CCN-CERT BP/18

Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia

Marzo 2020

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de Edición: marzo 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:

- Medidas de Seguridad para acceso remoto
- Ciberconsejos: CiberCOVID19; medidas de prevención de incidentes
- CCN-CERT IA-03/20 Informe Anual 2019. Dispositivos y Comunicaciones Móviles
- CCN-CERT IA-76/19 Medidas de actuación frente al código dañino EMOTET
- 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.

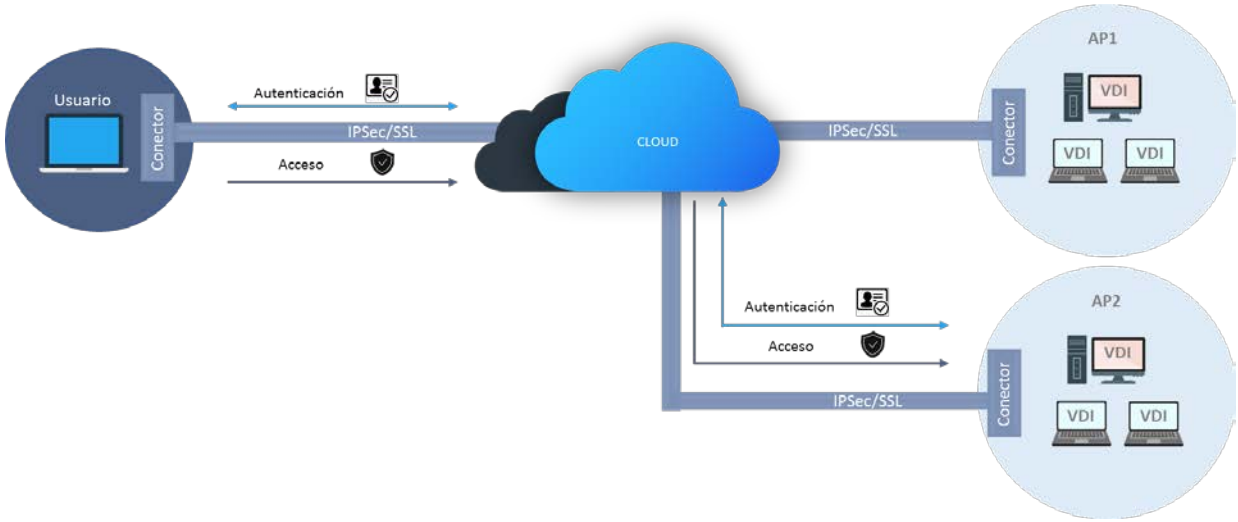


Fig. 1 Esquema de la arquitectura desplegada en una solución de acceso remoto seguro en la nube

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

Las soluciones tipo "VMware Workspace ONE", "Horizon Cloud" y "Citrix Cloud Services" proporcionan acceso a los equipos físicos de la organización manteniendo el máximo nivel de seguridad, pero permitiendo un ahorro de costes considerables ya que no se requiere infraestructura para el despliegue de escritorios virtuales (VDI).

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.

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.

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.

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

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.

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*), para el cifrado de los correos y así mantener la confidencialidad y no repudio.

5. 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.

5.1 Equipos terminales

5.1.1 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 securizado 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).

5.1.2 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.

5.2 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.

5.2.1 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]

5.2.2 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.

5.2.3 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*.

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

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.
- 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.

6. 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.

6.1 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.

6.2 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.

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.3 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.

6.4 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.

6.5 *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.

6.5.1 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.

6.5.2 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.

6.5.3 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.

6.5.4 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.

6.5.5 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.

6.5.6 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.

6.5.7 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.

6.6 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.

7. 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, sistemas de core, 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.

7.1 VULNERABILIDADES CONOCIDAS

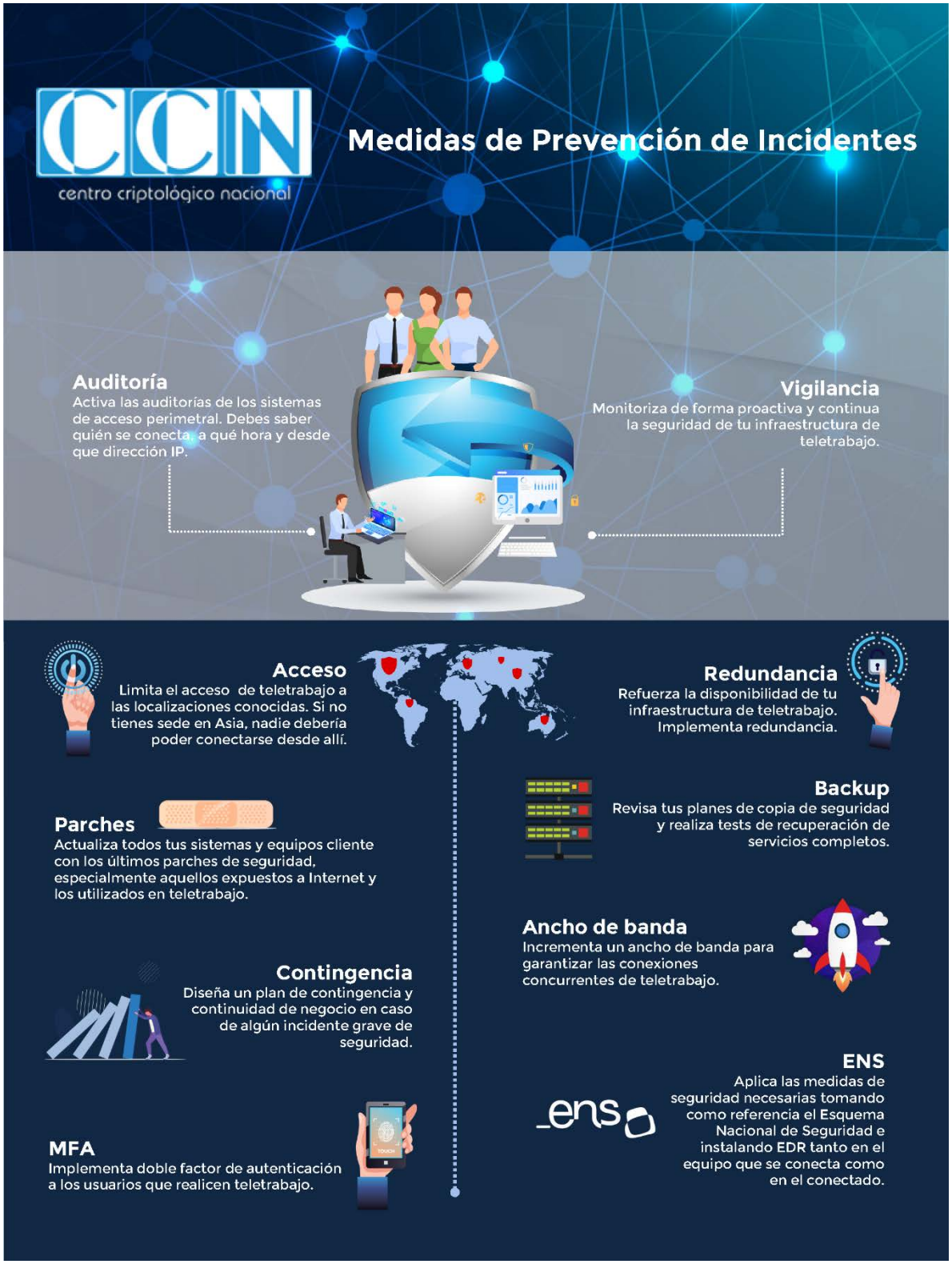
A la hora de redactar el presente documento, Microsoft ha publicado un aviso de vulnerabilidad en el protocolo SAMBA, en su versión 3. En este sentido, se ha dado a conocer un posible escaneo con NMAP:

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.

8. BUENAS PRÁCTICAS PARA PREVENIR INCIDENTES



9. 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
CISCO	- Acceso remoto seguro - DNS Seguro
Citrix / Sidertia	- Consultoría - Acceso remoto seguro
CSA	- Consultoría - Acceso remoto seguro - DNS Seguro
Entelgy Innotec Security	- Consultoría - Acceso remoto seguro
EMMA (Partners Certificados)	- Acceso remoto seguro
Eset	- Antivirus - Endpoint
Fortinet	- Acceso remoto seguro
ICA Sistemas y Seguridad	- Servicios gestionados de seguridad - Despliegue e Integración de infraestructura de seguridad - Consultoría
Ingenia	- Implantación soluciones acceso remoto y contingencia (seguridad y colaboración) - Monitorización de la seguridad - Consultoría de seguridad
McAfee	- Antivirus - Endpoint
Microsoft	- Consultoría - Acceso remoto - SIEM - Herramientas colaborativas
Mnemo	- Consultoría

[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.

Panda-Cytomic	- Antivirus - EndPoint
S2 Grupo	- Consultoría - SIEM
Sophos	- Antivirus - Endpoint

9.1 Cisco

9.1.1 Suministro de equipos y licencias

- Hasta 4 meses de Cisco WebEx para clientes de **Defensa, Inteligencia y Seguridad Nacional**, extensible, bajo petición a otras **AAPP**.
- 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.

9.2 Citrix/Sidertia

9.2.1 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.

9.2.2 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, Exchange y Azure para disponer de mecanismos de análisis en caso de afección por ciberataques.

9.2.3 Contacto

Jerónimo García Parra – Director Sidertia Solutions
Móvil: 646 116 305
Teléfono fijo: 91 400 64 47
Email: jgarcia@sidertia.com

9.3 CSA

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

9.3.1 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 **AAPP**.
- 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.

9.3.2 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, Checkpoint, PaloAlto, 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.

9.3.3 Contacto

La dirección para activar cualquiera de estos servicios es: covid-19@csa.es

9.4 Entelgy Innotec Security

9.4.1 Servicios

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).

9.4.2 Contacto

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

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

9.5 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).

9.5.1 EMMA: Vigilancia en Accesos Remotos

El firewall incluido en este módulo de EMMA, realiza de *frontend* 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.

9.5.1.1 EMMA: 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 el modelo de ROCÍO e integración con ANA (ambas soluciones del CCN) para incorporar y centralizar la evaluación de las mismas 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 de todo lo conectado a la red desde dentro (usuarios internos, externos, IoT, …), desde fuera (teletrabajo, proveedores de servicios) e infraestructura, además de trazabilidad sobre lo indicado.
- 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.

9.5.2 Soporte, instalación y contacto

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).

9.5.3 Contacto

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

9.6 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.

9.6.1 Contacto

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

9.7 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

Si se necesita soporte, la manera de contactar se explica en esta entrada:

https://fortixpert.blogspot.com/2014/04/abrir-casos-de-soporte.html

9.8 ICA Sistemas y Seguridad

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

9.8.1 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.

9.8.2 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.

9.8.3 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.

9.8.4 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.

9.8.5 Contacto

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

9.9 Ingenia

Ingenia puede proporcionar a las **AAPP** los siguientes servicios.

9.9.1 Implantación soluciones acceso remoto

Ingenia trabaja con los principales fabricantes del mercado (Fortinet, Palo Alto, Checkpoint, 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.

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

9.9.3 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

9.9.4 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 el teletrabajo sea ocasional o permanente), realización de planes de contingencia y recuperación antes desastres, planes de continuidad del negocio, etc.

9.9.5 Contacto

La siguiente dirección de correo electrónico: preventaisos@ingenia

9.10 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).

9.10.1 Contacto

Ángel Ortiz – Regional Director Spain
Móvil: 620.188.497
Fijo: 91 3478524
Email: angel_ortiz@mcafee.com

9.11 Microsoft

9.11.1 Visión general Recursos 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/

9.11.2 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		

9.11.2.1 Contacto

Oscar Sanz
Email: oscarsan@microsoft.com

9.12 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 COVID19.
- 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 COVID19.
- 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 COVID19.
- Apoyo en la detección e información sobre posibles estrategias y amenazas de phishing producidas durante la crisis.

9.12.1 Contacto

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

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

9.13 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**

9.13.1 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* (IOAs) 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

9.13.2 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

9.14 S2 Grupo

S2 puede colaborar con los **organismos públicos** mediante las siguientes acciones:

- Apoyo a servicios esenciales en el ámbito de crisis tipo COVID-19 (hospitales, FCSE, FAS...)
- Acceso online gratuito a material de concienciación (videos, infografías, ...), en especial en lo relativo a trabajo remoto seguro.
- Atención a consultas vía correo electrónico (covid19@s2grupo.es) en relación a criterios de ciberseguridad, incidentes, controles ante *ransomware*, etc.

9.14.1 Contacto

Antonio Villalón – Director de Seguridad S2 Grupo
Teléfono: 902 887 788
Email: antonio.villalon@s2grupo.es

9.15 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.

9.15.1 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 AAPP a nuestra red de Partners certificados para poder llevar a cabo despliegues rápidos de nuestra tecnología para aquellos organismos públicos que lo necesitaran.

9.15.2 Contacto

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

Resto AAPP
Email: inigo.stuyk@sophos.com
663 364 895

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

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-end point**. 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 *end point*.

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 END POINT

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 sobreescritura o el cifrado de la información.