CCN-CERT BP/18

Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia

Mayo 2020

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.05.10 02:49:34 +02'00'

Fecha de Edición: mayo de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. OBJETO DEL INFORME

Ante pandemias como la actual de COVID-19, en numerosas entidades y organizaciones se está generalizando el uso del teletrabajo como medida para evitar contagios y facilitar la confinación de los empleados. Aunque esta posibilidad ya era una realidad en algunas compañías en España, la realidad es que solo el 4% de las personas trabajadoras tenían esta opción antes de la crisis actual[1].

Así pues, numerosas organizaciones, públicas y privadas, han tenido que implantar en un tiempo muy reducido soluciones de teletrabajo que abarcan un gran número de aspectos: dispositivos corporativos, conexión a internet, aplicaciones de chat y/o mensajería, videoconferencia, acceso remoto a la red y sistemas de la organización, etc. Todo ello, sin contar con las medidas de seguridad habituales dentro del dominio de la organización y que en un tiempo récord tiene que trasladar para seguir protegiendo la información.

[1] Datos de la Encuesta de Población Activa (EPA).

Al tiempo que todo esto se pone en marcha, los ciberdelincuentes han aprovechado esta situación de vulnerabilidad para incrementar sus ataques de todo tipo: ransomware, phishing con el que obtener credenciales de acceso a sistemas, ejecución de código de forma remota, exfiltración de información, etc.

Por este motivo, se han de tener en cuenta una serie de pautas **que permitan garantizar la seguridad** de todas las herramientas y soluciones utilizadas en el teletrabajo y, de este modo, seguir manteniendo la confidencialidad, integridad y disponibilidad de la información, como si se estuviese en la oficina. Una responsabilidad de todos, tanto de los administradores de las redes y sistemas, como del propio trabajador.

Este informe se une a las diferentes publicaciones que el CCN-CERT ha ido desarrollando y cuya lectura se recomienda:

- #CiberCOVID19: prevenir los riesgos cibernéticos durante la crisis del #coronavirus
- Ciberconsejos: CiberCOVID19; medidas de prevención de incidentes
- Abstract: Medidas de Seguridad para acceso remoto
- Abstract: Limitación de la navegación hacia Internet mediante Listas Blancas como medida para reducir la superficie de exposición
- Abstract: El uso de Zoom y sus implicaciones para la seguridad y privacidad. Recomendaciones y buenas prácticas
- CCN-CERT IA-03/20 Informe Anual 2019. Dispositivos y Comunicaciones Móviles
- CCN-CERT IA 04/20 Informe Anual 2019 Hacktivismo y Ciberyihadismo
- CCN-CERT IA-76/19 Medidas de actuación frente al código dañino EMOTET
- CCN-CERT ID-05/20 Informe de Código Dañino sobre NetWalker
- Guía CCN-STIC 455E sobre seguridad en dispositivos iOS 13
- Guía CCN-STIC-453G Guía práctica de seguridad en dispositivos móviles Android 9
- CCN-CERT BP/04 Ransomware. Informe de Buenas Prácticas ante el Ransomware

3. SOLUCIONES TÉCNICAS DE ACCESO REMOTO SEGURO

La implementación de una solución de acceso remoto es un reto desde el punto de vista de la seguridad y la gestión para cualquier organización.

Las soluciones clásicas, basadas en el despliegue de sistemas locales u *on-premise*, requieren de capacidades, tanto de personal como de infraestructura, que no siempre están disponibles en organizaciones medianas o pequeñas. Por otro lado, aquellas con

mayor madurez podrán adaptar sus sistemas actuales para implementar un sistema de acceso remoto seguro que pueda desplegar los servicios que le sean necesarios.

A continuación, se presentan dos (2) soluciones para la implementación de este sistema en función de las capacidades de la organización.

3.1 Solución basada en la nube

Esta solución técnica se caracteriza por permitir el despliegue rápido de un servicio de acceso remoto seguro, aunque no se disponga de una gran capacidad dentro de la organización.

Ejemplos de estas soluciones son las ofrecidas por VMware: "Workspace ONE" y "Horizon Cloud" o "Citrix Cloud Services" en modalidad de pago por uso, que permiten proporcionar temporalmente acceso a la organización desde cualquier lugar con las medidas de seguridad adaptadas al tipo de información manejada. Ambas proporcionan una solución de acceso seguro, con doble factor de autenticación y trazabilidad total de las conexiones realizadas por los usuarios remotos.

Se basan en transmitir la capa de presentación de los sistemas corporativos a cualquier equipo remoto, siempre y cuando se haya realizado una autenticación adecuada. En este caso, se aísla completamente a la plataforma de acceso de la red corporativa impidiendo que las vulnerabilidades presentes en el cliente pongan en riesgo los sistemas corporativos. Las características principales de este sistema son[2]:

Característica	Descripción
Nivel de Seguridad	Medio / Alto
Infraestructura	Basada en soluciones Cloud
Sistema de Autenticación	Fuerte / Doble Factor
Tiempo puesta Producción	Mínimo
Complejidad TIC	Media / Baja
Equipo de trabajo Remoto	Cualquiera con acceso Internet

La arquitectura necesaria para proporcionar este tipo de acceso recae principalmente en la infraestructura que se encuentra en la nube. La única parte de la arquitectura responsabilidad de cada organización corresponde al despliegue de una pequeña máquina virtual, "Conector", que establezca una comunicación segura entre la nube y los servicios corporativos.

Las soluciones tipo "VMware Workspace ONE", "Horizon Cloud" y "Citrix Cloud Services" proporcionan acceso a los equipos físicos de la organización manteniendo el

[2] Los detalles técnicos de la solución de detallan en el anexo A.

máximo nivel de seguridad, pero permitiendo un ahorro de costes considerables ya que no se requiere infraestructura para el despliegue de escritorios virtuales (VDI).

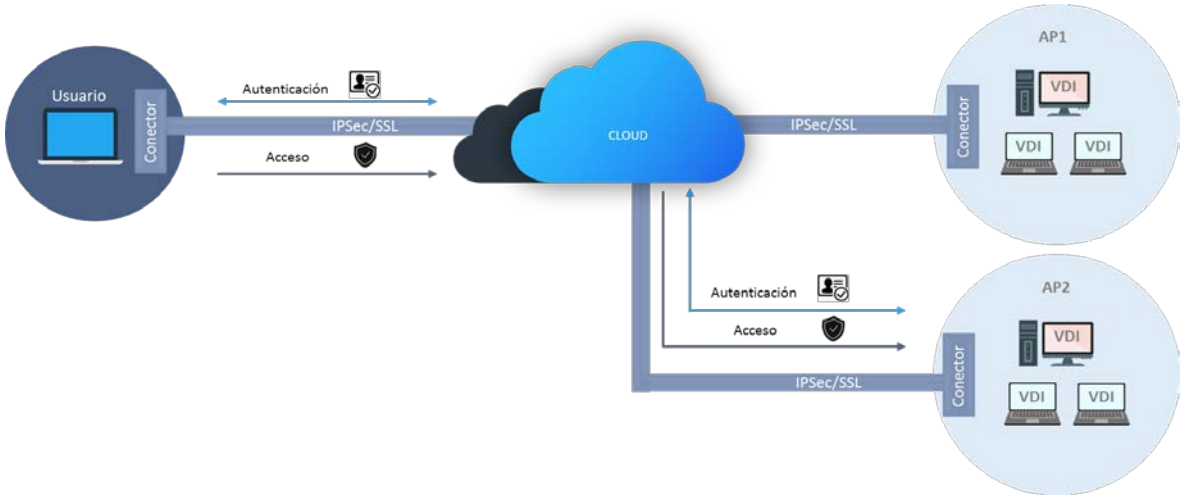


Figura 1.- Esquema de la arquitectura desplegada en una solución de acceso remoto seguro en la nube.

En cualquier caso, aunque en la solución presentada se ha tomado como referencia la de los fabricantes Citrix y VMware, podrían utilizarse otras soluciones que ofrezcan los mismos servicios con unas garantías de seguridad equivalentes.

Un ejemplo de ello es la solución alternativa sería la que ofrece Palo Alto Networks con Prisma Access en la cual no es necesario desplegar servidores VDI ni MSTC y tiene la ventaja de poder cursar de una manera segura el tráfico hacía internet (ya sea Nube pública, Software como servicio o navegación directa) sin tener que concentrar todo el tráfico en el centro de datos de la organización evitando así la degradación en la experiencia de usuario generado por el *delay* y la posible sobrecarga de los enlaces que lo conectan con el proveedor de servicio.

Se pueden encontrar más detalles sobre las soluciones en los anexos A y C de este documento.

3.1.1 Equipo cliente

Cada usuario de la organización haría uso de su propio equipo TIC (ya sea COBO, COPE o BYOD) para acceder a través de una página web y una autenticación fuerte o doble factor de autenticación (por ejemplo, token software en el teléfono móvil, un SMS, etc.) a portales tipo Citrix o VMware en la nube que les daría acceso a los sistemas corporativos.

3.1.2 Canal seguro de comunicaciones

La parte del canal de comunicaciones se delegaría en los servicios Cloud de VMware o Citrix. Por un lado, se asegura el segmento Cliente-Cloud mediante una conexión *https* y

servicios de autenticación fuerte y, por el otro, se establece una conexión segura Cloud-Servicios corporativos mediante una máquina "Conector".

Este "Conector" es una máquina virtual que se despliega en la infraestructura de la organización y permite interconectar la solución basada en las nubes de Citrix o VMware con la organización. Este componente es necesario para proporcionar una autenticación integrada con el actual *Active Directory* y poder establecer conexiones seguras con los servicios de la organización.

3.1.3 Acceso a servicios corporativos

Para el acceso a los servicios de la organización se plantean tres (3) escenarios:

a) **[NIVEL SEGURIDAD ALTO] Acceso a los servicios a través de Sistema VDI**: cada usuario dispondrá de una máquina virtual que a todos los efectos será un equipo de la propia organización.

b) **[NIVEL SEGURIDAD MEDIO] Acceso a los servicios a través de un Servidor de Escritorios Remoto (MTSC):** los usuarios accederían a un tipo de máquina virtual con acceso a los mismos servicios corporativos que si estuvieran en la oficina.

   Requiere del despliegue de un servidor con capacidad de dar servicio a todos los usuarios de la organización.

c) **[INSEGURO] Acceso directo a los propios equipos de los usuarios:** este tipo de alternativas se desaconseja de forma expresa, ya que supone un alto riesgo de infección por código dañino o *ransomware*, ya que la publicación de puertos de "Escritorio Remoto" o SSH representan un alto riesgo de seguridad y una alta carga administrativa para garantizar una conexión autorizada.

   En caso de que está sea la única alternativa posible, al menos se deberían aplicar las siguientes medidas complementarias:

   - Restringir las direcciones IP desde donde se van a originar las conexiones. Conviene tener el listado de estas direcciones asociado a los lugares desde donde se van a realizar las conexiones y así poder determinar las reglas de acceso adecuadas. Se recomienda, en estos casos, disponer de un mecanismo de doble factor de autenticación.
   - Es importante tener en cuenta que la gran mayoría de los usuarios contarán con conexiones a internet con direccionamiento IP dinámico, por lo tanto, es probable un aumento de la gestión administrativa diaria para poder autorizar de nuevo cada una de las nuevas direcciones IP que presentan los usuarios.
   - Será necesario contar con registros de auditoría asociados a las conexiones almacenando los siguientes datos:

- Dirección IP origen de las conexiones.
- Hora inicio y de fin de la conexión.
- Usuario.
- Comandos ejecutados.
- Ficheros ejecutados o accedidos.
- Unidades de red que se mapean directamente en el ordenador remoto, especialmente vulnerables ante ataques de *ransomware*.

3.2 Solución basada en sistemas locales (*on-premise*)

Esta solución técnica se caracteriza por extender los límites de la organización más allá de sus instalaciones. Se despliegan equipos portátiles configurados y bastionados por la organización para que puedan utilizar internet como medio de acceso a los servicios corporativos.

Permitir este nivel de acceso implica el despliegue de múltiples mecanismos de seguridad que garanticen que todos los elementos TIC involucrados cumplen los estándares necesarios para limitar el riesgo de exposición de los sistemas. Las características principales de esta solución[3] son:

Característica	Descripción
Nivel de Seguridad	Medio / Alto
Infraestructura	*On-premise*
Sistema de Autenticación	Certificados máquina / Simple
Tiempo puesta Producción	Alto
Complejidad TIC	Alta
Equipo de trabajo Remoto	Portátil corporativo

3.2.1 Equipo cliente

El equipo cliente sería un equipo corporativo que incluyera, además de todas las medidas de seguridad estándar de la organización, medidas adicionales que permitan la comunicación con los servicios corporativos a través de internet.

3.2.2 Canal seguro de comunicaciones

Se basa en establecer un canal de comunicaciones seguras entre el propio equipo portátil corporativo y la red de la organización.

[3] Los detalles técnicos de la solución se detallan en el anexo B.

Para el establecimiento de la comunicación será necesario validar la identidad del equipo; es decir, confirmar que se trata de uno de la organización, por ejemplo, estableciendo la comunicación VPN mediante autenticación con certificado de máquina. Puede ser la opción más habitual de conexión y conviene tener varias medidas para comprobar los requisitos de conexión.

Las medidas de validación de acceso deben ser revisadas para que no se produzcan duplicidades o se conozca la dimensión de los mismos. Las medidas para registrar las actividades de los usuarios, así como el registro de las conexiones, son muy importantes para evitar posibles incidentes o, llegado el caso, facilitar su investigación.

3.2.3 Acceso a servicios corporativos

Para el acceso a los servicios de la organización se plantean dos (2) escenarios:

a) **[NIVEL SEGURIDAD ALTO] Acceso a los servicios a través de Sistema VDI:** cada usuario dispondrá de una máquina virtual que a todos los efectos será un equipo de la propia organización.

b) **[NIVEL SEGURIDAD MEDIO] Acceso a los servicios a través de un Servidor de Escritorios Remoto (MTSC)**: los usuarios accederían a una especie de máquina virtual con acceso a los mismos servicios corporativos que si estuvieran en la oficina.

   Requiere del despliegue de un servidor con capacidad de dar servicio a todos los usuarios de la organización.

c) **[NIVEL DE SEGURIDAD BAJO] Acceso Directo a la red corporativa**: con este tipo de alternativa se permite acceder a la red corporativa (servidores o los propios equipos de los usuarios) de manera controlada. Para ello se deben de cumplir estas medidas de seguridad:

   - Restricción de direcciones IP origen desde las que se permite originar las conexiones.
   - Doble factor de autenticación.
   - Revisión de la postura de seguridad del equipo remoto, para garantizar que dispone de antivirus actualizado y cortafuegos.
   - Aplicación de listas de acceso en el finalizador del túnel para garantizar que solo se puede acceder a los servicios y aplicaciones específicas.
   - Registro de auditoria de conexiones (direcciones IP origen y destino, horario de inicio y fin y usuario).
   - Inspección del tráfico generado en el túnel.

3.3 Soluciones basadas en sistemas híbridos (Hybrid IT)

En esta solución técnica, se propone la implementación de un sistema unificado de control de acceso para organizaciones que disponen de una infraestructura IT apoyada en sistemas tanto *cloud* como *on-premise* y en el que adicionalmente los usuarios (humanos, IoT y aplicaciones) se pueden conectar desde dispositivos tanto corporativos como no corporativos en un mundo *Zero Trust*.

En este perfil el requerimiento se basa en ofrecer una solución unificada de control de acceso tanto a infraestructuras y aplicaciones ubicadas en sistemas *cloud* y *on-premise*, algo habitual en cualquier organización, simplificando la experiencia de usuario a través de *Single Sign On* (SSO), y permitiendo la validación, con el consiguiente perfilado, desde múltiples dispositivos.

La idea es la de anteponer una capa previa de control de acceso a los sistemas de la organización que permita tener visibilidad, unificar la gestión y eliminar los silos en el acceso a los sistemas de la información en un mundo en el que el perímetro se ha movido hacia el *endpoint*.

El control de acceso a las aplicaciones se realiza a través de un portal HTML 5 seguro en el que se presenta al usuario, una vez realizada la validación (Validación Zero Trust):

1. Comprobación de dispositivo.
2. Validación de usuario.
3. Perfilado.
4. Auditoría de uso.

El usuario se puede conectar desde múltiples dispositivos: corporativos, BYOD, móviles, domésticos, … pudiendo realizarse esta validación con cliente (en múltiples configuraciones de tipo *always on*, *on demand VPN*, etc..), sin cliente o embebiéndolas directamente en las aplicaciones a través de *Rest API* o *Per App VPN*.

Características	Descripción
Nivel de Seguridad	Medio/Alto
Infraestructura	Basada en soluciones *cloud*/*on-premise*/virtuales
Sistema de Autenticación	Fuerte/Doble factor o superiores
Tiempo de puesta en Producción	Mínimo
Complejidad TIC	Media/Baja
Equipo de trabajo Remoto	Cualquier usuario/múltiples dispositivos

La arquitectura necesaria para proporcionar este tipo de acceso recae principalmente en la plataforma servidor, que puede estar ubicada tanto *on-premise* (hardware o virtual) como en la nube (Azure, AWS, Google Cloud) desde la que se generará un portal web, que

tras la verificación del dispositivo/usuario permitirá el acceso de una manera segura a las aplicaciones de la organización acorde a la política de seguridad definida.

Este tipo de solución ha de interactuar con el resto de sistemas de seguridad de la organización, tales como Next Generation Firewalls, Antivirus, EDR, SIEM, …

En este sentido, las empresas Palo Alto Networks y Pulse Secure en este documento relatan sus aproximaciones sobre esta implementación.

3.3.1 Equipo cliente

Cada usuario de la organización haría uso de su propio equipo TIC (ya sea COBO, COPE o BYOD) para acceder a través de una página web y una autenticación fuerte o doble factor de autenticación (por ejemplo, token software en el teléfono móvil, un SMS, etc.) a un portal web que presentará el acceso a las aplicaciones corporativas a través de *bookmarks*, y en base a la evaluación del nivel de seguridad del dispositivo/usuario.

El sistema se integrará con el resto de infraestructuras del cliente no siendo necesario instalar ningún tipo de cliente en el usuario si no se desea.

3.3.2 Canal seguro de comunicaciones

La parte de canal de comunicación se basa inicialmente en la verificación del usuario siguiendo los patrones *Zero Trust* generando una conexión segura entre el usuario y el portal quiosco proveedor de acceso a las aplicaciones.

El acceso a las aplicaciones se realizará bajo el control del Firewall, integrándose con las diversas infraestructuras de *authentication*, *authorization* y *accounting* (AAA), doble factor que la organización tenga implementados, permitiéndose la interacción entre el sistema de control de acceso y los diversos dispositivos de control de seguridad de la organización.

3.3.3 Acceso a servicios corporativos

Para el acceso a los servicios de la organización se plantean dos (2) escenarios:

a) **[NIVEL SEGURIDAD ALTO] Acceso a través de cliente pesado:** el dispositivo tendrá un cliente, que se encargará de verificar, aplicar y auditar las políticas de seguridad definidas durante el período en el que el cliente esté conectado.

   El cliente puede ejecutarse bajo demanda del usuario, pero también para máquinas corporativas está disponible un cliente *always on* que asegura la conectividad segura en el momento que el usuario se conecte fuera de la red corporativa.

b) **[NIVEL SEGURIDAD MEDIO] Acceso sin cliente:** una vez el usuario se intente conectar al portal, como primer paso se realizará una comprobación del cumplimiento de los requisitos mínimos de seguridad definidos del dispositivo y usuario a través de un agente voluble que se cargará en memoria. Una vez realizado este chequeo, se autorizará el acceso seguro a las aplicaciones. En este caso, el *host checking* únicamente se realiza en el momento de la conexión.

Adicionalmente, se puede automatizar está encapsulación en *Apps* a través de *Split Tunneling*, generando el cifrado del canal únicamente en el momento que una aplicación se está utilizando y exclusivamente sobre el tráfico de dicha aplicación.

4. CORREO ELECTRÓNICO

Si se plantea un escenario en el que los usuarios puedan acceder al sistema de correo electrónico corporativo desde equipos informáticos no gestionados por la organización a través de internet, se recomienda reforzar la inspección de los *e-mails* antes de ser entregados a los usuarios.

De lo contrario, las probabilidades de ser víctima de un ataque se incrementan considerablemente, dado que los ordenadores particulares, en remoto, no garantizan una seguridad adecuada. Si se inspeccionan los correos electrónicos, como mínimo, la organización que tiene controlado el perímetro de seguridad, sí detectaría cualquier intento de ataque.

Además, es importante controlar los motores de antivirus e inspeccionar los buzones de correo electrónico hacia atrás en el tiempo de las personas que tengan tanto acceso remoto como acceso al correo electrónico corporativo.

No se debería utilizar datos sensibles de la organización o información que legalmente deba ser protegida en equipos que no pertenezcan a la organización.

Si los miembros de una organización deben enviarse correos internos, pero sin poder utilizar la red interna, es conveniente usar mecanismos de cifra, como PGP (*Pretty Good Privacy*) o tecnología IRM (*Information Rights Management*), para el cifrado de los correos y así mantener la confidencialidad y no repudio.

5. HERRAMIENTAS DE COMPARTICIÓN DE DOCUMENTACIÓN EN CLOUD Y DE TRABAJO COLABORATIVO

Las herramientas de compartición de documentación y almacenamiento de ficheros en plataforma *cloud*/*SaaS* pueden ayudar a tener un acceso ágil a la documentación corporativa en un entorno de teletrabajo. Estas plataformas (Ej. Microsoft OneDrive, Google Drive, Box, Dropbox, etc.) facilitan la compartición de documentación entre

usuarios internos y externos sin necesidad de enviar adjuntos vía correo electrónico o acceder con VPN a los servidores de ficheros corporativos.

Por otro lado, plataformas de trabajo colaborativo como Microsoft Teams o Slack pueden facilitar la comunicación de un equipo de trabajo distribuido, sin necesidad de utilizar el correo electrónico. Ofrecen una comunicación en tiempo real y más dinámica que las plataformas de correo electrónico, permitiendo también el intercambio de ficheros y documentación dentro de la plataforma.

En ambos casos, debemos tener en cuenta que la documentación que se almacena y comparte a través de estos tipos de plataformas, puede estar muy distribuida: en la propia plataforma en la nube, en los equipos de los usuarios que se lo descargan, etc.

Es recomendable revisar los permisos que se asignan a las carpetas y documentos que se almacenan en estas plataformas, asegurando que sólo tienen permisos las personas adecuadas y los documentos no se dejan accesibles de forma pública.

Por otro lado, para la documentación sensible o datos regulados (datos personales, financieros, etc.) es recomendable cifrarla de forma que, aunque se descargue de estas plataformas siguen estando protegidas y se sigue teniendo control sobre la misma. Para esto, son especialmente útiles tecnologías de IRM (*Information Rights Management*) que hacen que la documentación viaje protegida y cifrada allí donde esté y permiten auditar el uso de estos documentos e incluso revocar el acceso cuando se requiere que dejen de estar disponibles.

6. PROTECCIÓN DE DOCUMENTOS

Compartir documentos, enviarlos por correos electrónicos o simplemente auditar el acceso a los documentos es una tarea esencial en la protección de la información.

Disponer de mecanismo para poder tener una auditoría sobre los documentos en todo momento dota a los sistemas de una protección ante ex filtración de datos o detectar el robo de los mismos.

Se debe intentar proteger los documentos en los siguientes aspectos:

- La documentación tiene que ser accesible por las personas indicadas.
- Se debe poder tener trazabilidad del documento.
- Tener trazabilidad donde se abre un documento y quien realiza la acción.
- Intentar establecer permisos por cada usuario o grupo de usuarios que maneje el documento.
- Intentar en la mayoría de casos tener el documento cifrado cuando no se esté usando.

- Tener los documentos cifrados y protegidos cuando se suben a almacenamientos en nube o memorias USB.
- Tener trazabilidad y protección del documento al enviarse por correo electrónico.
- Conocer si el documento se intenta o se abre desde una ubicación extraña o no permitida o por un usuario sin permisos.

7. VIDEOCONFERENCIAS Y REUNIONES VIRTUALES

Las reuniones virtuales van a ser una herramienta de uso diario para trabajar en entornos colaborativos, organizar comités de seguimiento o para poder resolver incidencias comunes.

Las soluciones de videoconferencia o *web conferencia* hacen referencia a aquellas tecnologías que permiten la comunicación audiovisual a través de redes LAN o WAN con infraestructuras locales (*on-premise*), en la nube (*Cloud VaaS* o *SaaS*) o soluciones hibridas *on-premise* y *cloud* y con terminales (*endpoints*) físicos dotados de procesador (*códec*), cámara, micrófono y mando remoto (pantalla táctil o mando convencional); o soluciones software ejecutándose en diferentes plataformas hardware (sobremesa, portátiles, móviles y tabletas), con aplicativos software (MS Windows, iOS, Android o Linux).

Estos dispositivos pueden tener su pantalla incluida/embebida o utilizar pantallas y proyectores externos, así como altavoces, megafonía externa y diversos periféricos de interfaz humana que faciliten la interacción con los dispositivos.

7.1 Equipos terminales

7.1.1 Terminales de sala de reuniones

Equipos hardware instalados físicamente en una sala, fijos o móviles, basados en códec (codificador-decodificador) o en equipo con aplicativo software dedicados a reuniones de una o varias personas. Pueden ser de uso general para todo el personal o privativo en exclusiva para una persona.

- Deben estar en espacios de acceso vigilado o controlado, para evitar intrusiones físicas y suplantaciones de identidad en reuniones planificadas.
- Se debe desactivar la respuesta automática a llamadas entrantes.
- Se recomienda que la cámara tenga un indicador luminoso cuando está en funcionamiento o de forma accesoria un obturador físico de la lente que permita taparla.

- Los micrófonos de mesa deben tener un indicador luminoso de estado: abierto, en verde; cerrado, en rojo. En micrófonos embebidos, el indicador visual debe ser en pantalla.
- Se recomienda que la pantalla se active siempre que el equipo esté activo y se vaya a negro cuando el equipo entre en suspensión.
- Se debe garantizar la confidencialidad de las sesiones de audio y video, evitando cualquier dispositivo de captura o grabación externa, visible o no, como cámaras de vigilancia, móviles o micros.
- Deben tener su interfaz de control web configurado de manera segura con usuario y contraseña, y utilizar canales seguros basados en HTTPS o SSH cumpliendo estándares.
- Se recomienda que tengan bloqueado con código el acceso a opciones avanzadas.
- Deben estar actualizados a la última versión de firmware/software recomendada por el fabricante para evitar bugs conocidos y tener un plan proactivo de actualizaciones para vulnerabilidades de Día-0.
- El firmware/software de las aplicaciones que se ejecuten sobre el terminal debe provenir de repositorios verificados y autenticados, como pueden ser los repositorios del fabricante o los repositorios de aplicaciones de los proveedores de la plataforma (Microsoft, Google, Apple, Samsung, LG, etc.).
- Las sesiones de video deben de cumplir con al menos los siguientes requisitos relativos a la seguridad en las comunicaciones:
  - Utilizar canales seguros TLS 1.2 en las llamadas cifradas para la señalización y AES-128 o superior en el tráfico de media.
  - Recomendable el tráfico SRTP para audio, video y contenido (media) con cifrado AES-128 o superior.
  - En tráfico UDP, asegurar el cifrado AES-128 y que el intercambio inicial de claves sea sobre un canal seguro en TLS.
  - Se recomienda la utilización de certificados digitales (PKI) y listados de certificados verificados (CTL) para la autenticación entre los *endpoints* y su infraestructura de registro (SIP Register) y conmutación de video (MCU Bridge).

7.1.2 Terminales virtuales o móviles (App y software sobre plataformas)

Se consideran terminales virtuales a aquellas soluciones software tipo App o programas que emulan un terminal de video sobre una plataforma hardware de alta

movilidad -como podrían ser portátiles, móviles y tabletas de uso personal-, y generalmente asignadas y autenticadas con el nombre del usuario de la solución.

- La App/software debe provenir de repositorios verificados y autenticados como pueden ser los repositorios del fabricante o los repositorios de aplicaciones de los proveedores de la plataforma (Microsoft, Google, Apple, Samsung, LG, etc.).
- La identificación y autenticación mediante usuario y contraseña debe cumplir unos mínimos requisitos de fortaleza (ej.: longitud mínima recomendada de caracteres, combinación de letras, números y caracteres especiales, número máximo de intentos fallidos de autenticación, etc.).
- Las conexiones entrantes deben ser aceptadas por el usuario, no debe existir la posibilidad de autorespuesta.
- Deben ofrecer la posibilidad de acceder a la sesión con o sin video/audio.
- Las sesiones de video deben de cumplir al menos con los siguientes requisitos relativos a la seguridad en las comunicaciones:
  - Utilizar canales seguros TLS 1.2 en las llamadas cifradas para la señalización y AES-128 o 256 en el tráfico de media.
  - Recomendable el tráfico SRTP para audio, video y contenido (media) con cifrado AES-128.
  - En tráfico UDP asegurar el cifrado AES-128 y asegurar que el intercambio inicial de claves sea sobre un canal seguro en TLS.
- La compartición de documentos debe asegurar la confidencialidad de los datos y repositorios según determina el Esquema Nacional de Seguridad.

7.2 Infraestructuras

Se consideran infraestructuras a todos aquellos dispositivos de comunicaciones que proporcionan capacidades de registro de terminales, llamadas, reuniones multipunto, salidas y entradas de tráfico propio de la videoconferencia hacia internet a través de los cortafuegos. Se caracterizan por tener un comportamiento cliente-servidor.

Pueden ser infraestructuras locales (*on-premise*), en la nube (*Cloud VaaS* o *SaaS*), o soluciones híbridas mezcla de las soluciones *on-premise* y *cloud*.

Independientemente de su ubicación y tipología, todos los servidores o servicios de infraestructura deben cumplir de manera genérica los requisitos determinados según cada tecnología por el CCN-CERT en el Esquema Nacional de Seguridad (ENS) y específicamente algunos relativos a la tecnología de videoconferencia como los que se indican a continuación:

- Gestión segura con HTTPS y SSH.
- Autenticación H.235.
- H.460 Firewall Traversal.

Según sus funcionalidades las infraestructuras se pueden catalogar como:

- Sip Registrar y H323 Gatekeeper.
  - Registra y autentica terminales y otros dispositivos de infraestructura.
  - Dirige y monitoriza el tráfico de la videoconferencia.
  - Capacidades de centralita, planes de llamada.
  - Funciones de servidor proxy de video.
- Firewall Traversal
  - Asegura la comunicación LAN-WAN a través del firewall en conjunción con el SIP registrar o H323 Gatekeeper.
  - Funciones de Call Routing, Marcación URI y Registro DNS.
- Multipunto (Bridge MCU de Multiconference Unit en inglés)
  - Aloja las reuniones multipunto.
  - Aseguran la compatibilidad entre diferentes *códec* de audio y video.
  - Aseguran la compatibilidad entre diferentes plataformas de videoconferencia.
  - Compatibilizan llamadas entre equipos y dispositivos con diferentes anchos de banda o protocolos de comunicación.
  - Gestiona los parámetros de seguridad y administración de las sesiones.
- Grabadores y repositorios de contenido.
- Pasarelas multiprotocolo:
  - PSTN.
  - MS Skype/Teams.
  - Google Hangouts.

7.2.1 Infraestructuras en la nube

Soluciones ofrecidas por el proveedor en un modo de suscripción y tipología cliente-servidor. Normalmente el usuario solo accede a opciones básicas de configuración y

seguridad dejando en manos del proveedor el aprovisionamiento, seguridad y continuidad del servicio. Normalmente, se trata de soluciones Multitennant[4].

7.2.2 Infraestructuras locales

Soluciones específicas de una organización en modo de uso y gestión privativa, gestionadas y alojadas habitualmente en los centros de proceso de datos de la organización y en modo de licenciamiento perpetuo.

7.2.3 Reuniones Multipunto (VMR – Virtual Meeting Room)

Se define como *Virtual Meeting Room (VMR)* a aquellas conferencias audio/video con múltiples participantes, que pueden ser terminales de las diferentes tipologías mencionadas anteriormente o invitados mediante un enlace de un único uso a la reunión. Pueden estar alojadas indiferentemente en infraestructuras *on-premise* o *cloud*.

Una *Virtual Meeting Room* (VMR) debe cumplir los siguientes aspectos de seguridad en el control y acceso:

- La invitación de acceso a estas sesiones puede ser vía email con información anonimizada de cómo conectarse a la sesión en función del dispositivo o tecnología, a elección del destinatario, o bien, llamadas específicas del organizador a los diferentes participantes. Se recomienda esta última opción en sesiones altamente confidenciales.
- Se recomienda que los enlaces de entrada a la *VMR* sean de un solo uso y se destruyan tras finalizar la sesión, aunque pueden existir *VMR* personales con el mismo identificador de sesión, extremando la seguridad de acceso.
- La *VMR* debe tener PIN diferenciado de administrador e invitado.
- Los invitados no deben poder acceder a la sesión hasta que el organizador no entre en la sesión.
- Una vez iniciada la sesión, el organizador o moderador deben poder cerrar el acceso a la sesión a nuevos participantes.
- Se pueden programar sesiones con el número exacto de participantes para evitar intrusiones accidentales.
- El moderador debe saber con información veraz quiénes están conectados a la sesión, con identificadores y nombres. Se ha de valorar si también los participantes deben conocer o no quiénes están en la sesión.

[4] Aquellos servicios software o hardware en los cuales varios clientes comparten los mismos recursos.

- Cada vez que entre o salga un participante debe haber un indicador visual y sonoro.
- El moderador debe tener las pertinentes herramientas de control y moderación para poder gestionar las conexiones de los participantes o para conectar o expulsar participantes, cerrar micrófonos, deshabilitar video o contenidos.
- El moderador gestiona quiénes pueden grabar la reunión y siempre debe mostrarse a todos los participantes un indicador visual e incluso sonoro de que la sesión está siendo grabada.
- En la *VMR*, además de tener comunicación audiovisual, se pueden compartir contenidos como documentos ofimáticos, imágenes y videos.
- También se puede compartir el escritorio entero o seleccionar solo las aplicaciones a mostrar para garantizar la confidencialidad de los datos.
- El sistema debe garantizar que no se pueden realizar capturas de pantalla del contenido presentado, mostrando un fondo en negro si se lanza alguna App de captura de pantalla.
- Es recomendable poder distinguir entre participantes de la organización y participantes externos, bien durante la sesión en curso o bien cuando se ha generado la invitación de enlace a la *VMR*.
- Cuando el moderador abandona la sesión, esta se debe cerrar salvo que se cedan los derechos de moderación a un tercero.
- La *VMR* se puede cerrar automáticamente por inactividad al abandonar el último participante la sesión.

- **Estructura de las reuniones virtuales**
  - Es necesario disponer de servidores con infraestructura en la nube.
  - Es necesario disponer de un instalador en los equipos.
  - Utilizar un *plugin* de navegador o cliente.
  - Se debe establecer el volumen de asistentes concurrentes en la sala.
  - Las conexiones en el firewall únicamente se pueden abrir en modo saliente a la nube que ofrece el servicio, pues al instalarse en equipos que no van a tener supervisión se evita en la medida de los posible que sea una puerta de entrada de ataques.
- **Controles de acceso**
  - Describir el proceso de las invitaciones y los accesos a la sala virtual.

- Se debe establecer qué usuarios pueden grabar la reunión. Los asistentes deben conocer a quién se le ha concedido este permiso.
- Se puede establecer el auto cierre de la sala por inactividad.
- Configurar el envío de alertas para la notificación de abandono de la sala del administrador. También se puede establecer el cierre de la sala en caso de que el administrador la abandone. En este último caso se debe prestar atención a posibles cortes en la conexión.

- **Elementos que se pueden compartir**
  - Documentos ofimáticos.
  - Escritorio.
  - Pizarras virtuales.
- **Seguridad**
  - Se han de revisar los elementos que se comparten entre los miembros de la sala. El administrador ha de tener un control de quiénes acceden a la sala y quiénes están grabando.
  - Se recomienda la utilización de un sistema de gestión de eventos automatizado (SIEM) que monitorice los *logs* de los clientes, con objeto de obtener un informe de uso de la herramienta. Dado que los usuarios pueden instalar la herramienta en equipos sin supervisión, es muy importante controlar que la herramienta únicamente se usa en horario laboral y para ello debe poder enviar eventos de sesión a algún SIEM.
  - Si se habilita la compartición de escritorio, se tiene que comprobar si están registradas todas las acciones de los usuarios.
  - Se puede distinguir entre conexiones con equipos internos de personal interno a reuniones con personal externo si se considera necesario una mayor revisión de la seguridad.

8. VIGILANCIA

La vigilancia de los accesos remotos y los registros de los mismos cobra una vital importancia a la hora de detectar ciberincidentes. Se recomienda que todos los accesos remotos se realicen a través de canales cifrados mediante la utilización de redes privadas virtuales (TLS1.2 o superior, IPSec) y con autenticación robusta de doble factor de autenticación (2FA); intentando evitar servicios de terminales (SSH, RDP…) con acceso directamente desde internet.

Una vez autenticados, los accesos remotos deben ser controlados por el firewall corporativo. Se desaconseja expresamente el acceso SMB y NetBios, por la posibilidad de propagación o de impacto de código dañino en caso de compromiso del equipo origen, así como RDP.

En caso de que la organización disponga de servicios accesibles desde internet que permitan el acceso a información potencialmente sensible, como sistemas de webmail o de correo electrónico en movilidad, se deben aplicar sobre ellos las mismas salvaguardas que sobre los sistemas de acceso remoto.

Siempre que se envíe información sensible a través de estos sistemas, se recomienda utilizar herramientas como PGP (*Pretty Good Privacy*) para la protección de la confidencialidad, integridad y autenticidad de la información.

8.1 Autenticación de acceso y perfilado del equipo mediante canales cifrados

Con el objetivo de mitigar el riesgo que supone el acceso remoto, la conexión debe cumplir con las siguientes características:

- El canal de comunicación debe ser cifrado (red privada virtual) y terminar en un firewall.
- Se debe perfilar el dispositivo en el momento de la conexión antes de obtener el acceso.
- El usuario que se conecte a la red debe tener credenciales corporativas (*IDP Corporativo - Identity Provider*) para validar la identidad.
- Deben definirse unos requisitos mínimos de conexión (postura de seguridad) para el dispositivo usado en el acceso remoto, bien sea un dispositivo corporativo o no corporativo (BYOD).
- En función de la postura de seguridad, se podría permitir o denegar el acceso y/o informar al administrador del resultado.
- La conexión debe solicitar un segundo factor de autenticación para evitar la suplantación de identidad.
- Los datos de la conexión deben quedar registrados y estar disponibles para su consulta ante posibles análisis forenses.
- Se debe proteger los accesos al equipo del teletrabajador por parte de personas no autorizadas en el emplazamiento en que se esté realizando el acceso remoto que, al no ser el corporativo, presenta riesgos mayores (por ejemplo, acceso de amigos, familia, posibles visitantes…). Para ello, es precisa la configuración de un

adecuado control de acceso lógico al equipo de usuario (contraseñas adecuadas, bloqueo del puesto, etc.).

- Se han de controlar los privilegios de acceso remoto a recursos por parte del teletrabajador, que no tienen por qué ser los mismos que cuando se trabaja en local. Para ello, deberán implementarse mecanismos de control de acceso lógico a recursos corporativos desde accesos remotos.

8.2 Sistema de gestión de eventos (SIEM)

El sistema de gestión de eventos (SIEM) es el centro de avisos ante ataques o ciberincidentes, al recibir información de diferentes registros, de mediciones de equipos, así como de alertas de los dispositivos de los organismos.

Por ello, se ha de llevar a cabo una monitorización activa con reglas de correlación que aporten valor y muy dedicadas a detectar posibles incidentes. Del mismo modo, el SIEM debe contener reglas de correlación que detecten y alerten del uso indebido en los accesos remotos.

8.2.1 Fuentes

El SIEM debe recibir las siguientes fuentes:

- Logs de los clientes de acceso remoto.
- Logs de las conexiones a los equipos de acceso remoto.
- Horas de los equipos a los que se accede de forma remota.
- Direcciones IP externas permitidas o identificadas como legitimas en los accesos remotos.
- Netflows.
- Antivirus.
- EDR.
- Listado de usuarios que pueden acceder a cada máquina de acceso remoto.
- Volumetría y accesos de DNS (filtraciones de DNS).
- Logs de DNS (locales y de la empresa).
- Firewall.

8.2.2 Reglas de correlación

Se han de establecer las siguientes reglas de correlación:

- Accesos fuera de horario.
- Accesos desde terceros países (si no existe causa justificada).
- Múltiples errores de autenticación de un usuario desde varias direcciones IP en un intervalo de tiempo T.
- Múltiples errores de autenticación de varios usuarios desde una dirección IP en un intervalo de tiempo T.
- Accesos simultáneos del mismo usuario desde dos direcciones IP en un intervalo de tiempo T.
- Accesos correctos de diferentes usuarios desde la misma dirección IP en un intervalo de tiempo T.
- Accesos remotos, o intentos, desde direcciones en lista negra (rangos, países, etc.).
- Geolocalizaciones cambiantes.
- Descarga de datos por encima de umbral.
- Intentos de acceso desde redes privadas virtuales (VPN) a recursos no autorizados.
- Intentos de ejecución remota desde clientes VPN.

8.2.3 Alertas

Las alertas se deben registrar en el sistema de *ticketing* corporativo, que a su vez debe disponer de capacidad para enviarlas a las áreas operativas a través de múltiples canales: SMS, correo electrónico, mensajería instantánea, etc.

Se recomienda plasmar en un cuadro de mando el volumen y/o criticidad de alertas relativas a accesos remotos, en especial durante días de riesgo elevado.

8.3 Control de Acceso

Se deben implementar políticas de control de acceso a las infraestructuras por parte de usuarios y dispositivos (IoT, BYOD, etc.). Las políticas pueden estar basadas en autenticación, configuración del dispositivo o identificación de roles de usuario. Se podrían incluso implementar políticas posteriormente basándose en la integración con otros productos de seguridad. Por ejemplo, forzando una política de seguridad a un dispositivo final basándose en una alerta de un SIEM.

Se deben disponer de las siguientes capacidades:

- Visibilidad: Inventario de dispositivos, infraestructura y usuarios.

- Visibilidad continua automática en la conexión. Etiquetar activos críticos (GDPR, etc.) por riesgo de ciberseguridad.
- Control de acceso: Control de los activos en redes cableadas, Wifi y redes privadas virtuales (VPN) como punto único de decisión y aplicación de las políticas de acceso. Integración con otras soluciones de seguridad (NGFW, SIEM, etc.).
- Segmentación de red: Segmentación por redes y funciones.
- Cumplimiento de políticas de seguridad: Asegurar las políticas definidas por la Organización o de obligado cumplimiento. Definir y aplicar líneas base de seguridad para *endpoints*, *datacenters* y dispositivos de red (conmutadores y puntos de acceso). Respuesta ante vulnerabilidades. Agentes permanentes (personales) y solubles (de terceros) para control granular.

Las funcionalidades que se deben desarrollar son:

- Autenticación: control de identidad de las entidades (usuarios y dispositivos) que acceden a la red. La identidad se puede verificar frente a varios repositorios (Directorio Activo, certificado, dirección MAC y otros).
- Autorización: asignación de privilegios y permisos específicos en la red a cada entidad (asignación de VLAN, por ejemplo).
- Auditoría: recolección, agrupación y evaluación de eventos de acceso.
- Inventario: con información detallada de cada identidad conectada a la red.
- Perfilado: establecimiento y verificación de perfiles en una identidad que puede definirse como obligatorio para acceder a la red. Por ejemplo, un SO, un nivel de actualización y presencia de antivirus.
- Posicionado: evaluación en tiempo real del comportamiento de los dispositivos conectados para determinar si ese comportamiento se ajusta a los parámetros esperados y toma de acciones de corrección.
- Remediación: enlazado con el punto anterior, ejecución de acciones necesarias para remediar o minimizar las amenazas detectadas. Por ejemplo, mediante el aislamiento de la entidad comprometida.
- Doble factor de autenticación: especialmente entornos de VPN.

8.4 Mediciones de tráfico netflow y comportamiento

Las mediciones pueden llevarse a cabo mediante herramientas de control del tráfico, que genera alertas al salirse de:

- Mediana de tráfico.

- Picos de volúmenes de tráfico de red.
- Tráfico de red en horarios anómalos.
- Conexiones anómalas de los equipos.
- Conexiones habituales con mayor volumen de datos.

8.5 Endpoint Detection and Response (EDR)

Los sistemas de *Endpoint Detection and Response* (EDR) complementan y amplían las funcionalidades de los antivirus. En situaciones de riesgo, las amenazas pueden cambiar mucho; por ello, se ha de actuar contra las formas de ataques, el uso de programas mal intencionados o el uso indebido de programas legítimos.

Estas acciones malintencionadas pueden ser monitorizadas y paradas por los EDR. Para ello, se han de establecer las pautas que se describen a continuación:

- Identificar comportamientos anómalos.
- Intensificar las reglas de TTP.
- Establecimiento de mecanismos para prevenir *ransomware* o robos de información.
- Establecimiento de mecanismos de aviso.
- Monitorización continua de amenazas.
- Análisis forense, respuesta a incidentes, investigaciones guiadas y *malware hunting*.
- Contención en tiempo real de amenazas.
- Conexión con SIEM (bidireccional).
- Perfilado de acciones de usuario y aviso antes usos inesperados o poco habituales.

8.5.1 Identificación de comportamientos anómalos

Los EDR pueden detectar procesos o archivos sospechosos. Para cada ejecutable se proporcionan estadísticas granulares, como la reputación/popularidad, cuándo fue visto por primera vez, en cuántos ordenadores fue visto/ejecutado, cuántas operaciones de archivos/conexiones de red se establecieron, qué modificaciones realizó y otros metadatos que son útiles para identificar el comportamiento potencialmente sospechoso de cualquier ejecutable.

Dado que el EDR registra todo lo que sucede en nuestra red, es posible revisar si se está haciendo un uso indebido de las herramientas de trabajo de distintas formas:

- Se pueden buscar por ejecutables, para saber si se está haciendo uso de un programa no autorizado.
- También se pueden buscar los procesos o direcciones IP que usan estos procesos.
- Por último, se pueden generar reglas específicas para que avisen en caso de que detecten alguno de los puntos anteriores en nuestra red.

8.5.2 Intensificar las reglas de TTP

Se mapea la base de datos de conocimientos MITRE ATT&CK para el análisis posterior de las tácticas, técnicas y procedimientos de los cibercriminales.

8.5.3 Mecanismos para prevenir ransomware o robos de información. Contención en tiempo real de amenazas

Muchos EDR cuentan con una *sandbox* de seguridad en la nube que proporciona una capa de defensa adicional fuera de la red de la empresa para evitar que el código dañino como el *ransomware* se ejecute en un entorno de producción.

Los EDR monitorizan y evalúan todas las aplicaciones ejecutadas en función de su comportamiento y reputación. Están diseñados para detectar y bloquear procesos que se asimilan al comportamiento del determinado código dañino como el *ransomware*.

Mediante un EDR que incorpora la funcionalidad de "control de dispositivos", se puede monitorizar el uso de dispositivos en los equipos para permitir especificar qué usuarios pueden acceder a ellos (CD/DVD/USB, etc.). Al definir reglas para medios específicos, dispositivos y usuarios, el control de los dispositivos permite bloquear aquellos que no se encuentran autorizados e impide que los códigos dañinos se expandan a través de medios extraíbles, evitando además el uso de estos dispositivos para robar información de la empresa.

8.5.4 Mecanismo de aviso

Los paneles de administración de los EDR poseen un sistema de alertas en el cual podemos ver lo que está sucediendo en nuestra red en tiempo real. También es posible habilitar un sistema de notificaciones por correo electrónico en caso de que se desee recibir una notificación inmediata para algún aviso específico.

8.5.5 Conexión con SIEM

Es posible configurar el EDR y la consola de administración para que envíe notificaciones a un servidor de *Syslog*. Eventos de las siguientes categorías de registro se exportarán al servidor de *Syslog*: amenazas, cortafuegos, HIPS, auditoría y Enterprise Inspector.

8.5.6 Perfilado de acciones de usuario. Aviso ante usos inesperados o poco habituales

Una vez se ha detectado un uso inesperado o poco habitual de alguna aplicación, se deberá investigar, en primer lugar, si se trata de un uso legítimo o ilegitimo. Para ello, mediante el EDR y sus paneles de administración, se podrá ver el árbol de procesos hasta el cual se ha acabado haciendo uso de esa aplicación.

Adicionalmente, desde los paneles de administración también se puede ver de forma sencilla todos los indicadores de compromiso del proceso para que se sepa exactamente qué es lo que está sucediendo. Asimismo, se puede descargar el ejecutable de esa aplicación para enviarlo o analizarlo en una *sandbox*, en caso de que se disponga de ella.

Por último, en caso de que se detecte que se trata de una aplicación dañina, el EDR da la opción de aislar el ordenador desde la consola de administración o de bloquear esta aplicación mediante su firma de código *Hash*, para que esta no sea ejecutada más mientras se limpia el equipo afectado.

8.5.7 Análisis forense, respuesta a incidentes, investigaciones guiadas y malware hunting

El EDR recopila todo, tanto los *logs* del sistema operativo MS Windows como los de registros del antivirus, además de recopilar también los scripts y los ejecutables que hay en cada máquina.

Aunque no se tengan los datos necesarios en el momento, dado que se dispone de los registros de todo lo que ha sucedido, nunca se dará el caso de no saber qué ha sucedido por no tener los registros

El EDR contiene reglas específicas creadas por expertos en ciberseguridad que se dedican desde hace años a proteger los equipos de miles de usuarios en todo el mundo para lidiar con amenazas tanto genéricas como específicas, las cuales se van actualizando y mejorando diariamente.

Todas estas reglas, además, ofrecen información adicional sobre la alerta, una explicación de la propia regla, posibles causas dañinas, posibles causas benignas, una explicación de cómo encarar el proceso de resolución de la alerta e incluso identifica en qué tipos de ataques puede causarse esta alerta. Asimismo, ofrece la posibilidad de visitar la página de MITRE con la técnica del ataque que se puede estar sufriendo, donde se ofrecerán más detalles del mismo.

Las reglas pueden ser adaptadas y generadas para cada organismo. Se recomienda un número reducido de reglas para identificar lo antes posible comportamientos anómalos.

Además de poder generar reglas únicamente basadas en los procesos, también se pueden generar reglas basadas en los metadatos de los propios ficheros y en el sistema de

reputación; lo que, combinado con el resto de las posibilidades, ofrece una herramienta de gran potencia y flexibilidad para adaptarnos a cualquier circunstancia.

9. USO DE DNS CON PROTECCIÓN Y QUE OFREZCAN LOGS

Es necesaria la capacidad de obtener información de los logs de DNS y las resoluciones de DNS de los equipos. Estas medidas pueden dar señales de alerta ante conexiones indebidas o dominios sospechosos.

Existen alternativas en el mercado que ofrecen un servicio de DNS con reputación, intentado evitar conexiones dañinas. Para activar dicho servicio después de contratarlo con el proveedor, se debe cambiar la configuración de DNS de los equipos a la indicada por el proveedor para intentar impedir dichas conexiones maliciosas.

El servicio puede proveer de servicios de alerta ante la aparición de nuevos dominios dañinos o poco confiables. Si esto se une al SIEM y a los logs de los equipos puede no ser necesario el cambio de DNS (si no se puede abordar) para, al menos, estar prevenidos ante ataques.

La opción del cambio del DNS es una opción que necesita una planificación, pero puede dar un buen soporte ante conexiones ilegitimas.

10.GESTIÓN DE CREDENCIALES

Para ampliar la información les recomendamos revisar al Guía CCN-STIC 821 (Apéndice V: Normas de Creación y Uso de Contraseñas NP40).

10.1 Protección y credenciales

Un elemento fundamental para proteger a una organización frente a ataques de ciberseguridad es la correcta gestión de sus credenciales, que cobra especial importancia en situaciones de teletrabajo, en las que la coordinación entre equipos e individuos debe establecerse fuera de los canales habituales y de manera remota.

Las recomendaciones para la gestión, almacenamiento de contraseña están orientadas a:

- Almacenar de forma segura todos los secretos.
- Disponer de niveles de confidencialidad para las diferentes credenciales.
- Establecer una cadena de custodia de los secretos.
- Establecer mecanismos de compartición segura, utilizando canales seguros y cifrados.

- Disponer de controles de acceso y registro de auditoría sobre las modificaciones de credenciales en el repositorio.
- Evitar siempre la reutilización total o parcial de los elementos sensibles del secreto, lo cual permitiría inferir unos secretos a partir de otros.

10.2 Almacenamiento seguro de las credenciales

Las credenciales de los sistemas o de otros mecanismos de la organización se pueden almacenar en dispositivos digitales o según los casos en formato físico únicamente.

Para el almacenamiento digital de las contraseñas se puede recomendar:

- No se deben almacenar en claro.
- No almacenarlos en recursos cuyo acceso no esté controlado y limitado.
- Protegerlos mediante claves de acceso. Estas claves nunca deberán ser claves por defecto.
- En los casos que sean posible, habilitar el segundo factor para acceder al repositorio de credenciales.

El medio más común para el almacenamiento de secretos son los gestores de contraseñas, aplicaciones web o móviles que ofrecen a usuarios y grupos capacidades para guardar sus elementos sensibles de forma segura.

El uso de un gestor de contraseñas debe sopesarse cuidadosamente, teniendo en cuenta que:

- Debe almacenar todos los secretos cifrados, utilizando mecanismos criptográficos modernos y robustos, basadas en datos que sólo conoce el usuario.
- Debe disponer de mecanismos propios de autentificación de usuarios. El usuario debe definir sus credenciales de acceso al gestor de forma que:
  - Sean exclusivas del gestor y nunca se asemejen a otras credenciales empleadas en cualquier otro servicio.
  - Sean suficientemente robustas, preferiblemente frases de paso (*passphrase*), no vinculadas con información que podría inferirse conociendo al usuario o la organización.
- Proporcione información técnica suficiente sobre los mecanismos de almacenamiento y cifrado que emplea.
- Permita el uso de un segundo factor de autentificación (2FA).

- Ofrezca un generador automático de contraseñas aleatorias, que simplifique la tarea del usuario a la hora de crear nuevos valores seguros para un secreto.
- Tenga trazabilidad de quien y cuando realiza el cambio de credenciales en entornos colaborativos o de múltiples usuarios.

11.RECOMENDACIONES GENÉRICAS

En el presente apartado se enumeran una serie de medidas genéricas de protección, algunas de las cuales serán desarrolladas en los anexos del presente documento.

- Tener instaladas las últimas actualizaciones del sistema operativo.
- Tener actualizados los antivirus con la mayor frecuencia posible tanto en equipos y dispositivos perimetrales.
- Intensificar el uso del doble factor en los accesos a sistemas, equipos, accesos remotos, etc.
- Tener activados servicios de monitorización con alertas definidas.
- Activar las auditorías de los equipos receptores de las conexiones remotas
- Revisar los registros y auditorías de las conexiones remotas.
- Tener habilitados canales de comunicación para reuniones mediante internet.
- Restringir montar unidades mapeadas del organismo en equipos remotos inseguros.
- Evitar las opciones de "*Split-Tunneling*" en equipos inseguros o que no cumplan todas las medidas de seguridad.
- Revisar o tener más vigilados unidades para intercambiar información.
- Asegurar si los antivirus escanean los dispositivos USB conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.
- Tener listados telefónicos de fácil acceso para comunicarse con las diferentes personas.
- Tener listados de personas, direcciones IP, teléfonos, correos electrónicos corporativos y alternativos relacionados con el acceso a los sistemas de forma remota.
- Tener actualizado el listado de personas que pueden acceder remotamente a los equipos de la organización con la dirección IP de acceso y medio de conexión.
- Tener controladas las invitaciones, contraseñas y asistentes de las salas de reuniones.

- Conocer si en una sala de reunión algún integrante la está grabando.
- Compartir de forma segura todos los secretos, credenciales y otra información sensible empleada, por ejemplo, para el acceso a servicios, aplicaciones, sistemas, redes, VPN, reuniones remotas, etc.

11.1 Vulnerabilidades conocidas

A la hora de redactar el presente documento, Microsoft ha publicado un aviso de vulnerabilidad en el protocolo SAMBA, en su versión 3. En este sentido, se ha dado a conocer un posible escaneo con NMAP:

https://gist.github.com/nikallass/40f3215e6294e94cde78ca60dbe07394

En estos casos, se recomiendan las siguientes acciones:

- Conocer, al menos, que equipos pueden estar afectados por la vulnerabilidad para conocer sobre que equipos se deben aplicar futuras medidas de mitigación o contención.
- La actualización de sistemas operativos y elementos que proporcionen acceso remoto para prevenir posibles incidentes de seguridad.

12. TABLA RESUMEN DE COMPROBACIÓN

Acción	Responsable	Estado	Comentarios
Acciones relativas a los usuarios			
Concienciación COVID-19			
Concienciación Teletrabajo			
Concienciación Videoconferencia			
Acciones relativas al acceso remoto			
VPN – Registrar todos los eventos y todas las conexiones			
VPN – Activar los registros de auditoría			
VPN – Implementar 2FA y complejidad de contraseñas			
VPN – Verificar requisitos previos			
VPN – Limitar las conexiones			
VPN – Restringir conexiones SSH, RDP, SMB y NetBIOS			
VPN – Utilizar máquinas de salto			
VPN – Deshabilitar *Split-Tunneling*			
CITRIX-VDI – Registrar todos los eventos y todas las conexiones			
CITRIX-VDI – Activar los registros de auditoría			
CITRIX-VDI – Implementar 2FA y complejidad de contraseñas			
CITRIX-VDI – Verificar requisitos previos			
CITRIX-VDI – Deshabilitar el intercambio de información			
CITRIX-PdT(puesto de trabajo) – Registrar todos los eventos y todas las conexiones			
CITRIX-PdT – Activar los registros de auditoría			
CITRIX-PdT – Implementar 2FA y complejidad de contraseñas			
CITRIX-PdT – Verificar requisitos previos			
CITRIX-PdT – Deshabilitar el intercambio de información			
CITRIX-PdT – Desplegar solución Detección y Respuesta			
PdT – Mantener SO actualizado			
PdT – PIN/Contraseña + Bloqueo			
PdT – Mantener AV actualizado			
PdT – Configurar AV inspeccionar USB			
PdT – Proteger conexión a redes wifi			
PdT – Activar registros de auditoría			
PdT – Desplegar solución Detección y Respuesta			
PC-Propio (Personal) – Mantener SO actualizado			

PC-Propio – PIN/Contraseña + Bloqueo			
PC-Propio – Mantener AV actualizado			
PC-Propio – Configurar AV inspeccionar USB			
PC-Propio – Proteger conexión a redes wifi			
PC-Propio – Desplegar solución Detección y Respuesta			
Acciones relativas al correo electrónico			
Envío y recepción – Reforzar la inspección de los correos			
Envío y recepción – Bloquear correos con enlaces maliciosos			
Envío y recepción – Bloquear correos con macros			
Envío y recepción – Bloquear correos de listas negras			
Envío y recepción – Actualización del AntiSPAM frecuentemente			
Envío y recepción – Bloquear correos con scripts o ejecutables			
Acceso – Implementar 2FA y complejidad de contraseñas			
Acceso – Registrar todos los eventos			
Acciones relativas a la videoconferencia			
Utilizar *software* descargado desde la página oficial			
Contraseñas robustas y máximo número de intentos			
PIN diferente para roles administradores			
Enlaces de un solo uso			
Registrar todos los eventos			
Utilizar, al menos, TLS1.2 y AES-128			
Deshabilitar grabación y *streaming*			
No permitir capturas de pantalla/grabaciones			
Autocierre por inactividad			
Inspección técnica de seguridad			
Acciones relativas a la detección y vigilancia			
Logs SIEM – Autenticación VPN/CITRIX			
Logs SIEM – Autenticación acceso al correo			
Logs SIEM – Autenticación videoconferencia			
Logs SIEM – Eventos de seguridad del AntiSPAM			
Logs SIEM – Eventos de seguridad del Antivirus			
Logs SIEM – Eventos de seguridad del EDR			
Logs SIEM – Consulta de nuevos dominios en el DNS			

Logs SIEM – Eventos de seguridad de cortafuegos			
Reglas SIEM – Accesos remotos fuera del horario			
Reglas SIEM – Accesos (VPN/CITRIX/Correo/Video) desde 3os países			
Reglas SIEM – Múltiples errores de acceso (VPN/CITRIX/Correo/Video)			
Reglas SIEM – Múltiples accesos (VPN/CITRIX/Correo/Video)			
Reglas SIEM – Accesos internos no autorizados desde (VPN/VDI/PdT)			
Reglas SIEM – Conexiones puertos administración			
Monitorizar tráfico DNS interno			
Monitorizar conexiones internas Netflow (VPN/VDI/PdT y del resto)			
EDR – Detectar extracción de credenciales			
EDR– Detectar ficheros/servicios en “System32/SysWOW64”			
EDR/– Detectar carpetas aleatorias en AppData			
EDR/ – Detectar tareas programadas en AppData			
EDR/ – Detectar ficheros “.ryk”			
EDR/– Detectar ejecutables en la carpeta TMP			
EDR/– Monitorizar papelera de reciclaje			
Otras acciones			
Mantener actualizado el Sistema Operativo del parque completo			
Deshabilitar la ejecución de Macros en documentos de Office			
Restringir la ejecución de código de fuentes desconocidas			
No permitir la ejecución de Powershell en ningún equipo			
Registrar accesos a los Controladores de Dominio			
Revisar la configuración de los Controladores de Dominio			
Actualizar las firmas del Antivirus SEP con mayor frecuencia			
Bloquear las conexiones hacia Internet en Listas Negras			
Reforzar la configuración segura del correo (TLS, SPF, DKIM, DMARC)			
Revisar la política de copias de seguridad			

13. RECOMENDACIONES DE SEGURIDAD PARA REUNIONES VIRTUALES

Ante la generalización del uso de aplicaciones para la organización de reuniones virtuales y videollamadas, el Centro Criptológico Nacional ha elaborado un decálogo de recomendaciones de seguridad para el empleo seguro de estos servicios.

	Decálogo de seguridad para reuniones virtuales
1	**Aplicaciones de proveedores oficiales:** descarga únicamente aplicaciones de proveedores oficiales, como Google Play o Apple Store, o de los sistemas del proveedor (Microsoft, Google, Cisco, etc.), intentando mantenerlas actualizadas de manera permanente.
2	**Número exacto de participantes:** programa sesiones colaborativas, sean de audio o vídeo o contenido, con el número exacto de participantes. Cuando todos los usuarios entren en la sesión, es conveniente cerrar el acceso a nuevos participantes.
3	**Programa sesiones con identificador (ID) único de un solo uso por reunión:** evita usar las VMR permanentes, salvo que tengan bloqueado el acceso a nuevos usuarios o sólo se pueda acceder a ellas por invitación.
4	**Configura la sesión para que un indicador visual o sonoro avise de la entrada o salida de nuevos usuarios:** el moderador y si es posible el resto de los usuarios, deben de saber con información veraz quienes están conectados a la sesión, con identificadores o nombres, especialmente en las conexiones de solo audio.
5	**El moderador de la sesión (audio, video o contenido) gestiona si esta puede ser grabada:** si está siendo grabada, debe de mostrarse a todos los usuarios un indicador visual y sonoro de que se está produciendo la grabación.
6	**Uso de contraseña o PIN:** todos los usuarios que accedan a la reunión deberían de hacerlo con contraseña o PIN, y en la medida de lo posible, diferenciando para moderador e invitados.
7	**Contrala el contenido que compartes:** en la medida de lo posible, evita pinchar en enlaces que se compartan en el chat de la sesión, sobre todo si no conoces a la persona que lo ha compartido.
8	**Rol del moderador:** el moderador de la reunión deber poder gestionar la conexión de los participantes y tener capacidad de expulsar a usuarios, cerrar micrófonos o deshabilitar contenidos o señal de vídeo.
9	**Acceso a la sesión:** se recomienda que los participantes de la sesión no puedan acceder hasta que no se conecte el moderador. La sesión debe de poder cerrarse al salir el moderador.
10	**Enlace a la reunión:** no compartas públicamente el enlace a la reunión, ni su ID, ni el PIN de moderador o invitado.

14.BUENAS PRÁCTICAS PARA PREVENIR INCIDENTES

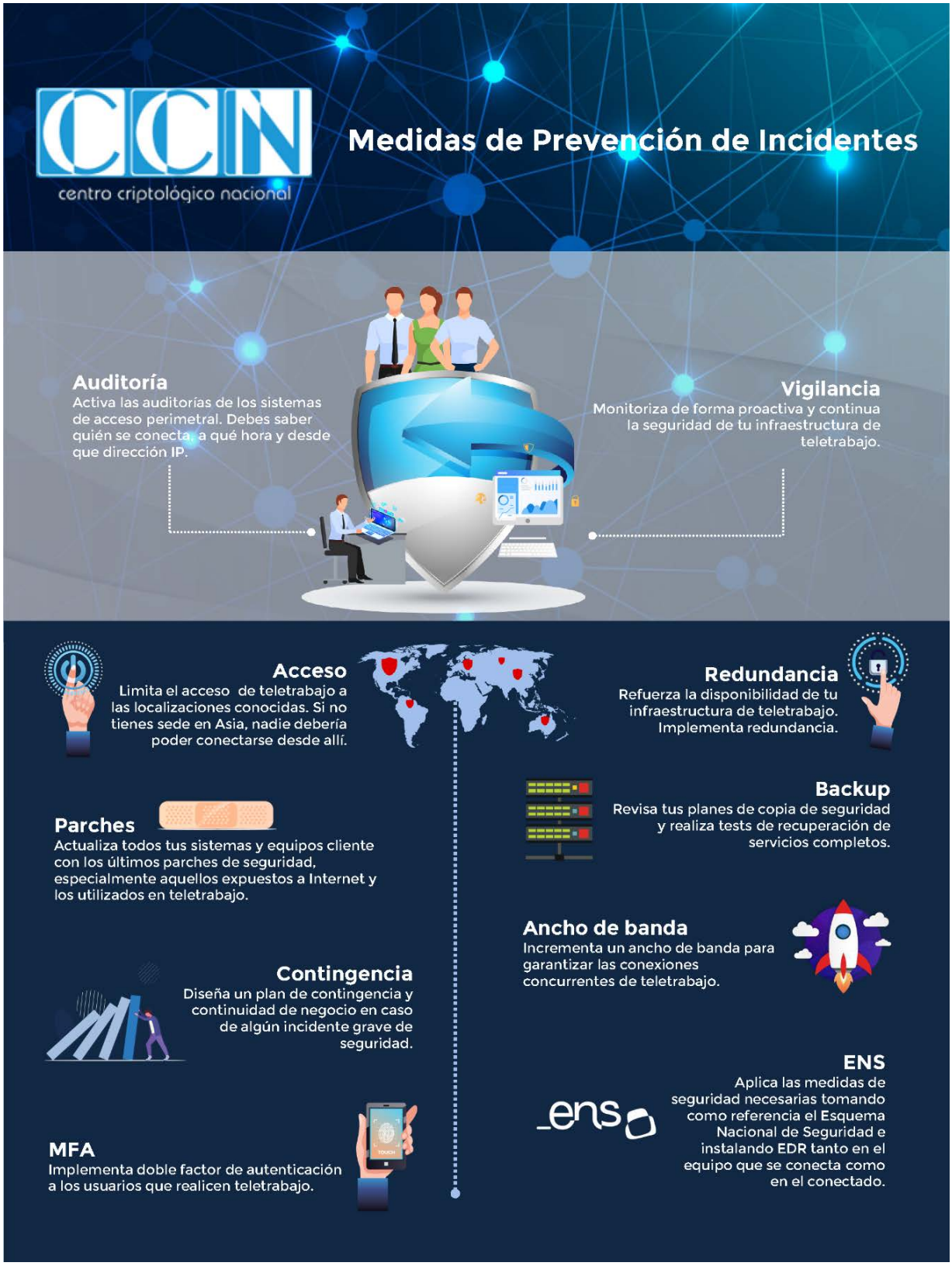


Ilustración 2.- Recomendaciones y medidas a tener en cuenta para prevenir incidentes de seguridad relacionados con teletrabajo.

15.ANEXOS Y APOYOS DE EMPRESAS

Coordinados por el CCN-CERT, diferentes empresas que operan en nuestro país en el sector de la ciberseguridad[5], han decidido ofrecer de manera altruista algunos servicios y soluciones para diferentes públicos.

En el siguiente apartado, se detalla el soporte que ofrecen estas compañías para mejorar la seguridad en situaciones de teletrabajo y el alcance del público que se puede beneficiar del mismo. La ayuda y colaboración va desde acceso remoto seguros, consultoría, licencias de antivirus y EDR a servicio de DNS seguro.

EMPRESA	SERVICIO
BE:SEC by Emetel	- Monitorización de la seguridad - Consultoría de seguridad
Check Point Software Technologies	- Plataforma de Acceso Remoto Seguro - Endpoint
CISCO	- Acceso remoto seguro - DNS Seguro
Citrix / Sidertia	- Consultoría de seguridad - Auditoría - Acceso remoto seguro
CSA	- Consultoría de seguridad - Acceso remoto seguro - DNS Seguro
DinoSec: GuardedBox	- Gestor online para almacenamiento y compartición seguros de secretos.
Entelgy Innotec Security	- Servicios gestionados de seguridad - Monitorización de la seguridad - Consultoría de seguridad - Acceso remoto seguro
EMMA (Partners Certificados)	- Acceso remoto seguro
Eset	- Antivirus - Endpoint
Extreme Networks	- IoT en entornos remotos
Fortinet	- Acceso remoto seguro
Grupo CIES	- Servicios gestionados de seguridad - Monitorización de la seguridad - Consultoría de seguridad

[5] NOTA DEL CCN-CERT: Las empresas aquí recogidas son aquellas que han ofrecido sus servicios de forma espontánea. No obstante, actualizaremos este documento en la medida que se vayan uniendo otras compañías.

Grupo TRC	- Servicios gestionados de seguridad
IBM	- Indicadores de compromiso
ICA Sistemas y Seguridad	- Servicios gestionados de seguridad - Despliegue e Integración de infraestructura de seguridad - Consultoría de seguridad
Ingenia	- Implantación soluciones acceso remoto y contingencia - Monitorización de la seguridad - Consultoría de seguridad
McAfee	- Antivirus - Endpoint
Microsoft	- Consultoría de seguridad - Acceso remoto - SIEM - Herramientas colaborativas
Mnemo	- Consultoría de seguridad
Mr. Looquer	- Descubrimiento de servicios - Monitorización de la seguridad
Nunsys	- Acceso remoto
OnRetrieval	- Recuperación de datos - Análisis forense
Palo Alto Networks	- Plataforma de Acceso Remoto Seguro - Endpoint
Panda-Cytomic	- Antivirus - Endpoint
Proconsi	- Consultoría de seguridad - Gestión de copias de seguridad
Pulse Secure	- Plataforma de Acceso Remoto Seguro
ReaQta	- Endpoint
S2 Grupo	- Servicios gestionados de seguridad - Monitorización de la seguridad - Consultoría de seguridad
S21Sec	- Endpoint - Indicadores de compromiso
SealPath	- IRM (Information Rights Management)
Sophos	- Antivirus - Endpoint
Sothis	- Servicios gestionados de seguridad - Indicadores de compromiso - Consultoría de seguridad

Stormshield	- Acceso remoto
Telefónica	- Servicios gestionados de seguridad - Monitorización de la seguridad - Consultoría de seguridad
ValoraData	- Gestión de copias de seguridad - Custodia externalizada de copias de seguridad (vaulting) - Soluciones Disaster Recovery
Wise Security Global	- Notificaciones certificadas

15.1 BE:SEC by Emetel

Desde BE-SEC, marca especializada en ciberseguridad de la consultora tecnológica EMETEL, se pone a disposición de las entidades públicas y empresas privadas un conjunto de servicios de seguridad que habiliten un teletrabajo seguro, ayuden a paliar los efectos negativos motivados por la crisis del COVID-19 y permitan iniciar un camino hacia una nueva forma de organizarse.

- Revisión del nivel de seguridad de las plataformas tecnológicas empleadas para el teletrabajo.

  Se recopila la información proporcionada por las distintas organizaciones con relación a dichas herramientas y se evalúa: (i) el nivel de seguridad de las mismas, en función del cumplimiento de los controles propuestos por los principales estándares y buenas prácticas internacionales de seguridad (NIST, ISO 27001, etc.) y (ii) la configuración según guías de bastionado ampliamente extendidas (NIST, CCN-CERT, etc.), en lo concerniente al acceso remoto a la red, los sistemas y la información corporativa.

- Detección y análisis de vulnerabilidades de las plataformas tecnológicas empleadas para el teletrabajo.

  Se realiza un escaneo automatizado de la solución de teletrabajo para la detección de potenciales vulnerabilidades y un análisis de las mismas, con el objetivo de confirmar si son explotables.

- Asesoramiento y soporte consultivo para el despliegue de plataformas de teletrabajo.

15.1.1 Contacto

Email: COVID19@be-sec.net

15.2 Check Point Software Technologies

Con el fin de ayudar durante la situación acontecida por el Covid19, Check Point Software Technologies pone a disposición de todos los organismos públicos (durante 2020 y primer semestre de 2021) a través de sus socios las siguientes soluciones.

15.2.1 Soluciones Acceso Remoto VPN

Para aquellos clientes u organismos que ya dispongan de equipamiento se pone a su disposición licencias temporales de hasta 3 meses para cualquiera de los servicios y/o de los agentes necesarios para permitir la conexión desde el puesto de trabajo.

Para aquellos clientes que no dispongan de equipamiento propio, podrá contar con apoyo de nuestros socios para provisionar tanto soluciones *on-premise*, como en *Cloud*. En ambos casos, las licencias tendrán una duración de al menos 3 meses sin coste.

https://www.checkpoint.com/es/products/remote-access-vpn/

15.2.2 Soluciones Seguridad Endpoint para el puesto de trabajo y dispositivos móviles

Sandblast Agent (EPP+EDR) y Sandblast Mobile están disponibles para Windows, Mac, Linux, Android, IOS.

Sandblast Agent ofrece protección avanzada:

https://www.checkpoint.com/es/products/advanced-endpoint-protection/

Sandblast Mobile para los sistemas operativos modernos (IOS, Android) ofrece:

https://www.checkpoint.com/es/products/mobile-security/

Check Point Software facilitará licencias ilimitadas tanto para la protección del puesto de trabajo como dispositivos móviles de manera gratuita durante un período de al menos (3) meses, a aquellos organismos u estamentos que lo requieran.

Se ofrecerá ayuda tanto en la configuración como en el despliegue durante el proceso de implantación, así como en la resolución de cualquier incidencia de ciberseguridad que pueda presentarse durante dicho periodo.

Además, a todos aquellos estamentos u organismos que decidan implantar de forma definitiva cualquiera de las soluciones, también se incluirá:

- Ayuda en la migración (en los casos que aplique).
- Ayuda a la configuración y puesta en marcha de la solución.

15.2.3 Soluciones de Seguridad para Correo en Nube, Herramientas de Compartición de Documentación en Cloud y Trabajo Colaborativo

Desde Check Point Software ofrecemos un Servicio en la nube que previene los ataques contra las empresas que usan aplicaciones SaaS. CloudGuard SaaS protegerá Office 365, G-Suite, Salesforce, Slack y otros servicios SaaS.

https://www.checkpoint.com/es/products/saas-security/

Check Point Software facilitará licencias ilimitadas de protección de Correo SaaS en Office 365 o Gmail de manera gratuita durante un período de al menos (3) meses a aquellos organismos que lo requieran.

Además, a todos aquellos estamentos u organismos que decidan implantar de forma definitiva la solución de CloudGuard SAAS, también se incluirá:

- Ayuda en la migración (en los casos que aplique).
- Ayuda a la configuración y puesta en marcha de la solución.

15.2.4 Soluciones de Seguridad para usuarios de consumo

Con el fin de llegar a todos, Check Point dispone de una gama de soluciones de seguridad de consumo, de licencia perpetua en la condición de uso o suscripción de la misma.

- ZoneAlarm Web Secure Free: Extensión para Chrome.
  https://www.zonealarm.com/software/web-secure-free.
- ZoneAlarm Free Firewall: Protección para firewall para el PC.
  https://www.zonealarm.com/software/free-firewall.
- ZoneAlarm Free Antivirus: solución antivirus robusta y firewall.
  https://www.zonealarm.com/software/free-antivirus.

15.2.5 Contacto

Antonio Cortés Molinillo
Móvil: 609 729 643
Email: acortes@checkpoint.com

Francisco Ramírez Arcia
Móvil: 699 075 065
Email: framirez@checkpoint.com

José Antonio Madroñal
Móvil: 608 588 766
Email: jmadronal@checkpoint.com

15.3 Cisco

15.3.1 Suministro de equipos y licencias

- Hasta 4 meses de Cisco WebEx para clientes de Defensa, Inteligencia y Seguridad Nacional, extensible, bajo petición a otras AA.PP.
- Hasta 4 meses de Cisco Umbrella, para aumentar la defensa basada en DNS y prevenir las actuales campañas de phishing y similares.
- Hasta 4 meses de DUO + AnyConnect, para permitir la creación de VPN seguras, con doble factor de autenticación.

15.4 Citrix/Sidertia

15.4.1 Citrix

Citrix Systems está plenamente comprometido con la situación que se está viviendo y se ha lanzado un programa especial sobre el Reto de la Continuidad de Negocio que las compañías están afrontando. Las organizaciones, tanto públicas como privadas, requieren ser tratadas de forma individual conforme a sus necesidades. Por ello, para buscar su solución adecuada pueden ponerse en contacto a través del email: citrixiberia@citrix.com, referenciando CCN-CERT en el asunto.

Debido a que cada entidad puede tener diferentes escenarios y tipos de licencias, no es posible indicar tarifas de descuento estándar de apoyo al impacto COVID-19, por eso, cada caso será tratado de forma individualizada para ofrecer la mejor opción y ventajas en cuanto a las modalidades de adquisición de licencias y en función de los diferentes escenarios que se puedan requerir por entidad.

15.4.2 Sidertia

La empresa SIDERTIA pone en marcha, y a disposición de Entidades Públicas y Privadas, mientras dure la estabilización del COVID-19, los siguientes servicios:

- Servicio de asesoramiento gratuito para la aplicación de “Medidas de seguridad para Acceso Remoto con tecnología Citrix” vinculados con peticiones de Citrix a través del correo citrixiberia@citrix.com y referenciando CCN-CERT en el asunto.
- Documento de plan preventivo de configuración de DIEZ MEDIDAS DE PREVENCIÓN DE INCIDENTES de seguridad para el acceso desde puesto cliente para teletrabajar de forma segura.
- Servicio gratuito de verificación de configuración mínima de bastionado en equipos cliente y servidor e interpretación de resultados mediante la solución CLARA ENS en su nivel BAJO.

- Ante el riesgo de posibles campañas de malware que puedan aprovechar el impacto del COVID-19 para realizar ataques mediante uso de correo electrónico o suplantación de identidades, ofrecer descuentos de consultoría para la configuración de los servicios de auditoría de los servidores de Directorio Activo, MS Exchange y MS Azure para disponer de mecanismos de análisis en caso de afección por ciberataques.
- Servicio de análisis de cambios de los sistemas de la Organización ante posibles ataques de "Phishing". La comparación de análisis realizados con CLARA-ENS alertará de cambios en configuraciones fundamentales de seguridad y ejecución de procesos y servicios, permitiendo comprobar si se han aplicado las medidas correctivas una vez detectada una brecha de seguridad.

15.4.3 Contacto

Jerónimo García Parra - Director Sidertia Solutions
Móvil: 646 116 305
Email: jgarcia@sidertia.com

15.5 CSA

CSA puede proporcionar servicios de tres (3) tipos: suministro, ingeniería y servicios críticos.

15.5.1 Suministro de equipos y licencias

Cualquier campaña de: Cisco, Fortinet o Microsoft, puede ser gestionada por nuestro personal. La gestión incluye la intermediación con el fabricante y el soporte de cualquier incidencia que se pudiera producir durante el servicio.

Se detalla a continuación la propuesta de CISCO:

- Hasta cuatro (4) meses de Cisco WebEx para clientes de Defensa, Inteligencia y Seguridad Nacional, extensible, bajo petición a otras AA.PP.
- Hasta cuatro (4) meses de Cisco Umbrella, para aumentar la defensa basada en DNS y prevenir las actuales campañas de phishing y similares.
- Hasta cuatro (4) meses de DUO + AnyConnect, para permitir la creación de VPN seguras, con doble factor de autenticación.

15.5.2 Servicios de ingeniería

- Equipo de Ingeniería de Red y Seguridad REMOTO, disponible para ayudar a diseñar o reconfigurar soluciones de acceso remoto o seguridad perimetral, que

ayuden a las organizaciones a afrontar su plan de contingencia. Tecnologías: Cisco, Fortinet, Check Point, Palo Alto Networks, Forcepoint, Stonesoft, …

- Equipo de Ingeniería de Red y Seguridad PRESENCIAL: como el anterior, pero con capacidad de operación inmediata en Madrid, Valladolid, Burgos, Sevilla, Murcia y Tenerife.

15.5.3 Contacto

Email: covid-19@csa.es

15.6 DINOSEC: GUARDEDBOX

La empresa DinoSec pone a disposición de toda la comunidad (individuos, organismos públicos y privados, administraciones o empresas), de manera gratuita, su solución GuardedBox, un gestor online de almacenamiento seguro y compartición de secretos.

La crisis sanitaria del Coronavirus (COVID-19) no solo está poniendo en riesgo la salud pública, sino también la información sensible, que queda colateralmente expuesta debido a las urgentes medidas de actuación que acompañan a la situación de emergencia actual, influenciadas principalmente por el teletrabajo.

A los problemas de dimensionamiento de las infraestructuras y los equipos tecnológicos hay que añadir un componente esencial: el intercambio y almacenamiento de secretos digitales de todo tipo, entre ellos, claves de acceso a sistemas y servicios, credenciales para la autenticación de usuarios (por ejemplo, en conexiones VPN), reuniones remotas, contraseñas que protegen ficheros confidenciales, certificados digitales, claves criptográficas y un largo etcétera. Poner a disposición de las personas estos secretos requiere de mecanismos de intercambio seguro.

GuardedBox, disponible en castellano e inglés, reúne los requisitos mínimos para almacenar e intercambiar secretos y datos sensibles de manera segura, de forma sencilla e intuitiva, ya que no requiere de conocimientos técnicos para su uso. Algunos de los principales elementos diferenciadores de GuardedBox son:

- Permite la compartición de secretos tanto entre individuos como entre grupos. Los grupos pueden tener carácter temporal (para compartición puntual) o permanente (equipos de trabajo).
- Utiliza técnicas de criptografía avanzada de manera totalmente transparente para el usuario, quien no necesita preocuparse de la gestión de sus claves ni de la de los usuarios y grupos con quienes comparte secretos.
- El servidor no almacena ningún dato sensible en claro y carece de capacidad para descifrar secretos del usuario, ya que todas las operaciones criptográficas se

realizan en el lado cliente, único lugar en el que residen las claves privadas del usuario.

- El compromiso del servidor por parte de un atacante no pone en riesgo los secretos de ningún usuario.

Se puede consultar la descripción detallada de GuardedBox y su documentación asociada en https://guardedbox.es, desde donde se puede acceder al servicio, tanto a nivel personal como profesional.

15.6.1 Contacto

Email: info@guardedbox.es

15.7 Entelgy Innotec Security

Desde Entelgy Innotec Security se plantea la prestación de los siguientes servicios para organismos públicos:

- Despliegue de solución de acceso remoto (basado en OpenVPN en caso de no tener nada, o con lo que tenga el cliente). Se necesita un servidor en el cliente y la administración, mantenimiento y soporte de la misma.
- Despliegue de la solución de bastionado del puesto de trabajo (Panda), y la administración, soporte y mantenimiento de la misma con las licencias que provee Panda.
- Apoyo a la configuración de sistemas de colaboración y videoconferencia (GSuite, Microsoft Teams, WebEx, ...) con las licencias que tengan o proporcione otro y su administración y soporte
- Monitorización de seguridad de la infraestructura y servicios principales.
- Avisos de seguridad y noticias relevantes durante la crisis (boletín diario).
- Soporte en la resolución de incidentes de seguridad para incidentes críticos.
- Revisiones de seguridad del perímetro (hacking ético).

15.7.1 Contacto

Esther Torres García
Móvil: 648 496 948
Email: esther.torres@innotec.security

Adicionalmente, la empresa ha activado una cuenta de correo electrónico soporte.covid19@entelgy.com para prestar cualquier tipo de ayuda/atención.

15.8 EMMA (Open Cloud Factory)

A través de los Partners se dimensionará el servicio atendiendo a las necesidades de los Organismos Públicos (volumetrías, físico o virtual y necesidades de instalación, nivel de soporte y características).

15.8.1 Vigilancia en accesos remotos

El firewall incluido en este módulo de EMMA, realiza de *front-end* para la finalización de túneles VPN con los clientes, mediante agente distribuido previamente (equipos conocidos y desconocidos). EMMA realiza la autenticación, autorización y auditoría contra el gestor de identidades corporativo del Organismo y permite añadir un segundo factor de autenticación (OTP).

Se recoge el inventariado y perfilado completo del equipo. Este perfilado se podrá utilizar en las políticas de acceso a la conexión remota. Se permite definir y aplicar políticas de acceso en función de una postura de seguridad basado en el nivel de bastionado deseado, pero también de factores como horario de la conexión.

15.8.2 Cumplimiento, visibilidad y respuesta

La vigilancia en Accesos Remotos con EMMA es solo un caso de uso, ya que EMMA es una solución de vigilancia que ofrece:

- Deficiencias en la capa de acceso y electrónica.

  Capa de acceso/electrónica: identifica deficiencias en la configuración de la electrónica mediante reglas definidas en ROCÍO e integración con ANA (ambas soluciones del CCN-CERT) con el fin de determinar el grado de cumplimiento con la política de seguridad establecida y las necesidades de mejora continua.

- Conectividad a la red.

  Visibilidad/perfilado, además de trazabilidad, de todo lo conectado a la red desde dentro (usuarios internos, externos, IoT, …), desde fuera (teletrabajo, proveedores de servicios) e infraestructura.

- La capacidad de respuesta ante eventos.

  Control de los activos en redes cableadas, Wi-Fi y redes privadas virtuales (VPN) con un punto único de decisión y aplicación de las políticas de acceso y respuesta. Integración con otras soluciones de seguridad (NGFW, SIEM, etc.).

Las políticas de acceso se puedan implementar a la hora de conectarse a la red y también en modo repuesta en el caso de identificar una nueva amenaza para identificar los equipos remotos afectados y dar respuesta a los mismos (desconexión de red o informar).

Toda la información quedará registrada y se podrá contrastar desde EMMA.

15.8.3 Soporte e instalación

La solución será provisionada como servicio para los Organismos Públicos interesados a través de los *partners* de EMMA Certificados (https://www.ccn-cert.cni.es/soluciones-seguridad/emma.html), con soporte 8x5 vía telefónico y 24x7 por email (ambos canales en español).

15.8.4 Contacto

Email: emma@ccn-cert.cni.es / emma@opencloudfactory.com

15.9 ESET

La empresa ESET facilitará licencias de protección EDR de manera gratuita durante un periodo de seis (6) meses aquellos organismos que lo requieran. Del mismo modo, facilitará licencias de protección *Endpoint* gratuitas también durante un período de seis (6) meses y servicios profesionales a los mismos organismos para que puedan solicitar su apoyo en la gestión e instalación de estas herramientas o en la resolución de cualquier incidencia de ciberseguridad que pueda presentarse, durante un período de seis (6) meses y también de manera gratuita.

Estos servicios se ofrecerán a cualquier empresa que reclame el soporte adecuado para la correcta implementación de las soluciones de seguridad ESET y de la protección EDR en su entorno. Este soporte incluirá:

- Servicio de migración, donde se le ayudará al cliente a configurar y a realizar un primer despliegue de nuestras herramientas.
- Servicio de configuración, para ayudar al personal técnico a configurar las soluciones de seguridad de ESET de forma correcta.

15.9.1 Contacto

David Sánchez García - Responsable Departamento Técnico ESET España
Teléfono: 962 913 348
Email: david@eset.es

15.10 Extreme Networks

Para la protección de dispositivos IoT en entornos remotos, se pueden emplear soluciones hardware dedicadas.

IoT Defender de Extreme Networks permite realizar una conexión segura de dispositivos IoT en remoto, fuera de la LAN Corporativa de la empresa que lo utilice. El

Defender es capaz de adoptar políticas creadas de forma centralizada para asegurar que el dispositivo IoT se comporta correctamente. La conexión contra el equipo central se realiza mediante un túnel IPSec, asegurando el cifrado y la integridad de las comunicaciones.

15.10.1 Descripción del funcionamiento y aplicación

La función principal del IoT Defender consiste en el despliegue de políticas en el dispositivo (las cuales son creadas y enviadas por el equipo central), de acuerdo a un perfil.

El Defender Adapter puede desplegarse sobre redes públicas: se crea un túnel IPSec entre el Adapter y el XCA que permite el envío y recepción de tráfico del dispositivo IoT de forma segura. Existen otros modos de despliegue que no son objeto de este documento.

En este caso, se sugiere la aplicación en un entorno hospitalario, donde puede necesitarse que el enfermo esté monitorizado en su vivienda (entorno remoto), sin ocupar una cama en el hospital, el dispositivo médico (bomba de infusión, equipo de medida, etc.), se conectaría al Defender Adapter.

15.10.2 Contacto

Francisco García
Móvil: 609 100 091
Email: francisco.garcia@extremenetworks.com

15.11 Fortinet

Fortinet agrupa su oferta de colaboración en los siguientes enlaces para activar teletrabajo de manera eficiente, simple, inmediata, sin coste y segura:
https://fortixpert.blogspot.com/2020/03/informacion-relacionada-con-el.html

15.11.1 Contacto

Si se necesita soporte, la manera de contactar se explica en esta entrada:
https://fortixpert.blogspot.com/2014/04/abrir-casos-de-soporte.html

15.12 Grupo CIES

Se proporciona una breve descripción de los servicios que se pueden ofrecer sin coste, con el objetivo de colaborar en la crisis del COVID-19.

- Monitorización de ciberseguridad (SOC).

  Despliegue y explotación de soluciones de monitorización y detección temprana de incidentes de seguridad mediante sistemas de detección de intrusiones, correlación de eventos y comprobación de indicadores de compromiso.

- Consultoría de seguridad.

  Apoyo en el diseño y despliegue seguro de tecnologías de acceso remoto y sistemas de protección del *endpoint*, así como validación de la correcta implantación de las mismas.

- Auditoría.

  Verificaciones del grado de exposición externo de las organizaciones mediante pruebas de hacking ético sobre los activos públicos de la organización.

- Cumplimiento.

  Desarrollo de normativa de seguridad para regular el teletrabajo (alineada con el Esquema Nacional de Seguridad). El servicio se acompaña de material formativo on-line para garantizar su correcta difusión y comprensión

- Servicios de concienciación.

  Acceso a material de concienciación orientado a mejorar la seguridad en entornos de teletrabajo.

15.12.1 Contacto

Email: covid19@institutocies.es

15.13 Grupo TRC

Grupo TRC, compañía integradora de soluciones tecnológicas, infraestructuras y de desarrollo de software, es capaz de desplegar rápidamente soluciones a medida (no basadas en un sólo fabricante) para implementar, garantizar, potenciar y proteger todo el ecosistema de teletrabajo, así como la parte de seguridad y absoluta movilidad de los mismos.

Implementa plataformas de escritorio virtual VDI (#virtualiza), conexiones VPN de rápido despliegue (#accede), seguridad fuera de perímetro a usuarios, archivos y documentos (#securiza), plataformas de backup (#respalda), soluciones en la nube (#trabaja) y opciones de conectividad 4G (#conecta).

Los servicios que se pueden ofrecer, con el objetivo de colaborar en la crisis del COVID-19:

- Apoyo en la configuración de sistemas de teletrabajo, colaboración y videoconferencia seguras.
- Evaluación de las contramedidas de los clientes frente a diferentes vectores de ataque.

- Servicios de formación y concienciación.

15.13.1 Contacto

Email: comercial@gruportc.com

15.14 IBM

Siguiendo con las aportaciones de IBM a la lucha contra COVID-19 y todo lo que conlleva a su alrededor, en el enlace adjunto están las recomendaciones que ha publicado el equipo de respuesta ante incidentes e inteligencia de seguridad de IBM (X-Force Incident Response and Intelligence Services -IRIS-) en relación al COVID-19, así como las iniciativas que están llevando a cabo.

https://securityintelligence.com/posts/ibm-x-force-threat-intelligence-cybersecurity-brief-novel-coronavirus-covid-19/

Como parte de estas iniciativas está el acceso sin coste durante 30 días a la plataforma de inteligencia de amenazas TruSTAR. TruSTAR combina inteligencia de X-Force IRIS con información de un amplio ecosistema y hace más accesible la información urgente sobre COVID-19 a la comunidad de usuarios de la plataforma.

En caso de que algún organismo del Gobierno de España decida acceder a esta plataforma, es posible organizar una sesión de formación en la que expertos de X-Force IRIS expliquen el funcionamiento del portal para que los usuarios puedan obtener provecho de la plataforma de la forma más rápida posible.

15.14.1 Contacto

Jesús Albo - Security Intelligence Client Executive
Móvil: 637 706 224
Email: jesus.albo@ibm.com

15.15 ICA Sistemas y Seguridad

ICA Sistemas y Seguridad, unidad especializada de Grupo ICA, pone a disposición de las **AA.PP.** su catálogo de servicios.

15.15.1 Monitorización asistida

Monitorización permanente de los Sistemas del Cliente desde el Centro de Operaciones de Grupo ICA, para la detección de amenazas, fallos, disponibilidad, incidentes de seguridad y ataques.

15.15.2 Garantía de fabricante

Servicio de gestión de la garantía de los productos del cliente de acuerdo al nivel de servicio contratado con el fabricante. A través de este servicio y en función del acuerdo establecido se realiza la gestión continua de:

- Incidentes con los fabricantes de tecnología, desde la apertura hasta la resolución.
- Seguimiento de estado, vigencia y renovación de la garantía.
- Almacén y gestión de stock para optimización y mejora de tiempos de resolución.
- Notificaciones de estado de producto y actualizaciones de seguridad.

15.15.3 Monitorización de Ciberseguridad

Servicio a través del cual se monitorizan activos del cliente orientado a la gestión de la seguridad. Se emiten informes con información de eventos y se trasladan por medio electrónico al cliente, dependiendo de necesidades comunicadas por el mismo. La monitorización incluye procesos internos de tratamiento, análisis automatizado y correlación.

15.15.4 Alerta Temprana de Ciberseguridad

Servicio gestionado de alerta de vulnerabilidades de las plataformas cliente que se desarrolla en modalidad cloud desde las instalaciones de ICA.

15.15.5 Contacto

Se establecen como contacto, las siguientes direcciones de correo electrónico: info@grupoica.com , seguridad@grupoica.com

15.16 Ingenia

15.16.1 Implantación de soluciones de acceso remoto

Ingenia trabaja con los principales fabricantes del mercado (Fortinet, Palo Alto, Check Point, Pulse, …) y está en disposición de ofrecer soluciones de acceso remoto con implantación rápida tanto con equipamiento físico como virtual, siguiendo las recomendaciones del CCN-CERT.

15.16.2 Despliegue de soluciones de contingencia (seguridad y colaboración)

Ingenia puede gestionar de forma inmediata soluciones que ponen los distintos fabricantes a disposición de las **AA.PP.** de forma temporal, entre ellas:

- Sistema de colaboración Cisco WebEx sin límite de usuarios.

- Sistema de protección de navegación mediante DNS Cisco Umbrella sin límite de usuarios.
- Sistema de doble factor de autenticación Cisco Duo sin límite de usuarios.
- Soluciones de Microsoft y Sophos indicadas en el apartado correspondiente de este documento.

15.16.3 Monitorización de la seguridad

Servicios de monitorización continua y 24/7 de los sistemas de seguridad de la organización prestando especial atención a los accesos remotos para evitar incidentes de seguridad. El servicio incluye:

- Despliegue y optimización de la herramienta SIEM.
- Monitorización de seguridad.
- Auditorías técnicas de seguridad.
- Gestión de incidentes de seguridad.
- Análisis forense.

15.16.4 Consultoría de seguridad

Asesoramiento en el cumplimiento de las medidas necesarias desde el punto de vista de seguridad normativa y legal: cumplimiento del ENS, establecimiento de políticas corporativas para teletrabajo, clausulado en los contratos para teletrabajo con los trabajadores (con independencia de que sea ocasional o permanente), realización de planes de contingencia y recuperación antes desastres, planes de continuidad del negocio, etc.

15.16.5 Contacto

Email: preventaisos@ingenia.es

15.17 McAfee

Atendiendo al portfolio de McAfee puede contribuir con las siguientes tecnologías:

- EPP/EDR.
- SIEM.
- Bastionado de entornos cloud (en la medida en que los organismos tengan activos ahí a los que vayan a acceder los trabajadores en remoto).

- Proxy Cloud (una forma rápida y sencilla de que las mismas políticas de navegación que aplicarían a los usuarios in-situ puedan aplicar a los usuarios remotos).

15.17.1 Contacto

Ángel Ortiz - Regional Director Spain
Móvil: 620.188.497
Email: angel_ortiz@mcafee.com

15.18 Microsoft

15.18.1 Visión general de recursos de acceso remoto

Microsoft ha publicado instrucciones para ayudar a las empresas a comprender las opciones disponibles para permitir que sus empleados usen Microsoft Teams.

Our commitment to customers during COVID-19 blog post

Igualmente se ha publicado un blog para ayudar a los CISO y responsables de seguridad a proteger los activos y recursos para trabajo en remoto: https://www.microsoft.com/security/blog/2020/03/12/support-working-from-home-securely/

15.18.2 Ofertas y pruebas de evaluación

En la tabla siguiente se describen las ofertas de los equipos que están disponibles para los clientes que aún no han implementado equipos en su organización.

Propuesta	Duración	Límite Usuarios	Detalles Adicionales
Office 365 E1	6 meses	2.500	A solicitar a través del equipo de cuenta
Microsoft Teams Cloud Solution Provider (CSP) Trial	6 meses	1.000	Clientes comerciales nuevos o existentes gestionados por un CSP
Microsoft Teams Exploratory Experience	Sin coste hasta enero de 2021	Ninguno (se asignan en grupos de 100)	Usuarios finales que tienen una cuenta de AAD como parte de un servicio de Microsoft existente
Microsoft 365 Trials (F1, E3, E5) - Windows Enterprise E3 o E5 (funcionalidad del EDR) - EMS - Office 365	1 mes	25	Posibilidad de ampliarlo, gestionado por el equipo de cuenta
Enterprise Mobility and Security (EMS) - Multifactor Authenticator (MFA) y acceso condicional - Gestión de dispositivos en movilidad con Intune - Protección de la información mediante etiquetado de documentos	1 mes	25	Posibilidad de ampliar gestionado por el equipo de cuenta

Cloud App Security (CASB)	1 mes	25	Posibilidad de ampliar gestionado por el equipo de cuenta
Despliegue Windows Virtual Desktop (escritorios remotos en Azure)	Hasta junio 2020		Posibilidad de inversión para clientes que desplieguen más de 25 usuarios activos
Trials de Project, Visio, PowerBI Pro, Power Apps, Power Automate	1 mes	25	Posibilidad de ampliar gestionado por el equipo de cuenta
Azure Sentinel (SIEM) - INGESTA: durante los 30-dias de trial de Sentinel y Azure Security Center sólo se contabilizarían en Azure los costes de ingesta de logs en workspaces de Log Analytics, salvo los logs que está categorizados como gratuitos en Sentinel: o Logs de actividad de Azure o Logs de auditoría de Office365 (incluidos logs de actividad de Exchange y Sharepoint) o Alertas de los productos Microsoft Advanced Threat Protection: Azure Security Center, Azure ATP, Office365 ATP, Windows Defender ATP, Microsoft Cloud App Security, Azure Information Protection.	30 días		

15.18.3 Contacto

Oscar Sanz
Email: oscarsan@microsoft.com

15.19 Mnemo

MNEMO puede colaborar con los **organismos públicos** prestando apoyo y soporte sobre la base de los servicios desplegados en su SOC-CERT. Específicamente para la ayuda en la situación de teletrabajo actual en los siguientes ámbitos:

- Servicio de alerta preventiva sobre las amenazas relacionadas con la situación provocada en el ámbito de COVID-19.
- Atención a consultas vía correo electrónico en la dirección soporte.covid19@mnemo.com, en relación con medidas de ciberseguridad, mejores prácticas, amenazas actuales, etc.
- Soporte para la configuración de sistemas de teletrabajo: configuración de VPN, políticas de acceso, control de usuarios, sistemas de colaboración, etc.
- Ayuda para la obtención de información relacionada con posible malware distribuido durante la crisis de COVID-19.
- Ayuda para la disponibilidad de información sobre inteligencia de amenazas basada en nuestro servicio de Cyber Threat Intelligence mientras dure la crisis.

- Apoyo a consultas para mejorar los procesos de monitorización y detección de incidentes relacionados con las posibles amenazas que se produzcan en el ámbito de COVID-19.
- Apoyo en la detección e información sobre posibles estrategias y amenazas de phishing producidas durante la crisis.

15.19.1 Contacto

Roberto Peña Cardeña - Director de Ciberseguridad de MNEMO
Móvil: 658 877 788
Email: r.peca@mnemo.com

Fernando García Vicent - Director de Operaciones de MNEMO
Móvil: 609 718 060
Email: f.garciav@mnemo.com

15.20 Mr. Looquer

Para desplegar este servicio solo es necesario, tener la petición de la organización y sus dominios o espacio direccional.

- Monitorización de Infraestructuras Gubernamentales, desplegadas, bien de forma presencial o temporalmente en infraestructuras públicas como Azure, Amazon y Google Cloud.
- Análisis del perímetro de las **AA.PP.** con monitorización continua.
- Apoyo al descubrimiento rápido del Shadow IT.

15.20.1 Contacto

Email: hi@mrlooquer.com

15.21 Nunsys

Conoce nuestro catálogo de soluciones de teletrabajo para que tu empresa no se vea afectada por las consecuencias del COVID-19.

https://mcusercontent.com/05b47d4522269a1c12a18b4d3/files/08d90114-4c25-42c3-afbd-7a2dabd207d2/Soluciones_Teletrabajo_Nunsys_V2.01.pdf

15.21.1 Contacto

Email: info@nunsys.com

15.22 OnRetrieval

OnRetrieval quiere aportar su granito de arena ante la Crisis del COVID-19 y ofrecer sus capacidades tecnológicas para contribuir a minimizar el impacto.

15.22.1 Recuperación de datos

Desde OnRetrieval, con relación a la Crisis del Coronavirus y ante el riesgo de continuidad en la prestación de Servicios esenciales por una incidencia de pérdida de datos, pone a disposición de todos los Organismos del sector público el laboratorio de Recuperación de Datos, para atender sin costo mientras permanezca el Estado de Alarma, cualquier recuperación de datos de cualquier dispositivo (discos duros, discos sólidos, tarjetas de memoria, sistemas RAID, móviles, etc.) que afecte a la prestación de estos Servicios.

El laboratorio de OnRetrieval está trabajando durante esta crisis siguiendo protocolos de esterilización de los dispositivos, para garantizar la salud de nuestros trabajadores y clientes.

15.22.2 Análisis Forense

Ofrecemos los servicios de adquisición de evidencias de dispositivos electrónicos para incidentes de seguridad que limiten la prestación de Servicios durante este Estado de Alarma. Poniendo nuestros medios tecnológicos y equipo humano a disposición de los organismos públicos.

15.22.3 Contacto

Teléfono gratuito: 900 900 381
Email: sac@onretrieval.com / forense@onretrieval.com

15.23 Palo Alto Networks

15.23.1 Soluciones disponibles de Acceso Remoto seguro

Ayudar a nuestros clientes y socios en tiempos de crisis es uno de nuestros valores prioritarios. Siguiendo las instrucciones de salud emitidas por el gobierno de España para limitar la propagación del COVID-19, se deben implementar cambios inmediatos para permitir que los empleados trabajen de forma remota.

Podemos ayudar durante este período crítico a través de Prisma Access. Esta solución, basada en una arquitectura en la nube, facilita la protección de los usuarios en cualquier lugar del mundo y en pocos minutos. Además, es fácilmente escalable y puede albergar a un gran número de usuarios sin intervención de la entidad.

Si no se es cliente de Palo Alto Networks, esta solución también está disponible sin tener que implementar ningún equipo en la red; solo es necesaria la instalación de un agente (GlobalProtect) en la estación de trabajo. Un agente único, una solución única para responder a los diferentes casos de uso.

Puesto que esta crisis de salud sin precedentes así lo requiere, se participa también activamente en la asistencia a los clientes o partners a través de:

- Para nuevos clientes de este servicio, con la implementación de una solución temporal de Prisma Access durante 45 días sin cargo. Si se desea optar por una solución definitiva, también se incluye sin coste un recurso técnico experto para ayudar en el despliegue.
- Para clientes ya existentes, a través de la capacidad de extender el número de usuarios que usan la solución hasta un 300% sin sobre coste, para absorber el pico de carga.
- Para clientes que deseen realizar los túneles VPN en sus propios equipos de Palo Alto Networks, ponemos a disposición de los clientes la suscripción de GlobalProtect (para mejorar la seguridad, poder evaluar el estado los dispositivos que se conectan) por un plazo de 90 días. Tan sólo es necesario solicitarlo y estará disponible de forma inmediata.

15.23.2 Soluciones disponibles de Orquestación/Automatización y EDR

Las operaciones de TI/Seguridad están bajo una gran presión ante esta crisis para adaptar su infraestructura de TI y ciberseguridad relacionada.

Es necesaria la automatización de las tareas de TI y ciberseguridad para liberar tiempo de operación mientras se mantiene el más alto estándar de seguridad:

- Versión completa de XSOAR (Demisto) gratis durante 3 meses con acceso completo a todos los casos de uso (*playbooks*) y soporte.
- Involucrar *partners* certificados para ayudar a construir la automatización necesaria de inmediato aprovechando los existentes y personalizando lo necesario para adaptarlo a cada escenario.
- Activar la comunidad local de XSOAR para aumentar el intercambio entre los clientes para una incorporación rápida.
- Automatizar no solo la gestión e investigación de incidentes sino también otras acciones como:
    - Recopilar información sobre aplicaciones, sistemas y usuarios para automatizar acciones, informes, programación, gestión de permisos, etc.

- Gestión de provisión de servicios TI durante la adquisición de nuevos ordenadores, contratación de nuevos empleados para cubrir los picos de demanda, etc… Se podría automatizar la provisión de credenciales, implementación de clientes VPN, provisión del correo electrónico, etc.

- Palo Alto también pone a disposición de sus clientes sus soluciones de XDR, con el fin de proteger el puesto de trabajo aliviando así a los equipos de seguridad tan sobrecargados en situaciones de crisis.

15.23.3 Contacto

Pablo Chapinal Uráin
Móvil: 618 154 900
Email: pchapinalura@paloaltonetworks.com

Miguel Ángel Torralba
Móvil: 606 396 875
Email:mtorralba@paloaltonetworks.com

15.24 Panda Cytomic

Cytomic (Unit of Panda Security) facilitará a todos los profesionales del sector salud licencias trial sin coste de su producto Cytomic EPDR durante el tiempo en el que dure el estado de alarma en nuestro país.

Todos aquellos profesionales del sector salud que deseen obtener esta licencia pueden escribir al correo electrónico sales.hq@cytomicmodel.com, indicando en el asunto: **CyberCOVID19 Cytomic**. Teléfono de soporte técnico: 900 840 407

15.24.1 Cytomic EDPR

Cytomic EPDR integra en una única solución un paquete completo de tecnologías preventivas en el *endpoint*, con capacidades EDR y el Servicio Zero-Trust Application. Cytomic EPDR previene, detecta y responde a cualquier tipo de malware conocido y desconocido, ataques sin archivos y sin malware.

El Servicio Zero-Trust Application evita la ejecución de malware en los ordenadores, servidores, entornos virtuales y dispositivos móviles. Además, Cytomic EPDR ofrece a los equipos de seguridad:

- Visibilidad total de las acciones de los adversarios.

- Sin impacto en los dispositivos y servidores ya que el agente es ligero y su arquitectura basada en la nube

- Detección de comportamientos anómalos en el *endpoint* (IOA) bloqueando al atacante.
- Contención remota desde la consola a los *endpoints* de forma masiva, como aislar o reiniciar equipos.

Para obtener las licencias sin coste de Cytomic EPDR se debe enviar un email a sales.hq@cytomicmodel.com

En el correo electrónico se debe proporcionar el nombre de la organización y un email de contacto donde se enviará un mail de bienvenida con las instrucciones necesarias para dar de alta el usuario inicial para acceder a la consola web de Cytomic EPDR. Se puede encontrar un guía completa aquí:

https://info.cytomicmodel.com/resources/guides/EPDR/v09/es/EPDR-guia-ES.pdf

15.24.2 Contacto

Todos aquellos profesionales del sector salud que deseen obtener esta licencia pueden escribir al correo electrónico:

Email: sales.hq@cytomicmodel.com
Indicando en el asunto: CyberCOVID19 Cytomic
Teléfono de soporte técnico: 900 840 407

15.25 PROCONSI

PROCONSI quiere apoyar a las organizaciones que en estos días se están encontrando con dificultades, proporcionando los servicios que a continuación se describen.

- Consultoría de seguridad.

  Servicio gratuito que tendrá como objetivo el asesoramiento a la organización en la implantación de medidas técnicas y organizativas adecuadas.

- Consultoría para implantación de teletrabajo y uso de herramientas de comunicación.

  Asesorar gratuitamente a la organización en la implantación del teletrabajo y las herramientas de comunicación interna y de videoconferencia disponibles que permitirán que el teletrabajo sea más efectivo.

- Formación en ciberseguridad.

  El servicio gratuito que se ofrece es un curso de formación básica en ciberseguridad de cuatro (4) horas de duración, en la modalidad online, con total libertad de horarios ya que estará disponible 24x7.

- Simulación de ataque de ingeniería social y seminario de concienciación.

  El servicio gratuito que se ofrece consiste en la realización de una simulación de un ataque de ingeniería social en la organización para comprobar el grado de concienciación del personal. Tras esta simulación se ofrece un seminario online de una duración de dos (2) horas con el objetivo de comentar los resultados obtenidos.

- Copia de seguridad en la nube.

  El servicio que se ofrece es el de backup online, o copia de seguridad en la nube, durante tres (3) meses de forma gratuita.

15.25.1 Contacto

Raúl Ordás Fernández
Email: covid19@proconsi.com

15.26 Pulse Secure

Se propone la implementación de un sistema unificado de control de acceso para organizaciones que disponen de una infraestructura IT apoyada en sistemas tanto *cloud* como *on-premise* y en el que adicionalmente los usuarios (humanos, IoT y aplicaciones) se pueden conectar desde dispositivos tanto corporativos como no corporativos en un mundo *Zero Trust*.

15.26.1 Suministro de equipos y licencias

- Suministro de licenciamiento y máquinas virtuales sin coste durante el período de adquisición de sistema de cara a ofrecer cobertura al cliente.
- En el caso de adquisición de plataforma basada en hardware, cobertura de servicio en cliente mientras se hace efectivo el suministro del hardware a través de plataformas virtuales.
- Licencia disponible ICE (In Case of Emergency).

15.26.2 Unificación de control de acceso en un mundo Zero Trust

La propuesta de Pulse Secure se presenta como una solución modular unificada bajo una misma plataforma/cliente, que permite adaptar y unificar el acceso de los usuarios en un entorno híbrido cambiante.

Se plantean diversos escenarios en los que se unifican acceso remoto y NAC, en entornos on-premise/IaaS/SaaS, teniendo la posibilidad de ofrecer plataformas hardware,

virtuales, *cloud* según requerimientos de cliente, optimizando los costes, analizando el volumen de conexiones a través de usuarios concurrentes.

15.26.3 Contacto

Email: info-iberia@pulsesecure.net

Luis Miguel García Escobar - Country Manager Iberia
Móvil: 699 422 986

Rafael Cuenca Carmona - Regional Channel Manager
Móvil: 601 086 253

15.27 ReaQta

ReaQta ha puesto en marcha el programa solidario BCP Enpoint Defense Package, consistente en un paquete gratuito hasta el día 15 de julio que incluye el software necesario EDR+EPP de inteligencia artificial, así como la gestión de los servicios necesarios de detección y respuesta durante un horario de operación limitado.

Dicho programa está dirigido fundamentalmente al sector sanitario y de administraciones públicas, que es el que mayor estrés está sufriendo en el momento actual de la pandemia de Covid-19, y a actividades esenciales en situación de teletrabajo.

Reaqta-Hive es una solución de protección de punto final que ofrece una visibilidad completa sobre la infraestructura, permitiendo consultas en tiempo real a los puntos finales, búsquedas extendidas e indicadores de comportamiento, junto con la extracción avanzada de datos para el descubrimiento de amenazas latentes.

Dos grupos diferentes de motores aplican el aprendizaje automático de última generación a los comportamientos de las aplicaciones, alertando automáticamente sobre amenazas activas o emergentes sin necesidad de un conocimiento previo de los ataques. Este enfoque sin firma, combinado con un análisis de comportamiento impulsado por inteligencia artificial asegura que las amenazas se detectan independientemente

15.27.1 Contacto

Raúl Fernández Santos
Móvil: 629792368
Email: raul@proyectoalbedo.com

15.28 S2 Grupo

Con limitación a organizaciones especialmente críticas durante esta situación (hospitales, FAS, FCSE, alimentación, …).

15.28.1 Servicios de concienciación

- Webinars para los teletrabajadores (periódicos en función de demanda) para garantizar la seguridad de las redes corporativas.
- Webinars para los teletrabajadores con recomendaciones para la ciberseguridad doméstica.
- Webinars de compras online seguras.
- Acceso online a material de concienciación (vídeos, infografías…) sobre trabajo remoto seguro.

15.28.2 Servicios de análisis

Escaneo de vulnerabilidades sobre los servicios de acceso remoto, con informe de recomendaciones urgentes.

15.28.3 Servicios de gestión de incidentes

- Soporte remoto a incidentes (IT y OT).
- En casos especiales, gestión de incidentes integral.

15.28.4 Servicios de vigilancia

- Suministro de agentes específicos para la detección de Trickbot.
- Monitorización de eventos de seguridad de equipos finales para la detección de amenazas mediante agentes específicos.
- En casos especiales, cesión temporal de un *appliance* de CARMEN con la posibilidad de desplegar agentes de *endpoint* de CLAUDIA.

15.28.5 Servicios de despliegue

- En casos de organizaciones que no dispongan de accesos VPN, instalación de un servidor OpenVPN y formación para su uso seguro.
- Asistencia al despliegue de un kit de herramientas gratuitas verificadas para la protección de dispositivos personales.

15.28.6 Servicios de información

Suscripción gratuita a servicios de lab52: alerta temprana, informes de inteligencia, inteligencia táctica (reglas, analizadores, IOC…).

15.28.7 Contacto

Email: covid19@s2grupo.es

15.29 S21Sec

En relación a la Crisis del Coronavirus, S21Sec pone disposición del sector público dos (2) tipos de iniciativas:

- Para los organismos sanitarios (Hospitales, Consejerías, Ministerios) relacionados con la gestión de la pandemia, una serie de medidas orientadas a proteger a nuestros profesionales sanitarios e instituciones y que puedan centrar sus recursos en la lucha contra la pandemia.
- Para los organismos públicos en general, una iniciativa de implantación y gestión de EDR ya que, con la introducción del acceso remoto y la utilización de puestos corporativos en redes domésticas se reduce el nuevo perímetro al *endpoint*.

Para todos aquellos clientes finales, instituciones y Organismos, públicos o privados, ofrecemos la suscripción a nuestro servicio de inteligencia "Cyberthreat Alerts", con información puntual sobre ciberamenazas de manera gratuita hasta el 30 de abril.

15.29.1 Soporte a Organismos y Profesionales Sanitarios

S21sec considera imprescindible garantizar que todos los organismos sanitarios, públicos o privados, se encuentran protegidos frente a cualquier amenaza de seguridad.

Por ello, pone a su disposición, de manera gratuita durante el estado de alerta, las siguientes iniciativas:

- Equipo de Respuesta ante Incidentes de Seguridad (DFIR), que asistirá a cualquier institución que pueda verse involucrada en un ataque grave de ciberseguridad, hasta el límite que imponga nuestra propia capacidad de atender la demanda.

  La activación de este servicio se realizará a través de la dirección de correo electrónico: covid19@s21sec.com (con asunto del correo [DFIR]) o a través del teléfono de nuestro SOC: 902 020 222, indicando que se trata de una solicitud de DFIR de una entidad del sector sanitario.

- La asistencia a cualquier profesional del sector Sanitario en materia de ciberseguridad, en su ámbito personal o profesional, que podrá ejercer a través de la dirección de correo electrónico: covid19@s21sec.com, donde distintos profesionales de S21Sec les podrán elaborar una respuesta y apoyarles para que puedan dedicar su tiempo a lo que a todos más nos importa, que es la lucha y contención del COVID-19.

15.29.2 Protección Avanzada del Endpoint (EDR)

Para aquellas instituciones que lo requieran, S21Sec puede colaborar en el despliegue, monitorización, gestión y enriquecimiento de las soluciones comerciales de EDR disponibles en el mercado español, con el objetivo de proporcionar un despliegue efectivo y sin necesidad de intervención *on-premise* para aquellos dispositivos que ya se encuentran fuera del perímetro de la organización.

S21Sec tiene acuerdos con varias de estas entidades (FireEye, Panda, Cybereason) para poder realizar un despliegue rápido y efectivo en los *endpoints* distribuidos. El EDR se integra después en la monitorización 7x24 desde nuestro SOC, enriquecido mediante los indicadores del fabricante y con los indicadores propios de S21Sec.

15.29.3 Suscripción sin coste a servicio de Indicadores de Amenazas (IOC)

Con el objetivo de minimizar el posible impacto de las ciberamenazas surgidas al calor del COVID-19, S21Sec ofrece un servicio de remisión de indicadores de compromiso, de manera gratuita, hasta el 30 de abril.

El servicio consiste el envío diario de un grupo de indicadores de amenazas, con indicadores que pueden ser utilizados en la protección y detección frente a las mismas, y permita que las organizaciones puedan anticiparse a los ataques que se están empleando en este momento.

Para poder activar el servicio, deben registrarse en la siguiente dirección:

https://www.s21sec.com/es/indicadores-de-ciberamenazas/

15.29.4 Contacto

Jorge Hurtado CSMO Grupo S21Sec
Email: covid19@s21sec.com

Para más información, ver la página: https://www.s21sec.com/es/coronavirus/

15.30 SealPath

En esta situación excepcional marcada por la crisis del COVID-19, SealPath podría dar respuesta a los riesgos de seguridad que se pueden plantear en estos momentos y un modelo de licencias y servicios ayudando, de esta manera, a Entidades y a Empresas Españolas en la protección y control de su información en situación de teletrabajo.

15.30.1 Protección Dinámica y Control Remoto de Datos

Herramientas como SealPath de Protección y Control de la Información permiten tener los datos cifrados, aunque se encuentren en un equipo remoto, controlar los

permisos de acceso (sólo ver, editar, copiar y pegar, etc.) y auditar los accesos a la información. No sólo eso, permite revocar el acceso a determinada información protegida en caso de que sea necesario para así evitar posibles fugas de datos.

SealPath ofrece a organizaciones del sector sanitario (Hospitales, Centros de Salud, Organismos Públicos relacionados) suscripciones gratuitas de su solución de Protección y Control de Información, durante el tiempo que dure el Estado de Alarma derivado de la pandemia de Covid-19. Estas organizaciones pueden solicitar las suscripciones en la dirección support-covid19@sealpath.com.

Adicionalmente, y para facilitar el acceso por parte del mayor número de empresas posibles en sus necesidades de teletrabajo, se han definido tres (3) paquetes cerrados, de licencias y servicios, que incluyen todo lo necesario para el despliegue de SealPath. Las empresas que se acojan a la campaña, limitada a 3 meses, tendrán unos precios especiales.

- Se ofrecerán también sin coste la posibilidad de ver y editar documentos protegidos sin agentes con SealPath Secure Browser en entornos Office 365, SharePoint, Box y Google Drive.
- Se ofrecerá de forma gratuita sesiones de formación online adicionales a las definidas en los paquetes, para que los usuarios puedan trabajar de forma segura y de la forma más rápida posible.
- Soporte especial a clientes actuales que quieran adaptar su estrategia de protección a este escenario de teletrabajo a través de la dirección support-covid19@sealpath.com

15.30.2 Contacto

Email: support-covid19@sealpath.com

15.31 Sophos

En coordinación con Centro Criptológico Nacional ponemos a disposición de **organismos públicos** nuestra tecnología más avanzada sin coste y sin ningún compromiso de compra por al menos tres (3) meses, prolongables según avancen los acontecimientos.

Dentro de un escenario de teletrabajo, donde los usuarios pueden y deben acceder desde prácticamente cualquier sitio, Sophos ofrece distintas soluciones para que se realice de la forma más segura posible.

Para ello, en el portfolio de Sophos se pueden ver diferentes productos que son gestionados desde una única plataforma, centralizada en la nube llamada Sophos Central (https://central.sophos.com). Es decir, no será necesario desplegar ninguna infraestructura *on-premise* para la administración de los productos.

15.31.1 Soporte, instalación y contacto

- Los productos descritos irán acompañados de un soporte 8x5 vía telefónico y por correo en castellano y 24x7 en inglés.
- Además, pondremos a disposición de las **AA.PP.** a nuestra red de Partners certificados para poder llevar a cabo despliegues rápidos de nuestra tecnología para aquellos organismos públicos que lo necesitaran.

15.31.2 Contacto

AGE y Madrid
Móvil: 663 364 895
Email: alvaro.fernandez@sophos.com

Resto AA.PP.
Móvil: 663 364 895
Email: inigo.stuyck@sophos.com

Técnicas
Móvil: 663 364 895
Email: Alberto.ruiz@sophos.com

15.32 Sothis

Durante el período de vigencia del estado de alerta, según lo descrito en el RD 463/2020, Sothis prestará a las empresas pertenecientes a los sectores críticos incluidos en el RD 463/2020, que no pueden permitirse especialmente en momentos como este, brechas de seguridad, los siguientes servicios sin costes de ningún tipo.

- Suscripción gratuita al servicio de alerta temprana.

  El servicio identificará las nuevas amenazas y riesgos que se detecten y comunicará, mediante un correo electrónico, la información necesaria y recomendaciones sobre las medidas de mitigación. Mediante este comunicado formal, se ayuda a los equipos de operaciones, a tomar las medidas necesarias para prevenir un ciberataque y, en el caso de que este se hubiese producido, se ayuda a contener su expansión y minimizar el impacto en el negocio.

  Dicho informe es construido por el equipo técnico de SOC Sothis ERIS-CERT®.

- Asesoramiento ante incidentes de Ciberseguridad.

  Este servicio identifica el incidente y la recomienda las medidas de contención y respuesta a tomar por parte del cliente, si procedieran. Ante la comunicación de un incidente de seguridad, Sothis asignará un interlocutor único para dar soporte

a la identificación de la amenaza y prescribir estas medidas de contención, respuesta y erradicación, según la metodología y criterio de Sothis.

Este servicio estará limitado a la capacidad de actuación del equipo de Sothis y los medios habilitados necesarios para su prestación (accesos al cliente, capacidad disponible, etc.).

Para obtener este asesoramiento, se deberá enviar un correo a security@sothis.tech con el asunto **[INCIDENTE]** o llamar al teléfono +34 902 88 35 33 de Sothis.

- Análisis de Phishing o Correos Sospechosos.

  Este servicio consiste en la comprobación del grado de seguridad de correos que sean susceptibles de riesgo para el receptor, para evitar la introducción de cualquier tipo de malware en la organización, o el robo de datos personales para suplantación.

  Este servicio estará limitado a la capacidad de actuación del equipo de Sothis y los medios habilitados necesarios para su prestación. (accesos al cliente, capacidad disponible, etc.).

  Para obtener este asesoramiento, se deberá reenviar el correo sospechoso a security@sothis.tech anteponiendo el texto **[INCIDENTE PHISHING]**.

- Asistencia de Notificación de Brechas de Seguridad.

  En caso de que la organización sufra un incidente de seguridad que afecte a datos de carácter personal, y por ende deba notificarlo a la AEPD como autoridad de control en materia de protección de datos, desde Sothis se le podrá prestar asistencia para cumplir con la notificación a la AEPD en los plazos requeridos, siguiendo un procedimiento que cumple estrictamente lo estipulado en el Reglamento General de Protección de Datos.

15.32.1 Contacto

Email: security@sothis.tech

15.33 Stormshield

Stormshield ha puesto a disposición de cualquier cliente que lo necesite firewalls (máquinas virtuales) SNS Elastic Virtual Appliance, para proteger su infraestructura y establecer conexiones VPN para conectarse a ella de forma segura, gratuitamente durante tres (3) meses con posibilidad de extensión si continúa la crisis de salud pública.

https://www.stormshield.com/products/virtual-appliances/

15.33.1 Contacto

Quien lo necesite, puede ponerse en contacto con iberia@stormshield.eu, para dimensionar correctamente el equipo necesario y generar automáticamente las licencias.

15.34 Telefónica

Con motivo de la crisis del COVID-19, y durante tres (3) meses, Telefónica a través de los servicios prestados por su SOC-CSIRT, pone a disposición tanto de Entidades Públicas como Privadas que necesiten cubrir actuaciones especiales en el estado de alarma y necesiten ayuda inminente, los siguientes servicios:

- Monitorización y Seguridad Gestionada.

  Evitar incidentes de seguridad propiciados por un uso indebido de las plataformas de acceso remoto mediante la notificación de alertas de nuestro servicio de Monitorización de Seguridad y de la gestión de nuestros expertos del SOC-CSIRT. Será necesario que la entidad proporcione los *logs* de sus plataformas de acceso remoto.

- Servicio WAF Gestionado.

  Con la limitación de estar acotado para servicios sanitarios críticos (hospitales, centros de atención médica y hoteles o centros medicalizados). Protección de hasta dos de sus aplicaciones web en Internet ante posibles ataques de indisponibilidad, malfuncionamiento, modificación del código, accesos indeseados o de sustracción de información corporativa, debidos a vulnerabilidades de seguridad existentes en el desarrollo web de las mismas.

- CSIRT.

  Apoyo de nuestro equipo de expertos de respuesta a incidentes como soporte para la resolución de incidentes críticos. Con limitación a organizaciones especialmente críticas durante esta situación (Entornos de Salud, Fuerzas y Cuerpos de Seguridad del Estado, Servicios Funerarios, Cadena de suministro critica, etc.).

- AntiDDoS.

  Desde la Red de Telefónica, detección de ataques de denegación de servicio volumétricos, de agotamiento de estados y algunos ataques de aplicación en la red de la entidad, así como la notificación del mismo. Se incluye una mitigación en caso de ataque y es necesario tener al menos una de las salidas a Internet con Telefónica. Acotado a servicios críticos del entorno de salud.

- Licencias de prueba.

  Totalmente funcionales, de productos desarrollados por TELEFONICA como Sealsign (Firma digital), FaasT (Pentesting Persistente) o Latch (Refuerzo del acceso a aplicaciones y servicios críticos mediante doble factor de autenticación, así como control de exposición de superficie de autenticación. Más información de los productos:

  https://www.elevenpaths.com/es/tecnologia/faast/index.html

  https://www.elevenpaths.com/es/tecnologia/sealsign/index.html

  https://latch.elevenpaths.com

15.34.1 Contacto

Email principal: covid19@elevenpaths.com
Email de soporte del SOC-CSIRT:dstsol.socseguridad@telefonica.com

15.35 ValoraData

ValoraData es una empresa tecnológica española especializada en continuidad de negocio. Llevamos más de 30 años de experiencia gestionando copias de seguridad y asegurando los contenidos y la información de empresas públicas y privadas.

ValoraData pone en marcha, a disposición de **organismos públicos** y mientras dure la estabilización del COVID-19, los siguientes servicios:

- Servicio gratuito de asesoramiento profesional y apoyo en las materias siguientes: gestión y políticas de copias de seguridad, utilización de herramientas de *backup*, implantación de medidas de continuidad de negocio y soluciones *Disaster Recovery*.
- Importantes descuentos en servicios de gestión de copias de seguridad (incluyendo alojamiento *cloud*, monitorización y soporte a usuarios).
- Importantes descuentos en servicios y soluciones *Disaster Recovery*.
- Servicio gratuito durante un período de 6 meses de custodia (*vaulting*) de copias de seguridad en instalaciones protegidas, incluyendo los servicios de transporte y entrega inmediata.

15.35.1 Contacto

Óscar de Eugenio - Director Comercial
Móvil: 670 414 978
Email: oeugenio@valoradata.com

15.36 WISE Security Global

La compañía Wise Security Global, mediante su solución de notificaciones certificadas MEE the Cybernotary (https://www.mee-thecybernotary.com/) abre de manera gratuita su servicio de emails certificados.

MEE the Cybernotary es la solución de notificaciones certificadas desarrollada por Wise Security Global. Desde cualquier dispositivo y a cualquier hora, certifica el envío de cualquier tipo de información con plena garantía jurídica, solidez y seguridad tecnológica, y autorizado como Tercero de Confianza por el Gobierno de España.

Mientras dure este estado de alarma, Wise Security Global pone a disposición de todos los profesionales, empresas y organismos que lo necesiten, un crédito ilimitado de emails certificados desde su solución tecnológica MEE the Cybernotary. Con ello, se podrán realizar comunicaciones o notificaciones importantes que quedarán registradas y certificadas con plena garantía y validez legal: ERTES, comunicados a plantillas, a organismos públicos, proveedores, justificantes laborales, etc.

15.36.1 Contacto

Móvil: +34 910 700 549
Email: info@wsg127.com

ANEXO A: DETALLES DE SOLUCIÓN BASADA EN NUBE

A.1 MEDIDAS ESPECÍFICAS DE LA ORGANIZACIÓN

Los equipos de acceso a los servicios corporativos disponen de las mismas medidas de seguridad que las establecidas en la Organización para el resto de sus equipos.

- **DMZ**. Esta DMZ alojará al "Conector" y dará acceso a los servicios corporativos a los que se tenga acceso en remoto.
- **PROXY en DMZ**. El acceso a internet será gestionado por un servidor proxy a través de la red corporativa, aplicando las políticas de seguridad establecidas en la Organización.
- **CONECTOR**. Despliegue del conector Citrix o VMware dentro de la Organización.

A.2 MEDIDAS ESPECÍFICAS DEL SERVICIO EN LA NUBE

- **IM (Suministrado por la Cloud)**. Siempre que sea posible, deberán utilizarse tecnologías de gestión de identidades, de cara a establecer distintos perfiles de permisos de acceso basados en las políticas de la organización.

  El control de acceso de los usuarios a los recursos y datos del sistema se hará en base a la existencia de diferentes perfiles de usuario. Como mínimo, se definirán dos (2) tipos de perfiles usuario(s) no privilegiado(s) y administrador(es) privilegiado(s).

  El control de accesos deberá permitir aplicar los siguientes criterios:

  a) Todo acceso debe estar prohibido, salvo concesión expresa.

  b) Los privilegios de cada usuario o proceso se reducirán al mínimo para cumplir con sus obligaciones (principio de mínimo privilegio).

  c) Cada usuario quedará identificado singularmente.

  d) La utilización de los recursos deberá estar protegida.

  e) La identidad del usuario deberá quedar previamente autenticada.

  f) Exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por el Organismo.

  g) Deberá implementar mecanismos de autenticación fuerte (doble factor) basada en certificados para acceder al servicio.

- **Notificación y respuesta ante incidentes**. Los proveedores conectados al Organismo deben reportar todos los incidentes de seguridad detectados en sus

instalaciones que afecten a los equipos prestadores de servicios al propio Organismo, añadiendo información de los mecanismos de solución y mitigación de los incidentes detectados.

A.3 MEDIDAS ESPECÍFICAS DEL CANAL

En esta arquitectura se establecerán dos canales (2) seguros:

- **Canal Organismo-proveedor de servicio en la nube**. Deberán establecerse canales cifrados mediante la utilización de redes privadas virtuales (VPN). Estas VPN deberán ser establecidas extremo a extremo entre el terminador de túneles del Organismo y el servicio en la nube. Para el establecimiento de dichas VPN se utilizarán protocolos seguros como IPSec o TLS 1.2 o superior.

  Proveerán autenticación fuerte extremo a extremo, basada en la utilización de certificados digitales, protección de la integridad y, en el caso de que se maneje información sensible, protección de la confidencialidad.

- **Canal Proveedor de servicio en la nube-endpoint**. El proveedor se encargará de dar acceso VPN mediante su tecnología y mecanismo de validación a sus usuarios. En este caso, serán canales https/TLS 1.2 o superior, al que serán de aplicación las indicaciones expuestas en el caso anterior.

ANEXO B: DETALLES SOLUCIÓN BASADA EN SISTEMAS ON-PREMISE

B.1 MEDIDAS ESPECÍFICAS DEL SERVICIO

El cumplimiento de estas medidas no garantiza la confiabilidad completa en el equipo remoto, pero permitirá reducir la superficie de ataque y mitigar amenazas derivadas del acceso remoto.

- **DMZ**. Todos los servicios a los que se tenga acceso en remoto deberán encontrarse en una DMZ. En esta DMZ se dispondrá de un proxy que controle el acceso a internet.
- **NAC**. Siempre que sea posible, deberán utilizarse tecnologías de control de acceso, de cara a establecer distintos perfiles de permisos de acceso basados en las políticas de la organización.

  Se establecerán elementos de seguridad que dictaminen en estado de salud del equipo cliente (estado del antivirus, conectividades y monitorización de usos y accesos, etc.).

  El control de acceso de los usuarios a los recursos y datos del sistema se hará en base a la existencia de diferentes perfiles de usuario. Como mínimo, se definirán dos (2) tipos de perfiles usuario(s) no privilegiado(s) y administrador(es) privilegiado(s).

  El control de accesos deberá permitir aplicar los siguientes criterios:

  a) Todo acceso debe estar prohibido, salvo concesión expresa.

  b) Los privilegios de cada usuario o proceso se reducirán al mínimo para cumplir con sus obligaciones (principio de mínimo privilegio).

  c) Cada usuario quedará identificado singularmente.

  d) La utilización de los recursos deberá estar protegida.

  e) La identidad del usuario deberá quedar previamente autenticada.

  f) Exclusivamente los administradores del sistema, podrán conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por el Organismo.

B.2 MEDIDAS ESPECÍFICAS DEL CANAL

Deberán establecerse canales cifrados mediante la utilización de redes privadas virtuales (VPN). Estas VPN deberán ser establecidas extremo a extremo entre el terminador de túneles del Organismo y el *endpoint*.

Para el establecimiento de dichas VPN se utilizarán protocolos seguros como IPSec o TLS 1.2 o superior. Proveerán autenticación extremo a extremo, basada en la utilización de certificados digitales, protección de la integridad y, en el caso de que se maneje información sensible, protección de la confidencialidad.

B.3 MEDIDAS ESPECÍFICAS DEL ENDPOINT

Por regla general, salvo causa justificada, deberán utilizarse:

a) **Herramientas EPP:** en cualquier tipo de sistema.

b) **Herramientas EDR:** se recomienda para los sistemas que manejen información sensible.

Estas herramientas deberán actualizarse con una periodicidad establecida por la política de seguridad del Organismo y que dependerá del nivel de seguridad exigido por la información que vaya a manejar.

El *endpoint* deberá contar con las medidas de seguridad establecidas por defecto para cualquier *endpoint* del organismo y, específicamente, deberán tenerse en cuenta las siguientes medidas adicionales.

- **Medidas HW**.
  - BIOS protegida con contraseña fuerte y configurada de acuerdo al principio de mínima funcionalidad.
  - Si son portátiles, dotados de filtros de privacidad (pantallas).
- **Medidas del sistema operativo**.
  - Autenticación fuerte y mediante directorio activo del Organismo. En caso de que se vaya a manejar información sensible se recomienda doble factor de autenticación.

    Se bloqueará el equipo tras intentos fallidos de autenticación consecutivos o después de un período de inactividad, de cara a evitar accesos no autorizados.
  - Sistema operativo con soporte y parches de seguridad actualizados.
  - Únicamente se podrá administrar el sistema desde un usuario administrador.
  - Se implementará una configuración que restrinja y controle la ejecución de software de acuerdo a las políticas de la Organización.
- **Herramientas de seguridad**.
  - Se instalarán herramientas antimalware. El software de detección de código dañino deberá configurarse para:

a) Analizar todo fichero procedente de fuentes externas antes de trabajar con él.

b) Revisar el sistema cada vez que arranque y realizar escaneos regulares para detectar software malicioso.

c) Actualizar periódicamente las firmas.

d) Implementar protección en tiempo real de acuerdo a las recomendaciones del fabricante.

- **Cortafuegos personal**.

  Se utilizará un cortafuegos personal que permita únicamente los flujos de comunicación autorizados conforme a las políticas del organismo y rechace el resto. En particular, mediante este cortafuegos se evitará que el equipo se conecte a otras redes no corporativas.

- **HIPS**.

  Para sistemas que manejen información de nivel alto de seguridad, se empleará un sistema para la prevención de intrusiones (HIPS) con el fin de detectar y bloquear en tiempo real cualquier intento de intrusión en éste.

  El conjunto de reglas predefinidas y patrones de firma utilizados para detectar posibles ataques deberán ser personalizados y actualizados periódicamente conforme a la Política de Seguridad del Organismo.

- **Gestión de eventos**.

  Se utilizarán mecanismos para el registro de logs y eventos de seguridad generados por el sistema y/o los usuarios, que puedan ser almacenados y retenidos durante el período que establezca la Política de Seguridad establecida en el Organismo. La modificación de la referencia de tiempo será una función del administrador.

- **Cifrado de datos**.

  Se deberán aplicar mecanismos criptográficos para la protección de la confidencialidad e integridad de la información de los sistemas que almacenen información sensible. Concretamente, estos mecanismos serán:

  – Cifrado off line: para la protección de la información sensible que vaya a ser enviada por o almacenada en un medio inseguro.

  – Cifrado *at rest* o cifrado de la información almacenada. Deberá utilizarse siempre que la solución de *endpoint* sea móvil o portátil para sistemas que guarden información sensible.

- **Prevención de Fuga de Datos (DLP)**.

  Siempre que sea posible, para sistemas que manejen información sensible, se aplicarán mecanismos que permitan controlar la salida de información desde el sistema.

- **Borrado seguro**.

  Todos aquellos archivos que contengan información sensible deberán ser borrados de manera segura cuando finalice su uso utilizando una herramienta de borrado seguro para el tipo de soporte en donde se encuentre almacenada.

  El mecanismo de borrado seguro utilizado podrá consistir en una o varias pasadas de sobrescritura o el cifrado de la información.

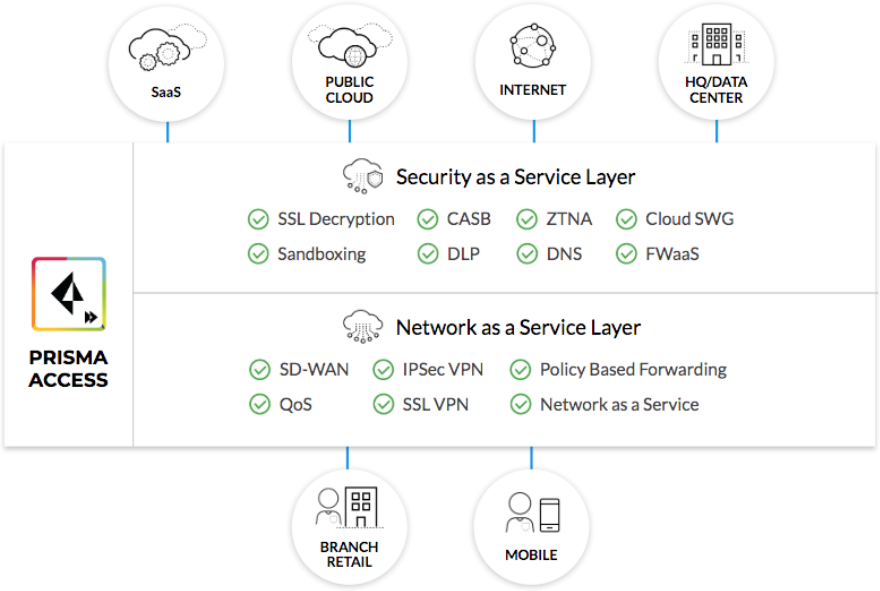
ANEXO C: DETALLES SOLUCIÓN CONEXIÓN REMOTA

Una solución alternativa a lo ya indicado la ofrece Palo Alto Networks con Prisma Access en la cual no es necesario desplegar servidores VDI ni MSTC y tiene la ventaja de poder cursar de una manera segura el tráfico hacía internet (ya sea nube pública, software como servicio o navegación directa) sin tener que concentrar todo el tráfico en el centro de datos de la organización o los equipos de la organización, evitando así la degradación en la experiencia de usuario generado por el *delay* y la posible sobrecarga de los enlaces que lo conectan con el proveedor de servicio.

Prisma Access es una solución SASE (Security Access Service Edge) que ofrece servicios de seguridad coherentes y acceso a las aplicaciones en la nube (ya sea nube pública, privada o software como servicio), entregados a través de un marco común para garantizar una experiencia de usuario impecable.

Prisma Access brinda protección completa a través de nuestras soluciones NGFW en la nube con varios objetivos:

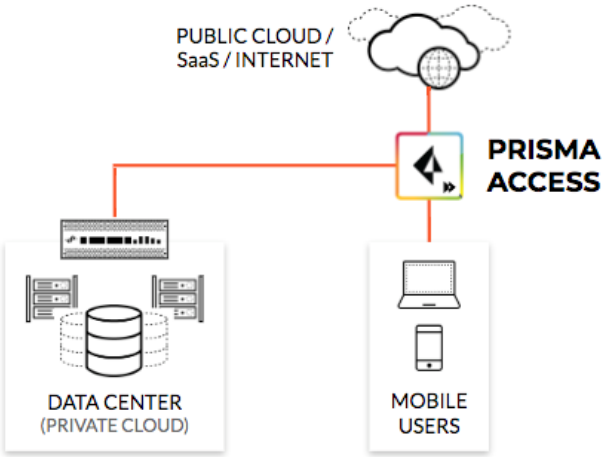
- Proporcionar conectividad a todos los empleados que teletrabajan para acceder a diferentes recursos donde sea que estén (DC, internet, SaaS).
- Permitir la verificación de la identidad del usuario, así como el estado de la estación de trabajo que desea acceder a los recursos (postura de seguridad).
- Proteger contra cualquier tipo de amenaza, conocida o desconocida, pero también el acceso a dominios maliciosos.
- Extender y fortalecer la solución de seguridad ya existente en las redes *on-premise*, que seguramente no es lo suficientemente grande, para acomodar todas las conexiones que surgen de los usuarios que ahora teletrabajan.



Los usuarios itinerantes necesitan una seguridad coherente para acceder a las aplicaciones del centro de datos y a las alojadas en la nube. El acceso remoto mediante redes privadas virtuales (VPN) resulta insuficiente, ya que los usuarios suelen conectarse a una puerta de enlace para acceder a las aplicaciones del centro de datos, pero luego se desconectan de la VPN cuando acceden a aplicaciones web o alojadas en la nube, anteponiendo el rendimiento a la seguridad.

Prisma Access «aproxima» la protección a sus usuarios, de modo que el tráfico llegue a la nube sin necesidad de pasar previamente por la sede central de la organización mediante una conexión de red de retorno. Funciona junto con la aplicación GlobalProtect™ en el teléfono inteligente, la tableta o el portátil de un usuario.

La aplicación crea automáticamente un túnel VPN IPsec/SSL que conecta con Prisma Access. De este modo, se garantiza la aplicación de la política de seguridad sin tener que desviar el tráfico a la sede central mediante una conexión de red de retorno. Con Prisma Access, todos los usuarios tienen acceso rápido y seguro a cualquier aplicación, ya esté en la nube, en internet o en su centro de datos.



En determinadas situaciones, es posible que un gran número de usuarios tenga que trasladarse a otro sitio, ya que las conferencias, el clima y los desastres naturales pueden afectar a la infraestructura local. Prisma Access supervisa la situación en todo momento y da más capacidad a las regiones que lo necesitan de forma automática.

C.1 MEDIDAS ESPECÍFICAS EN EL CLIENTE

En el caso de la solución Prisma Access de Palo Alto Networks, el cliente debe usar la aplicación de GlobalProtect (disponible para Windows, MacOS, Linux y dispositivos móviles), la cual soporta múltiples métodos de autenticación como credenciales locales, integración con directorios corporativos (Active Directory/RADIUS), certificados digitales de cliente, complementados con múltiples factores de autenticación.

Esta aplicación permite establecer políticas de acceso basadas en el perfil de información de host (HIP, por sus siglas en inglés). Las políticas de seguridad creadas de esta manera son aún más detalladas y, cuando se accede a aplicaciones que requieren una atención especial, tienen en cuenta las características del dispositivo (p. ej., su sistema operativo, las revisiones aplicadas, parches del sistema operativo instalados o si tiene instalado un determinado programa).

En el caso de la solución Prisma Access de Palo Alto Networks, el canal de comunicaciones se divide en tres (3) partes:

- Canal de comunicaciones entre el usuario final (aplicación GlobalProtect) y Prisma Access): configurado de manera segura con IPSEC (o SSL en el caso de que el usuario no tenga conectividad IPSec). El tráfico accede a Prisma Access y es inspeccionado por un NGFW virtual en el cual se puede implementar la misma política de seguridad que la organización tenga en su centro de datos.
- Canal de comunicaciones entre Prisma Access y el centro de datos de la organización: configurado de manera segura con IPSEC. Este canal transporta únicamente el tráfico que va dirigido a los servicios alojados en el centro de datos de la organización.
- Canal de comunicaciones entre Prisma Access e internet: estas comunicaciones se cursan directamente desde Prisma Access sin tener que pasar por el centro de datos corporativo de forma que evitan el retardo, mejoran la experiencia de usuario sin impactar en la seguridad de las comunicaciones.