referencia a conexiones entre clientes y servicios ofrecidos desde una infraestructura *on premise*. No obstante, existe una derivada adicional en el caso de que se utilicen servicios *cloud* de un tercero. Aunque podría utilizarse la misma conexión VPN desde el cliente hacia el entorno corporativo y, desde ahí, establecer la conexión con el servicio *cloud*, proporcionaría una experiencia de usuario insatisfactoria e ineficiente, generando retardos en la conexión y alejándose de la solución óptima.

Una alternativa a este modelo de conexión es la interacción directa entre el cliente y el servicio *cloud*. Para este tipo de conexiones, el propio proveedor de soluciones *cloud* puede aportar su modelo o se puede recurrir también a las denominadas **VPN *Cloud, Hosted* VPN *o* VPN *as a Service*** (**VPNaaS**). Las VPNaaS ofrecen servicios de VPN basadas en IPsec, específicamente diseñados para conectar un equipo cliente (a través de una pieza de *software* específica, desplegada en dicho equipo) con un entorno *cloud*, conectar dos entornos *cloud* entre ellos (*cloud-to-cloud*) o incluso conectar el entorno corporativo con su extensión en la nube.

En este caso es importante valorar la confiabilidad del proveedor de la VPNaaS, ya que buena parte del tráfico corporativo se gestionará a través de sus servidores.

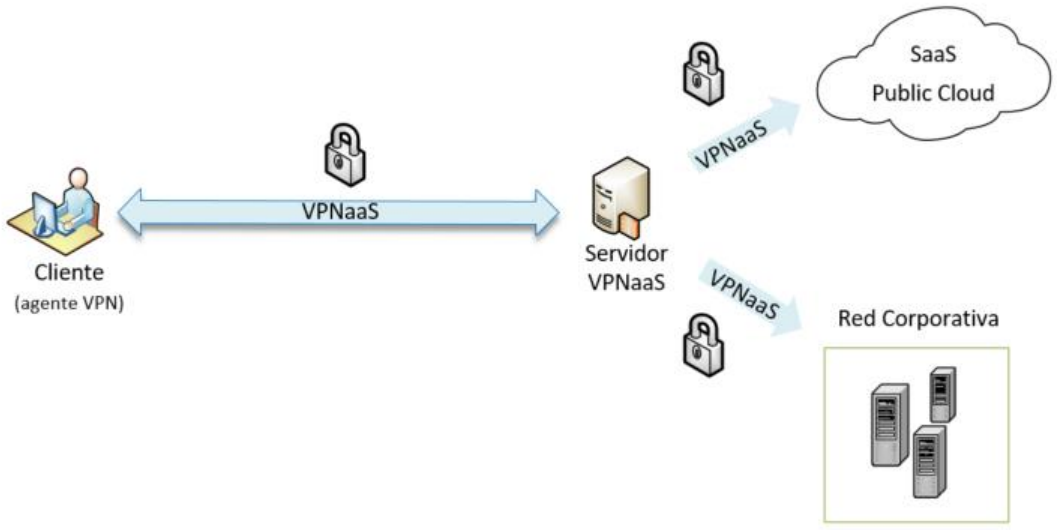

Ilustración 10. Infraestructura VPNaaS.

Portal Web

Como ya se ha comentado en el apartado anterior para la opción específica de los VPN SSL Portal, existe una alternativa para proveer a los usuarios de un acceso seguro a aplicaciones o recursos corporativos sin necesidad de desplegar ningún tipo de *software* en el equipo cliente. Estas soluciones se basan en la creación de portales web, a los que el usuario se conecta a través de un navegador con una conexión a internet estándar (con un ancho de banda suficiente) y que le proporcionan un punto de acceso centralizado a aplicaciones corporativas específicas, comunicaciones o noticias corporativas, repositorios u otros servicios susceptibles de ser accesibles a través de una interfaz web. Es posible el acceso a servicios que no soporten protocolos web, pero en este caso será necesario que el servidor realice funciones de conversión de protocolo y no es la mejor opción entre aquellas disponibles.

Este modelo lo soporta el servidor (web HTTPS o VPN SSL), en el que se implementa el portal y las aplicaciones o elementos que se instalan en él para acceder a los recursos de la organización. Es precisamente este servidor el que se encarga de aportar la capa de seguridad más importante a esta infraestructura. En concreto, realiza las funciones de *proxy* inverso gestionando las conexiones entre el cliente y los recursos internos, protege las comunicaciones cliente-red interna a través del cifrado de los

datos (fundamentalmente utiliza protocolo HTTPS/TLS), ejerce control de acceso y de autenticación de los usuarios y, potencialmente, puede evitar la extracción o descarga de información desde la red interna hacia el dispositivo cliente (depende de la configuración específica que realice la organización).

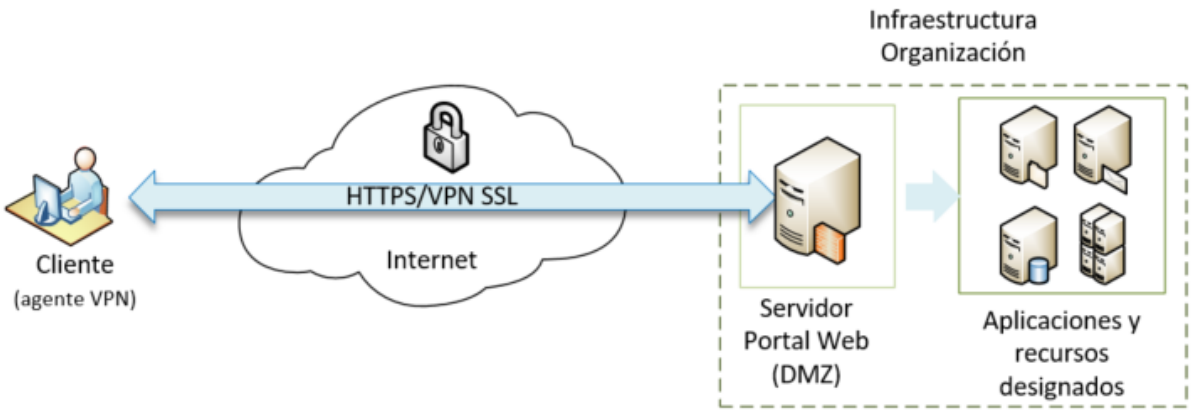

Ilustración 11. Infraestructura Portal Web.

Este tipo de servicio es susceptible de ser prestado desde una infraestructura *on premise* (propiedad de la organización) o como un servicio de nube (al margen de opciones específicas que incluyan externalizaciones de infraestructura).

Escritorios virtuales

Para las situaciones en las que se requiera alargar la vida de los dispositivos cliente, proteger y controlar cualquier acción realizada dentro del entorno o cualquier dato manejado, posibilitar la conexión de muchos tipos de dispositivos diferentes hacia un mismo entorno de características concretas o la escalabilidad recurrente de los componentes de *hardware* para soportar las diferentes aplicaciones o recursos de la organización (las tareas de computación se ejecutan desde el servidor), existe una opción tecnológica denominada "Escritorio Virtual" cuya base de funcionamiento es, precisamente, alojar los escritorios virtualizados en servidores de la organización (o en la nube de un proveedor de servicios), permitiendo que se conecten los clientes (habitualmente *Thin Clients* o clientes ligeros con limitados recursos *hardware*) aprovechando el potencial ofrecido por los servidores. De esta forma, el sistema operativo y todos los datos, aplicaciones y recursos que se ejecuten o a los que se acceda permanecen en los propios servidores de la organización, aprovechando fundamentalmente los recursos gráficos y multimedia del dispositivo cliente, así como una conexión con ancho de banda suficiente.

Aunque existen diferentes tecnologías y marcas comerciales de escritorio virtual, las más difundidas y utilizadas son VDI (*Virtual Desktop Infrastucture*) y RDS (*Remote Desktop Services*). Aunque pueden desplegarse en *cloud*, las tecnologías anteriores se dirigen principalmente a entornos *on premise*. En el

caso de los servicios en nube, han sido desarrolladas evoluciones tecnológicas sobre los estándares anteriores específicas para estos entornos como son el VDI Híbrido o el DaaS.

- VDI (*Virtual Desktop Infrastructure*): esta tecnología basa su operación en una infraestructura de máquinas virtuales (MVs) desplegadas en un centro de datos. Estas máquinas virtuales se despliegan, a través de un *hypervisor* o *software* de gestión de virtualización, sobre los servidores físicos o *host* y permiten provisionar en ellas escritorios virtuales en los que se pueden desplegar aplicaciones. A estos escritorios virtuales son, precisamente, a los que acceden los usuarios utilizando para ello su conexión con el centro de datos y siendo gestionada la asignación usuario-escritorio virtual por un *connection broker* o controlador de sesión (elemento de la infraestructura que se encarga de la correcta asignación de los escritorios virtuales a los usuarios, evitando errores de doble asignación o asignaciones incorrectas si la VDI es persistente); el usuario percibe una interfaz de sistema operativo equivalente a la que tendría en un equipo físico de escritorio y es capaz de interactuar normalmente con las aplicaciones. La conexión se debe mantener de manera constante entre el usuario y el servidor para que el sistema funcione adecuadamente.

  Desde el punto de vista del usuario, existen dos tipos de VDI:

  - **VDI persistente:** el usuario accede siempre al mismo entorno de escritorio; de este modo, puede hacer una configuración específica que se mantendrá en el tiempo cuando cierre la sesión, recuperándola al volver a iniciar sesión.

  - **VDI no persistente:** el usuario accede siempre a un escritorio genérico que no conserva las configuraciones específicas de cada usuario al cerrar la sesión.

  En función del fabricante de la solución, existen diferentes arquitecturas VDI pero, básicamente, todas ellas resumen sus elementos en tres componentes principales:

  - **Capa de recursos:** aúna los recursos físicos y el *software* necesarios para proporcionar el servicio a los usuarios finales. En ella se concentran los servidores, recursos de almacenamiento, *software hipervisor* y los escritorios virtuales o aplicaciones. Se gestiona a través de la capa de control.

  - **Capa de control:** su cometido es el de gestionar los recursos (físicos y lógicos), así como las conexiones, y entregarlos a los usuarios de forma adecuada. Entre sus funciones están la validación de los usuarios (se encargará de validar los accesos y asignarles un escritorio adecuado, sobre todo en entornos persistentes), monitorización y gestión de las conexiones, monitorización y gestión de los recursos y la gestión de los protocolos de presentación.
    Sus componentes principales son un *gateway* que se encarga de las conexiones de los usuarios, un controlador para la gestión de los recursos (a veces estos dos componentes

se unen y forman el *connection broker*) y una base de datos interna o externa que almacene información relevante para el sistema (por ejemplo, los datos de los usuarios que accedan).

- **Protocolo de presentación:** se encarga de la comunicación entre el usuario y la capa de control, incluyendo el establecimiento de la sesión. Esta capa hace posible que el usuario interactúe con el sistema y estas interacciones sean comprensibles para el sistema y sus respuestas para el usuario. Las comunicaciones que implican a este protocolo deben ser cifradas; por ello, muchos fabricantes utilizan soluciones tipo VPN SSL Portal (por ejemplo, XenDesktop y XenApp de Citrix).

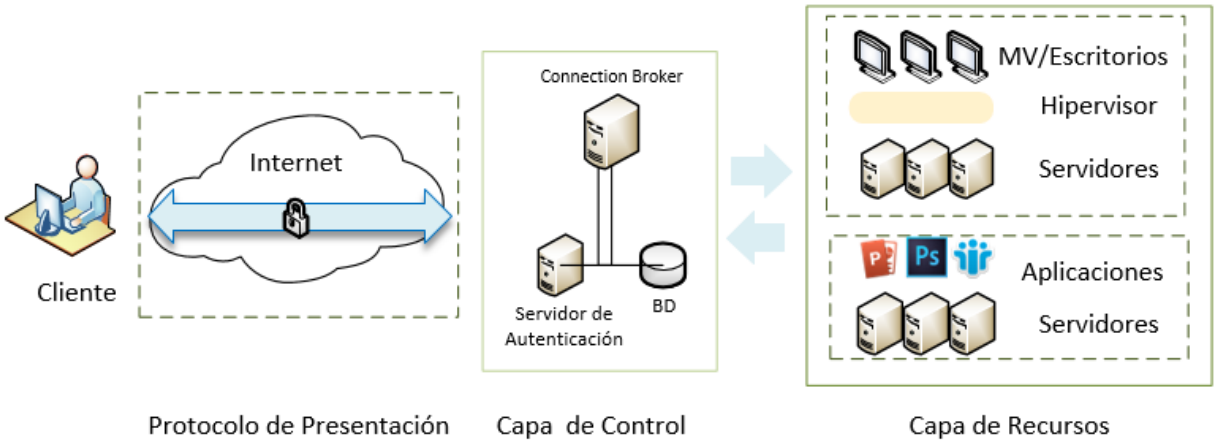

Ilustración 12. Infraestructura VDI.

- RDS (*Remote Desktop Services*): esta tecnología (también conocida como *Terminal Services*) se basa en el protocolo de escritorio remoto RDP (*Remote Desktop Protocol*) y es propietaria de Microsoft. Permite a los usuarios acceder de forma remota a escritorios y aplicaciones Windows centralizados en servidores que utilicen sistemas operativos Windows Server.
  A nivel de usuario, la percepción del funcionamiento es similar al de una VDI, es en el aspecto técnico donde difieren. Mientras que un sistema VDI utiliza tecnología de virtualización de máquinas, sobre las que despliega sistemas operativos uno a uno y se da acceso a un usuario por cada máquina, un sistema RDS utiliza un servidor (*host*) que inicia "n" sesiones (en función de su capacidad) de un mismo sistema operativo, a las que va dando acceso a "n" usuarios conservando la ratio de un usuario por cada sesión iniciada. Considerando lo anterior, es posible concluir que en una infraestructura VDI los recursos virtuales se dedican (por MV) a cada usuario, y en un servicio RDS los recursos físicos se comparten entre todos los usuarios del mismo, quedando aislados a nivel de sesión. Este funcionamiento aplica para escritorios de tipo Windows Server.

- VDI Híbrido: este modelo es similar a la VDI tradicional, pero alojando la capa de control o la de recursos en la nube y manteniendo la contraria en los servidores locales de la organización. Se

añade un elemento denominado conector que se ocupa de comunicar los entornos *cloud* y *on premise*.

- DaaS *(Desktop as a Service)*: el "Escritorio como Servicio" se trata fundamentalmente de un sistema VDI alojado por completo en la nube. Esto hace que, al conectarse, el usuario lo haga directamente a la nube en la que se aloja el servicio, pudiendo disponer de un mayor grado de escalabilidad y mejorando los tiempos de respuesta en localizaciones (en caso de configurar redundancia geográfica). Desde el punto de vista de la administración del sistema, tanto la capa de control como la de recursos se encuentren en la nube, y la responsabilidad sobre el mantenimiento de los sistemas decrece en el lago de la organización.

  Dentro del DaaS existen diferentes servicios en función del grado de administración requerido. Desde la infraestructura lógica VDI gestionada por completo por la organización (el apartado físico quedaría del lado del proveedor de *cloud*), pasando por un nivel de gestión medio sobre la infraestructura (esta versión se materializa, por ejemplo, en el servicio Windows Virtual Desktop sobre la nube Azure de Microsoft), hasta llegar a un nivel mínimo en el que el proveedor de nube gestiona casi todo el sistema e infraestructura. Este último caso se ha materializado en 2021 para la tecnología de Microsoft Windows a través de Windows 365, que proporciona al usuario un acceso directo a un escritorio Windows virtual a través de un centro de aplicaciones similar al de Office 365, y, sin necesidad de desplegar ningún agente en el equipo cliente, desde cualquier dispositivo (pc, tableta, *smartphone*, …).

Escritorios remotos

Esta tecnología permite la conexión remota entre un equipo cualquiera y un equipo de la organización. Es necesario que el equipo al que se accede cuente con los elementos de *software* adecuados para realizar la conexión, que también utiliza un protocolo de presentación, como la VDI.

No es una tecnología diseñada específicamente para trabajar de manera habitual remotamente, ya que requiere conexiones a equipos físicos y que estos permanezcan encendidos durante la conexión. Se utiliza, fundamentalmente, para prestar asistencia remota.

Acceso directo a aplicaciones

Aunque en esencia su funcionamiento a nivel técnico se basa tecnologías ya comentadas en este listado, cabe destacar que, en algunos casos, la opción de publicar aplicaciones concretas, de forma individual, para el acceso directo de los usuarios, es un beneficio para la organización. La manera más habitual de hacerlo es a través de páginas web que utilizan HTTPS y no requieren despliegue de *software* en el equipo cliente, aunque también podría usarse una conexión directa (por ejemplo, VPN) utilizando un agente instalado en el equipo cliente. En cualquier caso, el propio servidor que ofrece la aplicación se suele encargar también de autenticar al usuario. Se utiliza fundamentalmente para acceso a correo electrónico, sistemas ERP/CRM o servicios de *ticketing*.

Espacio de trabajo digital (*Digital Workspace*)

Este espacio de trabajo reúne varias tecnologías de las ya comentadas en este listado para ofrecer a los usuarios un punto de acceso único (SSO o *Single-Sign-On*) a aplicaciones, datos, escritorios virtuales y entornos de colaboración con otros usuarios y a los administradores del sistema, un punto de administración de terminales unificado. Es habitual que estos entornos incluyan también la automatización de ciertos flujos de trabajo habituales, aprovechando el aprendizaje automático (*machine learning*), lo que implica una monitorización constante del sistema, que aumenta la seguridad del entorno al ser más sencillo detectar comportamientos anómalos, intentos de conexión indebida o manipulación de datos no permitida.

3.3. Riesgos y amenazas en el puesto de trabajo

Antes de analizar la casuística específica del puesto de trabajo, se hace necesario aclarar qué implicaciones y diferencias existen entre las vulnerabilidades y las amenazas. Según el Instituto Nacional de Ciberseguridad (INCIBE) [19], una **vulnerabilidad** (en términos de informática) "Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible". El mismo organismo define una **amenaza** como

> Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas [20].

Basado en lo anterior, se puede concluir que las vulnerabilidades indican una situación que implica un riesgo para los sistemas y la amenaza es el modo en el que se materializa una acción que aprovecha la vulnerabilidad para generar un impacto.

La materialización de una amenaza puede generar un impacto en la continuidad del negocio de la organización y conllevar, en función del objeto de la misma, implicaciones legales y económicas.

Aunque las capas de interacción con el usuario en los sistemas informáticos tienden, en general, a ser cada vez más sencillas e intuitivas, lo cierto es que la diversidad de entornos, tecnologías y nuevas soluciones avanzadas han provocado el aumento significativo de la complejidad de estos sistemas, generándose de manera paralela nuevos riesgos y amenazas que se hace necesario conocer, prevenir y, en el peor de los casos, gestionar sus efectos.

Considerando el objetivo de estas amenazas, o el origen de sus vulnerabilidades, es posible hacer una segmentación en dos áreas: tecnología y usuario (factor humano). Se comprobará, no obstante, cómo existen algunas amenazas transversales que afectan a ambos elementos.

Tal y como refleja ENISA (Agencia Europea para la Ciberseguridad) en su informe anual sobre ciberamenazas para el periodo 2019 – 2020 ENISA *Threat Landscape – 2020* [21], las 15 principales amenazas en el ámbito de las TI se han mantenido dentro del *ranking* con respecto a 2018, variando en algunos casos su peso relativo con respecto al resto de las amenazas (Ilustración 13) [21]. Como se verá a continuación, entre estas 15 amenazas se encuentran algunas relacionadas con los aspectos técnicos y otras relativas a vulnerabilidades más "humanas".

Las amenazas y vulnerabilidades pueden tener también un origen físico (incendios, terremotos, sobrecargas eléctricas, etc.). No obstante, el alcance de este informe se limitará a aquellas de orígenes tecnológicos (ciberamenazas) o humanos (comportamientos delictivos o inapropiados de los propios usuarios).

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking:** ↗ Going up, — Same, ↙ Going down

Ilustración 13. Principales 15 amenazas 2019-2020 (ENISA).

Tecnología

Entre las 15 principales **amenazas** que contempla ENISA en el comentado informe anual, se detallan a continuación las más relevantes relacionadas de forma directa (origen u objeto) con aspectos fundamentalmente técnicos y tecnológicos.

- *Malware*: Tal y como lo define el fabricante de seguridad Avast [25]:

> *Malware* es un término general para referirse a cualquier tipo de "*malicious software*" (*software* malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de *malware* y cada uno busca sus objetivos de un modo diferente. Sin embargo, todas las variantes comparten dos rasgos definitorios: son subrepticias y trabajan activamente en contra de los intereses de la persona atacada.

Básicamente, este término hace referencia de manera genérica al código dañino que se utiliza para atacar sistemas ajenos. Según el informe *List of top 15 threats* 2019-2020 de ENISA [21], el *malware* continúa ostentando la primera posición en la lista de amenazas a nivel mundial. Existen diferentes tipos de *malware* en función de su diseño, objetivo y comportamiento. Los principales son:

- ***Ransomware***: en general, viene precedido de un sondeo de red, robo de credenciales o infiltración de otro tipo de *malware*. Una vez el atacante ha conseguido el acceso, emplea el *ransomware* para atacar a los equipos y servidores, bloqueándolos y encriptándolos. Se suele emplear para exigir rescates a cambio de liberar los equipos.

- ***Spyware***: se emplea en la vigilancia constante de personas concretas, a las que se les sustraen datos, en el ámbito corporativo, principalmente relacionados con el ámbito de la organización, como las credenciales de inicio de sesión. Estos datos se utilizan a posteriori para cometer ciberdelitos.

- ***Worm***: conocidos en castellano como gusanos, su objetivo principal es la infiltración en un sistema y la replicación constante dentro del mismo. Se utilizan fundamentalmente para saturar el ancho de banda de la red y como vectores de otro tipo de *malware*.

- ***Adware***: se relaciona con publicidad no deseada. Recaba datos de los usuarios y los utiliza para presentarles insistentemente publicidad personalizada. En general, no representan un problema grave para una organización, pero pueden generar saturación del ancho de banda y problemas posteriores en caso de robo de información.

- **Toyano**: se presenta como *software* legítimo pero, una vez se ha internado en el objetivo, despliega sus capacidades infectando el sistema y, en muchos casos, introduciendo otros tipos de *malware*.

- ***Botnets***: las redes de robots (*botnets*) se trata de conjuntos de equipos que, de manera inconsciente para sus usuarios y/o administradores, son infectados por un *software* de control remoto y se convierten en zombis, parte de una misma red que, habitualmente, se dedica a propósitos criminales o poco éticos, aprovechándose de los recursos de cada uno de estos dispositivos.

- Ataques basados en la web: los ataques basados en la web ocupan la segunda posición en el *ranking* ENISA de amenazas. Representan la primera amenaza que implica directamente al usuario y por ello son una amenaza transversal para ambas áreas (tecnología y usuario). Fundamentalmente a través del engaño, se conduce al usuario hacia una web o enlace ilegítimo que genera una descarga de *malware* en su sistema. También se puede materializar a través de falsos formularios web que generan el robo de información personal o corporativa y otras alternativas como navegadores web y sistemas de gestión de contenidos.

- Ataques a aplicación web: El objetivo de estas amenazas son los servicios de aplicaciones publicadas a través de la web. Representan un riesgo para la organización que aloja la aplicación, para la propietaria (en caso de ser diferentes), para los propios usuarios que acceden y para los datos que contiene la misma aplicación.

  Estas amenazas se materializan a través de diversos procedimientos, entre los que destacan los siguientes:

  - ***Cross-Site Request Forgery* (CSRF)**: aprovecha la confianza de la web en el navegador de un usuario legítimo (que previamente se ha autenticado) para llevar a cabo acciones delictivas.

  - **Inyección de SQL (SQLi)**: ante una vulnerabilidad conocida del sistema de base de datos, el atacante se vale de ella para introducir sentencias SQL con las que extrae información almacenada.

  - **Ataques de Denegación de Servicio y Denegación de Servicio Distribuido (DDoS)**: el fundamento de estos ataques se encuentra en la saturación de las capacidades de la red y del servidor que recibe las peticiones. Utilizando uno, o "n" dispositivos (frecuentemente se trata de dispositivos *bots* o zombis integrados en una *botnet*) se lanzan reiteradas peticiones al servicio objetivo hasta que se consigue que aquel se sature y se desconecte, eliminando la entrega del servicio para cualquier usuario.

Para poder segurizar de forma adecuada un entorno, es fundamental conocer en profundidad sus **vulnerabilidades**. A nivel general, más allá de las que pueda presentar un *software* o dispositivo concretos, es importante considerar vulnerabilidades que potencialmente pueden afectar a cualquier sistema informático. Estas pueden comenzar con la **falta de los sistemas y mecanismos de seguridad** adecuados para el entorno, pero también pueden encontrarse a través de una **incorrecta configuración** de esos mismos sistemas por parte de los administradores. Ejemplos de esta última circunstancia pueden ser el empleo de elementos de seguridad para un cometido no adecuado o la falta de definición e implementación de una línea base de seguridad apta para el entorno en cuestión.

Asimismo, es recomendable también utilizar *hardware* y *software* de fabricantes reconocidos, con las garantías adecuadas, y mantener todos los **sistemas siempre actualizados** con los últimos parches disponibles.

Usuario

Como se puede inferir de todo lo expuesto hasta el momento, el factor humano, en lo tocante a las amenazas y vulnerabilidades de un sistema informático, es un elemento crítico. Por ello, se vuelve fundamental conocer las amenazas existentes que apuntan directamente a este elemento y las vulnerabilidades que se derivan de sus acciones.

En el ya mencionado informe de ENISA, en el que se recogen las 15 principales ciberamenazas entre 2019 y 2020, se mencionan varias de aquellas que afectan directamente al elemento humano.

- Ingeniería social: este concepto condensa una serie de importantes amenazas y representa la piedra angular de los ataques que tienen como objetivo el error humano. Todos los ataques de ingeniería social buscan manipular y engañar al sujeto objeto del ataque para conseguir información (credenciales de acceso, datos personales, etc.). Este tipo de amenazas han supuesto, y suponen a día de hoy, un gran problema para las organizaciones, y existen versiones específicas para entornos corporativos como el denominado “fraude del CEO”, en el que una persona de la organización con responsabilidad financiera recibe reiteradas comunicaciones de un superior (frecuentemente el CEO de la compañía), que ha sido suplantado, para ejecutar transacciones monetarias de alto valor de forma ágil y silenciosa.
  Los tipos más relevantes de ataques de ingeniería social son:

    - ***Phishing***: este tipo de fraude basa su operación en una comunicación directa (fundamentalmente a través de correo electrónico) con el usuario objetivo, suplantando a un remitente legítimo en el que el destinatario confía, con la intención de que el usuario responda al correo incluyendo cierta información, acceda a través de un enlace falso, rellene un formulario cuya información llega directamente al ciberdelincuente o descargue un *malware* que asista al atacante en

el robo de datos. Representa uno de los tipos de ataque de ingeniería social más extendido y, aunque es ampliamente conocido y existe gran cantidad de información al respecto, continúa teniendo éxito en multitud de ocasiones.

- ***Vishing***: entre los distintos tipos de *phishing* que existen, el *vishing* es uno de los que han tomado mayor relevancia en los últimos tiempos. Utilizando la voz (a través de llamadas telefónicas, contestadores automáticos, etc.) el atacante se hace pasar por una persona u organización con intereses legítimos para obtener información personal o profesional de la víctima con la que posteriormente atacar a la organización objetivo.

- ***Spam***: aunque el *spam* no representa en sí un tipo de ataque, sí puede convertirse en un vector en caso de que el atacante incluya en la comunicación masiva un enlace malicioso*, malware* adjunto o instrucciones que inviten a la víctima a compartir datos personales o profesionales que posteriormente serán utilizados en un ataque de otro tipo.

- *Data breach*: también conocido como fuga de datos o filtrado de datos en castellano, representa uno de los ciberincidentes más significativos a los que se puede enfrentar una organización. No es necesario que los datos salgan lógica o físicamente de los sistemas de la organización, sino que en el momento en el que datos protegidos o con acceso restringido quedan expuestos al personal no autorizado (de la organización o externo), se considera una fuga de datos.
  Este tipo de incidentes son aprovechados por los ciberdelincuentes para chantajear a las organizaciones y obtener un beneficio económico o para utilizar los datos (por ejemplo, de acceso) en posteriores ataques o ciberespionaje.
  Aunque estos incidentes se pueden derivar de ataques perpetrados por ciberdelincuentes, muchas veces ocurren de manera accidental por no tener una configuración de los sistemas de seguridad correcta, una política de acceso adecuada o una asignación de roles supervisada.
  Según el informe de ENISA [21] sobre el panorama de amenazas 2019 – 2020, en su apartado específico para *data breach*, las fugas de datos en organizaciones aumentaron en un 54% entre 2018 y 2019, y un 71% del total de los incidentes tienen una motivación económica.

- *Insider threat*: en este tipo de amenaza, existe un actor que trabaja en o para la organización y que, por esta condición, tiene acceso a la red interna. Existen diferentes variantes en función de que el actor interno sea el atacante o lo sea un tercero externo a través de él, o de si el actor interno ejerce una acción voluntaria o involuntaria. En múltiples ocasiones el incidente se produce por un descuido o una falta de conocimiento que un tercero aprovecha en su favor. También existen casos en los que es el propio actor interno el que busca dañar a la organización u obtener un rédito o beneficio con su acción.
  Tal y como muestra el informe ENISA [21] sobre amenazas 2019 – 2020 en el documento específico para las amenazas internas, más de la mitad de este tipo de ataques generan un daño en la reputación y finanzas de la organización.

En general, cada amenaza está relacionada con una o varias **vulnerabilidades** del sistema o, en este caso, del propio usuario que accede a dicho sistema. En el caso de las personas, la mayoría de las vulnerabilidades se derivan de falta de conocimiento o insuficiente formación, inexperiencia o descuidos. No obstante, también pueden darse casos en los que se realice un uso inadecuado de los servicios de la organización de manera consciente, actuando de mala fe, o permitiendo que terceras partes lo hagan.

Una adecuada política de roles y control de identidades reduce el impacto de las posibles acciones negligentes por parte del usuario. Asimismo, un control exhaustivo del tráfico del correo electrónico (vía de entrada de gran cantidad de *malware* y *spam*, y de salida de información de la organización) y una correcta gestión de las reglas de contraseñas y autenticación de los usuarios reduce notablemente los riesgos que representan gran cantidad de las amenazas existentes.

3.4. Conclusiones

A lo largo de este apartado se ha podido comprobar cómo el paradigma del teletrabajo ha evolucionado desde su concepción, y su actual modelo sienta sus bases sobre una tecnología que permite a los usuarios acceder a los recursos de la organización desde cualquier punto del planeta en el que dispongan de una conexión suficientemente potente a internet.

Se han revisado también los nuevos modelos de servicio que ofrecen los proveedores de nube, que contribuyen a consolidar esa deslocalización física de los usuarios y la ubicuidad virtual de los recursos tecnológicos propuesta.

Asimismo, como ocurre con cualquier circunstancia o situación cambiante, se han comentado las amenazas y vulnerabilidades que esta evolución ha conllevado, así como los diferentes métodos técnicos que mejoran la seguridad de este tipo de conexiones.

Esta revisión situacional no hace sino confirmar que es necesario para las organizaciones implementar soluciones de seguridad complejas, que se adapten a sus circunstancias específicas y garanticen el máximo nivel de protección posible ante eventos que pueden generarles un impacto irreparable. No se puede perder de vista tampoco el más que importante papel de los usuarios de dicha tecnología, puesto que el apartado técnico es sólo una pieza y para completar el puzle se hace necesario formar y concienciar a todos los usuarios de la organización. La tecnología ha dejado de ser un nicho del departamento de TI para convertirse en una pieza fundamental en casi todos los aspectos y áreas de multitud de organizaciones, conservando un doble filo que debe ser correctamente gestionado.

A lo largo de los siguientes apartados, se revisarán las principales herramientas que existen para segurizar los entornos de puesto de trabajo y se expondrá el diseño de una solución para un entorno genérico.

4. Segurización del entorno

Partiendo de la premisa de que no es posible conseguir un grado de seguridad total en los sistemas de información, el objetivo debe fijarse en la minimización del riesgo a través de la consecución de un nivel de seguridad aceptable, estimando la condición de "aceptable" de manera específica para cada organización en función del nivel de riesgo que le sea posible asumir.

En este documento se busca establecer el diseño de una solución que confiera un nivel de seguridad lógica razonable a un escenario genérico de infraestructura con múltiples conexiones remotas y servicios en nube.

Previamente a realizar cualquier diseño de seguridad, se hace necesario determinar qué es la seguridad informática, en primer lugar, y cómo se evalúa, en segundo lugar.

Según Netec (empresa de formación en el área de las TI integrada en la red Global Knowledge) [29], "Es el proceso de eludir y localizar el uso no autorizado de un sistema informático con el objetivo de proteger la integridad y la privacidad de la información almacenada en un sistema informático". Esta definición localiza la información contenida y manejada por el sistema informático como elemento más importante dentro de este concepto. Y es que, aunque hay otras cuestiones paralelas que son relevantes para garantizar que estos sistemas cumplan su cometido (continuidad de operación, velocidad de proceso, etc.), todas ellas inciden en la información y los datos como núcleo y producto de un sistema informático.

Una vez comprendido lo anterior, es posible plantearse cómo evaluar el grado de seguridad de un sistema informático o de información. En el caso de España, la legislación prevé esta cuestión en el Real Decreto 951/2015[2], por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y determina 5 dimensiones de la información de la siguiente manera:

> A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:
>
> a) Disponibilidad [D].
>
> b) Autenticidad [A].

[2] RD 951/2015. De 23 de octubre, que modifica el RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Seguridad Electrónica.

c) Integridad [I].

d) Confidencialidad [C].

e) Trazabilidad [T].

En el anexo IV de la misma norma, se establecen los significados de las mencionadas dimensiones:

- Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

- Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

- Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

- Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Se infiere de todo lo anterior que la seguridad de los sistemas de información no es una cuestión que dependa exclusivamente del departamento de TI de la organización, sino que debe contar con el compromiso de todo el personal, incluidos de manera especial los niveles superiores. Conseguir garantías para que el entorno se pueda calificar como seguro conlleva aplicar una metodología que contemple, como mínimo, una definición precisa de la política de seguridad y los roles que en ella intervienen con sus funciones asignadas, la asignación de dichos roles a integrantes concretos de la organización, la definición de procedimientos para la resolución de conflictos relativos a esta gestión, la revisión de las recomendaciones sobre medidas de seguridad estipuladas en el Anexo II del Real Decreto 951/2015, de 23 de octubre, y, para cada caso, la existencia y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI), cuyo detalle será definido a continuación.

La figura del sistema de gestión de la seguridad de la información está contemplada en el Esquema Nacional de Seguridad y se podría definir como un elemento fundamental para la gestión de la seguridad en una organización, que permite conocer, manejar, prever y reducir los riesgos a los que está expuesta la organización. Tal y como lo concibe la organización ISO en su norma ISO/IEC 27000, un SGSI debe estar encuadrado en un proceso cíclico continuo que haga evolucionar de manera permanente el sistema de gestión y evite su obsolescencia. En concreto, dicha norma establece el modelo PDCA (*Plan-Do-Check-Act*, por sus siglas en inglés) planteado por Deming en 1986, como la referencia a seguir.

La organización ISO propone, a través de su norma ISO/IEC 27003 [30], una guía normalizada para la correcta implantación de un sistema de gestión de la seguridad de la información, así como de su monitoreo y seguimiento a lo largo del tiempo.

Para que resultase verdaderamente efectiva en un entorno concreto de una organización determinada, la solución diseñada en este informe debería adecuarse a los particulares contenidos en el SGSI de dicha organización, en especial a lo dispuesto en el plan de tratamiento de riesgos, ya que los elementos contemplados en esta solución componen salvaguardas lógicas para el sistema en cuestión.

4.1. Normativa RGPD y LPI

Por defecto, toda organización que esté registrada y/u opere en territorio nacional está sujeta a la legislación española. En concreto, todo sistema de información (y por ende la organización que lo opera) que gestione datos personales o propiedad intelectual, está sujeto a la normativa aplicable al respecto. En el caso de España, dicha normativa se contiene en el Reglamento General de Protección de Datos (RGPD) y la Ley de la Propiedad Intelectual (LPI)[3] para todas las organizaciones, en la Ley de Servicios de la Sociedad de la Información (LSSI)[4] para aquellas que aplique y en la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)[5] y el Esquema Nacional de Seguridad (ENS)[6] para las entidades públicas y colaboradores o contratistas.

Resulta de especial interés por su relevancia y amplio ámbito de aplicación el RGPD, trasladado al derecho español a través de la Ley Orgánica 3/2018[7].

Esta norma establece los límites y requisitos para el tratamiento de cualquier tipo de dato de carácter personal, los derechos fundamentales de las personas con respecto a sus propios datos personales (de acceso, de rectificación, de supresión, a la limitación del tratamiento, a la portabilidad de los datos y a la oposición al tratamiento) y establece nuevas obligaciones para las figuras del responsable del tratamiento (quien requiere el tratamiento, define la finalidad y establece los medios) y el encargado del tratamiento (quien efectivamente se encarga de realizar el tratamiento).

Considerando un escenario de una organización cualquiera que cuente con un sistema de información, la organización será siempre la responsable del tratamiento de los datos que transiten por su sistema, se localice éste *on premise* o en *cloud*. Pero mientras que si el sistema se localiza *on premise* la organización concentrará también el rol de encargado del tratamiento, en caso de que se utilicen servicios *cloud* el encargado puede pasar a ser el prestador de servicios de nube. Cobran, por lo tanto, una especial relevancia en este caso para la organización en cuestión, dos requisitos que el RGPD establece como necesarios a la hora de manejar datos personales:

[3] RDL 1/1996 de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (BOE 97, de 22 de abril de 1996).
[4] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE166, de 12 de julio de 2002).
[5] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE 150, de 23 de junio de 2007).
[6] RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE 25, de 29 de enero de 2010).
[7] LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 294, de 6 de diciembre de 2018).

- **Principio de responsabilidad activa**: tanto el encargado como el responsable del tratamiento deben ocuparse de garantizar que en todo momento el tratamiento sea conforme a lo dispuesto en el RGPD. Asimismo, es también su responsabilidad acreditar que se hayan dispuesto las medidas adecuadas para que se cumpla lo anterior.

- **Principio de protección de datos desde el diseño**: es imperativo que se apliquen las medidas apropiadas para garantizar el cumplimiento de los principios establecidos en el Reglamento desde el diseño de los propios sistemas y metodologías empleados.

En lo relativo a este informe, será un requisito indispensable garantizar el cumplimiento de esta regulación para cualquier solución *cloud* contemplada en el diseño final. No se podrá garantizar el cumplimiento de las soluciones *on premise* sin un SGSI implantado de forma particular para la organización a la que aplique en cada caso.

4.2. Modelo de confianza cero y línea base de seguridad

En el ámbito de la seguridad de los sistemas de información, en las condiciones actuales es preferible desarrollar una estrategia basada en el modelo de confianza cero (Zero Trust), debido a la gran cantidad, diversidad y complejidad que pueden tener los ataques que se produzcan, así como sus diferentes orígenes (incluida la propia red interna de la organización). Este modelo establece la regla básica de no confiar en ninguna solicitud, independientemente de su origen (incluso proviniendo del interior de la propia red interna), suponiendo que pueda haber incumplimientos y comprobando cada una de ellas.

De la misma manera que lo hacen otras organizaciones, Microsoft establece tres principios básicos como definitorios para el modelo de confianza cero [33]:

- **Comprobar de forma explícita**: autentica y autoriza siempre en función de todos los puntos de datos disponibles, lo que incluye la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías.

- **Utilizar acceso con privilegios mínimos**: limita el acceso del usuario con acceso suficiente y justo a tiempo (JIT/JEA), directivas adaptables basadas en los riesgos y protección de datos para ayudar a proteger los datos y la productividad.

- **Asumir la vulneración**: minimiza el radio del alcance y segmenta el acceso. Verifica el cifrado de extremo a extremo y usa los análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

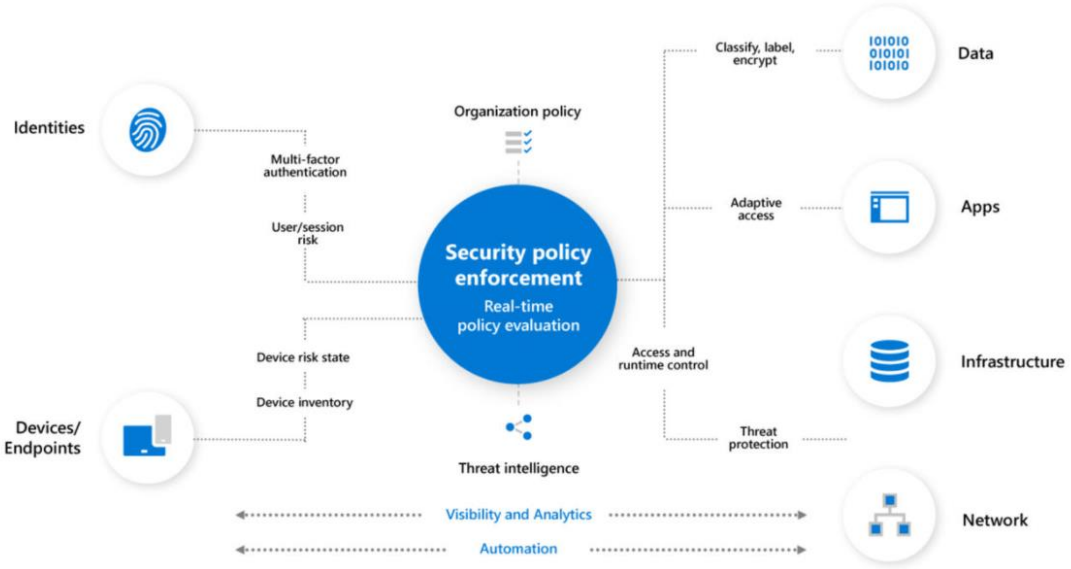

Ilustración 14. Diagrama de seguridad Confianza Cero

De una forma más práctica, el NSCS (National Cyber Security Center) [34], entidad dependiente del gobierno británico, establece diez pautas a seguir para construir un entorno seguro partiendo del modelo de confianza cero. A continuación, se enumeran las mencionadas pautas traducidas al castellano:

- Conoce tu arquitectura incluyendo usuarios, dispositivos y servidores.
- Crea una única y sólida identidad de usuario.
- Crea una sólida identidad de dispositivo.
- Realiza autenticación en cada punto.
- Conoce el estado de seguridad y cumplimiento de tus dispositivos y servicios.
- Monitoriza de forma específica dispositivos y servicios.
- Establece políticas acordes al valor del servicio o de los datos.
- Controla el acceso a tus servicios y datos.
- No confíes en la red, incluyendo la red interna.
- Utiliza servicios diseñados desde la confianza cero

El modelo de confianza cero representa una base teórica que aplicar para conseguir un mayor grado de seguridad en los sistemas. No obstante, se hace necesario contar con un vehículo para su implementación práctica. Dicho vehículo lo constituyen las líneas base de seguridad (*baseline*).

Una línea base de seguridad establece los requerimientos mínimos que implementar para considerar un entorno como seguro, según los parámetros específicos definidos. Cada organización es diferente y tiene su propia estructura y objeto, por lo que, para que la línea base resulte efectiva, se hace necesario considerar siempre los siguientes aspectos a la hora de definirla:

- Tipo de organización (pública, privada, etc.).
- Tamaño de la organización.
- Estructura de la organización.
- Identificación de activos de la organización.
- Tipos de datos gestionados por la organización (niveles de categorización de los datos).
- Identificación de las redes y subredes de la organización.
- Modelo de infraestructura de la organización (*on premise*, *cloud*, *hosted*, etc.).
- Cualquier otra particularidad de la organización o sus sistemas de información e infraestructuras que deban ser tenidas en cuenta.

Puede tener diferentes vertientes: en este caso, como se ha comentado anteriormente, el foco serán los dispositivos *endpoint* (dispositivos de usuario), por lo que se revisará qué elementos de seguridad van a ser desplegados y de qué manera se van a configurar. Para ello, se seguirán las recomendaciones de buenas prácticas establecidas por el CCN (Centro Criptológico Nacional), siguiendo las guías CCN-STIC [35], y Microsoft, como fabricante de los productos y soluciones y organización experta en el ámbito.

Son reseñables también las directrices y recomendaciones establecidas en este ámbito por el NIST [36] en su SP 800-53 sobre gestión del riesgo (para la implementación de *baselines*) y las STIG (*Security Technical Implementation Guides*) de DISA (Defense Information Systems Agency) [37], ambos organismos del gobierno estadounidense.

Es habitual denominar a la implementación práctica de las *baselines* de seguridad como *hardening* o bastionado de los sistemas, infraestructuras, redes o equipos.

4.3. Identificación y definición de herramientas

Una vez establecidas las características del entorno a segurizar y la estrategia a seguir, se hace necesario identificar las herramientas de *software* y *hardware* (en caso de ser necesario) que se emplearán para llevar a cabo la implementación del plan. Una vez definidas a nivel genérico, se particularizarán en función de las opciones disponibles en el mercado y que mejor se adecúen a las circunstancias de la organización. Como ya se ha comentado, en este caso se utilizarán herramientas del fabricante Microsoft.

Para desarrollar la tarea de determinar qué herramientas serán necesarias para segurizar técnicamente el puesto de trabajo, se prestará atención a la taxonomía de producto desarrollada por el INCIBE (Instituto Nacional de Ciberseguridad de España) [40] en su “Catálogo de empresas y soluciones de ciberseguridad” en los ámbitos de aplicación de “Gestión de acceso e identidad”, “Seguridad en el puesto de trabajo” y “Seguridad en aplicaciones y datos”.

CATEGORÍA DE PRODUCTO	ÁMBITO DE APLICACIÓN				
	Gestión de acceso e identidad	Seguridad en el puesto de trabajo	Seguridad en aplicaciones y datos	Seguridad en los sistemas	Seguridad en la red
Anti-fraude Anti-phising, Anti-spam, Herramientas de filtrado de navegación, UTM, Appliance		✓	✓	✓	✓
Anti-malware Anti-virus, Anti-Adware, Anti-spyware, UTM, Appliance		✓	✓	✓	✓
Auditoría técnica Análisis de logs y puertos, vulnerabilidades, Auditoría de contraseñas, Auditoría de sistemas y ficheros	✓		✓		✓
Certificación normativa SGSI, Análisis de riesgos, Planes y políticas de seguridad, Normativas de seguridad		✓	✓	✓	✓
Contingencia y continuidad H. de gestión de planes de contingencia y continuidad, Copias de seguridad, Infraestructura de respaldo, Virtualización, Cloud		✓	✓	✓	✓
Control de acceso y autenticación Control de acceso a red, NAC, Gestión de identidad y autenticación, Single Sign-On, Certificados digitales, Firma electrónica	✓				
Cumplimiento legal Herramientas de cumplimiento legal (LOPD, LSSI,...), Borrado seguro, Destrucción documental	✓	✓	✓		
Inteligencia de seguridad Gestión de eventos de seguridad, SIM/SIEM, Big Data, Herramientas de monitorización y reporting			✓	✓	✓
Prevención de fuga de información Control de contenidos confidenciales, Gestión del ciclo de vida de la información, Herramientas de cifrado		✓	✓		✓
Protección de las comunicaciones Cortafuegos (firewall), VPN, IDS, IPS, UTM, Appliance, Filtro de contenidos, P2P, Gestión y control de ancho de banda		✓	✓	✓	✓
Seguridad en dispositivos móviles Seguridad para dispositivos móviles, Seguridad para redes inalámbricas, BYOD		✓			✓

Ilustración 15. Taxonomía de productos

Herramientas

- **Anti-fraude**: se trata de herramientas destinadas fundamentalmente a la prevención de ataques de ingeniería social. Deberán ser implementadas directamente en el equipo cliente o en los servicios *cloud* que el usuario utilice.

- **Anti-*malware***: destinados a prevenir o mitigar los efectos del *malware*, en esta categoría pueden incluirse desde los tradicionales antivirus hasta algunas herramientas contra amenazas avanzadas.

- **Auditoría técnica**: en este grupo se incluyen aquellas herramientas que ayudan a la organización a revisar y evaluar su nivel de seguridad.

- **Certificación normativa**: son herramientas que facilitan la verificación o implantación de estándares o normativas. En este caso, más que como herramientas en sí, se aplicará como característica verificando que aquellas herramientas *cloud* incluidas en el diseño final cumplan con la normativa aplicable.

- **Contingencia y continuidad**: este grupo engloba a aquellas herramientas y servicios que ayudan a la recuperación y continuidad de operación en caso de desastre (fallo o ataque). Se contemplan funcionalidades como copias de seguridad (*backup*) o recuperación de desastres (*disaster recovery*).

- **Control de acceso y autenticación**: su cometido está orientado hacia la identificación y validación de los usuarios que intenten acceder: no sólo que estén autorizados a acceder al sistema, sino que posean el nivel de acceso adecuado. Estas herramientas son fundamentales para mantener un control férreo sobre posibles infiltraciones en la red interna, y se deben mantener siempre actualizadas utilizando métodos de identificación fuerte siempre que sea posible.

- **Cumplimiento legal**: a través de estas utilidades se facilita el cumplimiento de la legislación aplicable. En este caso, se tomará como una funcionalidad añadida (o varias), dentro del espectro de soluciones seleccionadas, que permita el cumplimiento del RGPD y la LPI.

- **Inteligencia de seguridad**: este tipo de herramientas se encargan de monitorizar la red (o parte de ella), los dispositivos y sus comunicaciones, de tal forma que son capaces de detectar síntomas y signos indicativos de ataques o situaciones anómalas que ayuden a prevenir ataques o a mitigar sus efectos. Aunque no sean herramientas que estén exclusivamente relacionadas con los equipos cliente, son relevantes a la hora de mantener la seguridad en toda la red (incluidas las conexiones remotas), por lo que se harán menciones al respecto.

- **Prevención de fuga de información**: también conocidas como herramientas DLP (*Data Loss Prevention*, por sus siglas en inglés), su papel es garantizar que las dimensiones de la seguridad de la información (confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad) no sean violadas, principalmente ante posibles ataques internos.

- **Protección de las comunicaciones**: su cometido es el de garantizar que las comunicaciones se mantienen, funcionan de manera adecuada y mantienen la integridad de las dimensiones de la seguridad de la información.

- **Seguridad en dispositivos móviles**: aunque algunas de las herramientas contempladas en este apartado no resultan de interés para este informe por ser aplicables a dispositivos no contemplados en la solución, sin embargo hay ciertas características y funcionales que sí lo son por ser los dispositivos objeto del diseño susceptibles de realizar conexiones remotas.

5. Diseño de la solución

A lo largo de este epígrafe se hará una exposición del entorno a segurizar (sistemas y aplicaciones relacionadas con los usuarios y perfilado de usuarios con sus respectivos niveles de acceso asignados), se establecerá una línea de seguridad base a nivel lógico para el entorno de usuario considerado, se identificarán las herramientas con marca comercial Microsoft que serán usadas en la solución final para cumplir con la línea base y se establecerán unas directrices mínimas relativas a la formación y adopción tecnológica por parte de los usuarios, siendo este último un punto indispensable para el éxito de cualquier estrategia de seguridad.

Para alcanzar el diseño final, se partirá de una estrategia de confianza cero y compromiso con el cumplimiento de la normativa de protección de datos desde el diseño, garantizando que, desde un punto de vista técnico, se establezcan todos los medios necesarios para llevar a término dicho cumplimiento.

La solución aquí planteada está acotada al puesto de trabajo del usuario. No obstante, para garantizar que el nivel de seguridad alcanzado sea el requerido, será necesario constatar que el resto de la infraestructura de la organización cumple los mismos estándares.

5.1. Definición del entorno a segurizar

A continuación, se definirá el abanico de elementos que componen el entorno genérico aquí contemplado, así como los distintos perfiles de usuario y sus niveles de acceso recomendados a cada uno de los elementos del entorno. Tal y como se ha indicado previamente, debido a la amplia penetración del mercado y con el objeto de garantizar la compatibilidad entre los elementos, se primará el uso de tecnologías Microsoft, tanto en nube como *on premise*.

No se contemplan en este entorno posibles accesos a la red interna o servicios web de usuarios externos a la organización ni de socios o colaboradores.

Aplicaciones y herramientas del entorno

Para el entorno en estudio, se define un grupo de elementos genérico con el que cuentan la mayor parte de las organizaciones. El objetivo es que este planteamiento resulte útil al máximo número de organizaciones posible.

- **Correo electrónico**: el servicio se presta desde la nube, a través de las capacidades de Exchange que Microsoft proporciona bajo sus servicios SaaS de O365 (Office 365). Se contempla la posibilidad de desplegar un cliente pesado de Outlook en los equipos de los usuarios, así como su acceso online.

- **Repositorio documental**: se utilizan las capacidades ofrecidas por Sharepoint a través del SaaS O365 completamente desde el entorno de nube. Aunque éste es el repositorio oficial de la organización, se permite a los usuarios aprovechar las funcionalidades de One Drive y Teams (también parte del entorno SaaS de O365) como herramientas de colaboración documental. Su acceso es siempre online.

- **Herramientas de comunicación y colaboración**: se define Teams como la herramienta principal para la comunicación y colaboración de los usuarios de la organización. Esta herramienta ofrece mensajería instantánea, llamadas y videollamadas directas entre usuarios, organización de reuniones virtuales, calendario, gestión de tareas, foros de colaboración, repositorios e integración con multitud de herramientas Microsoft y de otros fabricantes. Se contempla el despliegue del cliente pesado en los equipos de los usuarios y su uso online. Asimismo, se permite el uso de One Drive como almacenamiento propio a nivel de usuario.

- **Herramientas ofimáticas**: los usuarios tienen a disposición la *suite* ofimática completa de Microsoft 365 Applications. Se dispone de aplicación de cálculo, procesador de textos, gestor de datos, *software* de presentación y el resto de las herramientas tradicionales de la *suite* de Office de Microsoft. Se contempla la implementación del cliente pesado en el equipo del usuario y su acceso online.

- **ERP**: se utiliza un ERP (*Enterprise Resource Planning*) genérico para dar soporte a la gestión interna de la organización. Su acceso es remoto (web), sin posibilidad de desplegar un cliente pesado en los equipos de los usuarios.

- **Aplicación de negocio**: se considera el uso de una aplicación de negocio genérica para dar soporte al negocio de la organización. Su acceso es remoto (web), sin posibilidad de desplegar un cliente pesado en los equipos de los usuarios.

- **Herramienta de *ticketing***: se considera el uso de una aplicación de *ticketing* genérica para dar soporte a los procesos internos y gestión de incidencias de la organización. Su acceso es remoto (web), sin posibilidad de desplegar un cliente pesado en los equipos de los usuarios.

- **Intranet corporativa**: está basada en un *site* de Sharepoint y tiene un uso limitado a publicación de noticias y anuncios internos, gestión de documentación pública de la organización y gestión de cuestiones relativas a los recursos humanos de la organización.

- **Dispositivos físicos de acceso de usuario**: los usuarios cuentan con ordenadores portátiles genéricos, equipados con Windows 10. No se contemplan dispositivos Apple o Linux ni otros sistemas operativos.

- **Servicios de directorio**: se utiliza el servicio *Active Directory Domain Services*, basado en Windows Server de Microsoft [43], como base de datos de registro de recursos del entorno y sistema de autenticación y autorización *on premise*.

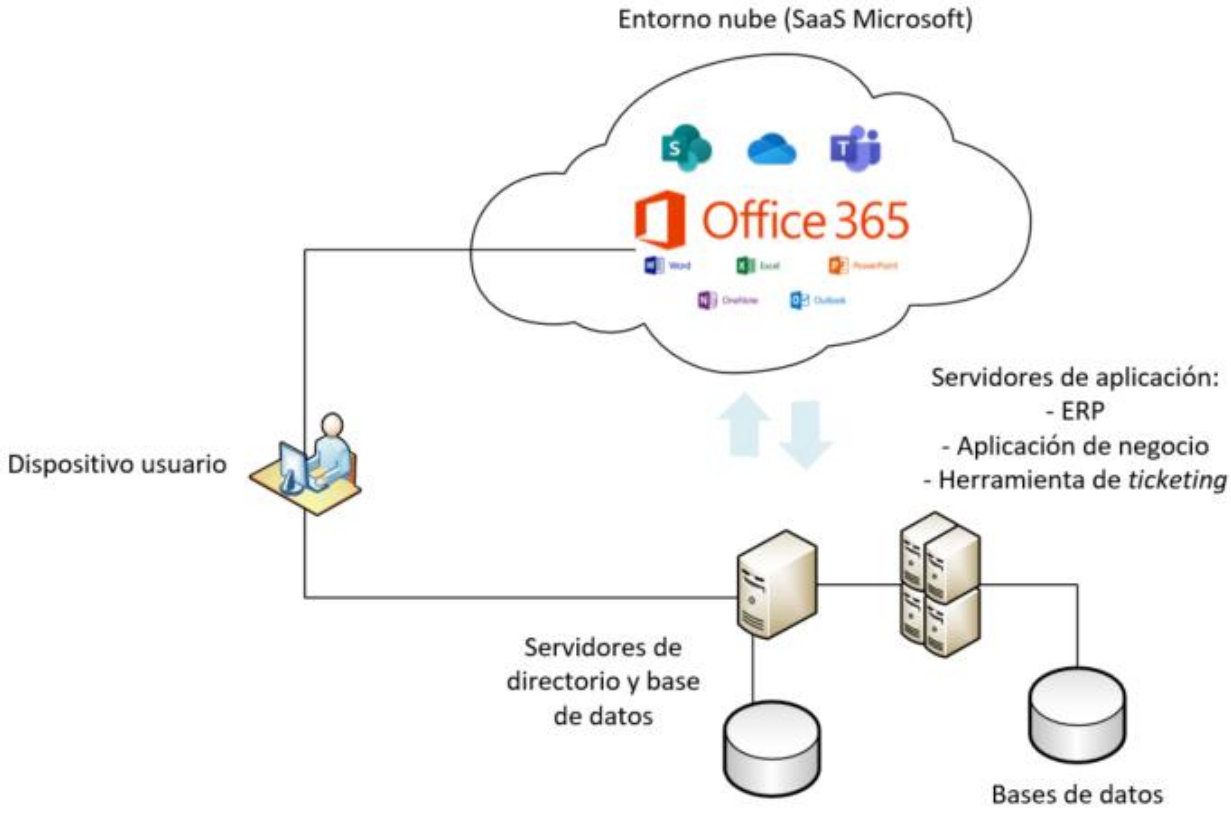

Ilustración 16. Elementos del entorno.

La infraestructura completa de la organización la complementan elementos adicionales. Dichos elementos no se enumeran porque no se consideran dentro del alcance de este informe.

Perfilado de usuarios

A continuación, se describen los diferentes tipos de perfiles de usuario que se consideran en la organización. Se definen también los niveles de acceso para cada uno de ellos, por cada aplicación o servicio.

- **Usuario 1**: administrador del sistema. Forma parte del departamento de TI y tiene derechos de acceso y administración privilegiados sobre los sistemas.

- **Usuario 2**: VIP. Se asigna a los más altos directivos de la organización. Tiene privilegios de acceso sobre la información de negocio.

- **Usuario 3**: negocio. Forma parte de los equipos de ventas o con relación directa con el negocio de la organización. Sus derechos de acceso son limitados en todos los aspectos.

- **Usuario 4**: administración y Operaciones. Dan soporte al negocio y a la organización en general. Sus derechos de acceso son limitados en todos los aspectos.

Los niveles de acceso definidos serán siempre relativos a la aplicación o herramienta en cuestión, y a los perfiles que los ostenten. Se establecen los siguientes:

- **Nivel 1**: nivel de acceso restringido. Es el nivel de acceso más limitado (considerando que se permita algún tipo de acceso). En términos generales, será un acceso fundamentalmente de consulta, la edición tendrá derechos mínimos o restringidos a un área del aplicativo.

- **Nivel 2**: nivel de acceso amplio. Permite una mayor capacidad de operación sobre la herramienta. En ciertos casos, la diferencia entre los niveles 1 y 2 estará basada fundamentalmente en la capacidad para realizar aprobaciones dentro de la herramienta.

- **Nivel 3**: nivel administrador. Asignado al recurso competente, en función de la herramienta, del área de TI, este nivel es el que más riesgo presenta al tener capacidades totales sobre el aplicativo.

- **Sin Acceso (SA)**: el perfil al que se le asigne no tiene permisos de acceso a este aplicativo o herramienta.

	Perfil			
Herramienta	**Usuario 1**	**Usuario 2**	**Usuario 3**	**Usuario 4**
ERP	3	2	1*	1
Aplicación de negocio	3	2	1	SA
Repositorios documentales**	3	2	2	2
Correo electrónico	3	2	2	2
Aplicaciones ofimáticas	3	2	2	2
Herramienta de *ticketing****	3	1	1	2
Herramientas de colaboración	3	2	2	2
Intranet corporativa******	3	2	1	1
Sistema operativo cliente	3	1	1	1
Servicios de directorio	3	1	1	1

Tabla 1. Niveles de acceso por perfil.

*Acceso restringido a nivel de aprobaciones.

**Excepto al administrador, se limitará el acceso en función de la información contenida en cada repositorio.

***Los usuarios 2 y 3 sólo tendrán capacidad de creación de *tickets* y consulta. El resto dependerá del equipo de administración y operaciones.

****Los usuarios 2 podrán realizar publicaciones. Los usuarios 3 y 4 sólo podrán consultar.

5.2. Definición de la línea base de seguridad

En el "Anexo I: Líneas base de seguridad" a este documento, se detallan las líneas base de seguridad definidas para cada uno de los elementos del entorno contemplado en este informe. Dichas líneas base son genéricas y están construidas en base a las guías de seguridad de las TIC (STIC) para la configuración segura del CCN [35] y las recomendaciones de Microsoft [52] para cada producto en los casos en los que aplique. Dado que estás líneas base se ocupan de establecer mínimos genéricos para entornos similares, a la hora de implantarlas en una organización concreta será necesario particularizarlas de forma apropiada considerando las circunstancias específicas de esa organización en cuestión.

5.3. Selección de herramientas Microsoft

Dado que cada fabricante tiene su propio porfolio de productos, es posible que ciertas características de las herramientas descritas en el apartado 4.3 se combinen en un solo producto, o, al contrario, se dividan en varios productos. Esto se considerará asumible mientras se cumplan con solvencia los criterios de funcionalidad establecidos.

-  **Azure Active Directory (Azure AD)**: servicio de directorio activo en nube de Microsoft que O365 utiliza para identificar a los usuarios y asignarles roles y grupos. Se utilizará como vía de autenticación (modelo de identidad híbrida) para cualquier acceso a los servicios *cloud* de Microsoft, y será este servicio también el que se ocupe de administrar la autenticación sobre el directorio local. Esto implica que las configuraciones de autenticación que en él se configuren aplicarán a todo el entorno (tanto nube como local). Provee de un servicio de inicio de sesión único (SSO) para todo el entorno. Sus conexiones son cifradas y utilizan el protocolo TLS.
  Permite establecer diferentes criterios de contraseña, así como de la periodicidad de su renovación y bloqueos de cuenta ante la reiteración de intentos de inicio de sesión fallidos. Permite la configuración del factor múltiple de autenticación (MFA). Permite la configuración de varias tipologías de acceso condicional de dispositivo (en conjunción con Intune) o usuario.
  La creación de nuevas cuentas se realizará en el directorio local por parte del administrador, sincronizándose éste con Azure AD a través de Azure AD Connect, un elemento del sistema desplegado localmente que se utiliza para facilitar la comunicación entre Azure AD y el AD DS. Azure AD Connect permite realizar un filtrado de las cuentas que se sincronizan desde el AD DS hacia Azure AD.
  Se utilizará Azure AD Connect Health para hacer seguimiento del tráfico de inicio de sesión y recuperar métricas de uso del servicio, además de generar alertas sobre los eventos relevantes según la configuración definida. Previene y facilita la gestión de ataques de *malware* o tipo DDoS.

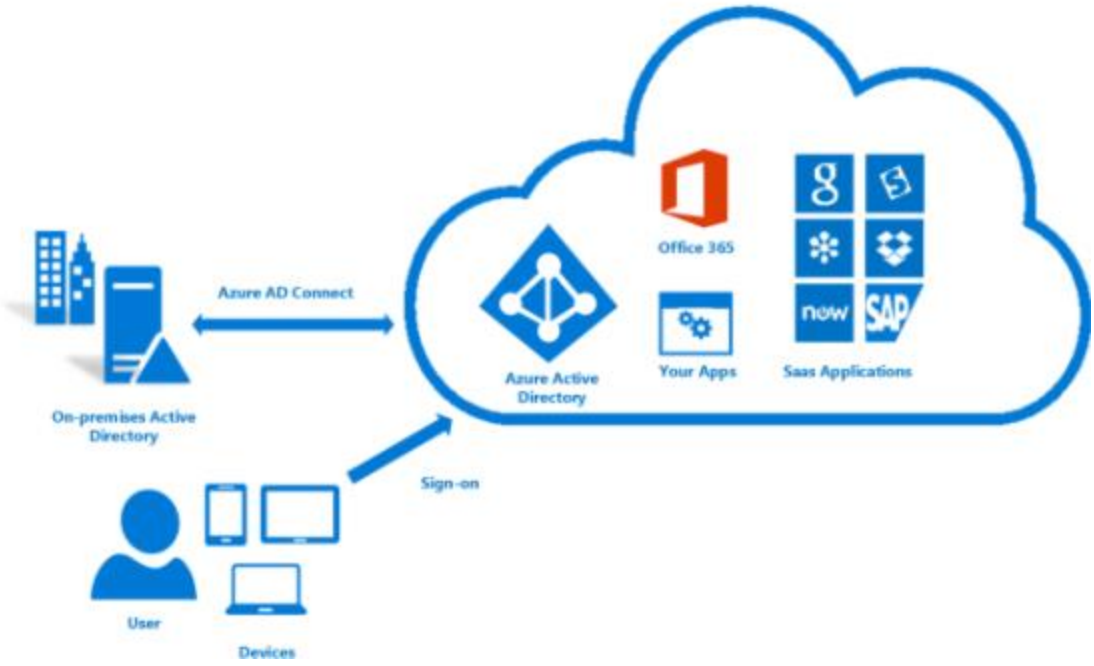

Ilustración 17. Conexión local a través de Azure AD Connect.

- **Azure AD Application Proxy**: de manera específica, para las aplicaciones locales accedidas a través de web (ERP, aplicación de negocio y herramienta de *ticketing*) se utilizará la funcionalidad Application Proxy de Azure AD. Esta funcionalidad ofrece la posibilidad de publicar una URL HTTPS pública en Azure o publicar el acceso a las aplicaciones locales en el portal de aplicaciones (portal web), y permite mantener el sistema SSO que habilita Azure AD para todo el entorno y todas las características de autenticación, gestión de identidades, contraseñas y cuentas de usuario que permite Azure AD; así como definir los niveles de acceso en función del grupo al que pertenezca el usuario.

  Application Proxy actúa como un elemento de filtrado del tráfico que se dirige hacia las aplicaciones, lo que implica que los accesos sean autenticados previamente a su llegada a la aplicación y que los servidores de *back-end* no se expongan al tráfico HTTP directo, lo que mejora la protección contra ataques DoS.

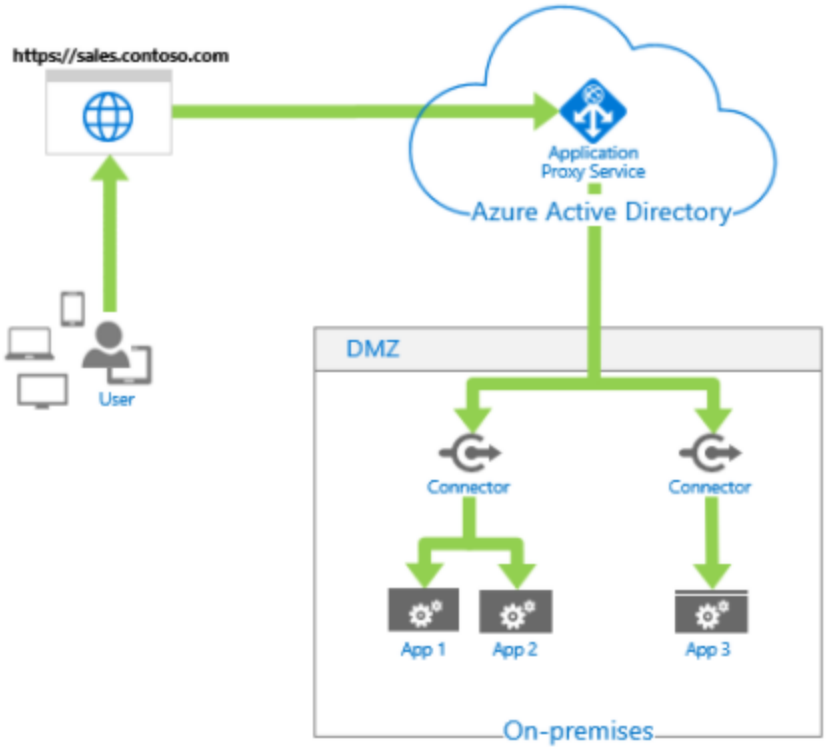

Ilustración 18. Flujo de conexión Azure Application Proxy.

- **Exchange Online**: proporciona al usuario acceso a correo electrónico, calendario, contactos y tareas desde equipos de escritorio (a través del cliente pesado Outlook), dispositivos móviles y vía web. Se integra completamente con Azure AD, por lo que aprovecha todas sus capacidades de gestión de identidades y prevención de amenazas.

  Dispone del servicio Exchange Online Protection, que se trata de un servicio de filtrado de correo electrónico complejo, basado en la nube, que permite realizar un filtrado *antimalware* con cierto grado de personalización, filtrado de conexiones, protección y directivas contra la suplantación de identidad, purga automática de hora cero, aplicación de directivas personalizadas sobre mensajería entrante y saliente, aplicación sobre flujo de correo, auditoría y supervisión de actividad, aplicación de directivas sobre prevención de pérdida de datos (DLP), así como cifrado de comunicaciones, mensajes y archivos.

  Microsoft realiza copias de seguridad *(backup)* para prevenir posibles fallos de *hardware* o *software* en sus centros de procesamiento de datos (CPDs), y existe la posibilidad de solicitar una copia en caso de desastre durante un corto espacio de tiempo.

  A modo de copia de seguridad para el usuario o administrador, existe la figura del archivado (buzón de archivado) que permite establecer políticas de retención a largo plazo. Dispone también de retención de buzones por cuestiones legales (*Legal Hold*).

Cuando se produce el borrado de la carpeta “Eliminados”, existe una carencia de 14 días (ampliables a 30) durante la que los elementos pasan a una carpeta denominada “Elementos recuperables”. Superado ese tiempo, los datos se borran definitivamente.

- **Sharepoint Online**: este servicio, basado en la nube, ofrece capacidades para compartir y administrar el conocimiento de la organización y contenidos de diversas tecnologías y aplicaciones. Todo ello con el objetivo de facilitar la colaboración y el trabajo en equipo dentro de la organización, facilitando la tarea a través de búsquedas inteligentes y el historial de versiones, mientras aporta un entorno seguro para ello.

  Como el resto de las herramientas de O365, aprovecha todas las características de Azure AD para la validación de usuarios y control de acceso.

  En relación al apartado de seguridad y cumplimiento, se beneficia (como el resto de las herramientas de O365) de las funcionalidades aportadas por el Centro de Seguridad y Cumplimiento de Microsoft y de los componentes de seguridad específicos como Defender para O365, entre las que se encuentran las siguientes: análisis de *malware*, administración avanzada de amenazas y protección específica ante ataques de *phishing* o suplantación de identidad, prevención de pérdida de datos (DLP), etiquetado de retención y confidencialidad de archivos e información manual y automático, directivas para la retención de información genéricas y en base al etiquetado, auditoría de uso y registro y cifrado de información y comunicaciones.

  En el entorno contemplado, tanto los repositorios documentales como la intranet corporativa están basados en Sharepoint.

- **One Drive**: es el servicio de almacenamiento en nube de Microsoft para uso individual de los usuarios. Esta herramienta facilita un espacio propio a cada usuario, dentro del entorno en O365 de la organización, para almacenar la documentación y archivos que necesite. Ofrece también la posibilidad de compartir archivos o un cierto espacio (carpetas) para colaborar con otros usuarios de la organización.

  Al formar parte del abanico de herramientas de O365, One Drive se beneficia de las funcionalidades aportadas por Azure AD y el Centro de Seguridad y Cumplimiento de Microsoft, y están disponibles la mayoría de las funcionalidades específicas de seguridad presentadas anteriormente para Sharepoint.

  One Drive está considerada una herramienta de colaboración dentro del entorno en estudio.

- **Teams**: esta herramienta proporciona un *hub* de comunicaciones y colaboración para los usuarios de la organización. Provee de mensajería instantánea, llamadas de audio y video internas, reuniones con posibilidad de compartir contenido, “equipos” de colaboración con

repositorios específicos para compartir archivos y datos e integración con multitud de aplicaciones de Microsoft y de terceros.

La validación de la identidad de los usuarios se realiza a través de Azure AD, como en las otras herramientas de O365, y se pueden establecer diferentes niveles de administración por roles, así como permisos de actividad para los usuarios.

La seguridad en Teams también se puede gestionar desde el Centro de Seguridad y Cumplimiento, de manera que las comunicaciones son cifradas y es posible aplicar etiquetado a la información que permite la aplicación de directivas de retención y confidencialidad, prevención de pérdida de información y *legal hold*.

Teams también permite definir directivas sobre la gestión, a nivel de usuario, de chats y equipos.

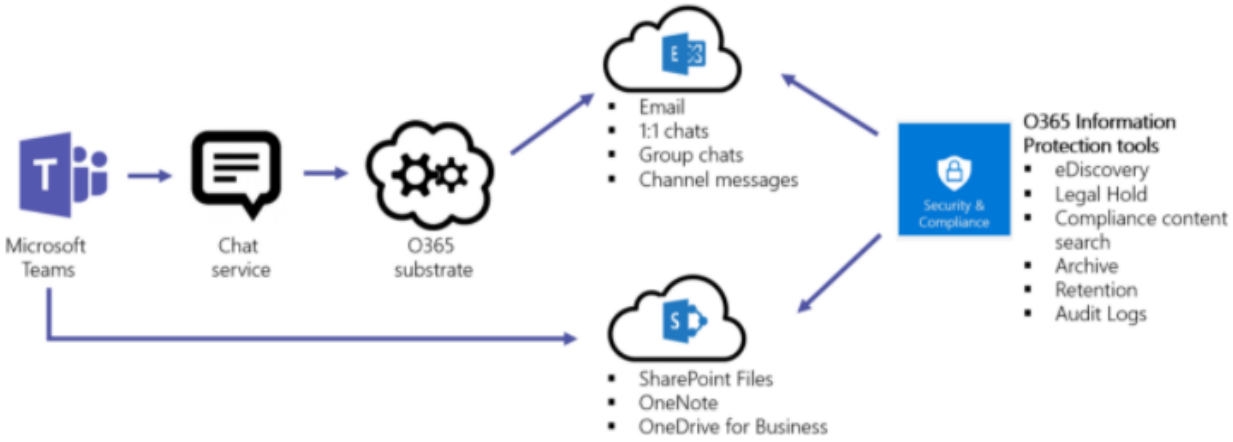

Ilustración 19. Flujo de información entre Teams, Exchange y Sharepoint.

- **Windows 10**: representa el sistema operativo más avanzado de Microsoft, hasta la próxima llegada – prevista para octubre de 2021 – de Windows 11. En el entorno actual, se considerará la versión Windows E5, derivada del licenciamiento nube de O365 y que aporta ciertas características de integración con las herramientas y funcionalidades de la *suite*, lo que mejora la gestión de la seguridad en el entorno.

  La administración del entorno de sistema operativo se realiza por completo desde la herramienta central Endpoint Manager. Esta herramienta reúne varios servicios que antiguamente operaban por separado, entre los que destacan Intune (MDM y MAM de Microsoft) y Configuration Manager (administrador de dispositivos y herramienta para la gestión de la configuración *on premise).* Esta consolidación afianza las bases del *co-management*, que se venía planteando desde hace algún tiempo (gestión centralizada de los entornos local y O365,

muy utilizado para dispositivos móviles), y facilita significativamente al administrador la gestión del espectro completo de dispositivos.

Desde Microsoft Endpoint Manager es posible tanto gestionar las directivas establecidas sobre el sistema operativo (relativas a inicio/cierre de sesión, uso de puertos físicos del dispositivo, conectividad inalámbrica, configuraciones de navegador, etc.), como generar informes de auditoría sobre los sistemas y gestionar características de seguridad, tales como el uso del *firewall* integrado o de Microsoft Defender, que se encarga de proteger al equipo frente a amenazas, tradicionales y avanzadas, y que se nutre en tiempo real de la experiencia de millones de usuarios en todo el mundo para detectar nuevas amenazas a través del análisis de comportamientos anómalos, y así reducir el impacto de un posible ataque de día cero.

Así mismo, Microsoft Endpoint Manager permite el cifrado del disco duro del dispositivo gestionado a través del uso de Bitlocker.

- **Microsoft 365 Apps for Enterprise**: las aplicaciones de escritorio de Office, también conocidas como clientes pesados, representan las versiones completas instalables de las aplicaciones web de O365 y son equivalentes al paquete tradicional de Microsoft Office. Al derivarse de un licenciamiento nube (O365) y tener funcionalidades compartidas con los recursos en nube, su acceso y validación también estarán gobernados por Azure AD. No obstante, al ser aplicaciones instaladas en un equipo (en este caso físico), se requerirán una identificación y autenticación iniciales que las aplicaciones se encargarán de verificar periódica y automáticamente, y que estarán controladas por el inicio de sesión en el dispositivo.

  Estas aplicaciones soportan el uso de las directivas de grupo de O365 y la aplicación de etiquetado sobre los archivos para prevenir las posibles fugas de información.

- **Centro de Seguridad y Cumplimiento de Microsoft**: se ha comentado anteriormente cómo a través del Centro de Seguridad y Cumplimiento de Microsoft se gobierna todo lo relativo a la seguridad y el cumplimiento en O365, tanto en la nube de Microsoft como en sus extensiones *on premise* en las infraestructuras y dispositivos de la organización.

  Resulta relevante el hecho de que, salvo algunas características específicas de algunas herramientas, la centralización de la gestión y de las capacidades de seguridad para todo el entorno genera evidentes beneficios para la organización. El hecho de poder contar con un etiquetado válido y transversal a todas las herramientas del entorno – y que por lo tanto las directivas de retención y confidencialidad sean globalmente válidas –, o la recopilación de datos de auditoría y posteriores análisis conjuntos y cruzados – que puede favorecer la detección temprana de ataques o amenazas – hacen que se aprovechen al máximo las capacidades del sistema.

  Cabe recordar que, al ser servicios *cloud*, las herramientas de O365 se mantienen constantemente actualizadas.

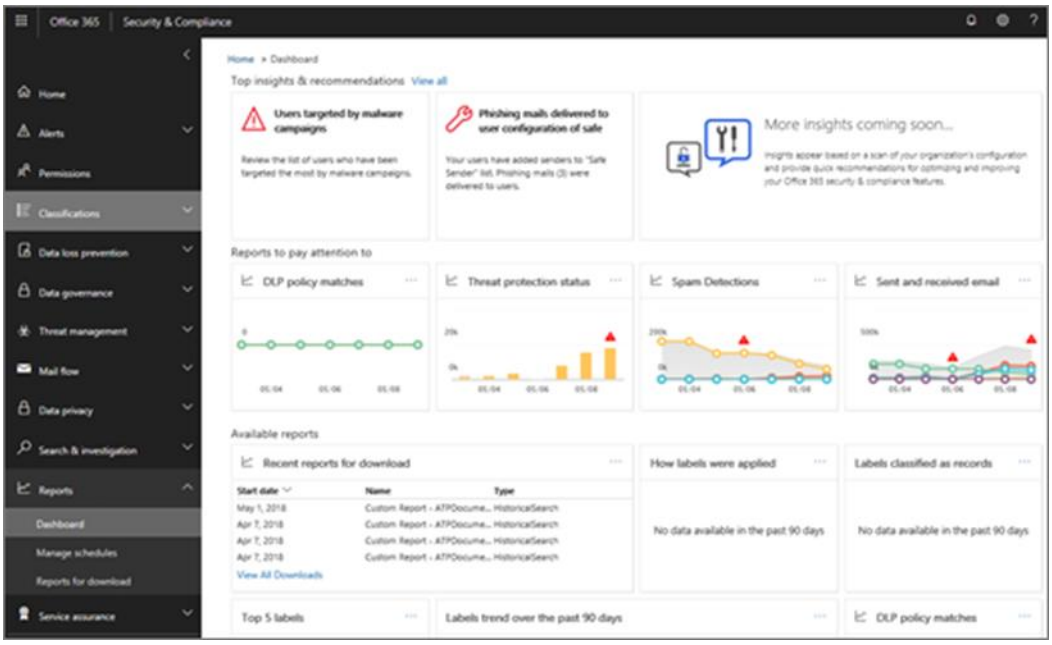

Ilustración 20. Cuadro de mando de informes. Centro de Seguridad y Cumplimiento de Microsoft.

A lo largo de este epígrafe se ha hablado de múltiples herramientas y funcionalidades de Microsoft. Cabe destacar que el licenciamiento de los entornos Microsoft es complejo y en ocasiones ciertos sistemas necesitan de licenciamientos adicionales para proveer de todas las características y funcionalidades para las que tienen potencial, por lo que no se han mencionado aquí todos los productos requeridos desde un punto de vista comercial.

Para solucionar las necesidades de este entorno, se ha considerado un licenciamiento por usuario de Microsoft 365 E5 (M365 E5), una *suite* que contempla todos los subproductos necesarios para cumplir con los requisitos planteados. Como referencia, se ha incluido en el Anexo II de este documento un cuadro resumen con los elementos de licenciamiento que integran M365 E5.

Las herramientas *cloud* de Microsoft Office 365 cumplen con la norma ISO 27001 (entre otras) y con el RGPD, y proveen a sus usuarios de herramientas para facilitar su cumplimiento en aquellas áreas que se encuentren dentro del ámbito de sus servicios, pero fuera de sus competencias (configuraciones inadecuadas, acciones indebidas por parte de los usuarios, etc.).

Toda la documentación se puede encontrar en el Service Trust Portal de Microsoft [46]. Además, el Centro de Seguridad y Cumplimiento proporciona gran cantidad de informes específicos actualizados, relativos a la auditoría del uso de las herramientas, registro de amenazas, gobierno de datos, etc., que ayudan a la organización a cumplir con los requisitos de RGPD y a mejorar su propia seguridad.

5.4. Formación y adopción tecnológica

En el epígrafe 3.2. de este documento (*Riesgos y amenazas en el puesto de trabajo*), se hace referencia al hecho de que las amenazas y vulnerabilidades no provienen solamente de elementos tecnológicos, sino que la intervención humana es indiscutible y muchas veces puede ser definitiva. Por este motivo, para conseguir un nivel de segurización adecuado para el entorno de cualquier organización, es imprescindible hacer partícipes a los usuarios de las amenazas a las que se pueden enfrentar y concienciarles sobre los riesgos que implican, así como de las medidas que deben aplicar para reducir dichos riesgos.

Es habitual que, excepto aquellos usuarios que dependen del departamento de TI, muchos usuarios de la mayor parte de las organizaciones tengan un conocimiento tecnológico e informático limitado. De hecho, para cumplir con el principio de la seguridad desde el diseño, es fundamental que la organización implemente un plan de formación y concienciación interno para todos los usuarios. Este plan, además de formar sobre las amenazas existentes y las medidas que los usuarios pueden aplicar para reducir los riesgos, también debe considerar la adopción tecnológica de las soluciones que la organización vaya implantando (fundamentalmente en momentos de cambio). Esto es así porque si el usuario conoce la tecnología con la que trabaja y el modo adecuado de utilizarla, es mucho más sencillo que detecte gran cantidad de las posibles amenazas existentes e incluso las evite al dejar de cometer errores por desconocimiento.

El objetivo principal de toda formación es la transmisión de conocimiento a los individuos que son formados, de tal forma que consigan asimilar y comprender esos conocimientos hasta el punto de poder aplicarlos de forma efectiva en aquellas tareas en las que se requieran. Dado que los individuos que deben ser formados no son iguales, sino que cada uno tiene sus particularidades, habrá contenidos que deban organizarse de forma general y otros que deberán ser específicos.

En el caso concreto de la formación y adopción tecnológica en un ambiente profesional, es recomendable determinar contenidos que sean asumibles para todos los usuarios de la organización que serán impartidos de forma común, y diferenciar contenidos más específicos en función de cada perfil. En el caso que nos ocupa se generarían 4 perfiles diferentes (TI, VIP, Negocio y administración/operaciones), y deben ser considerados como críticos los usuarios de TI – por el nivel de permisos de administración que ostentan y la necesidad de que lideren la organización a nivel tecnológico y de ciberseguridad – y los usuarios VIP – por las competencias que se les asignan y la alta capacidad de decisión que tienen, lo que puede poner en un alto riesgo a la organización si caen en un engaño –.

Dado que el mundo de la tecnología evoluciona a alta velocidad, es necesario que los planes de formación sean diseñados con una filosofía de continuidad y que, de manera periódica, se aporten nuevos conocimientos a los usuarios y se refuercen los anteriores.

Un ejemplo de herramientas formativas que pueden ser usadas en paralelo a las formaciones tradicionales son las píldoras informativas sobre buenas prácticas – contenidos sucintos que versan sobre una idea o concepto concreto, exponiendo de forma clara y atractiva o vistosa la acción a tomar –, que pueden presentarse en diversos formatos (videos, infografías, diagramas, etc.).

Por último, no se debe perder de vista la verificación de la efectividad de las formaciones. Tests anónimos de evaluación de conocimientos o pruebas prácticas reales pueden ayudar a medir esta cuestión.

Existen multitud de metodologías de adopción aplicables a los cambios en un entorno de TI. Una de las que más éxito tienen en los entornos corporativos es la metodología ADKAR (*Awarness*, *Desire*, *Knowledge*, *Ability* y *Reinforcement*) de Prosci [49], el cual plantea una aproximación a la gestión del cambio basada en sus cinco pilares, que giran alrededor del individuo.

5.5. Incorporación de nuevas herramientas con continuidad de cumplimiento

Unida a la evolución tecnológica de cualquier sistema, se encuentra la incorporación de nuevos recursos y herramientas de *software* que permitan aplicar los últimos avances a la operativa de la organización. Para mantener el mismo nivel de seguridad, dentro de un entorno para el que se han definido e implementado unas líneas base específicas, así como otras tareas relacionadas con la seguridad, se hace necesario que esas nuevas herramientas superen un proceso de homologación antes de permitir su despliegue. Dicho proceso variará y será único para cada organización, pero siempre debe contemplar el análisis y testeo de la herramienta en primer lugar, y una revisión de la integración que ofrece con el resto de los sistemas ya implantados y las medidas de seguridad definidas.

Una vez comprobado lo anterior, deberá ser definida una línea base de seguridad específica para esta herramienta que garantice que se cumplen los mismos mínimos requeridos por la organización, previamente establecidos para el resto de las herramientas.

Por último, esta herramienta deberá ser integrada en los procesos generales de actualización, monitorización y formación establecidos para el resto de las herramientas.

6. Identificación de nuevas amenazas y vulnerabilidades

Es un error habitual suponer que, una vez se ha diseñado el plan de seguridad y se han llevado a cabo los proyectos contemplados, elevando el nivel de segurización del entorno hasta el objetivo propuesto, la organización puede trabajar de un modo seguro de forma indefinida, sin prestar mayor atención a este tema. En contra de este planteamiento, la realidad se impone a través de los ciberdelincuentes, que evolucionan constantemente sus métodos de ataque, o de las propias vulnerabilidades no conocidas de los sistemas, que son aprovechadas para realizar ataques de día cero. Esta dinámica fuerza a las organizaciones a no descuidar ni sus sistemas ni sus procesos, para evitar que el riesgo existente se transforme en impacto.

Como medidas de precaución recomendables para mantener un nivel de seguridad adecuado de forma continua, una vez implementadas las líneas base de seguridad, se encuentran las siguientes:

- **Mantener los sistemas actualizados y bajo soporte de fabricante**: es importante que el licenciamiento de *software* con el que cuente la organización le permita desplegar los parches y actualizaciones de seguridad que el fabricante publique. Asimismo, Será imprescindible realizar dichas actualizaciones en cuanto sea posible. Con respecto al *hardware*, es importante mantener equipos que soporten todas estas actualizaciones con solvencia. En caso contrario, se deberá estudiar su reemplazo.
  En ciertos casos, puede resultar beneficioso también contar con el soporte técnico del propio fabricante.

- **Información actualizada**: los responsables técnicos y de seguridad de la compañía deben mantenerse al tanto de las novedades más importantes que se produzcan en el universo de la ciberseguridad.
  Algunas medidas que ayuden a cumplir con este precepto pueden ser la revisión periódica de las alertas que publica el CCN-CERT [50], involucrarse en foros corporativos de ciberseguridad o mantener reuniones periódicas con los principales fabricantes de seguridad para conocer las novedades, tanto en amenazas y ataques detectado como en soluciones existentes para contrarrestarlos.

- **Monitorización de los sistemas**: del mismo modo que mantener actualizados los sistemas es fundamental, monitorizar la actividad y el comportamiento de aquellos y de los usuarios con los que interactúan también es una gran fuente de información. La recolección de *logs* y eventos, así como de comportamientos inusuales, y aplicar la analítica de datos sobre ellos desde el punto de vista de la seguridad, es labor de cierto tipo de herramientas denominadas SIEM (*Security Information and Event Management*) [51]. Estas herramientas tienen la capacidad de recoger información de todo el entorno (infraestructura de servidores, componentes de red, terminales de usuario, dispositivos móviles, dispositivos IoT, etc.) y relacionarla de tal forma que ayudan a generar alertas tempranas y evitar ataques.

- **Ejecutar pruebas de seguridad**: este tipo de ejercicios se centran en encontrar puntos débiles en la seguridad de la organización, en un entorno controlado, para poder solventarlos antes de que se produzca un ataque real. Simulaciones de ataques de penetración (*pentesting*) o ejercicios avanzados de *Red Team* para entornos complejos ya probados, ayudan a la organización a detectar y corregir vulnerabilidades desde el punto de vista del atacante que de otro modo no encontraría.
  Dentro de los ejercicios de seguridad que se pueden realizar, existen también algunos sencillos que involucran a los usuarios (de forma inconsciente para estos), como los intentos de *phishing* simulados. Ejecutando envíos de e-mails sospechosos que superan los filtros de *spam* y llegan al buzón de entrada del usuario, el equipo de seguridad puede determinar qué porcentaje de usuarios de la organización está preparado para detectar posibles intentos de fraude, lo que ayuda a asignar un nivel de riesgo ante ataques de ingeniería social.

7. Conclusiones

Habiendo recorrido este camino, que partía del gran peso que ha tomado la tecnología en las décadas más recientes, el cual se ha visto incrementado en los últimos 20 meses debido a la particular situación vivida por la humanidad, y cómo esta mayor relevancia ha incrementado los beneficios, pero también los riesgos, para las organizaciones; conociendo las recomendaciones e imposiciones normativas que las organizaciones de estandarización y los gobiernos han definido para regular este ámbito, y transitando por el proceso completo de segurización de una parte del entorno habitual de cualquier organización a día de hoy, mientras se revisaban las medidas técnicas para la defensa cibernética más novedosas, así como los mejores criterios de buenas prácticas, se hace posible aseverar

que, en gran parte de las ocasiones, el ser humano continúa siendo el eslabón más débil. Precisamente por esto, se hace necesario para las organizaciones implementar una política de seguridad basada en la gestión de roles e identidades que garantice que a la identidad de cada usuario le sea asignado el rol correcto, con los mínimos permisos requeridos para que pueda desarrollar su actividad profesional adecuadamente, reduciendo el riesgo para la organización. Esta política no estará completa si no incluye un plan de formación y concienciación adecuado que involucre a todos y cada uno de los usuarios de la organización.

Otra de las cuestiones que nunca volverán a ser como solían es lo que implica la democratización de la nube pública. Es un hecho que la dirección de este modelo es la del crecimiento, y la realidad es que propone unas condiciones que pueden contribuir sensiblemente a la mejora de la ciberseguridad. Actualización continua de sistemas, red mundial hiperconectada para la detección y control de nuevas amenazas, sistemas centralizados más robustos, … La cuestión no es si aprovecharlo, sino cómo hacerlo para que reporte el máximo beneficio a la organización.

Un buen resumen de las cuestiones que una organización debe tener en cuenta en el mundo actual para determinar qué es la ciberseguridad y cómo afrontarla podría basarse en los siguientes principios:

- **Seguridad desde el diseño**: en la definición de cualquier solución, entorno o sistema a implementar o desplegar, se deben valorar posibles fallas o vulnerabilidades y concretarlo de tal forma que sea sencillo supervisarlo y controlarlo, pero no acceder, modificarlo o eliminarlo para elementos ajenos o indeseados.

- **Confianza cero**: no resulta suficiente con validar el acceso inicial, se deben presuponer posibles errores o fallos en el perímetro, o incluso la existencia de elementos internos que pueden resultar dañinos. La validación y monitorización deben ser continuas.

- **Control férreo de acceso**: sólo debe acceder aquel que esté autorizado y exclusivamente a aquello para lo que está autorizado. Cualquier usuario que acceda debe estar perfectamente identificado.

- **Reducción de la superficie de exposición**: minimizar los recursos visibles desde fuera de la red interna implica reducir los puntos inmediatos de ataque y facilitar el control de estos. Colocar puntos intermedios en los accesos, sean propios o de terceros de confianza, que puedan actuar como filtro y barrera ante ataques, aumenta la seguridad.

- **Eliminación de *shadow IT***: no hay seguridad si no hay control sobre el entorno. Desconocer posibles debilidades del entorno, o elementos que pueden suponer un riesgo por no estar bajo control es un fallo grave de seguridad. El entorno debe estar controlado y monitorizado al completo para garantizar que las medidas tomadas sean efectivas, y que el riesgo real es verdaderamente el asumido.

- **Formación y concienciación**: todo usuario de los sistemas debe comprender y asumir los riesgos que se plantean y sus posibles consecuencias, así como las acciones que debe ejecutar para

reducirlos. Para garantizar la seguridad es imprescindible que exista un compromiso con ella por parte de todos los actores involucrados.

8. Desarrollos futuros

A lo largo del documento, se ha hecho patente en multitud de ocasiones que los entornos tecnológicos son (y deben ser) dinámicos y están en constante cambio. En este contexto, es evidente que una correcta política de seguridad debe contemplar vías para afrontar los posibles cambios y evoluciones que puedan producirse a lo largo del tiempo.

El entorno que se ha considerado en este documento es un entorno parcial y acotado que contempla solamente un caso de uso, como son las conexiones remotas de usuarios en una organización para la

que prima la tecnología de un fabricante concreto. A continuación, se proponen tres vías de evolución del entorno que, necesariamente, implicarán la generación de nuevos casos de uso.

- **Desarrollo de un ecosistema de seguridad multifabricante**: no cabe duda de que, una vez se revise el entorno completo de la organización, desde el punto de vista de los sistemas de seguridad, existirá por defecto un ecosistema en el que componentes de múltiples fabricantes deben convivir.
  Para segurizar el puesto de trabajo remoto, ha sido posible ceñirse a componentes de *software* u ofrecidos por un proveedor de nube como servicio. En el caso de las redes físicas en un entorno *on premise*, esto deja de ser viable. *Firewalls*, *switches* u otros componentes de red son necesarios para garantizar la correcta gestión de las comunicaciones de la organización, pero al mismo tiempo suponen un punto básico en cualquier esquema de seguridad.
  Asimismo, hay otros componentes de *software* o servicios que pueden complementar la solución actual. Por ejemplo, Office 365 ofrece diferentes funcionalidades de retención y archivado, pero si se requiriese un *backup* tradicional, sería necesario buscar una alternativa de un tercero.

  Una de las piezas clave de un buen sistema de seguridad es la integración entre sus elementos. Por eso, la primera acción a realizar antes de llevar a cabo despliegue alguno es realizar un análisis teórico de compatibilidad entre elementos, con ayuda de los propios fabricantes u otros socios de negocio expertos en la materia si fuese necesario.
  Una vez se ha seleccionado una solución (o varias) que cubre las necesidades y es teóricamente compatible, lo más recomendable es realizar una prueba de concepto (PoC) en un entorno controlado, en condiciones similares al real, pero sin que los resultados afecten al área de producción.
  Habiendo superado exitosamente los dos pasos anteriores, y contando con la experiencia que hayan aportado, se debe definir una línea base de seguridad para la configuración del elemento que, a la hora del despliegue, sirva de guía para garantizar que se haga en el orden correcto y se mantenga la compatibilidad estudiada con el resto de los elementos del entorno.

  El proceso anterior se debe consolidar, estandarizar y documentar para su posterior ejecución por defecto como paso previo a la implantación de cualquier nuevo elemento de seguridad. Esto se resume en establecer un plan de homologación para los nuevos elementos del sistema, ya sean *hardware* o *software*.

- **Entorno multidispositivo**: el entorno analizado contempla un solo tipo de dispositivo: ordenador portátil con Windows 10. Aunque en organizaciones pequeñas puede existir, lo habitual es encontrar un parque de dispositivos variopintos. Equipos Windows, MacOS o incluso Linux (fundamentalmente en las áreas de desarrollo), y dispositivos móviles (*smartphones*, *tablets*, etc.) son comunes en muchos entornos actuales. Esta diversidad aporta retos adicionales, centrados principalmente en la compatibilidad y la integración, pero también en el ciclo de vida de su *hardware* y *software*, y mecanismos de control y gestión que en ocasiones se

requiere que sean específicos. Estos dispositivos requieren un análisis específico y la creación de líneas base de seguridad dedicadas – cuestiones que se podrían desarrollar en un futuro – que podrían diferir en los aspectos formales con respecto a las diseñadas para los equipos del escenario aquí planteado, pero no deberían hacerlo en los aspectos de fondo. La cuestión principal es que conceptualmente se respeten las mismas medidas básicas de seguridad en todo el parque de dispositivos, de tal forma que se consiga alcanzar el nivel de reducción del riesgo deseado.

Caso aparte es el uso de dispositivos propios en el entorno profesional. La evolución de la tecnología y la penetración de esta en la sociedad han hecho posible que, en algunos entornos, cada usuario pueda utilizar sus propios dispositivos privados para uso profesional. Este concepto de uso, conocido como *Bring Your Own Device* (BYOD), genera una necesidad de replanificar ciertos aspectos de seguridad en el entorno al que se vinculan, y requieren que el usuario ceda parte del control de su dispositivo a la organización que le emplea.
Una posible evolución de este informe podría centrarse en el nuevo planteamiento que sería necesario desarrollar para integrar una política BYOD en la organización, manteniendo el nivel y los estándares de seguridad global del entorno.

- **Implementación de escritorios virtuales**: como se refería al inicio del informe, hay diversas formas de ofrecer a los usuarios remotos conexión con los sistemas y datos de la organización. En función de las condiciones y cómo sean utilizados, pueden redundar en un aumento o disminución de la seguridad global con respecto a otras alternativas.

  En el caso práctico planteado, se propone una conexión directa con los sistemas SaaS, entregados por el fabricante Microsoft desde su nube, y una conexión con las aplicaciones locales a través de un servicio *proxy* de aplicación también proporcionado por Microsoft desde su nube. En estas condiciones, el usuario utiliza un dispositivo corporativo para conectarse a los sistemas de la compañía, utilizando métodos seguros de conexión y validación centralizados en la nube de un proveedor. Todo esto implica que, aunque muchas de las tareas se desarrollen remotamente y el equipo del usuario tenga aplicadas todas las medidas de seguridad definidas, el equipo podría encontrarse físicamente en condiciones de vulnerabilidad, creando un posible riesgo para la organización de fuga de información o intentos de penetración en la red de la organización (por ejemplo, si el dispositivo es robado, existe un cierto riesgo de que se acceda al contenido de su disco duro o se aproveche su condición de dispositivo registrado en el dominio de la organización para evitar reglas de acceso condicional).

  Una posible solución para reducir este riesgo en aquellos casos en los que sea rentable (y técnicamente factible) para la organización, sería aprovechar una arquitectura de escritorios virtuales. Ya sean desplegados en la infraestructura local, o utilizando servicios en nube de un proveedor, los escritorios virtuales proporcionan un entorno seguro para los datos y sistemas de la organización, de tal manera que el usuario no está trabajando en su dispositivo corporativo directamente, sino que lo hace aprovechando las capacidades físicas y lógicas de este (como teclado, ratón, tarjeta de red o *software* de conectividad), para desarrollar su actividad en una

máquina virtual que se encuentra alojada en la infraestructura (nube o local) de la organización. Esto facilita el control, monitorización y operación sobre la máquina que un administrador de la organización puede tener, y minimiza el riesgo de que existan fugas de información, ya que todo el trabajo que se realice y los datos que se manejen por parte del usuario permanecerán en los servidores de origen.

En el ámbito de la nube pública, la última evolución de este servicio la ha protagonizado este agosto Microsoft con Windows 365. Esta solución proporciona un servicio de DaaS (escritorio como servicio) al que se puede acceder desde un navegador común, utilizando un dispositivo de sobremesa, portátil o incluso dispositivos Android o iOS, al mismo tiempo que requiere unas tareas de administración mínimas en comparación con las soluciones tradicionales de VDI.

No se ha comentado en este documento el proceso relativo a la preparación y entrega de los dispositivos físicos a sus usuarios y la posible reutilización de esos mismos dispositivos en caso de que se produjesen bajas y altas de nuevos usuarios que se incorporen a la organización. En el contexto actual, y el que está por venir en los próximos años, esta cuestión resulta interesante, pues la cadena de suministro y la custodia del dispositivo pueden suponer también un riesgo para la organización. Una incorrecta manipulación, previamente al despliegue de la imagen del sistema operativo de la organización y de las políticas de seguridad, puede suponer la entrada de *malware* o la apertura de puertas traseras que, posteriormente, podrían redundar en un ataque silencioso a los sistemas de la organización a través de ese agujero de seguridad.

Como vía de prevención para este tipo de errores o vulnerabilidades provocadas, los fabricantes proponen soluciones que simplifican el proceso de despliegue de imagen y configuración de nuevos equipos hasta el punto de que prácticamente salgan de fábrica con ello hecho. En el caso concreto de Microsoft, la herramienta Autopilot permite a los fabricantes registrar los dispositivos en la nube de Microsoft antes de que salgan de fábrica, utilizando un número de referencia específico. De esta forma, el dispositivo se envía directamente al usuario, que habrá recibido sus credenciales corporativas por otra vía, que encenderá el equipo e introducirá sus datos de identificación. Una vez validado su usuario y proporcionada una vía de conexión válida a internet, Autopilot se encargará a través de un proceso automatizado de desplegar la imagen corporativa en el equipo y realizar las configuraciones que el responsable de la organización haya definido en función del perfil del usuario.

Este proceso simplifica la entrega de nuevos dispositivos (o de aquellos reacondicionados) y garantiza que cada equipo cuente con las medidas de seguridad establecidas por la organización para el perfil de usuario concreto que lo vaya a utilizar.

Bibliografía

[1] Check Point Software Technologies Ltd, «Cyber Attack Trends,» 2021. [En línea]. Disponible en: https://pages.checkpoint.com/cyber-attack-2021-trends.html. [Último acceso: 19 Julio 2021].

[2] Barracuda Networks, «Spear Phising: Top Threats and Trends,» Julio 2021. [En línea]. Disponible en: https://assets.barracuda.com/assets/docs/dms/spear-phishing_report_vol6.pdf. [Último acceso: 12 Agosto 2021].

[3] J. L. Abellán, «CAPEX,» Economipedia, 8 Junio 2018. [En línea]. Disponible en: https://economipedia.com/definiciones/capex.html. [Último acceso: 17 Julio 2021].

[4] DICCADMINN3G0, «Diccionario de Negocios. Capex,» 14 Marzo 2018. [En línea]. Disponible en: https://diccionariodenegocios.com/c/capex/. [Último acceso: 26 Julio 2021].

[5] C. Joric, «El teletrabajo nació de otra crisis,» *La Vanguardia,* 15 Diciembre 2020.

[6] IBM, «¿Qué es Traiga su propio dispositivo (BYOD)?,» [En línea]. Disponible en: https://www.ibm.com/services/digital-workplace/byod. [Último acceso: 8 Agosto 2021].

[7] P. a. G. T. Mell, "The NIST Definition of Cloud Computing," Septiembre 2011. [Online]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. [Accessed 25 Julio 2021].

[8] CCN-PYTEC, Centro Criptológico Nacional., «Arquitecturas de Acceso Remoto Seguro,» 31 Agosto 2020. [En línea]. Disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/335-pildorapytec-31ago2020-arquitecturas-de-acceso-remoto-seguro/file. [Último acceso: 25 Mayo 2021].

[9] AENOR, Asociación Española de Normalización y Certificación., «ISO/IEC 7498-1:1994,» 17 Noviembre 1994. [En línea]. Disponible en: https://tienda.aenor.com/norma-iso-iec-7498-1-1994-020269. [Último acceso: 25 Mayo 2021].

[10] Wikipedia, «Modelo OSI,» 21 Agosto 2021. [En línea]. Disponible en: https://es.wikipedia.org/wiki/Modelo_OSI. [Último acceso: 23 Agosto 2021].

[11] CEC, Confederación de Empresarios de La Coruña., «VPNaaS: arquitectura moderna de tecnología VPN diseñada para la Cloud,» 30 Abril 2020. [En línea]. Disponible en: https://noticias.cec.es/index.php/2020/04/30/vpnaas-arquitectura-moderna-de-tecnologia-vpn-disenada-para-la-cloud/. [Último acceso: 26 Mayo 2021].

[12] F5, «¿Qué es la VPN SSL?,» [En línea]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/ssl-vpn. [Último acceso: 28 Junio 2021].

[13] IBM, «¿Qué es la infraestructura de escritorio virtual (VDI)?,» 23 Marzo 2021. [En línea]. Disponible en: https://www.ibm.com/cloud/blog/what-is-virtual-desktop-infrastructure. [Último acceso: 26 Mayo 2021].

[14] VMware Tech Zone, «Arquitectura Horizon,» [En línea]. Disponible en: https://techzone.vmware.com/resource/horizon-architecture#introduction. [Último acceso: 17 Agosto 2021].

[15] CIBERSEGURIDAD.blog, «VPNaaS, el acceso remoto que necesitas,» 29 Marzo 2020. [En línea]. Disponible en: https://ciberseguridad.blog/vpnaas-el-acceso-remoto-que-necesitas/. [Último acceso: 18 Junio 2021].

[16] Citrix, «Arquitectura de referencia para la solución Acceso con Remote PC de Citrix,» 22 Abril 2021. [En línea]. Disponible en: https://docs.citrix.com/es-es/tech-zone/design/reference-architectures/remote-pc.html. [Último acceso: 7 Julio 2021].

[17] Microsoft, «Te damos la bienvenida al PC en la nube Windows 365,» [En línea]. Disponible en: https://www.microsoft.com/es-es/windows-365. [Último acceso: 16 Agosto 2021].

[18] Citrix, «¿Qué es el espacio de trabajo digitlal?,» [En línea]. Disponible en: https://www.citrix.com/es-es/solutions/digital-workspace/what-is-digital-workspace.html. [Último acceso: 17 Agosto 2021].

[19] INCIBE, Insituto Español de Ciberseguridad., «Glosario de términos de ciberseguridad,» 2020. [En línea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf. [Último acceso: 1 Julio 2021].

[20] INCIBE, Instituto Nacional de Ciberseguridad, «Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?,» 20 Marzo 2017. [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian. [Último acceso: 1 Agosto 2021].

[21] ENISA, Agencia Europea de Seguridad de las Redes y de la Información, «Panorama de amenazas de ENISA,» 2020. [En línea]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends . [Último acceso: 5 Junio 2021].

[22] CCN-CERT, Centro Criptológico Nacional., «Ciberamenazas y Tendencias,» 31 Mayo 2019. [En línea]. Disponible en: https://www.ccn-cert.cni.es/en/reports/public/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html. [Último acceso: 3 Junio 2021].

[23] INCIBE Y OSI, Insituto Nacional de Ciberseguridad y Oficina de Seguridad del Internauta., «Guía de ciberataques,» 18 Octubre 2020. [En línea]. Disponible en: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf. [Último acceso: 5 Junio 2021].

[24] INCIBE, Insituto Nacional de Ciberseguridad., «Ciberamenazas contra entornos empresariales,» 2020. [En línea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf. [Último acceso: 30 Julio 2021].

[25] I. Belcic, «¿Qué es el malware?,» 19 Mayo 2021. [En línea]. Disponible en: https://www.avast.com/es-es/c-malware. [Último acceso: 8 Junio 2021].

[26] D. Bodnar, «Qué es la ingeniería social y cómo evitarla,» 19 Mayo 2021. [En línea]. Disponible en:

https://www.avast.com/es-es/c-social-engineering. [Último acceso: 30 Julio 2021].

[27] J. Jiménez, «Todos los ataques a aplicaciones web de los servidores,» 17 Julio 2021. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/principales-ataques-aplicaciones-web-servidores/. [Último acceso: 1 Agosto 2021].

[28] Microsoft, «Bienvenida a servicios de escritorio remoto,» 22 Febrero 2017. [En línea]. Disponible en: https://docs.microsoft.com/es-es/windows-server/remote/remote-desktop-services/welcome-to-rds. [Último acceso: 13 Agosto 2021].

[29] Netec, «¿Qué es la seguridad informática?,» 2021. [En línea]. Disponible en: https://www.netec.com/que-es-seguridad-informatica. [Último acceso: 8 Agosto 2021].

[30] ISO, International Organization for Standardization., «ISO/IEC 27003:2017,» Marzo 2017. [En línea]. Disponible en: https://www.iso.org/standard/63417.html. [Último acceso: 13 Agosto 2021].

[31] Colegio Oficial de Ingenieros de Telecomunicación, «Implantación de sistemas de gestión de la seguridad de la información ((SGSI) según la anorma ISO 27001,» [En línea]. Disponible en: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf. [Último acceso: 17 Agosto 2021].

[32] AEPD, Agencia Española de Protección de Datos., «Directrices para la elaboración de contratos entre responsables y encargados del tratamiento,» 2019. [En línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf#:~:text=El%20encargado%20del%20tratamiento%20es%20la%20persona%20f%C3%ADsica,trata. [Último acceso: 19 Agosto 2021].

[33] Microsoft, «Adoptar una seguridad proactiva con Confianza cero,» [En línea]. Disponible en: https://www.microsoft.com/es-es/security/business/zero-trust. [Último acceso: 30 Julio 2021].

[34] S. H, «Principios de diseño de arquitectura de confianza cero,» 20 Noviembre 2019. [En línea]. Disponible en: https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles. [Último acceso: 20 Agosto 2021].

[35] CCN-CERT, Centro Criptológico Nacional., «Defensa frente a las ciberamenazas.,» 26 Agosto 2021. [En línea]. Disponible en: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html. [Último acceso: 27 Agosto 2021].

[36] NIST, National Institute of Standards and Technology., «Centro de recursos de seguridad informática,» 4 Agosto 2021. [En línea]. Disponible en: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53. [Último acceso: 16 Agosto 2021].

[37] DoD CYBER EXCHANGE Public, Department of Defense., «Guía de implementación técnica de seguridad (STIG),» [En línea]. Disponible en: https://public.cyber.mil/stigs/. [Último acceso: 14 Agosto 2021].

[38] UAH, Universidad de Alcalá de Henares., *Auditoría informática, apuntes de clase de la asignatura 201074,* Alcalá de Henares, 2019-2020.

[39] UAH, Universidad de Alcalá de Henares., *Seguridad informática, apuntes de clase de la asignatura 201849,* Alcalá de Henares, 2019-2020.

[40] INCIBE, Instituto Nacional de Ciberseguridad., «Catálogo de empresas y soluciones de ciberseguridad,» Abril 2016. [En línea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/catalogo_ciberseguridad.pdf . [Último acceso: 10 Agosto 2021].

[41] Microsoft., «¿Qué es Azure Active Directory?,» 5 Junio 2020. [En línea]. Disponible en: https://docs.microsoft.com/es-es/azure/active-directory/fundamentals/active-directory-whatis. [Último acceso: 20 Agosto 2021].

[42] Microsoft., «Uso de Azure AD Application Proxy para publicar aplicaciones locales para usuarios remotos.,» 27 Abril 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/azure/active-directory/app-proxy/what-is-application-proxy. [Último acceso: 20 Agosto 2021].

[43] Microsoft, «Introducción a AD DS,» 7 Agosto 2018. [En línea]. Disponible en: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/ad-ds-getting-started. [Último acceso: 22 Agosto 2021].

[44] Microsoft, «Microsoft 365 de licencias para el cumplimiento de & la seguridad,» 18 Agosto 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance. [Último acceso: 30 Agosto 2021].

[45] Microsoft, «Security &Compliance Center,» 17 Agosto 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center. [Último acceso: 23 Agosto 2021].

[46] Microsoft, «Informes de auditoría,» [En línea]. Disponible en: https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=d1172883-7a12-45e9-. [Último acceso: 21 Agosto 2021].

[47] CCN. Centro Criptológico Nacional., «Medidas de seguridad para acceso remoto.,» 13 Marzo 2020. [En línea]. Disponible en: https://www.ccn-cert.cni.es/informes/abstracts.html?own=0. [Último acceso: 27 Agosto 2021].

[48] INCIBE. Instituto Nacional de Ciberseguridad., «Concienciación y formación. Políticas de seguridad para la pyme.,» [En línea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/concienciacion-y-formacion.pdf. [Último acceso: 23 Agosto 2021].

[49] Prosci., «¿Qué es ADKAR?,» [En línea]. Disponible en: http://www.prosci.es/es/que-es-adkar-faculta. [Último acceso: 25 Agosto 2021].

[50] CCN-CERT. Centro Criptológico Nacional., «Alertas CCN-CERT.,» 2 Septiembre 2021. [En línea]. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert.html . [Último acceso: 2 Septoembre 2021].

[51] VIEWNEXT, «¿Qué es un SIEM?,» 9 Enero 2020. [En línea]. Disponible en: https://www.viewnext.com/que-es-un-siem/ . [Último acceso: 31 Agosto 2021].

[52] Microsoft, «Documentación acerca de la seguridad,» 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/security/. [Último acceso: 20 Agosto 2021].

Bibliografía de ilustraciones

[1] Ilustración 1. Teletrabajo, «La mar de Onuba.,» [En línea]. Disponible en: http://revista.lamardeonuba.es/a-la-espera-de-una-ley-del-teletrabajo-esta-es-la-normativa-vigente/. [Último acceso: 28 Julio 2021].

[2] Ilustración 2. Modelos de servicio en la nube. Microsoft, «¿Por qué Azure?,» [En línea]. Disponible

en: https://whyazure.in/public-cloud-shared-responsibility/. [Último acceso: 13 Agosto 2021].

[3] Ilustración 3. Modelos de implementación en nube. Sashi, «Blogs de eTech,» 8 Agosto 2020. [En línea]. Disponible en: http://www.etechblogs.com/cloud-deployment-models-public-private-hybrid-community-cloud/. [Último acceso: 6 Junio 2021].

[4] Ilustración 4. Infraestructura local. Elaboración propia, 2021.

[5] Ilustración 5. Infraestructura en nube. Elaboración propia, 2021.

[6] Ilustración 6. Infraestructura híbrida. Elaboración propia, 2021.

[7] Ilustración 7. Diagrama de arquitecturas de acceso remoto y sus respectivos destinos. CCN-PYTEC, Centro Criptológico Nacional, «Diagrama de arquitecturas de acceso remoto y sus respectivos destinos.,» 31 Agosto 2020. [En línea]. Disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/335-pildorapytec-. [Último acceso: 30 Mayo 2021].

[8] Ilustrción 8. Arquitecturas de acceso remoto. CCN-PYTEC, Centro Criptológico Nacional., «Arquitecturas de acceso remoto.,» 31 Agosto 2020. [En línea]. Disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-. [Último acceso: 30 Mayo 2021].

[9] Ilustración 9. Conexión VPN. Elaboración propia, 2021.

[10] Ilustración 10. Infraestructura VPNaaS. Elaboración propia, 2021.

[11] Ilustración 11. Infraestructura Portal Web. Elaboración propia, 2021.

[12] Ilustración 12. Infraestructura VDI. Elaboración propia, 2021.

[13] Ilustración 13. Principales 15 amenazas 2019-2020 (ENISA). ENISA, «Principales 15 amenazas 2019-2020 (ENISA),» 2020. [En línea]. Disponible en: https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-enisa-list-of-top-15-. [Último acceso: 14 Agosto 2021].

[14] Ilustración 14. Diagrama de seguridad Confianza Cero. Microsoft, «Adoptar una seguridad proactiva con confianza cero.,» [En línea]. Disponible en: https://www.microsoft.com/es-es/security/business/zero-trust. [Último acceso: 18 Agosto 2021].

[15] Ilustración 15. Taxonomía de productos. INCIBE, Insituto Nacional de Ciberseguridad, «Catálogo de empresas y soluciones de ciberesegurdad. Taxonomía de producto.,» Abril 2016. [En línea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/catalogo_ciberseguridad.pdf. [Último acceso: 16 Agosto 2021].

[16] Ilustración 16. Elementos del entorno. Elaboración propia & iconos de Microsoft, «New Design Office 365 app icon package zip,» [En línea]. Disponible en:

https://www.dropbox.com/s/94kq7dtaqx3spya/NewDesign_Office365_app_icon_package.zip?dl=0&file_subpath=%2FNewDesign_Office365_app_icon_package%2FP. [Último acceso: 20 Agosto 2021].

[17] Tabla 1. Niveles de acceso por perfil. Elaboración propia, 2021.

[18] Ilustración 17. Conexión local a través de Azure AD Connect. Microsoft, «Conexión local a través de Azure AD Connect.,» 1 Agosto 2020. [En línea]. Disponible en: https://docs.microsoft.com/es-es/azure/active-directory/hybrid/whatis-azure-ad-connect. [Último acceso: 20 Junio 2021].

[19] Ilustración 18. Flujos de conexión Azure Applications Proxy. Microsoft, «Flujos de conexión Azure Applications Proxy.,» 27 Abril 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/azure/active-directory/app-proxy/what-is-application-proxy. [Último acceso: 30 Agosto 2021].

[20] Ilustración 19. Flujo de información entre Teams, Exchange y Sharepoint. Microsoft, «Flujo de información entre Teams, Exchange y Sharepoint.,» 31 Agosoto 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/microsoftteams/security-compliance-overview. [Último acceso: 1 Septiembre 2021].

[21] Ilustración 20. Cuadro de mando de informes. Centro de Seguridad y Cumplimiento de Microsoft. Microsoft, «Cuadro de mando de informes. Centro de Seguridad y Cumplimiento de Microsoft.,» 28 Agosto 2021. [En línea]. Disponible en: https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/reports-and-insights-in-. [Último acceso: 29 Agosto 2021].

[22] Anexo l. Tabla 2. Formulario línea base de seguridad, servicios de directorio. Elaboración propia, 2021.

[23] Anexo l. Tabla 3. Formulario línea base de seguridad, sistema operativo. Elaboración propia, 2021.

[24] Anexo l. Tabla 4. Formulario línea base de seguridad, aplicaciones ofimáticas. Elaboración propia, 2021.

[25] Anexo l. Tabla 5. Formulario línea base de seguridad, correo electrónico. Elaboración propia, 2021.

[26] Anexo l. Tabla 6. Formulario línea base de seguridad, herramientas de colaboración. Elaboración propia, 2021.

[27] Anexo l. Tabla 7. Formulario línea base de seguridad, intranet corporativa. Elaboración propia, 2021.

[28] Anexo l. Tabla 8. Formulario línea base de seguridad, repositorios documentales. Elaboración propia, 2021.

[29] Anexo l. Tabla 9. Formulario línea base de seguridad, herramienta de ticketing. Elaboración propia, 2021.

[30] Anexo l. Tabla 10. Formulario línea base de seguridad, aplicación de negocio. Elaboración propia,

2021.

[31] Anexo l. Tabla 11. Formulario línea base de seguridad, ERP. Elaboración propia, 2021.

[32] Anexo ll. Ilustración 21. Esquema licenciamiento Microsoft 365. Microsoft, «GitHub. Aaron Dinnage,» Junio 2021. [En línea]. Disponible en: https://github.com/AaronDinnage/Licensing. [Último acceso: 31 Agosto 2021].

Anexo I: Líneas base de seguridad

Formulario línea base de seguridad servicios de directorio		
Índice	**Configuración**	**Comentarios**
1	Comunicaciones cifradas	-
2	Modelo de identidad híbrida. Validación de usuarios única y centralizada (SSO)	Gestión única de acceso a nube y local. Acceso directo a AD local sólo a administradores y en caso de caída del servicio con habilitación manual
3	Acceso a directorio activo local sólo para el administrador global	Se recomienda tener entre 2 y 4 administradores globales en la organización.
4	Gestión de directorio activo central sólo por parte del administrador global	Se recomienda tener entre 2 y 4 administradores globales en la organización.
5	Uso de cuentas de usuarios reales	Evitar la creación de cuentas genéricas
6	Uso de doble factor de autenticación	-
7	Requisito de contraseña fuerte	Restringir las contraseñas a las denominadas *strong password*
8	Renovación periódica de contraseña	Requerimiento de cambio de contraseña periódico
9	Historial de contraseñas	Impedir el uso de las dos últimas contraseñas utilizadas al renovar la contraseña
10	Control de acceso por roles	Asignación del rol menos permisivo
11	Bloqueo de cuenta	Bloqueo de cuenta de usuario después de 3 intentos erróneos de acceso
12	Registro de acceso	Establecer un registro de todos los intentos de acceso, exitosos o no
13	Asignación de rol en el momento de la creación de la cuenta	-
14	Limitación de la asignación de cuentas de administrador parcial y administrador global	Los permisos de administrador (global o local) deberán ser concedidos bajo estricta aprobación, en aquellos casos considerados necesarios. Siempre se seguirá la regla de otorgar los permisos mínimos indispensables
15	Creación y asignación de grupos de seguridad en función de perfiles	-
16	Creación y asignación de grupos de Microsoft 365 en función de perfiles	-
17	Control de grupos por parte del administrador	-
18	Creación de nuevos usuarios sólo bajo aprobación	Flujo de aprobación a determinar por parte de la organización
19	Verificación mensual de usuarios activos	Dar de baja a usuarios inactivos según políticas de la organización
20	Eliminación de usuarios inactivos	Establecer flujo de aprobación.
21	Implementación de acceso condicional por dispositivos	Sólo se permitirá el acceso a los recursos de la organización desde dispositivos registrados en el dominio. Se podrán utilizar también otras características del acceso condicional como "el viaje imposible" o la conformidad de dispositivos (que cumplan con los requisitos de seguridad establecidos)
22	Actualización de los servicios de directorio	Tanto en nube como local
23	Sistema de defensa ante DDoS	-
24	Implementación de SSO para entorno nube y local	Centralización de la administración del acceso único de sesión (SSO)

Tabla 2. Formulario línea base de seguridad, servicios de directorio.

Formulario línea base de seguridad sistema operativo		
Índice	**Configuración**	**Comentarios**
1	Requerir contraseña al arranque del dispositivo	-
2	Política de contraseña fuerte	Registrar historial de contraseñas para evitar repetición, cambio de contraseña periódico
3	Requerir contraseña previa activación de la sesión	-
4	Auditoría Inicio/Cierre de sesión de la cuenta	-
5	Seguimiento detallado, auditar actividad dispositivos PNP *(Plug and Play)*	-
6	Uso de privilegios, auditar uso de privilegios confidenciales	-
7	Auditar integridad del sistema	-
8	Directiva de cifrado de disco con BitLocker	-
9	Bloquear la reproducción automática para los dispositivos	-
10	Bloquear el control del usuario sobre las instalaciones en el dispositivo	Limita la instalación de aplicaciones si el usuario no es administrador
11	Bloquear el uso de puertos USB y tarjetas SD del dispositivo	-
12	Limitar uso de navegadores a Microsoft Edge	-
13	Requerir SmartScreen para Microsoft Edge	-
14	Bloquear el acceso a sitios malintencionados	-
15	Bloquear el acceso a sitios de almacenamiento o servicios en nube no permitidos	-
16	Bloquear la descarga de archivos no comprobados	-
17	Bloquear el administrador de contraseñas en el navegador	-
18	Impedir que el usuario invalide los errores de certificado	-
19	Bloquear la instalación de dispositivos de hardware por clases de instalación	-
20	Bloquear características específicas del consumidor	-
21	Definir minutos de inactividad de la pantalla de bloqueo hasta que se activa el protector de pantalla	-
22	Habilitar *firewall*	-
23	Bloquear arrastrar y colocar, o copiar y pegar archivos en la zona de Microsoft Edge	-
24	Bloqueo del inicio de aplicaciones de comunicación de Office en un proceso secundario	-
25	Activar la protección en tiempo real	-
26	Examinar archivos de almacenamiento	-
27	Activar la supervisión de comportamiento	-
28	Impedir robo de credenciales	-
29	Acción frente a aplicaciones potencialmente no deseadas de Windows Defender	-
30	Habilitar la protección de red	-
31	Auditar inicialización de controladores de arranque del sistema	Verificación de posible *malware* en arranque a través de revisión de arranque temprano.
32	Habilitar Windows Update	-

Tabla 3. Formulario línea base de seguridad, sistema operativo.

Formulario línea base de seguridad aplicaciones ofimáticas		
Índice	**Configuración**	**Comentarios**
1	Acceso con autenticación de doble factor	-
2	Política de contraseña fuerte	-
3	Registro de auditoría	-
4	Cifrado de comunicaciones	-
5	Configuración de alertas ante actividades sospechosas	A través del centro de seguridad y cumplimiento de Office 365
6	Establecer políticas de retención genéricas	Determinar acciones sobre la información una vez superado un periodo de tiempo concreto
7	Definir etiquetas de retención y confidencialidad	Estas etiquetas permiten categorizar lainformación y gestionar adecuadamente los niveles de acceso
8	Asignar automáticamente etiquetas de retención	-
9	Definir directivas y alertas relacionadas con las etiquetas de retención	-
10	Asignación de licencias	-
11	Bloquear acceso a otras aplicaciones de Office 365 que no sean las homologadas por la organización	-
12	Actualización constante de la herramienta/servicio	-

Tabla 4. Formulario línea base de seguridad, aplicaciones ofimáticas.

Formulario línea base de seguridad correo electrónico		
Índice	Configuración	Comentarios
1	Cifrado de comunicaciones	-
2	Acceso con autenticación de doble factor	-
3	Política de contraseña fuerte	-
4	Asignación de roles de administración	-
5	Configuración de alertas ante actividades sospechosas	Centro de Seguridad y cumplimiento de Office 365
6	Creación de directivas de roles de usuario	-
7	Restringir creación de buzones compartidos	-
8	Asignar derechos sobre buzones compartidos	Establecer flujo de aprobación
9	Configuración de alertas ante actividades sospechosas	Centro de Seguridad y cumplimiento de Office 365
10	Bloqueo de creación y subida de archivos .pst	-
11	Activar *proxy* de imagen para webmail	Para la versión web de Outlook, activar la funcionalidad *proxy* de imagen, que previene los riesgos que pueden suponer algunas imágenes en correos electrónicos.
12	Establecer una lista de remitentes definidos como correo no deseado	-
13	Establecer directiva de retención de mensajes	-
14	Establecer protección contra *malware*	-
15	Establecer protección frente a direcciones URL (vínculos seguros) y archivos malintencionados en correo electrónico y documentos de Office	-
16	Establecer protección contra suplantación de identidad	-
17	Establecer protección contra correo no deseado	-
18	Establecer purgado automático de cero horas	Funcionalidad que detecta y elimina mensajes con posible contenido de *phishing, spam* o *malware* incluso una vez entregados.
19	Establecer registro de auditoría	-
20	Directiva de alerta por *clicks* en URLs potencialmente maliciosa	-
21	Directiva de alerta por reglas de redirección/reenvío de correo a otro buzón	-
22	Directiva de alerta por concesión de permisos de administración	-
23	Directiva de alerta por retirada de correo con malware o URLs maliciosas después de la entrega	-
24	Directiva de alerta cuando se detecte un número elevado de recepción de malware	-
25	Directiva de alerta ante actividad sospechosa en una cuenta	-
26	Directiva de alerta cuando el tenant se defina como sospechoso por Microsoft	-
27	Directiva de alerta cuando el usuario pasa a estado comprometido	-
28	Aplicación de etiquetas de clasificaciónde la información	-
29	Crear directivas sobre las etiquetas de clasificación	-
30	Definir reglas internas de cifrado de correo interno y saliente	-
31	Recuperación de correos borrados	-
32	Establecer reglas de correo en tránsito	Por ejemplo, para el correo entrante externo a la organización: añadir en el asunto el prefijo "[EXTERNAL]"
33	Establecer filtros específicos para usuarios VIP	Se deberá determinar en función de las necesidades del usuario VIP en concreto, respetando siempre el principio de mínima exposición posible.
34	Habilitar firmas DKIM	Reduce el riesgo de suplantación de identidad
35	Establecer directivas anti-phishin específicas para usuarios VIP	-
36	Actualización constante de la herramienta/servicio	-
37	Establecer flujo de aprobación para archivado de buzón	-
38	Activar protección ante ataques DDoS	-

Tabla 5. Formulario línea base de seguridad, correo electrónico.

Formulario línea base de seguridad herramientas de colaboración		
Índice	**Configuración**	**Comentarios**
1	Cifrado de comunicaciones	-
2	Acceso con autenticación de doble factor	-
3	Política de contraseña fuerte	-
4	Asignar roles de administración	-
5	Bloquear acceso a usuarios externos a la organización	-
6	Configuración de alertas ante actividades sospechosas	A través del centro de seguridad y cumplimiento de Office 365
7	Activar protección frente a amenazas	-
8	Alerta por volumen elevado de eliminación de archivos	-
9	Alerta por volumen elevado de *malware* detectado	-
10	Generar etiquetas de retención	-
11	Automatizar etiquetado de contenido crítico o confidencial	-
12	Habilitar por defecto el control de versiones	-
13	Bloquear acceso a otras aplicaciones de Office 365 que no sean las homologadas por la organización	-
14	Actualización constante de la herramienta/servicio	-
15	Bloquear acceso externo	El acceso externo se utiliza para comunicarse a través de Teams con usuarios externos al dominio de la organización
16	Bloquear el acceso de invitado	Se bloquea el acceso a Teams de usuarios externos a la organización
17	Bloquear uso compartido de archivos para las herramientas no aprobadas	-
18	Creación de equipos bajo aprobación	Se deberá generar un flujo de aprobación interna, ya que por defecto Teams permite la creación de equipos a cualquier usuario
19	Revisión periódica de equipos creados y eliminación de no aprobados y obsoletos	-
20	Asignar permisos de propietario o miembro de equipo	-
21	Activar registro de auditoría	-
22	Definir etiquetas de retención	Puede aplicar a Teams (chats y canales), Sharepoint One Drive, Exchange y Grupos de O365.
23	Definir directivas de retención	-
24	Activar asignación automática de etiquetas de retención	-
25	Establecer flujo de aprobación para archivado de equipos	-
26	Activar protección ante ataques DDoS	-
27	Limitar eliminación de mensajes	-
28	Bloquear accesos de aplicaciones no aprobadas	-
29	Establecer política sobre directivas de voz	-
30	Establecer política sobre directivas de reunión	-
31	Establecer política sobre directivas de chat	-

Tabla 6. Formulario línea base de seguridad, herramientas de colaboración.

Formulario línea base de seguridad intranet corporativa		
Índice	**Configuración**	**Comentarios**
1	Cifrado de comunicaciones	-
2	Acceso con autenticación de doble factor	-
3	Política de contraseña fuerte	-
4	Los usuarios, por defecto, tendrán rol de visitante	-
5	Identificar usuarios con perfil de miembros	A priori, los propietarios serán los administradores del sistema. Se deberá establecer un flujo de solicitud y aprobación de permisos
6	Bloquear acceso a usuarios externos a la organización	-
7	Configuración de alertas ante actividades sospechosas	A través del centro de seguridad y cumplimiento de Office 365
8	Definir sitios de comunicación	-
9	Crear directivas de administración de información para documentación confidencial o sensible	Se define quién tiene acceso, durante cuánto tiempo y para qué
10	Creación de sitios bajo aprobación	No se podrán crear sitios sin aprobación previa
11	Detección continua de amenazas en tiempo real	-
12	Permitir *scripting* sólo bajo aprobación y auditoría previa	Establecer flujo de aprobación y auditoría
13	Activar registro de actividad	-
14	Alerta por volumen elevado de eliminación de archivos	-
15	Alerta por volumen elevado de malware detectado	-
16	Generar etiquetas de retención	-
17	Automatizar etiquetado de contenido crítico o confidencial en bibliotecas	-
18	Habilitar por defecto el control de versiones	-
19	Actualización constante de la herramienta/servicio	-
20	Activar protección ante ataques DDoS	-

Tabla 7. Formulario línea base de seguridad, intranet corporativa.

Formulario línea base de seguridad repositorios documentales		
Índice	**Configuración**	**Comentarios**
1	Acceso con autenticación de doble factor	-
2	Política de contraseña fuerte	-
3	Actualización constante de la herramienta/servicio	-
4	Cifrado de comunicaciones	-
5	Configuración de alertas ante actividades sospechosas	Centro de Seguridad y cumplimiento de Office 365
6	Definir sitios de grupo	
7	Creación de sitios de grupo bajo aprobación	No se podrán crear sitios sin aprobación previa
8	Por defecto, todos los sitios serán privados con gestión de solicitud de acceso	Se deberá establecer un flujo de solicitud y aprobación de acceso
9	Otorgar nivel de permisos bajo aprobación (propietario, miembro o visitante)	-
10	Por defecto, se bloquea que un usuario pueda compartir información del sitio, archivos o realizar invitaciones a usuarios externos al grupo.	Se deberá establecer un flujo de solicitud y aprobación
11	Cierre de sesión inactiva	Ante un tiempo determinado de inactividad, se cierra automáticamente la sesión del usuario
12	Detección continua de amenazas en tiempo real	-
13	Permitir *scripting* sólo bajo aprobación y auditoría previa	Establecer flujo de aprobación y auditoría
14	Activar registro de actividad	-
15	Bloquear acceso a usuarios externos a la organización	-
16	Alerta por volumen elevado de eliminación de archivos	-
17	Alerta por volumen elevado de malware detectado	-
18	Generar etiquetas de retención	-
19	Automatizar etiquetado de contenido crítico o confidencial en bibliotecas	-
20	Crear directivas de administración de información para documentación confidencial o sensible	Se define quién tiene acceso, durante cuánto tiempo y para qué
21	Bloquear descargas para clientes sin conexión (One Drive)	Para aquellos documentos que lo requieran, evitar que el control sea continuo
22	Habilitar por defecto el control de versiones	-
23	Control exhaustivo de acceso a la papelera de reciclaje de segundo nivel	Sólo administrador, bajo petición
24	Recuperación de archivos borrados	-
25	Activar protección ante ataques DDoS	-

Tabla 8. Formulario línea base de seguridad, repositorios documentales.

Formulario línea base de seguridad herramienta de *ticketing*		
Índice	**Configuración**	**Comentarios**
1	Cifrado de comunicaciones	-
2	Uso de cuentas de usuarios reales	-
3	Requisito de doble factor de autenticación	-
4	Requisito de contraseña fuerte	-
5	Renovación periódica de contraseña	-
6	Asignación de permisos en función del nivel asignado	-
7	Control de acceso por permisos	-
8	Registro de acceso	-
9	Verificación mensual de usuarios activos	-
10	Filtrado de tráfico entrante	-
11	Actualización constante de la herramienta/servicio	-

Tabla 9. Formulario línea base de seguridad, herramienta de ticketing.

Formulario línea base de seguridad aplicación de negocio		
Índice	**Configuración**	**Comentarios**
1	Cifrado de comunicaciones	-
2	Uso de cuentas de usuarios reales	-
3	Requisito de doble factor de autenticación	-
4	Requisito de contraseña fuerte	-
5	Renovación periódica de contraseña	-
6	Asignación de permisos en función del nivel asignado	-
7	Control de acceso por permisos	-
8	Registro de acceso	-
9	Verificación mensual de usuarios activos	-
10	Filtrado de tráfico entrante	-
11	Actualización constante de la herramienta/servicio	-

Tabla 10. Formulario línea base de seguridad, aplicación de negocio.

Formulario línea base de seguridad ERP		
Índice	**Configuración**	**Comentarios**
1	Cifrado de comunicaciones	-
2	Uso de cuentas de usuarios reales	-
3	Requisito de doble factor de autenticación	-
4	Requisito de contraseña fuerte	-
5	Renovación periódica de contraseña	-
6	Asignación de permisos en función del nivel asignado	-
7	Control de acceso por permisos	-
8	Registro de acceso	-
9	Verificación mensual de usuarios activos	-
10	Filtrado de tráfico entrante	-
11	Actualización constante de la herramienta/servicio	-

Tabla 11. Formulario línea base de seguridad, ERP.

Anexo II: Licenciamiento de servicios Microsoft 365

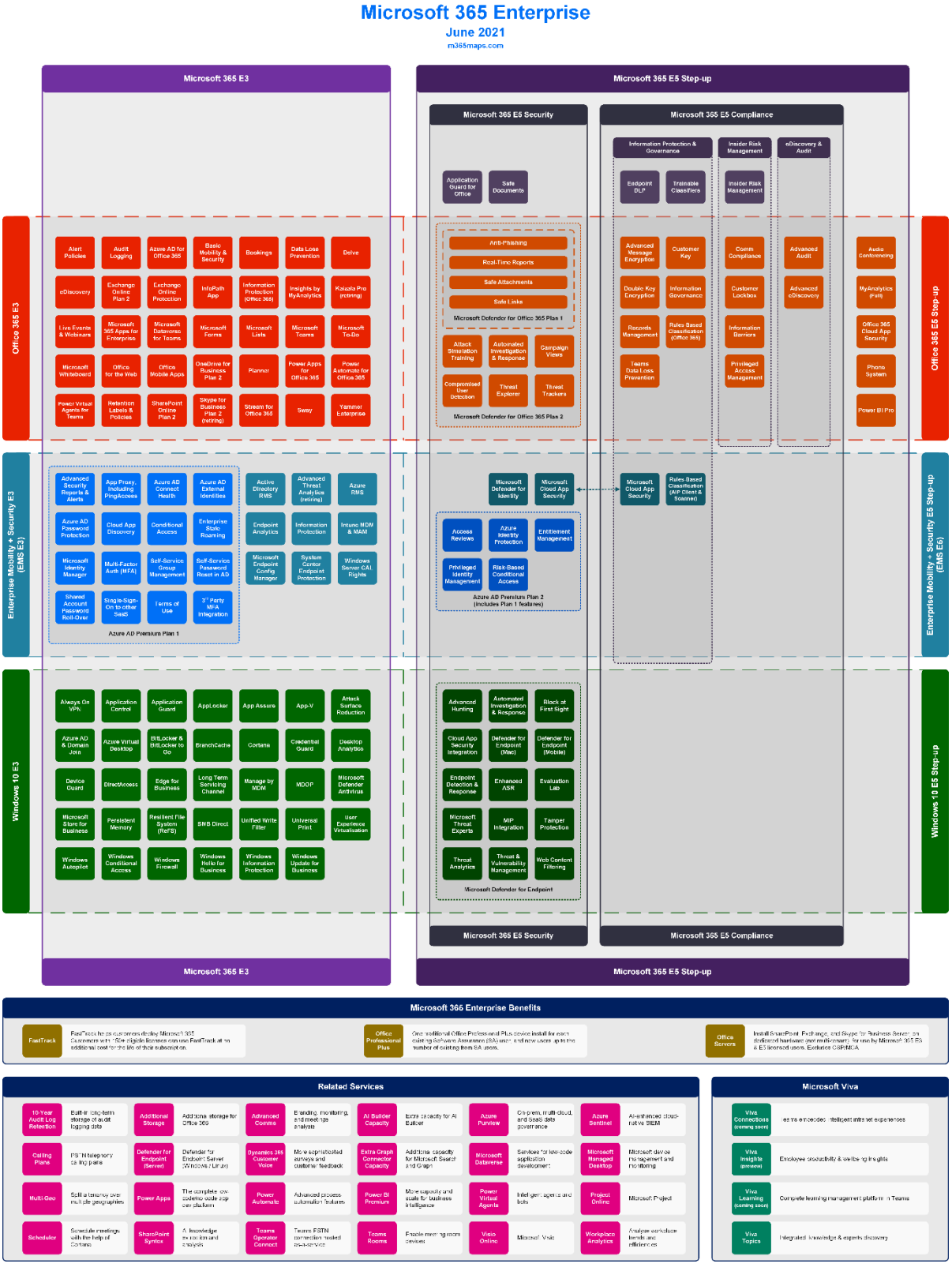

Ilustración 21. Esquema licenciamiento Microsoft 365.