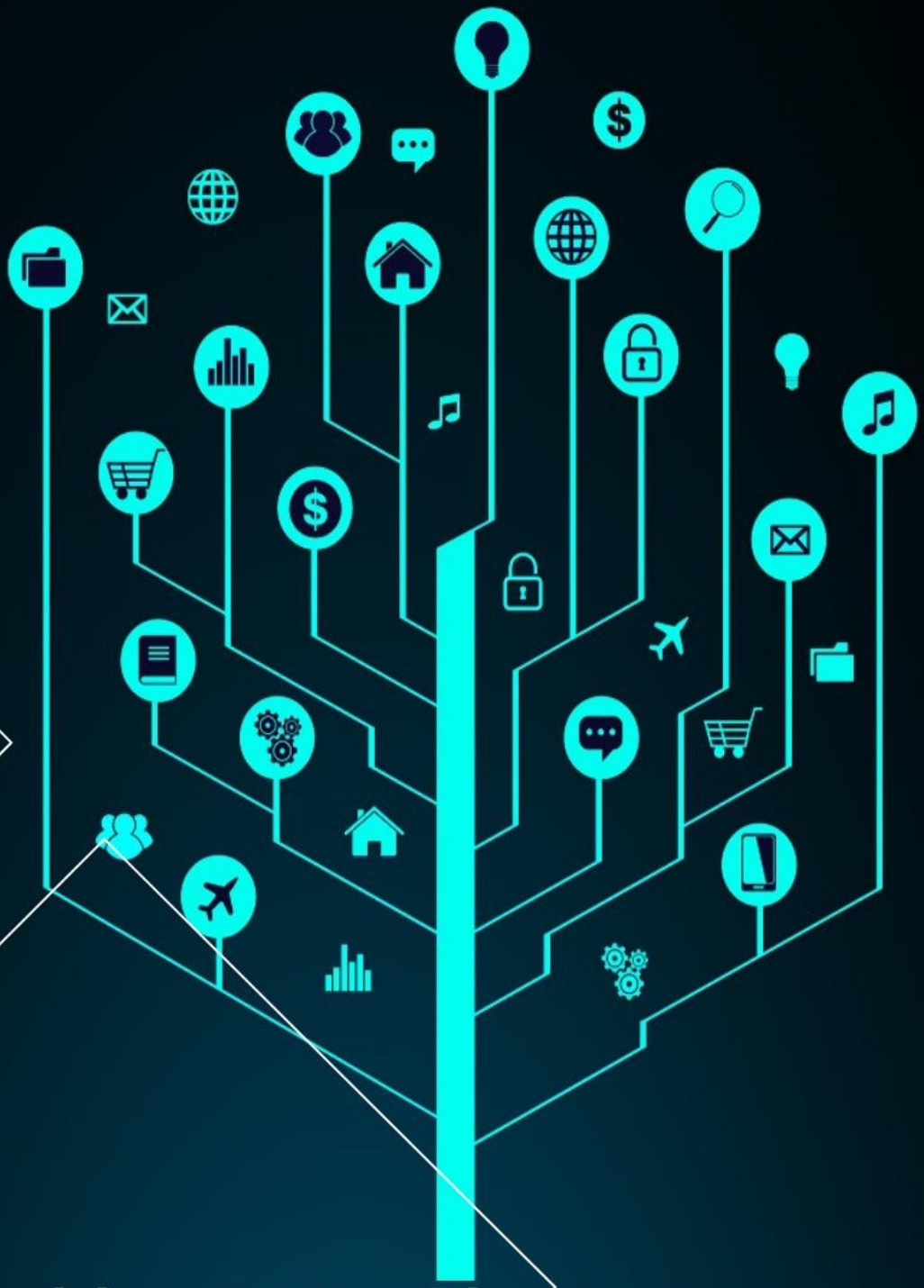

Dispositivos IoT en el entorno empresarial

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. DISPOSITIVOS IOT EN EL ENTORNO EMPRESARIAL

1.1. Antecedentes

El término Internet de las cosas, del inglés *Internet of Things* o IoT [1], se emplea para denominar a todos aquellos dispositivos cotidianos, que tras un proceso de digitalización, tienen la capacidad de estar interconectados, ya sea directamente a través de Internet o de una red interna.

La variedad de este tipo dispositivos es muy heterogénea, ya que podemos encontrar actuadores, sensores, vehículos, implantes médicos, asistentes virtuales, ropa y un largo etcétera.

Debido a esta amplia variedad de dispositivos IoT [2] y las bondades que ofrecen, es normal que cada vez se encuentren más presentes en las organizaciones y empresas, independientemente del tamaño de estas. Por ello, es indispensable contar con una política de seguridad que defina las medidas necesarias para garantizar conexiones seguras, asegurar los datos a los que acceden los dispositivos y definir los métodos de acceso a los dispositivos IoT, así como las configuraciones necesarias que deben cumplir dichos dispositivos, ajustándose a las necesidades y estructura de la empresa.

1.2. Objetivos

- Garantizar la seguridad de la información y los recursos a los que acceden y gestionan los dispositivos IoT, así como asegurar el acceso físico a los mismos.
- Concienciar a los empleados de la importancia de desplegar y utilizar de modo seguro estos dispositivos.

1.3. *Checklist*

A continuación se incluye una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **dispositivos IoT en el entorno empresarial.**

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Acceso seguro al dispositivo** Como administrador de dispositivos IoT utilizas una contraseña fuerte y habilitas siempre que sea posible el doble factor de autenticación en todos los perfiles de la organización.	☐
A	TEC	**Comunicaciones seguras** Empleas técnicas criptográficas para cifrar la información que se comparte en las comunicaciones con los dispositivos IoT. Usas protocolos seguros HTTPS en aplicaciones web y conexiones VPN como medidas de seguridad para preservar las comunicaciones.	☐
B	PRO	**Política de actualización** Elaboras una política de actualización de los dispositivos IoT que contempla los procedimientos necesarios para corregir las últimas vulnerabilidades descubiertas y tenga en cuenta las últimas funcionalidades implementadas por el fabricante. Además, incluyes los dispositivos IoT como parte de la política de actualizaciones de *software*.	☐
A	TEC	**Seguridad perimetral** Palias las debilidades de los dispositivos IoT aplicando medidas de seguridad en otros dispositivos y capas de la red de la empresa.	☐
A	TEC	**Despliegue de los dispositivos** Utilizas una red propia segmentada y, en caso de tener que acceder desde Internet, implementas una DMZ empleando las configuraciones de seguridad necesarias.	☐
B	TEC	**Servicios y permisos mínimos** Activas únicamente los servicios y permisos precisos para cumplir con sus funciones, deshabilitando el resto.	☐
B	PRO	**Restricciones de acceso** Limitas el acceso físico a los dispositivos para evitar manipulaciones indebidas.	☐
B	PRO/TEC	**Estar al día de las amenazas** Estás informado de las distintas campañas utilizadas por los ciberdelincuentes para conseguir acceso a los dispositivos IoT.	☐
B	PRO	**Evitar errores humanos** Formas a los empleados en ciberseguridad para minimizar los riesgos relativos al uso de esta y otras tecnologías.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Acceso seguro al dispositivo**. Preservar la seguridad de los paneles de administración, ya sea mediante una interfaz web, aplicación o acceso físico de los dispositivos IoT, es fundamental. Cambiar las credenciales por defecto y aplicar, si es posible, mecanismos de acceso multifactor [3], son medidas de seguridad esenciales, ya que un ciberdelincuente que consiguiese acceder al dispositivo podría comprometer al resto de dispositivos de la empresa, los datos a los que estos tengan acceso o incluso inhabilitarlos.
- **Comunicaciones seguras**. El empleo de técnicas criptográficas para cifrar [4] la información que se comparte en las comunicaciones con el dispositivo IoT es indispensable para evitar que la información se vea comprometida durante la transmisión de información. El uso de protocolos seguros HTTPS en aplicaciones web o el uso de conexiones VPN [5] son algunas de las medidas de seguridad necesarias para preservar las comunicaciones con los dispositivos IoT. De otro modo, los ciberdelincuentes podrían espiar las comunicaciones.
- **Política de actualización.** Un aspecto muy importante para cualquier *software* o dispositivo es mantenerlo actualizado [6]. Las actualizaciones no solo permiten añadir mejoras o nuevas funcionalidades, sino que uno de sus principales propósitos es la de arreglar fallos de seguridad que puedan presentar. Los dispositivos IoT también reciben este tipo de actualizaciones, y es fundamental mantenerlos actualizados, ya que un dispositivo IoT desactualizado podría ser vulnerable y servir como vía de entrada de ciberdelincuentes a los recursos e información de la empresa.
- **Seguridad perimetral**. La versatilidad de los dispositivos IoT hace que tengan carencias en algunos aspectos, como puede ser no disponer de herramientas de gestión o seguridad propias (cortafuegos, antivirus, etc.). Debido a esto, los dispositivos IoT son más vulnerables ante los ciberataques, y por eso, es necesario que otros dispositivos asuman sus carencias en seguridad. Por este motivo, es recomendable configurar un cortafuegos o *firewall* [7], que filtre las conexiones que se establecen con estos aparatos IoT para que solo se permitan las conexiones desde los dispositivos y servicios necesarios.
- **Despliegue de los dispositivos.** No existe una configuración segura si los dispositivos IoT se encuentran en la red de la empresa con conexión a Internet, pues podrían ser utilizados por los ciberdelincuentes para acceder a dicha red. Para asegurar esta conexión es recomendable crear una o varias redes específicas para estos dispositivos y configurarlas como zona desmilitarizada o DMZ [8].
- **Servicios y permisos mínimos.** Algunos fabricantes pueden dejar habilitados servicios o herramientas que realmente no son necesarios para que el dispositivo cumpla con su función. Cuantos más servicios tenga instalados y habilitados, más posibilidades habrá de que alguno de ellos pueda ser vulnerable, y por tanto, ser objetivo de los ciberdelincuentes. La configuración más segura será habilitar los servicios y permisos precisos para que el dispositivo pueda cumplir con sus

funciones y deshabilitar el resto. Asimismo, cambiar su contraseña [9] de fábrica por defecto es otro de los pasos imprescindibles para aumentar su seguridad.

- **Restricciones de acceso.** Existe una gran variedad de dispositivos IoT que han sido concebidos para estar desplegados tanto dentro como fuera de las instalaciones corporativas. Al tratarse de dispositivos que manejan información importante es indispensable asegurar que nadie pueda manipularlos ni acceder a la información que aloja el dispositivo. Por ello, es importante poner todas las medidas físicas necesarias para evitar cual manipulación indebida.
- **Estar al día de las amenazas.** Conocer en detalle cuáles son los principales problemas de ciberseguridad que amenazan a las empresas [10] es una valiosa línea de defensa contra los ciberdelincuentes. La suscripción al boletín de avisos [11] de Protege tu empresa, de INCIBE, te permite estar al día de las posibles vulnerabilidades que puedan afectar a tus dispositivos IoT, así como cualquier otra amenaza que pueda poner en riesgo la seguridad de tu organización.
- **Evitar errores humanos.** El error humano puede poner en peligro los sistemas, y por ende, la información de la organización. Contar con un plan de formación [12] en ciberseguridad en la empresa permitirá una mejor gestión de las tecnologías por parte de todo el personal, disminuyendo así el riesgo de sufrir un incidente de seguridad que ponga en riesgo la continuidad del negocio [13].

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Guía – Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/seguridad-instalacion-y-uso-dispositivos-iot-guia-aproximacion-el

[2]. INCIBE - Protege tu empresa – Temática IoT https://www.incibe.es/protege-tu-empresa/tematicas/iot

[3]. INCIBE - Protege tu empresa – Blog – Asegura tus cuentas de usuario con la autenticación de doble factor https://www.incibe.es/protege-tu-empresa/blog/asegura-tus-cuentas-usuario-autenticacion-doble-factor

[4]. INCIBE - Protege tu empresa – Blog – ¿Por qué cifrar la información sensible? https://www.incibe.es/protege-tu-empresa/blog/cifrar-informacion-sensible

[5]. INCIBE - Protege tu empresa – Blog – Recomendaciones de seguridad en el empleo de redes VPN https://www.incibe.es/protege-tu-empresa/blog/recomendaciones-seguridad-el-empleo-redes-vpn

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

[7]. INCIBE - Protege tu empresa – Blog – Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades https://www.incibe.es/protege-tu-empresa/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

[8]. 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

[9]. Incibe – Protege tu empresa – Blog – Día Mundial de las Contraseñas, ¿aún utilizas 123456? https://www.incibe.es/protege-tu-empresa/blog/dia-mundial-las-contrasenas-aun-utilizas-123456

[10]. Incibe - Protege tu empresa - Guía - Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/blog/ciberamenazas-entornos-empresariales-guia-aproximacion-el-empresario

[11]. Incibe - Suscripción a boletines de INCIBE https://www.incibe.es/suscripciones

[12]. Incibe - Protege tu empresa - Formación https://www.incibe.es/protege-tu-empresa/formacion

[13]. Incibe - Protege tu empresa - ¿Qué te interesa? -Plan de Contingencia y Continuidad de Negocio https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio