Seguridad en la instalación y uso de dispositivos IoT:

Una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

El término Internet de las Cosas, en inglés *Internet of Things* o IoT **[Ref. - 1]**, hace referencia a la digitalización de todo tipo de dispositivos desde sensores y actuadores hasta objetos comunes como vehículos, cámaras de grabación, implantes médicos, ropa, etc. La conectividad digital de estos dispositivos permite enviar y recibir información para realizar tareas que hasta no hace mucho podrían parecer imposibles como monitorizar el estado de una flota de vehículos o ver las cámaras de seguridad de la empresa desde un *smartphone*. Se podría decir que con el IoT se inicia una revolución en la forma en que vivimos y trabajamos. Sus aplicaciones son muy diversas: domótica, en edificios y ciudades o en aplicaciones en industria 4.0.

1.1. Panorama del IoT para empresas

El IoT aplicado al mundo empresarial puede suponer una gran mejora en diversas áreas de negocio: seguridad, gestión de inventarios, logística, etc. Los datos obtenidos por los diferentes dispositivos servirán, entre otras cosas, para monitorizar activos, diagnosticar posibles fallos de funcionamiento o mejorar un determinado proceso haciéndolo más eficiente.
Sin embargo, como sucede con cualquier tecnología emergente, el uso de IoT nos enfrenta a mucha incertidumbre. Su adopción en entornos empresariales todavía no está muy extendida, muchas compañías son reticentes a su implantación y otras deciden apostar por esta tecnología, pero no terminan de obtener todo su beneficio debido a la gran cantidad de información a manejar.

La consultora Gartner **[Ref. - 2]** pronostica que para el año 2021 habrá unos 25 mil millones de dispositivos IoT conectados en sectores tan dispares como:

- **Domótica.** Las casas inteligentes o *smart homes* serán cada vez más comunes. Los usuarios podrán automatizar muchos procesos diarios, como iluminación o calefacción (medidores de energía y termostatos), y gestionarlos remotamente haciendo que la demanda y diversidad de este tipo de dispositivos aumente.

- **Salud**. Este es otro sector al que la incorporación de dispositivos IoT beneficia. Su uso puede ser muy amplio, desde monitorizar el estado de un paciente a llevar un control sobre sus hábitos alimenticios.

1

- **Transporte y logística**. Con esta tecnología es posible realizar un seguimiento en tiempo real de un determinado activo, por ejemplo, un paquete o un vehículo. Además, la monitorización y análisis de los datos generados puede redundar en beneficios para la empresa, ya que permitirán la optimización de las tareas asociadas.

- **Seguridad y vigilancia**. Gracias a la incorporación de dispositivos IoT las empresas que ofertan este tipo de servicios pueden monitorizar cámaras de vigilancia, sensores de presencia o alarmas de multitud de clientes de una sede central y activar diferentes elementos de disuasión a través de Internet.

"La **gran conectividad** de estos dispositivos es a su vez su talón de Aquiles, puesto que los **ciberdelincuentes** podrían utilizarlos en su **propio beneficio**"

La gran conectividad de estos dispositivos es a su vez su talón de Aquiles, puesto que los ciberdelincuentes podrían utilizarlos en su propio beneficio. Otro aspecto que puede ser un lastre para el IoT es la recolección masiva, en algunos casos, de datos de carácter personal que podría implicar riesgos para empresas y usuarios. Por otra parte, los dispositivos IoT que presentan vulnerabilidades técnicas en los mecanismos de autenticación y limitaciones de cálculo, que dificultan la implantación de cifrado tanto en la información en tránsito como en la almacenada. Por último, los ciclos de vida de estos dispositivos son muy cortos, quedando obsoletos y sin soporte poco tiempo después de que se haya completado su despliegue, lo que podría suponer un riesgo añadido.

Estos retos obligan a las empresas a revisar sus procedimientos, políticas de seguridad y adecuación a la normativa al incorporar dispositivos IoT, considerando también su administración, su ciclo de vida y toda la información que generan e intercambian.

1

1.2. Capacidades de interacción y comunicación de los dispositivos IoT

Los dispositivos IoT incorporan elementos que les permiten interactuar con el entorno, como es el caso de un termostato inteligente, que podrá realizar mediciones de la temperatura ambiental. Estos elementos les confieren la capacidad de interacción con el mundo físico:

- **Sensores**: son capaces de realizar mediciones del mundo físico que serán procesadas, transformadas y analizadas en el mundo digital, entre otras:
  - Temperatura,
  - presión,
  - calidad en el aire,
  - humedad,
  - sonido,
  - luminosidad,
  - radiación de luz infrarroja,
  - velocidad,
  - CO2 en el aire.

- **Actuadores**: tienen la capacidad de modificar elementos del mundo físico en base a las mediciones realizadas por los sensores o por órdenes recibidas de cualquier otro elemento como un ordenador remoto. Algunas de las acciones que pueden hacer son:
  - Abrir o cerrar una válvula o un interruptor;
  - actuar sobre un motor, por ejemplo, para subir o bajar una persiana o abrir o bloquear una puerta;
  - poner una canción.

"Algunos dispositivos IoT tienen la capacidad de **recibir órdenes y ofrecer información** directamente a los usuarios que los estén utilizando. A este medio de comunicación entre el humano y la máquina se le conoce como **interfaz de usuario**"

Algunos dispositivos IoT tienen la capacidad de **recibir órdenes y ofrecer información directamente a los usuarios** que los estén utilizando. A este medio de comunicación entre el humano y la máquina se le conoce como **interfaz de usuario**. Esta interfaz puede consistir en pantallas, aplicaciones para móviles u otros elementos como teclado, ratón o micrófono, como ocurre en los **asistentes personales** y otros dispositivos que reciben órdenes por voz.

1

Para enviar y recibir órdenes e información entre dispositivos necesitan un medio de comunicación, también conocido como **interfaz de red**. Los dispositivos IoT suelen tener **capacidad para conectarse con otros dispositivos** dentro de su red local por medio de diferentes estándares como Ethernet, wifi o Bluetooth. Pero además, como disponen de acceso a Internet, también tienen la capacidad de **conectarse con otros dispositivos ubicados en cualquier parte del mundo**.

2 AMENAZAS PARA EL DISPOSITIVO

Los dispositivos IoT pueden ser una presa fácil para los ciberdelincuentes que buscan este tipo de dispositivos como punto de entrada a las redes de las empresas o a otros puntos que se encuentran más protegidos. El ciberataque y compromiso de estos dispositivos puede dar lugar a consecuencias graves para la seguridad como:

- infectarlos para formar parte de una red zombi que los utilicen para realizar ciberataques, por ejemplo, de denegación de servicio distribuida o DDoS **[Ref. - 3]**;
- utilizarlos como puente o punto de entrada para atacar otros equipos de la misma red, para robar información o comprometer servidores o para realizar otras acciones delictivas;
- o reconfigurarlos para inhabilitarlos o cambiar sus condiciones de utilización.

Repasamos a continuación las distintas amenazas que afectan a estos dispositivos **[Ref. - 4]** con el objeto de poner de manifiesto cómo afecta su uso en la seguridad de nuestras empresas, así como las consecuencias que puede acarrear su deficiente instalación, configuración y mantenimiento.

2.1. Amenazas para el dispositivo

La conectividad a Internet, principal característica de este tipo de dispositivos, es también su principal punto débil. De estar mal configurado, tener vulnerabilidades de diseño o contraseñas débiles o por defecto, cualquiera podría acceder al dispositivo si se dieran las circunstancias idóneas.

Por otra parte, además de los buscadores como Google o Bing que indexan contenido de Internet como páginas web, existen otros buscadores cuyo objetivo es indexar dispositivos y servicios accesibles desde Internet, como es el caso de Shodan **[Ref. - 5]**. Con estos buscadores podemos encontrar dispositivos IoT (*smartmeters*, cámaras IP…) conectados a Internet y averiguar detalles sobre su tecnología o configuración.

Los ciberdelincuentes podrían identificar dispositivos vulnerables y automatizar ciberataques. Cuando un ciberdelincuente consigue infectar

2

para tener bajo su control multitud de dispositivos, estaremos hablando de lo que se denomina red *botnet* **[Ref. - 7]**. Cada uno de los dispositivos infectados se denomina bot o zombi. Este tipo de redes controladas por ciberdelincuentes pueden realizar todo tipo de acciones maliciosas como robar información, difundir *spam*, *malware* o llevar a cabo ciberataques de denegación de servicio distribuido o DDoS **[Ref. - 3]**. Los ciberataques DDoS consisten en saturar un servicio, como por ejemplo una web, por medio de multitud de conexiones al mismo tiempo. Uno de los más grandes fue ejecutado por la ***botnet* Mirai** **[Ref. - 6]**, compuesta principalmente por dispositivos IoT.

"Los ciberdelincuentes podrían enfocar sus esfuerzos en **atacar su funcionalidad**, siendo la denegación de servicio uno de los principales peligros, dejándolos **inoperativos o no accesibles**"

Además, los propios dispositivos IoT no son inmunes a las amenazas. Los ciberdelincuentes podrían enfocar sus esfuerzos en atacar su funcionalidad, siendo la **denegación de servicio uno de los principales peligros**, dejándolos inoperativos o no accesibles. En algunos aparatos IoT será fácil volver a la normalidad, ya que un reinicio o restauración del *software* será suficiente, pero en otros, por diferentes razones como su ubicación o la complejidad para reiniciarlo o restaurarlo, puede no resultar una tarea sencilla y podría derivar en situaciones peligrosas. Por ejemplo, para dispositivos de salud o en ubicaciones remotas puede que su restauración no sea viable, por lo que las víctimas podrían, en caso de tratarse de un *ransomware* **[Ref. - 7]**, verse obligadas a pagar el rescate.

No obstante, las amenazas a los dispositivos IoT no se reducen a las derivadas de su conectividad a Internet. Muchos de estos aparatos cuentan también con capacidades de conexión inalámbrica como wifi, Bluetooth o Zigbee, lo que puede suponer otro vector de ataque para ciberdelincuentes si se encuentran dentro de su rango de acción.

2.2. Amenazas para la privacidad

Los ciberdelincuentes no centran sus esfuerzos exclusivamente en los propios dispositivos puesto que la **información que manejan también es de gran importancia**. ¿Cuál sería el precio de poder acceder a dispositivos de reconocimiento facial o médicos para algunas organizaciones criminales? Podrían utilizar la información robada en su propio beneficio o venderla al mejor postor, comprometiendo así la privacidad y seguridad de los afectados.

3 VECTORES DE ATAQUE EN DISPOSITIVOS IOT

Los vectores de ciberataque son los **métodos que puede utilizar un ciberdelincuente para hacerse con su objetivo**, por ejemplo, obtener información o tomar el control del dispositivo. Para los dispositivos IoT, por cómo están diseñados, los ciberdelincuentes cuentan con varios vectores de ciberataque que podrían aprovechar para comprometer su seguridad. A continuación se describen los más críticos.

3.1. Fallos en la implantación

La implantación adecuada de los dispositivos IoT en la red de la empresa es clave para garantizar la seguridad de la organización. Uno de los principales fallos que se cometen a la hora de implantar soluciones IoT es no segmentar adecuadamente la red, permitiendo que los dispositivos IoT conectados a la misma red de la empresa puedan ser la puerta de entrada de los ciberdelincuentes **[Ref.- 8]**.

3.2. Interceptar datos de tránsito

La transmisión de datos es una parte fundamental de los dispositivos IoT, ya que estos se han diseñado para interactuar con el mundo físico, siendo el envío y recepción de información esenciales para su funcionamiento. Si un ciberdelincuente consigue acceso a la red local o LAN donde se encuentra el dispositivo IoT o el receptor de la información, podría acceder a la información o incluso modificarla. A este tipo de ciberataques se los conoce como Hombre en el Medio o MitM, por sus siglas en inglés *Man in the Middle* **[Ref. - 9]**.

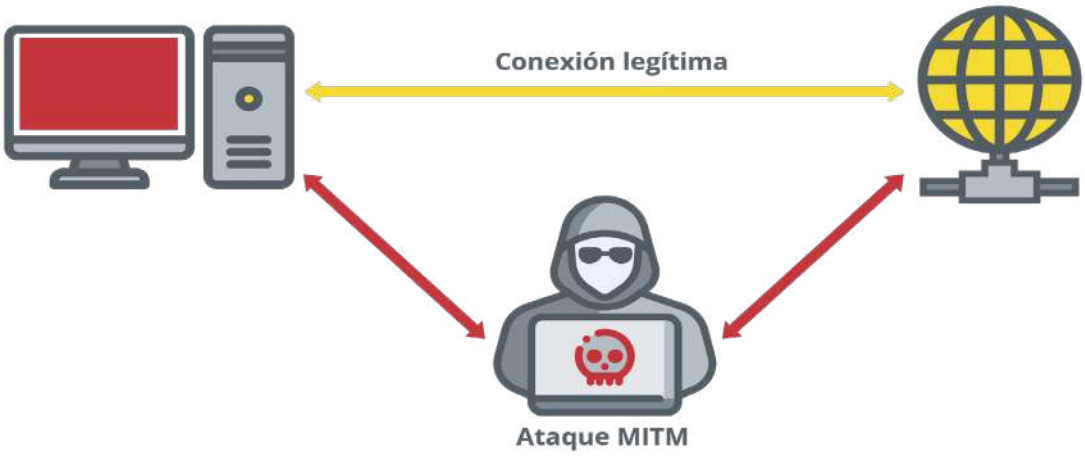

Ilustración 1 Esquema de un ataque Man in the Middle

3

"Si la interfaz web tiene alguna **vulnerabilidad** o no cuenta con las medidas de seguridad necesarias para evitar accesos **no autorizados**, los ciberdelincuentes podrían acceder a ella y controlar el dispositivo **a su antojo**"

Cuando un ciberatacante realiza un MitM dispone de dos variantes:

- MitM pasivo. En esta modalidad el ciberatacante intercepta el tráfico, es decir, los mensajes hacia o desde el dispositivo, y los envía de nuevo a su destinatario **sin alterarlos**, pudiendo obtener datos sensibles e información confidencial de la empresa.

- MitM activo. En este caso, el ciberatacante **intercepta el tráfico y además lo modifica** antes de enviarlo de nuevo a su destinatario. Esto podría permitir que el ciberatacante actuara sobre el dispositivo IoT a su voluntad o alterara la información que recibe el usuario.

Pongamos un ejemplo de lo que sucedería en un escenario en el que se estuviera produciendo uno de estos ciberataques. Una empresa que gestiona un aparcamiento ha decidido instalar cámaras de seguridad IP que ayudarán al personal a garantizar la seguridad de los vehículos. Un grupo de ciberdelincuentes ha descubierto que son vulnerables a ataque MitM. Para ello, interceptan los datos que se envían desde las cámaras a la sala de control para ver cuantos vehículos hay, si alguno es de su interés y cuál es el mejor momento para proceder con el robo.

3.3. Acceso a la plataforma de administración

Los dispositivos IoT, principalmente debido a su tamaño, no cuentan con los típicos elementos que permiten interactuar con ellos, como una pantalla o un teclado. Para suplir esta carencia suelen contar con una **interfaz web o aplicación móvil que permite su administración** por medio de un navegador. Si la interfaz web tiene alguna **vulnerabilidad o no cuenta con las medidas de seguridad necesarias** para evitar accesos no autorizados, los ciberdelincuentes podrían acceder a ella y controlar el dispositivo a su antojo.

3

3.4. Vulnerabilidad en el *software*

Una de las principales vulnerabilidades en el *software* de los dispositivos IoT tiene que ver con las **credenciales de administración**. En algunos casos **no es posible modificar** las credenciales que tienen por defecto, lo que supone un grave riesgo ya que éstas generalmente son de dominio público y cualquier ciberdelincuente las puede obtener de la documentación del fabricante. Las credenciales de acceso **embebidas** en el código del dispositivo o la existencia de cuentas con privilegios elevados utilizadas por el fabricante y no documentadas también suponen un riesgo.

Además, los dispositivos IoT, como cualquier otro dispositivo TI, **no están exentos de sufrir otro tipo de vulnerabilidades** como desbordamientos de búfer o *buffer overflow*, condiciones de carrera, denegaciones de servicio, etc. que pueden comprometer su seguridad y la de los datos que gestionan.

"Los dispositivos IoT, como cualquier otro dispositivo TI, **no están exentos** de sufrir otro tipo de **vulnerabilidades** como desbordamientos de **búfer o buffer overflow**..."

3.5. Configuraciones por defecto

La mayoría de dispositivos IoT **no aplican** los principios de seguridad por defecto. De aplicarlos, los valores de fábrica del dispositivo proporcionarían la mínima funcionalidad para su administración y operación, con los permisos estrictamente necesarios para permitir un uso ordinario sencillo y seguro. De este modo, para utilizar el dispositivo de forma insegura sería necesario un acto consciente por el usuario. No obstante, al incorporar la seguridad por defecto no se ha de descuidar **la experiencia del usuario**, pues si a causa de los mecanismos de seguridad se dificulta el uso normal para el usuario, este encontrará la forma de evitarlos.

Algunos fabricantes de dispositivos IoT pueden dejar **habilitados servicios o herramientas que realmente no necesitaría** el aparato o el usuario para un uso normal. Cuantos más servicios tenga instalados y habilitados más posibilidades habrá de que uno de ellos tenga una vulnerabilidad que pudiera ser explotada por los ciberdelincuentes.

3

Por ejemplo, si para el funcionamiento del dispositivo únicamente es necesario tener habilitado un servidor web para su administración, sería un error dejar también habilitadas otras vías de administración remota que podrían ser la puerta de entrada de ciberatacantes. Además, en muchas ocasiones **los propios usuarios desconocerían la existencia de esos servicios**, por lo que aplicar las medidas de protección oportunas se vuelve mucho más complicado.

Otro de los fallos de seguridad que pueden tener muchos dispositivos es que vienen de fábrica con **credenciales de acceso por defecto inseguras**. En algunos dispositivos IoT con un simple «admin/admin» se conseguiría acceso. Esto sería posible mitigarlo forzando, desde el diseño y por defecto, el cambio de la contraseña en el primer uso.

"Otro de los **fallos de seguridad** que pueden tener muchos dispositivos es que vienen de fábrica con credenciales de acceso **por defecto inseguras**"

Por ejemplo, en la *botnet* Mirai **[Ref. - 10]**, uno de los principales vectores de ciberataque utilizados fue la existencia de credenciales por defecto o muy simples en los aparatos afectados.

3.6. Acceso físico al dispositivo

El **acceso físico al dispositivo por parte de ciberdelincuentes** es otra de las vías que se podría utilizar para obtener información confidencial o tomar su control. Este tipo de ciberataques no es inherente a los dispositivos IoT, aunque por su uso en exteriores o en los casos en los que tienen que hacer pública su ubicación para su funcionamiento, están más expuestos. En dispositivos que se encuentran en un lugar controlado como una nave industrial o una empresa es menos probable que se dé esta situación, pero en dispositivos ubicados en sitios remotos puede suponer un grave riesgo de ciberseguridad.

Si un ciberdelincuente consigue acceso físico al dispositivo podría **robarlo o destruirlo**, causando una denegación del servicio, que podría dejar de estar accesible para los usuarios, con las consiguientes pérdidas económicas que se derivarían de la pérdida de funcionalidad. Asimismo, podría **acceder a la información almacenada** en el propio dispositivo para buscar datos confidenciales como credenciales de acceso, direcciones URL sensibles, registros de actividad o *logs*, etc.

3

3.7. Los usuarios

El usuario es el eslabón más importante en la cadena de la ciberseguridad y también podría constituir un vector de ciberataque. Un mal uso por parte del usuario de forma accidental, intencional o por el engaño de un ciberdelincuente puede comprometer la seguridad del dispositivo IoT, y por lo tanto de la empresa.

El tipo de ciberataque más común que llevan a cabo los ciberdelincuentes contra las personas de una organización está basado en lo que se conoce como **ingeniería social** **[Ref. - 11]**. Mediante diferentes técnicas de engaño y manipulación psicológica los ciberdelincuentes fuerzan a la víctima a revelar información confidencial como credenciales de acceso o a instalar archivos infectados con *malware*.

"El tipo de **ciberataque más común** que llevan a cabo los ciberdelincuentes contra las personas de una organización está basado en lo que se conoce como **ingeniería social**"

Generalmente, los ataques de ingeniería social se llevan a cabo por medio de un correo electrónico en el que los ciberdelincuentes suplantan la identidad de una empresa conocida, un miembro de la propia empresa como un técnico de informática o cualquier otra identidad en la que el usuario confía y que sirva para su propósito. Además del correo pueden utilizar otro tipo de canales como llamadas telefónicas o incluso realizar el engaño en persona.

4 MEDIDAS DE SEGURIDAD

Una vez que se conocen los principales vectores de ciberataque que podrían utilizar los ciberdelincuentes contra los propios dispositivos, la información que gestionan o los usuarios, se presentan a continuación las medidas de seguridad necesarias para tener un entorno lo más seguro posible. Las siguientes pautas servirán para conseguir minimizar los riesgos de sufrir un incidente de seguridad.

En los dispositivos IoT no se suelen utilizar las soluciones habituales de ciberseguridad como antivirus o cortafuegos; por ello, las siguientes medidas de seguridad están destinadas a proteger el propio dispositivo y, por consiguiente, toda la organización.

4.1. Acceso seguro al dispositivo

La **interfaz de acceso al propio dispositivo IoT es en muchos casos la parte más crítica**. Si un ciberdelincuente consigue acceso podría tener el control total sobre el dispositivo. Como ya se indicó anteriormente, para acceder a la interfaz de administración los fabricantes generalmente implementan 2 vías distintas: interfaz web y aplicación móvil.

Con independencia de la interfaz usada, es esencial llevar un correcto **control de acceso a la administración del dispositivo**, sobre todo si esta interfaz es accesible desde Internet. A la hora de escoger un dispositivo se ha de verificar que cuenta, al menos, con mecanismos de autenticación basados **en la dupla usuario y contraseña**.

Como ya se indicó en el apartado anterior **"Configuraciones por defecto"**, los dispositivos IoT que cuentan con mecanismos de autenticación por defecto o en su configuración inicial suelen venir configurados con contraseñas débiles o que no pueden ser cambiadas por los usuarios. Si el dispositivo permite crear nuevos identificadores de usuario con privilegios de administrador es recomendable crear uno nuevo siguiendo las siguientes pautas y eliminar el usuario por defecto existente:

- Para el **nombre de usuario** se ha de **evitar usar nombres genéricos** como «admin», «administrador», «root», etc., y nombres fácilmente adivinables como el de la empresa.

4

“Como alternativa a las **comunicaciones no cifradas**, y siempre que sea necesaria la comunicación con el dispositivo vía Internet, existe la opción de utilizar **redes privadas virtuales o VPN”**

- Se ha de **utilizar una contraseña robusta** que incluya mayúsculas, minúsculas, números y símbolos y tenga una longitud de ocho caracteres como mínimo, siempre considerando que **cuantos más caracteres tenga y más variados sean más robusta será**.

En caso de no poder eliminar el usuario de administración por defecto, se modificará la contraseña siguiendo las mismas recomendaciones citadas anteriormente.

Otros fabricantes ofrecen a sus usuarios acceso al dispositivo IoT por medio de una aplicación móvil. Al igual que para cualquier otra **aplicación que descarguemos en los móviles, debemos comprobar que es legítima, descargarla únicamente desde la tienda oficial**, bien sea la App Store o Play Store, y **mantenerla siempre actualizada a la última versión**. Las recomendaciones de seguridad para acceder por medio de usuario y contraseña serán las mismas que para los otros escenarios.

4.2. Comunicaciones seguras

La interfaz para acceder al dispositivo, además de contar con credenciales de acceso robustas, tendrá que **utilizar técnicas criptográficas que cifren la información**. Cuando se accede al dispositivo por medio de un navegador se comprobará que al comienzo de la dirección se utiliza el protocolo HTTPS **[Ref. - 12]**. Esto es fácilmente identificable cuando en la barra de navegación la dirección comienza por «https://».

Como alternativa a las comunicaciones no cifradas, y **siempre que sea necesaria la comunicación con el dispositivo vía Internet, existe la opción de utilizar redes privadas virtuales o VPN**, por sus siglas en inglés *Virtual Private Network* **[Ref. - 13]**. La implementación de una VPN ofrece comunicaciones seguras con el dispositivo IoT desde cualquier tipo de conexión, incluidas redes wifi públicas.

En caso de que el acceso al dispositivo **no cuente con el protocolo de comunicación HTTPS se recomienda no administrarlo desde Internet** si no se utiliza algún mecanismo de seguridad complementario, como una red privada virtual o VPN, ya que en ese caso las credenciales de acceso se transmitirán

4

por un canal no seguro y cualquier ciberdelincuente podría hacerse con ellas. Como alternativa se recomienda acceder al aparato IoT utilizando la misma red local y un dispositivo seguro.

Cuando el acceso se realiza por medio de una aplicación móvil se aconseja comprobar en las especificaciones de la propia aplicación si se utilizan mecanismos seguros de comunicación. En caso de no indicarlo es necesario contactar con el fabricante para que informe si los datos en tránsito están protegidos o no. Si la aplicación no cifra las comunicaciones, de la misma forma que sucede con el acceso por medio de una interfaz web, se debe utilizar una VPN.

"Cuando el acceso se realiza por medio de una **aplicación móvil** se aconseja comprobar en las **especificaciones** de la propia aplicación si se utilizan **mecanismos seguros** de comunicación"

Además del acceso al propio panel de administración del dispositivo, **toda la información que envía es recomendable que viaje cifrada. En caso de no ser posible se deberán aplicar otras medidas de seguridad como la segmentación de redes o las VPN**. La información, dependiendo del tipo de aparato elegido, puede ser sensible y de ser interceptada por un ciberdelincuente puede utilizarse con fines maliciosos.

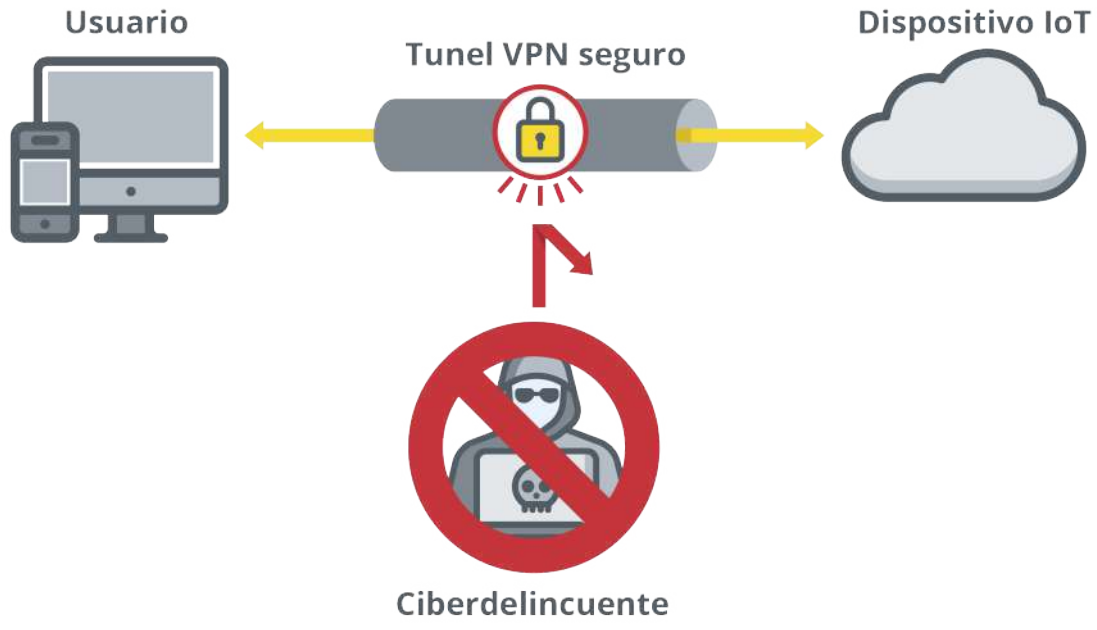

Ilustración 2 Conexión VPN a un dispositivo IoT

4

4.3. Actualizaciones de seguridad

Las actualizaciones de seguridad son una de las principales líneas de defensa de cualquier dispositivo, sea o no IoT. **Aplicar las últimas actualizaciones y parches de seguridad será una prioridad**, así se corregirán las últimas vulnerabilidades descubiertas y se contará con las últimas funcionalidades implementadas por el fabricante. Además, los dispositivos IoT deberán formar parte de la **política de actualizaciones de *software*** **[Ref. - 14]** de la organización.

Los dispositivos IoT, debido a las funciones que realizan dentro de la organización, **no tendrían que ser considerados como cualquier otro elemento**, como puede ser un PC o un servidor dentro de la política de actualizaciones. Los dispositivos IoT en muchos casos realizan tareas continuas en el tiempo y su apagado o desconexión no es habitual. Por ello, **la política de actualizaciones debe contemplar todas las casuísticas posibles** como pueden ser los mantenimientos programados y los no programados.

La política de actualización para dispositivos IoT, como cualquier otra política, debe estar basada en las necesidades de la propia organización y nunca se debería basar en la de otra empresa, ya que cada una es diferente.

El proceso de actualización variará dependiendo del fabricante. En algunos casos se podrá realizar de forma semiautomática desde el panel de administración del propio dispositivo, mientras que en otros será necesario descargar la actualización de *software* o *firmware* del sitio web del fabricante y actualizar el dispositivo manualmente.

"La **política de actualizaciones** debe contemplar todas las casuísticas posibles como pueden ser los **mantenimientos programados y los no programados**"

4

"Es recomendable **configurar un cortafuegos o firewall** que filtre las conexiones que se establecen con los dispositivos IoT para que solo sean permitidas aquellas **conexiones desde determinados dispositivos y servicios"**

Cuando se tenga que descargar la actualización de seguridad de forma manual siempre se hará desde el **sitio web oficial del fabricante**, accediendo al portal directamente con el navegador. Nunca se instalarán actualizaciones de seguridad que provengan de otro sitio que no sea el oficial o de ficheros adjuntos en correos electrónicos. Una de las técnicas usadas por los ciberdelincuentes para hacerse con el control de los dispositivos IoT es por medio de actualizaciones de seguridad falsas que hacen llegar a sus víctimas generalmente por este medio. A la hora de decantarse por un dispositivo u otro siempre es recomendable elegir aquel cuya empresa distribuidora tenga una buena reputación y disponga de un buen departamento de soporte que actualice sus dispositivos de forma regular.

4.4. Dispositivos de seguridad perimetral

Los dispositivos IoT, debido a sus capacidades de procesamiento reducidas, no suelen tener la posibilidad de implementar herramientas de seguridad como cortafuegos o antivirus ni protegerse ante ciberataques como denegaciones de servicio o DoS. Para paliar esta debilidad es necesario **aplicar las medidas de seguridad en otros dispositivos y capas de la red de la empresa**.

Es recomendable configurar un **cortafuegos o *firewall*** **[Ref. - 15]** que filtre las conexiones que se establecen con los dispositivos IoT para que solo sean permitidas aquellas conexiones desde determinados dispositivos y servicios. No es una configuración segura que el dispositivo IoT se encuentre en la red corporativa de la empresa con conexión a Internet, pues podría ser utilizado para acceder a dicha red. Para resolverlo, es recomendable crear una o varias redes específicas para estos dispositivos y configurarlas como **DMZ o zona desmilitarizada** **[Ref. - 16]**.

Los dispositivos IoT comúnmente tienen habilitados varios servicios para su gestión cuyo acceso se hace por medio de diferentes puertos, **[Ref. - 17]** como por ejemplo el 80 al servicio «http» o el 23 al «servicio telnet» **[Ref. - 18]**. Se han de filtrar las conexiones a los puertos que no sean necesarios por medio de algún dispositivo de red perimetral como un cortafuegos o *router*, ya que reduciendo el nivel de exposición disminuye el nivel de riesgo. En caso de ser

4

posible, se deshabilitarán además los servicios que no sean necesarios para su administración como telnet, cuyo uso no es recomendable al existir alternativas más seguras.

Si el dispositivo IoT se encuentra dentro de una red inalámbrica, como puede ser una red wifi **[Ref. - 19]** o ZigBee **[Ref. - 20]**, esta también debe contar con las suficientes medidas de seguridad.

4.5. Seguridad física

La seguridad física del dispositivo es una parte importante para proteger la información que gestiona. Esto es especialmente relevante en aquellos aparatos ubicados en lugares fuera de la protección de las instalaciones de la empresa, como por ejemplo en **dispositivos de campo** **[Ref. - 21]**.

Es posible que en caso de que un ciberataque remoto no tenga efecto, los ciberdelincuentes se decanten por realizar uno físico contra el dispositivo, bien sea sustrayéndolo, interceptando las comunicaciones, accediendo a sus componentes internos, etc. Será necesario tomar las medidas de seguridad necesarias para que la información que gestiona esté protegida:

- Se ha de comprobar la **cubierta protectora** del aparato y cuán difícil es acceder a sus componentes internos. En caso de que sea fácil su acceso se deberá añadir una protección más robusta.

- Se revisará si el dispositivo cuenta con **puertos USB u otro tipo de puertos específicos de administración fácilmente accesibles** que den acceso a información sin desmontar ningún tipo de protección exterior. En caso afirmativo se protegerá el acceso a esos puertos. Si los puertos USB no son necesarios y la interfaz de administración del dispositivo lo permite, se deshabilitarán.

- Toda **información que se almacene localmente en el dispositivo se hará cifrada** para protegerla ante accesos no autorizados.

- El canal de comunicación también debe protegerse utilizando, si no hubiese alternativa más segura, **conexiones de datos móviles** en lugar de wifi.

"Toda información que se almacene **localmente** en el dispositivo se hará cifrada para protegerla ante **accesos no autorizados"**

4

4.6. Concienciación en seguridad de los usuarios

Los dispositivos IoT, como cualquier otro elemento que compone la estructura TIC de la empresa, están diseñados en última instancia para que sean utilizados, administrados y aporten un servicio a los empleados de la organización. Por esa razón, los ciberdelincuentes además de atacar a los dispositivos pueden intentar acceder a ellos y su información por medio de las personas que los gestionan, utilizando técnicas de ingeniería social. La ingeniería social consiste en utilizar la persuasión y el engaño contra los empleados de la empresa para que realicen una determinada tarea como facilitar credenciales de acceso o ejecutar código malicioso, sin que estos se den cuenta del engaño.

"Los **ciberdelincuentes**, utilizando diferentes técnicas de **ingeniería social**, consiguen que la víctima termine instalando **malware**..."

Es frecuente que este tipo de ciberataques contra el personal de la organización tengan su origen en el correo electrónico. Los ciberdelincuentes, utilizando diferentes técnicas de ingeniería social **[Ref. - 11]**, consiguen que la víctima termine instalando *malware*, por ejemplo mediante una actualización falsa, para realizar cualquier actividad fraudulenta como realizar espionaje industrial.

La **formación y concienciación es la principal medida de seguridad** que se puede llevar a cabo para prevenir este tipo de ciberataques. El Kit de concienciación **[Ref. - 22]** es una buena forma de que todos los miembros de la empresa mejoren sus habilidades en ciberseguridad.

El buen uso de las contraseñas de acceso necesita una mención especial. Es recomendable cambiar periódicamente las contraseñas en los dispositivos IoT y se debe concienciar a los empleados sobre este hábito. Además, esta práctica debería estar incluida en la política de contraseñas para dispositivos IoT de la compañía.

4

4.7. Otras recomendaciones de seguridad

Existenotraseriederecomendacionesdeseguridadatenerencuenta para mejorar la seguridad de los dispositivos IoT de la empresa:

- Se comprobará cada cierto tiempo la visibilidad de los dispositivos IoT en Internet con herramientas específicas como Shodan.
- Si el dispositivo lo permite se habilitará un registro de *logs* que guarde los eventos que se producen como accesos, cambios de contraseña, actualizaciones, etc.
- En caso de ser posible, se ha de habilitar algún mecanismo de notificación cuando se produce un evento que pueda afectar a la seguridad del dispositivo.
- Se monitorizarán de forma centralizada los dispositivos IoT para comprobar su correcto funcionamiento y que no se producen eventos que puedan afectar a su seguridad o a la de la empresa.
- Se comprobará regularmente la web del fabricante en busca de nuevas actualizaciones de seguridad tanto de *firmware* como de *software* siempre que no exista un método alternativo que avise sobre ello.

"Si el dispositivo lo permite se habilitará un **registro de logs** que guarde los eventos que se producen como accesos, cambios de contraseña, actualizaciones, etc."

5 DECÁLOGO DE RECOMENDACIONES DE SEGURIDAD

A continuación se enumeran las principales recomendaciones que se han de seguir a la hora de utilizar cualquier tipo de dispositivo IoT en la empresa.

1. Minimizar el uso de dispositivos IoT en la empresa utilizando únicamente los que sean estrictamente necesarios.

2. No usar, en la medida de lo posible, dispositivos IoT que transmitan información o cuya gestión se realice desde servidores externos «en la nube» aunque sea del fabricante.

3. Comprobar las configuraciones por defecto del dispositivo, especialmente antes de permitir su acceso desde Internet y, de ser posible, elegir aquellos dispositivos que permitan un elevado nivel de seguridad.

4. Si no es posible establecer configuraciones de seguridad robustas no se permitirá el acceso al dispositivo desde Internet y preferiblemente tampoco desde la red local.

5. Establecer siempre contraseñas de acceso y administración robustas. Siempre que sea posible se forzará su uso.

6. Mantener actualizado el dispositivo a la última versión.

7. Mantener abiertos a Internet únicamente aquellos servicios que sean necesarios para su administración remota y los que no lo sean se deben deshabilitar. También hay que cambiar los puertos de los servicios cuando sea posible.

8. Utilizar dispositivos de seguridad perimetral como cortafuegos para proteger la seguridad del dispositivo IoT.

5

9. Emplear mecanismos que permitan asegurar la autenticidad, integridad y confidencialidad de las comunicaciones, especialmente si estas se realizan vía wifi.

10. Auditar periódicamente los dispositivos IoT.

11. Concienciar a los empleados sobre la importancia de la ciberseguridad en el día a día de su trabajo y en la administración y uso de este tipo de dispositivos.

12. Comprobar la seguridad física del dispositivo y aplicar las medidas necesarias que eviten manipulaciones de terceros.

"**Concienciar a los empleados** sobre la importancia de la **ciberseguridad** en el día a día de su trabajo y en la administración y uso de este tipo de dispositivos"

6 REFERENCIAS

[Ref. - 1]. **Wikipedia - Internet de las cosas -** https://es.wikipedia.org/wiki/Internet_de_las_cosas

[Ref. - 2]. **Gartner – Newsroom – Press Releases - Gartner Identifies Top 10 Strategic IoT Technologies and Trends -** https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

[Ref. - 3]. **INCIBE – Protege tu empresa – Blog - Medidas de prevención contra ataques de denegación de servicio -** https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

[Ref. - 4]. **TREND Micro - Internet of Things - IoT Attack Opportunities Seen in the Cybercrime Underground -** https://blog.trendmicro.com/trendlabs-security-intelligence/iot-attack-opportunities-seen-in-the-cybercrime-underground/

[Ref. - 5]. **Shodan -** https://www.shodan.io

[Ref. - 6]. **INCIBE-CERT – Blog - DDoS de actualidad: IoT y los DNS de Dyn -** https://www.incibe-cert.es/blog/ddos-actualidad-iot-y-los-dns-dyn

[Ref. - 7]. **INCIBE – Protege tu empresa - Servicio AntiRansomware -** https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[Ref. - 8]. **INCIBE-CERT – Alerta temprana – Bitácora de ciberseguridad - Fuga de información en un casino a través de un termostato IoT -** https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/fuga-informacion-casino-traves-termostato-iot

[Ref. - 9]. **INCIBE-CERT – Blog - ARP Spoofing -** https://www.incibe-cert.es/blog/arp-spoofing

[Ref. - 10]. **INCIBE-CERT – Blog - Greatest Hits 2016 -** https://www.incibe-cert.es/blog/greatest-hits-2016

[Ref. - 11]. **INCIBE – Protege tu empresa – Blog – Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse -** https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

[Ref. - 12]. **Wikipedia - Protocolo seguro de transferencia de hipertexto -** https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto

6 REFERENCIAS

[Ref. - 13]. INCIBE – Protege tu empresa – Blog - Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN - https://www.incibe.es/protege-tu-empresa/blog/conectate-tu-empresa-forma-segura-cualquier-sitio-vpn

[Ref. - 14]. INCIBE – Protege tu empresa – Herramientas de ciberseguridad – Políticas de seguridad para la pyme – Actualizaciones de software - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-software.pdf

[Ref. - 15]. INCIBE – Protege tu empresa – Blog - UTM, un firewall que ha ido al gimnasio - https://www.incibe.es/protege-tu-empresa/blog/utm-firewall-ha-ido-al-gimnasio

[Ref. - 16]. INCIBE - Protege tu empresa – Blog – Qué es una DMZ y cómo te puede ayudar a proteger tu empresa - https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

[Ref. - 17]. Wikipedia - Puerto (informática) - https://es.wikipedia.org/wiki/Puerto_(inform%C3%A1tica)

[Ref. - 18]. Wikipedia – Telnet - https://es.wikipedia.org/wiki/Telnet

[Ref. - 19]. INCIBE – Protege tu empresa – Guías - Seguridad en redes wifi: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

[Ref. - 20]. INCIBE-CERT – Guías y estudios – Guías - Ciberseguridad en las Comunicaciones Inalámbricas en Entornos Industriales - https://www.incibe-cert.es/guias-y-estudios/guias/ciberseguridad-las-comunicaciones-inalambricas-entornos-industriales

[Ref. - 21]. INCIBE-CERT – Guías y estudios – Guías - Guía de acceso seguro a los dispositivos de campo - https://www.incibe-cert.es/guias-y-estudios/guias/guia-acceso-seguro-los-dispositivos-campo

[Ref. - 22]. INCIBE – Protege tu empresa – Kit de concienciación - https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[Ref. - 23]. INCIBE-CERT – Blog - Riesgos y retos de ciberseguridad y privacidad en IoT - https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

6 REFERENCIAS

[Ref. - 24]. INCIBE-CERT – Blog - La importancia de la seguridad en IoT. Principales amenazas - https://www.incibe-cert.es/blog/importancia-seguridad-iot-principales-amenazas

[Ref. - 25]. INCIBE-CERT – Blog - Iniciativas y mejores prácticas de seguridad para el IoT - https://www.incibe-cert.es/blog/iniciativas-y-mejores-practicas-seguridad-el-iot

[Ref. - 26]. INCIBE-CERT – Blog - IoT: protocolos de comunicación, ataques y recomendaciones - https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa