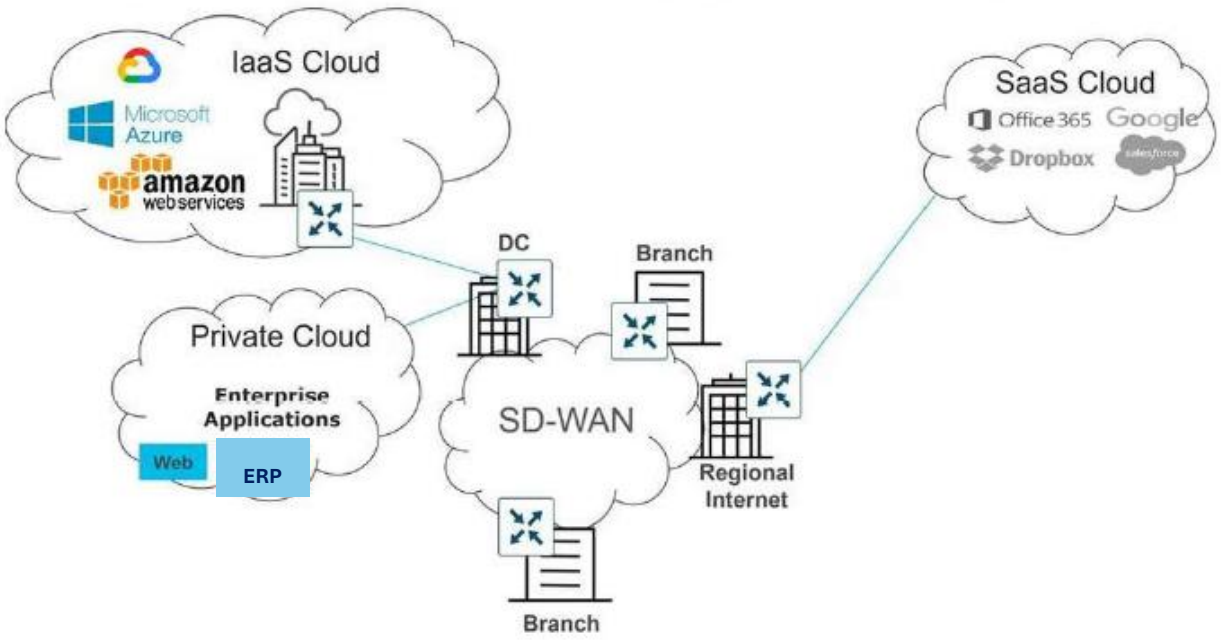
INGENIERÍA DE SEGURIDAD US

Avda. Reina Mercedes s/n. 41012 Sevilla

MEJORA DEL NETWORKING, LA SEGURIDAD Y LA PRIVACIDAD DE LA INFORMACIÓN PARA UNA COMPAÑÍA DE VUELOS COMERCIALES

Una compañía de vuelos comerciales desea mejorar el networking y la seguridad de las comunicaciones que realiza con sus 138 oficinas a lo largo de todo el mundo y con los servicios/aplicaciones de las nubes públicas y privadas mediante tecnologías SD-WAN y SASE con sus correspondientes puntos de presencia física distribuidos globalmente que actúan como nodos de conexión y seguridad en la arquitectura de SASE**.**

La topología de red empresarial de dicha compañía que se pretende dar soporte con la SD-WAN y SASE es la que se presenta en la figura siguiente, que es la que presentan muchas empresas que venden servicios.



También dicha compañía desea mantener **la privacidad de la información que se recibe o se dispone de los clientes frente a terceros y a la propia compañía**, para ello propone **publicar una Política de Privacidad que recoja todos los detalles organizativos tecnológicos que usa en sus aplicaciones y servicios para ello.**

Finalmente, la compañía es conocedora de las últimas noticias relacionadas con los importantes avances conseguidos por la computación cuántica y sus implicaciones en la seguridad y privacidad de su información empresarial. En concreto, nos comentan que **se encuentran bastante preocupados con el nuevo procesador Cóndor de IBM aparecido el pasado mes de diciembre de 2023 y que tiene capacidad para alcanzar y superar los 1000 qubits, que implicaría ya que se pueden romper los algoritmos más conocidos de criptografía asimétrica**. Están considerando debido a ello si empezar ya a usar para la confidencialidad y el firmado digital de los algoritmos criptográficos quantum-resistant que han sido aprobados pr el NIST.

CONSULTA 1. NETWORKING EFICIENTE Y SEGURIDAD EN LAS REDES EMPRESARIALES DE LA COMPAÑÍA DE VUELOS COMERCIALES DE A TRAVÉS DE TECNOLOGÍAS SD-WAN Y SASE

En esta consulta el cliente nos solicita lo siguiente:

1. **Propuesta tecnológica comercial de SD-WAN para mejorar las características de networking y seguridad de la transmisión de la información empresarial a través de redes WAN para cada uno de los edificios de oficinas (branch office) que se pretende que dispongan de comunicación eficiente para conectarse a las infraestructuras/servicios/aplicaciones en las diferentes nubes**

   Debido a una demanda continua de un ancho de banda suficiente y la calidad en la transmisión de la información que gestiona la compañía, les ha llevado a considerar la adopción para dichas comunicaciones con las nubes públicas y de unas soluciones de redes WAN más flexibles y simples, lo que significa que las arquitecturas WAN convencionales basadas en MPLS (circuitos dedicados para preservar la seguridad y fiabilidad de la conectividad) para enrutar el tráfico entre las sedes regionales y el DataCenter empresarial se vaya sustituyendo por **una arquitectura WAN** basada en la arquitecturas SD-WAN (Software-Defined-Network para las WAN) mediante el uso de los correspondientes **white-box appliances** para llevar a cabo ello.

   Se solicita al equipo consultor de una propuesta tecnológica comercial concreta de SD-WAN que permita configurar características tales como:

   1. **Path selection** (capacidad para dinámicamente seleccionar la mejor ruta para cada aplicación basándose en políticas y prioridades),
   2. **QoS** para los diferentes servicios y aplicaciones empresariales (que permita priorizar tráfico de red de acuerdo con su importancia y urgencia y asignar los recursos y ancho de banda apropiados a cada aplicación),
   3. **Seguridad** (*end-to-end encryption, firewalling, intrusion prevention, web filtering, detección avanzada de malware y acceso seguro*) y
   4. **Reporting** (posibilidad de disponer en un cuadro de mandos de diferentes métricas tales como bandwitdh, latency, jitter, packet loss, throughput and QoS).

   La implementación de la solución SD-WAN que se proponga nos comunica el cliente que requeriría cubrir los siguientes objetivos:

   1. Mejorar el rendimiento y disponibilidad de las aplicaciones y servicios críticos tales como ERP, CRM, Bases de Datos, Office365, Salesforce y AWS. Se pretende alcanzar en estas aplicaciones un ancho de banda de WAN de hasta 450 Mbps.
   2. Reducir el costo operacional del networking actual en al menos un 15% aprovechando las características de las SD-WAN que se podrían configurar de acuerdo a lo especificado anteriormente.
   3. Poder incrementar la escalabilidad y flexibilidad del networking permitiendo la adición o eliminación de sitios o aplicaciones a o desde la SD-WAN.

4. Facilidad para asegurar la transmisión de los datos sensibles y transacciones empresariales.

MUY IMPORTANTE Para el informe de esta consulta debe tenerse en cuenta que el producto comercial recomendado cubre todas las características especificadas anteriormente por el cliente, justificando bien todo ello. Además, se debe tener en cuenta la topología de la red empresarial y el número de oficinas que se tienen en todo el mundo. Puede usarse para determinar la propuesta tecnológica comercial el Cuadrante Mágico respecto a SD-WAN que ha elaborado la prestigiosa consultora Gartner en septiembre de 2023.

2. **Propuesta tecnológica comercial de SASE para mejorar las características de networking y seguridad de la transmisión de la información empresarial a las infraestructuras/servicios/aplicaciones en las diferentes nubes.**

En esta consulta se trata de proponer a la compañía de vuelos comerciales **el proveedor de SASE que se considera más conveniente para ofrecer los servicios de networking y seguridad que necesita la compañía de vuelos comerciales.** Se debe tener en cuenta que el cliente tiene oficinas y está trabajando en los cinco continentes y por tanto necesita una buena cobertura geográfica para dichos servicios. Por tanto, hay que tener en cuenta los **Points of Presence (PoPs)** de la arquitectura SASE que puede proporcionar el proveedor de SASE. El cliente conoce que estos PoPs actúan globalmente como nodos de conexión y seguridad en la arquitectura de SASE, proporcionando los servicios de networking y seguridad que nos requiere la compañía, y en este aspecto nos indican que es muy importante para ellos que se tenga **un acceso seguro y con alto rendimiento del acceso a los servicios/aplicaciones** en la nube **por parte de los empleados desde las ubicaciones que tiene repartidas por todo el mundo**. Para esta consulta se recomienda usar el Cuadrante Mágico respecto a SASE que ha elaborado la prestigiosa consultora Gartner en Agosto de 2023.

3. **Comparativa entre las propuestas tecnológicas SD-WAN y SASE recomendadas anteriormente para mejorar las características de networking y seguridad de la transmisión de la información empresarial a las infraestructuras/servicios/aplicaciones en las diferentes nubes.**

Se debe tener en cuenta para esta comparativa que la compañía está muy preocupada tanto en los gastos que debe realizar para adquirir tales tecnologías como en simplificar la gestión operativa del networking y la seguridad, por tanto, reducir los costos operativos. Ello significa, poner el foco de atención tanto en el CapEx (gastos de capital) como en el OpEx (gasto operativo) cuando se acude a usar estas dos tecnologías. Además, nos indica el cliente que además de ello es muy importante también el factor de cobertura geográfica, la variedad de funciones de seguridad y red ofrecidas por las dos tecnologías, la facilidad de implementación y administración. El cliente agradecería, en **el informe, la presentación de la correspondiente tabla o tablas comparativas que permita de un vistazo conocer cuál de las dos tecnologías recomienda el Security Team para mejorar el networking y la seguridad de su red empresarial.**

Es muy importante para que el cliente quede satisfecho con el informe de la consultoría que los comentarios técnicos sean rigurosos y bien fundamentados desde el punto de vista de la seguridad/performance.

CONSULTA 2. PRIVACIDAD EN EL PROCESAMIENTO DE LA INFORMACIÓN DE LOS CLIENTES DE LA COMPAÑÍA DE VUELOS COMERCIALES.

La compañía de vuelos comerciales desea mantener la privacidad de la información que se recibe o se dispone de los clientes frente a terceros y a la propia compañía, para ello propone **publicar una Política de Privacidad que recoja todos los detalles organizativos tecnológicos que usa en sus aplicaciones y servicios para ello.** Se puede decir que

una política de privacidad (***privacy policy***) es una presentación por escrito de todas las medidas que aplica una empresa u organización para **garantizar la seguridad y el uso lícito de los datos de los usuarios o clientes** que recoge en el contexto de la relación comercial. La política de privacidad web también describe en detalle la forma en que se recolectan, se almacenan y se utilizan estos datos, así como si se envían a terceros y, en caso afirmativo, de qué manera.

En concreto nos han indicado que desean preservar la privacidad de las cantidades que se gastan en sus viajes los clientes con objeto de suministrarles tarjetas premium si superan unas cantidades determinada, estos datos son almacenados en una nube pública. Además, desean preservar también la privacidad de los datos de sus clientes cuando se le requieren por las autoridades gubernamentales el listado de los pasajeros de los distintos vuelos para comprobar los posibles delincuentes o terroristas entre los pasajeros en sus diferentes vuelos. Finalmente, se desea preservar la privacidad cuando se requiere por los clientes la recuperación de información de sus bases de datos de cara no hacer seguimiento de sus peticiones, por ejemplo, cuando los clientes solicitan precios de vuelos de la compañía. Por ello en esta consulta el cliente nos solicita:

1. **Privacidad del procesamiento de datos personales de los clientes de la compañía de vuelos comerciales en nubes públicas**

   En esta consulta el cliente nos comunica que en la infraestructura de la nube desean preservar la privacidad de los clientes y por tanto **nos requiere una implementación básica de algún algoritmo a ejecutar en la nube mediante algunas de las técnicas que pueden preservar la privacidad para que los datos enteros de los gastos de cada pasajero se vayan sumando**. La compañía de vuelos comerciales mantiene en una nube pública los datos de los gastos de viaje que realizan los clientes de tal forma que se puede hacer procesamientos en la nube sobre los gastos de cada uno por año, sin que la nube tenga conocimiento de dichos gastos. El cliente nos solicita:

   - La implementación llevada a cabo para dar respuesta a solicitud, indicando el algoritmo de criptografía usado y el tamaño de la clave que se recomienda.
   - Una descripción detallada de las pruebas que se han realizado y los correspondientes resultados obtenidos (tenga en cuenta para las pruebas que pueden sumarse desde números pequeños a números mucho mayores).
   - Una valoración de la eficacia (resultados permanecen íntegros a pesar del cifrado) y eficiencia (incrementos de tiempos de procesamiento con datos cifrados frente al procesamiento con datos no cifrado) del algoritmo propuesto por el Equipo Consultor.
   - El párrafo que se añadirá a la Política de Privacidad y que se publicará en la página Web de la compañía, para que los clientes conozcan que se hace un uso lícito de sus datos cuando se envía a terceros, como es el caso de las nubes públicas.

2. **Privacidad de datos empresariales en procesos de colaboración contra la delincuencia y el terrorismo con autoridades gubernamentales**

   También la compañía de vuelos comerciales nos solicita llevar a cabo la implementación de un protocolo u algoritmo para preservar la privacidad de tal forma que se puedan identificar los posibles delincuentes, personas buscadas por la justicia y terroristas que pudieran viajar sin que se puedan identificar el resto de las personas que realizan los vuelos. El cliente nos solicita:

- La implementación llevada a cabo para responder a la solicitud,
- Una descripción detallada de las pruebas que se han realizado y los correspondientes resultados obtenidos.
- Finalmente nos pide una valoración de la eficacia y eficiencia del protocolo propuesto por el Equipo Consultor.
- El párrafo que se añadirá a la Política de Privacidad y que se publicará en la página Web de la compañía, para que los clientes conozcan que se hace un uso lícito de sus datos cuando se envía a terceros, como es en este caso a las autoridades gubernamentales.

Como prototipo de la función más importante de dicho protocolo a desarrollar podríamos tener la siguiente función:

```
func  buscaComunes (Set_de_delincuentes_Confid, Set_de_pasajeros_vuelo_Confid)
{
    Set_de_Comunes= Set_de_delincuentes_Confid ∩ Set_de_pasajeros_vuel_Confid;
    return Set_de_Comunes;
}
```

Nota importante para el informe: Debe indicarse al cliente las condiciones que deben tener los parámetros de entrada a esta función para que realmente la propuesta que se hace tenga la eficacia deseada.

3. Privacidad en la recuperación de datos empresariales de sus diferentes centros de datos

Finalmente, la compañía aérea desea que tanto la recuperación de sus datos empresariales, por ejemplo, los precios de los vuelos sean privados para los clientes (si un cliente desea el precio de un vuelo i, el servidor no pueda conocer dicho i), tanto como la información que se le presenten a los clientes sea la mínima para llevar a cabo el vuelo que requieran. Nos ha comentado que conocen varias alternativas tecnológicas relacionadas con los protocolos de Recuperación de Información Privada (PIR) :

- ***Tor-PIR: Basada en las redes Tor***
- ***Oblivious Transfer Protocol***
- ***Secure MultiParty Computation***
- ***Homomorphic Encryption***
- ***Zero Knowledge Proofs (ZKPs)***

Teniendo en cuenta todo ello, el cliente nos solicita:

1. **Especificar e implementar el protocolo recomendado por el Security Team**, tal que preserve la privacidad requerida por la compañía cuando sus clientes solicitan los precios de vuelos concretos.
2. Además, nos solicita que le indiquemos las pruebas realizadas sobre la eficiencia y eficacia de dicho protocolo, mostrando los resultados de dichas pruebas.
3. El párrafo que se añadirá a la Política de Privacidad y que se publicará en la página Web de la compañía, para que los clientes conozcan que se hace un uso lícito de sus datos cuando se solicitan los precios de los vuelos, por tanto, no se realiza seguimiento alguno de sus peticiones.

CONSULTA 3. RIESGOS Y OPORTUNIDADES DE LA COMPUTACIÓN CUÁNTICA PARA LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA COMPAÑÍA DE VUELOS COMERCIALES.

Finalmente, la compañía de vuelos comerciales nos ha solicitado una consultoría sobre "*Seguridad Post-Cuántica*" pues se encuentra bastante alarmada de los importantes avances que está alcanzando la computación cuántica, y nos presenta un conjunto de consultas para empezar a considerar este tipo de computación en sus nuevas propuestas de seguridad de la información y de ciberseguridad en sus nuevos proyectos empresariales. Aunque también consideran que hay oportunidades de la computación cuántica que se pueden aprovechar para mejorar la seguridad de la información empresarial.

Dada nuestras competencias en Ingeniería del Software y Ciberseguridad nos propone que le presentemos de forma empírica de algunos desarrollos software en los lenguajes de programación cuántica existentes para computación cuántica, de tal forma que se identifiquen los riesgos y oportunidades reales/actuales que puede representar esta nueva tecnología para la seguridad de la información empresarial. Por todo ello en esta consulta el cliente nos solicita:

1. **Implementación, ejecución y pruebas de dos desarrollos de software cuántico que representan amenazas a la seguridad de la información empresarial través de la computación cuántica**

   En esta consulta nos solicita el cliente que le presentemos **la implementación, la ejecución y los resultados obtenidos (número de shots usados, tiempos de cómputo, número de qubits usados, resultados en forma de distribución de probabilidad) al menos para dos desarrollos de script/programas** en alguno de los lenguajes de programación existentes para computación cuántica que les permita comprender las posibles amenazas reales que existen con respecto a la seguridad de la información cuando se usa la computación cuántica. En concreto el cliente nos ha indicado que se encuentra **especialmente preocupado por los desarrollos de los algoritmos de Shor, Gover y Simon.**

   Se valorará muy positivamente por **el cliente que se muestre en el informe el plan de pruebas establecido para mostrar estas amenazas y que se realice la ejecución de dichas pruebas sobre computadores cuánticos reales del mayor número de qubit posible frente a simuladores de la computación cuántica**. Indicar los resultados obtenidos en dichas pruebas con la idea de comparar tanto los resultados obtenidos como los tiempos de ejecución de dichos scripts/programas para diferentes números de shots.

   Finalmente se requiere por el cliente que de acuerdo a lo que se ha implementado y elaborado se presente **una valoración técnica por parte del Security Team sobre el estado de madurez de esta tecnología** para tenerlas en cuenta como posibles amenazas a la seguridad de la información empresarial.

2. **Implementación, ejecución y pruebas de dos desarrollos de software cuántico que muestren las posibles oportunidades de la computación cuántica para mejorar la seguridad de la información de la compañía.**

En esta consulta nos solicita el cliente que le presentemos la implementación, ejecución y los resultados obtenidos al menos dos desarrollos de un script/programa cuántico en alguno de los lenguajes de programación para computación cuántica existente que les permita comprender los posibles beneficios que existen con respecto a la seguridad de la información cuando se usa la computación cuántica. En concreto el cliente nos ha indicado que se encuentra bastante esperanzado con las expectativas que presentan los desarrollos de los algoritmos cuánticos de ***Generación de Números Aleatorios Cuánticos (QRNG)*** basado en la incertidumbre cuántica inherente a las mediciones de propiedades cuánticas, y que permitiría verdaderos generadores de claves aleatorias, el de ***Distribución de claves cuánticas (QKD),*** que permite el intercambio de claves más seguro que en la criptografía clásica, consiguiendo que dicha clave de cifrado no pueda ser interceptada o duplicada por un tercero y el algoritmo de ***Corrección de errores cuánticos (QEC)*** que es una técnica para proteger los qubits de errores que pueden ocurrir debido a ruido o perturbaciones externas y por lo tanto son muy adecuadas para asegurar la integridad en el procesamiento cuántico.

Se valorará muy positivamente por el **cliente que se muestre en el informe el plan de pruebas establecido para comprobar estos beneficios y que se realice la ejecución de dichas pruebas sobre computadores cuánticos reales frente a simuladores de la computación cuántica**. Indicar los resultados obtenidos en dichas pruebas sobre computadores cuánticos, con la idea de comparar tanto los resultados obtenidos como los tiempos de ejecución de dichos scripts/programas para diferentes shots.

Finalmente se requiere por el cliente que de acuerdo a lo que se ha implementado y elaborado se presente **una valoración técnica por parte del Security Team sobre el estado de madurez de esta tecnología** para tenerlas en cuenta como posibles oportunidades para mejorar la seguridad de la información empresarial.

3. **Eficacia y eficiencia de un algoritmo quantum-resistant para el cifrado o firmado de la información empresarial frente a los algoritmos clásicos.**

Existen actualmente en los lenguajes de programación numerosas bibliotecas que ofrecen implementaciones de algoritmos criptográficos resistentes a ataques cuánticos. El cliente nos solicita que de forma empírica (mediante los correspondientes planes de pruebas) de una comparación de la eficacia de alguno de dichos algoritmos frente al algoritmo clásico de cifrado o firmado. También el cliente se encuentra interesado en conocer si la complejidad computacional del algoritmo de cifrado o firmado con estos algoritmos quantum-resistant es mucho mayor o no que la de los algoritmos clásicos y si las claves que se usan son mucho mayores que la de los algoritmos clásicos o no.

Se valorará muy positivamente por el **cliente que se muestre en el informe el plan de pruebas establecido para comprobar la eficacia y eficiencia de un determinado algoritmo, que debería estar dentro de los que se han aprobado ya por el NIST.**