Medidas de seguridad para acceso remoto

Abstract: en la actualidad, existen múltiples campañas de *ransomware* activas y dado que las conexiones remotas pueden ser una vía de entrada de código dañino a los sistemas, se considera clave poder garantizar la seguridad de estas conexiones y accesos.

Contenido:

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

El presente documento proporciona al Sector Público una serie de soluciones que permiten implementar, de forma ágil, acceso remoto a los recursos de una Organización minimizando el impacto en los recursos IT y optimizando el tiempo para su puesta en producción.

El proceso, tipología y componentes utilizados en un despliegue específico de una organización dependerá de una serie de factores, entre los que se incluyen:

- Perfil de riesgo de la organización.
- Aspectos financieros.
- Legislación aplicable.
- Capacidad técnica de la organización.
- Arquitectura admitida por las capacidades técnicas de la organización.
- Modelos de propiedad permitidos en la organización (**COBO, COPE, BYOD**).

Cada organización es responsable de conocer y evaluar los factores que le son de aplicación previamente al diseño o replanteo del sistema, la reserva de recursos y la selección de componentes a incluir.

La organización que realiza el despliegue debe realizar un análisis del nivel de seguridad requerido para la información que se va a manejar en los puestos de trabajo remotos o móviles

de la Organización, según la legislación vigente, antes de realizar el diseño del sistema o reservar recursos para su puesta en marcha.

En los anexos del presente documento, se incluyen una serie de medidas que deberán tenerse en cuenta en la implantación de dichas soluciones para que el sistema ofrezca unas mínimas garantías de seguridad.

3. SOLUCIONES TÉCNICAS

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, organizaciones 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 un sistema de acceso remoto seguro en función de las capacidades de la organización.

3.1 SOLUCIÓN BASADA EN NUBE

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

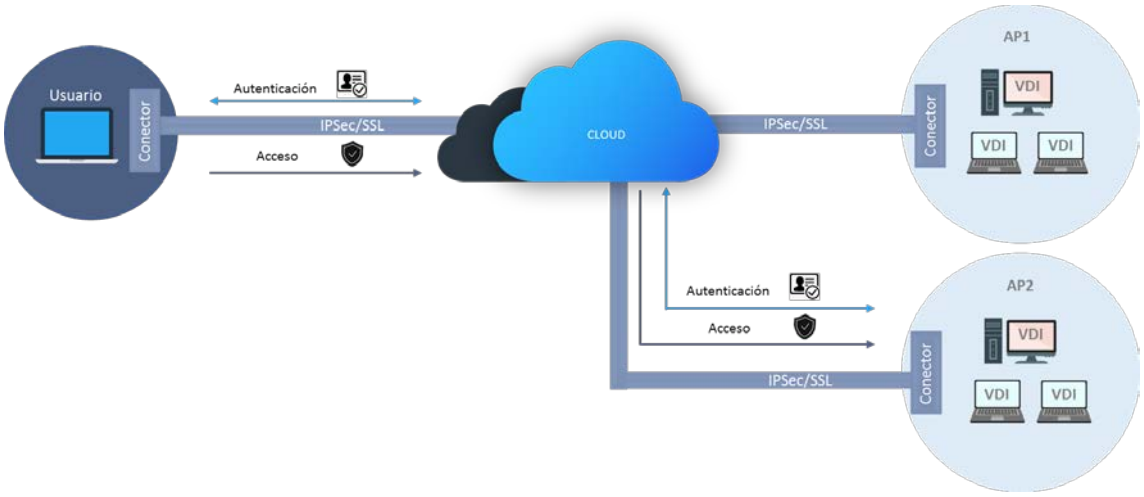
La solución consiste en desplegar una solución de servicio en la nube como las ofrecidas por VMware: “Workspace ONE” y “Horizon Cloud” o “Citrix Cloud Services” en modalidad de pago por uso que permita proporcionar temporalmente acceso a la organización desde cualquier lugar con las medidas de seguridad necesarias al tipo de información manejada. Esta solución proporciona una solución de acceso seguro con doble factor de autenticación y trazabilidad total de las conexiones realizadas por los usuarios remotos.

Se basa 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 a los sistemas corporativos.

Las características principales de este sistema son:

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 (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 componente "Conector" consiste en 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 de la organización 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 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) **[INSEGURO] Acceso directo a los propios equipos de los usuarios:** este tipo de alternativas se desaconseja de forma expresa, ya que suponen un alto riesgo de infección por código dañino o *ransomware*, ya que la publicación de puertos de "Escritorio Remoto" o SSH suponen 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 direcciones IP 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 para acceder de forma segura a los servicios corporativos.

Permitir este nivel de acceso a la organización implica el despliegue de múltiples mecanismos de seguridad que garanticen que todos los elementos TIC involucrados cumplen los estándares de seguridad necesarios para limitar el riesgo de exposición de los sistemas.

Las características principales de este sistema 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

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

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 un equipo informático 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 de acceso 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 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.

4. CORREOS ELECTRÓNICOS

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 correos electrónicos antes de ser entregados a los usuarios.

En este caso, pueden aumentarse las probabilidades de ser víctimas de ataques al poder tener implementadas medidas menos seguras en los ordenadores remotos y que en la organización se detectarían y tratarían al tener controlado el perímetro de seguridad, aspecto que en los equipos remotos no se puede garantizar.

Es importante controlar los motores de antivirus e inspección de 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 ya no se puede 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. SALAS DE REUNIONES VIRTUALES

Si se plantea un escenario en el que los usuarios puedan acceder a salas de reuniones/conferencias de forma virtual o telemática desde equipos informáticos no gestionados por la organización a través de Internet, se debería revisar la seguridad o haberse aplicado los parches de seguridad correspondientes.

Además, se debe tener un listado de servicios acordados para mantener reuniones de forma virtual, conocer las licencias de las que se disponen o si se van a utilizar herramientas gratuitas.

En todos los casos conviene tener controlados los accesos a la red y sistemas del organismo, además de tener la posibilidad en los dispositivos perimetrales de habilitar reglas con fecha y hora de inicio y finalización.

Cuando se inicien reuniones por medio de estos canales, se debe revisar que los asistentes son los invitados y no se tienen duplicados, personas no invitadas o desconocidas en la reunión.

Se debe revisar si la reunión es grabada, que quede registro de las personas conectadas, donde se almacena y que personas pueden grabar la reunión dentro de la misma.

6. PROCEDIMIENTOS DE ACTUACIÓN DE LAS PERSONAS O EQUIPOS CON ACCESO REMOTO

Se recomienda disponer, de forma diaria, los portátiles o equipos para acceder remotamente a los organismos por si se activa algún protocolo de actividad extraordinaria fuera de la oficina.

En estas situaciones conviene realizar pruebas de conectividad de los diferentes usuarios que pudieran utilizar el acceso remoto comprobando su funcionalidad y registrando las direcciones IP de acceso remoto, credenciales y accesos disponibles mediante la conexión remota.

Si para tener acceso remoto se debe dejar el equipo del organismo encendido, asegurarse de las siguientes medidas:

- Tener actualizado el puesto de trabajo con los últimos parches de seguridad (Sistema operativo, herramientas de seguridad, aplicaciones, etc.).
- Cerrar todas las conexiones que no sean estrictamente necesarias.
- Cerrar todas las aplicaciones cuando no se estén utilizando.
- Realizar análisis programado de los antivirus (exhaustivos) a los puestos de trabajo, aunque los ordenadores no se reinicien.
- Aplicar las actualizaciones programadas en la Organización, para ello puede ser necesario apagar y encender los equipos de forma periódica.
- Prever mecanismos que permitan el reinicio de estas máquinas de forma remota y acceder por canales establecidos a las mismas desde fuera de la organización una vez se reiniciara el equipo.

Se recomienda tener un listado de las direcciones IP de los posibles orígenes remotos de las conexiones.

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 activados servicios de monitorización con alertas definidas.
- 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.

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. DEFINICIONES

BYOD *Bring Your Own Device.* En un escenario BYOD, el usuario final es propietario del dispositivo (teléfono móvil, Tablet, portátil), donde el Administrador IT de la organización genera un Workspace, también llamado contenedor o Perfil de Trabajo (WorkProfile), dentro del cual exclusivamente administra políticas y restricciones de seguridad, a través de una aplicación agente dentro del Workspace, mediante una aplicación especial agente (*Profile Owner*).

COPE *Corporate Owned Personal Enabled*. En los escenarios COBO y COPE el dispositivo (teléfono móvil, Tablet, portátil) es propiedad de la organización, y el Administrador IT tiene acceso a control total del dispositivo, implementando políticas de seguridad y restricciones. En el escenario COPE, existe una aplicación agente en el área personal, denominada DO (*Device Owner*), que realizará la configuración de políticas en el conjunto del dispositivo, como por ejemplo WiFi, además de restricciones en el área personal del usuario, normalmente restricciones mínimas y básicas de seguridad. Al ser un escenario COPE, existirá también un Workspace, con su agente gestor denominado (*Profile Owner*) dentro de él. El Administrador IT de la organización, realizará una configuración de seguridad más estricta en Workspace/Contenedor, que complementará la configuración básica del área personal del usuario.

COBO *Corporate Owned Business Only*. El escenario COBO, se utiliza en despliegues que requieren mayor seguridad, donde el usuario final no dispone de área personal, ya que el conjunto del dispositivo está fuertemente restringido. En un escenario COBO, solamente existe un agente DO, y ningún Workspace/Contenedor es creado.

ANEXO A: DETALLES DE SOLUCIÓN BASADA EN NUBE

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.

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.

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 LOCALES (ON-PREMISE)

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.

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.

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 sobrescritura o el cifrado de la información.