Sidertia

IMPLEMENTACIÓN DEL TELETRABAJO EN PEQUEÑOS ORGANISMOS Y AYUNTAMIENTOS

Recursos para permitir el teletrabajo

CONTENIDO

- Servicios y tecnologías para teletrabajar.
- El correo electrónico como herramienta fundamental.
- Compartición y edición de documentos corporativos.
- Mensajería instantánea y reuniones virtuales.
- Medidas de seguridad a adoptar durante el teletrabajo en pequeños organismos y ayuntamientos.

INTRODUCCIÓN

- En estos **momentos complicados con la crisis de Covid-19**, muchas pequeñas organizaciones y organismos han visto como, casi de forma obligada, han tenido que buscar soluciones imaginativas para poder habilitar el teletrabajo a sus empleados.
- Muchas de ellas habrán encontrado **grandes dificultades**, sobre todo si no se habían previsto con antelación mecanismos de acceso remoto o de colaboración entre usuarios.
- En esta sesión se analizarán algunas **soluciones eficaces, fáciles de implementar y de costes reducidos**, que permiten hoy en día habilitar el teletrabajo, sin dejar de lado los importantes aspectos de la **seguridad** que siempre se deben adoptar, independientemente de la situación o la urgencia de tener el servicio disponible.

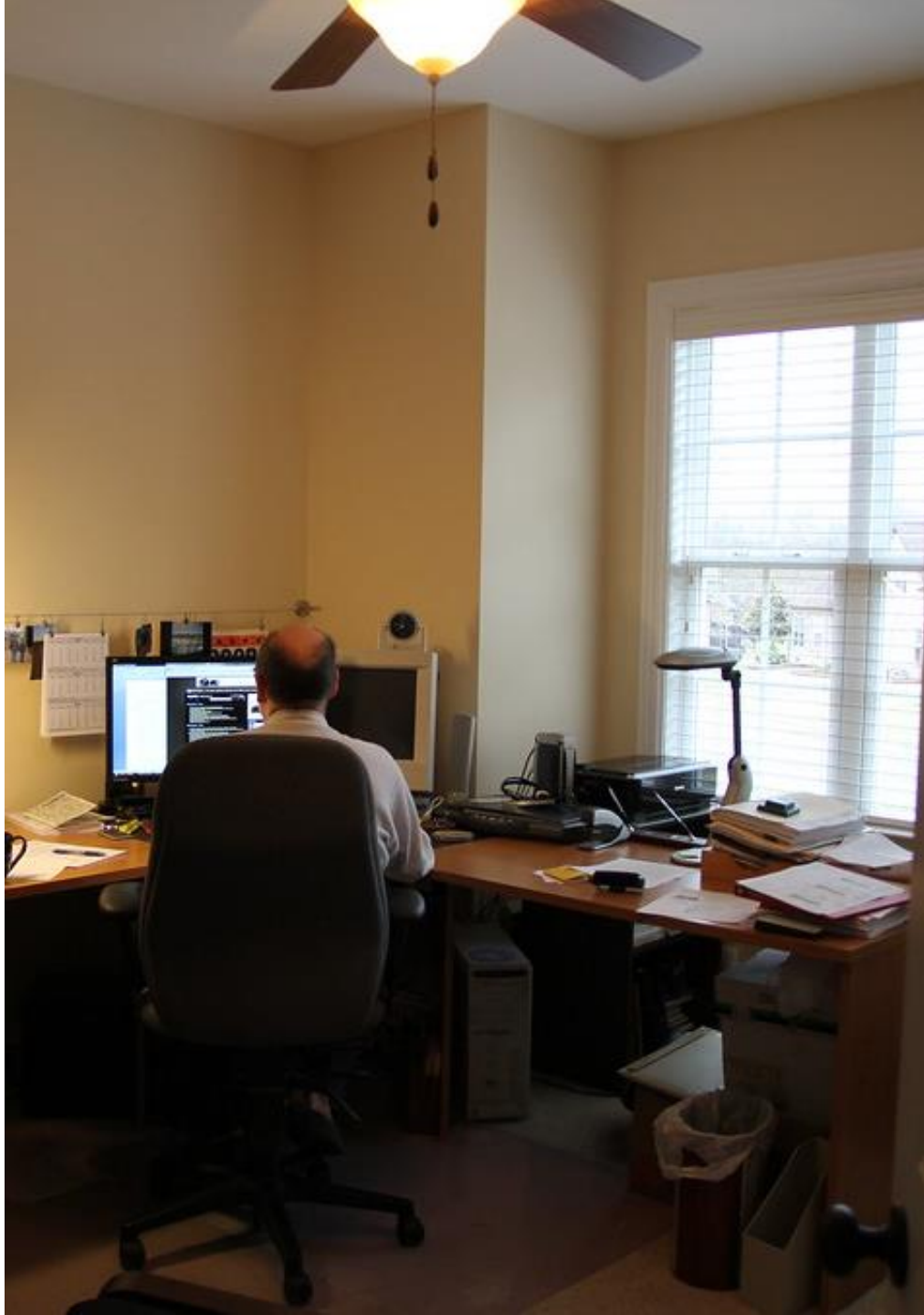
Sidertia

SERVICIOS Y TECNOLOGÍAS PARA TELETRABAJAR

Sidertia.Sistemas

SITUACIÓN ACTUAL

- Las **pequeñas organizaciones** no suelen disponer de tecnología para el **teletrabajo** debido a diversos factores**:**
  - Costes de implementación.
  - No había existido una necesidad real hasta ahora.
  - El desarrollo fundamental de la actividad no está relacionado con acciones que puedan realizarse desde casa.
  - Otros (Medios tecnológicos, soluciones adaptadas a las necesidades, etc.).
- El **Covid-19 ha obligado a:**
  - Buscar soluciones en el mercado.
  - Desplegar rápidamente y sin planificación medios para el teletrabajo.
  - Hacer uso de otros medios y soluciones no estudiadas (no solo lo relativo a la tecnología).
- Esto puede llevar a tener que **asumir unos riesgos excesivos** en materia de seguridad.
- Estos riesgos deben ser **identificados, analizados y minimizados**.



SERVICIOS Y TECNOLOGÍAS PARA TELETRABAJAR

- Afortunadamente, existen hoy en día soluciones que permiten de una forma **rápida y segura** habilitar capacidades de teletrabajo, sin necesidad de implementar complejas arquitecturas.
- Cuando se selecciona una solución se **deberá tener en cuenta**:
  - Ámbito de aplicación requerido.
  - Requerimientos técnicos.
  - Facilidad de puesta en marcha.
  - Coste.
  - **Seguridad.**

Ámbito de aplicación requerido

- No todas las pequeñas organizaciones tienen las **mismas necesidades**.
- Es **fundamental identificar** donde se encuentra la necesidad tecnológica y cubrir dicha necesidad con la solución adecuada:
  - Necesidad de **acceso remoto** a los servidores y estaciones de trabajo de la organización.
  - Necesidad de **compartir y colaborar** en documentos entre usuarios.
  - Necesidad de **comunicación y mensajería** instantánea.
  - Necesidad de **videoconferencia** y reuniones virtuales.
  - Necesidad de espacios de trabajo "**modern workplace**": en cualquier sitio, en cualquier momento, desde cualquier dispositivo.

Requerimientos técnicos

- Desde el punto de vista de requerimientos técnicos, las **soluciones basadas en la nube** permiten disponer de soluciones completas **sin ningún tipo de instalación**.
- Las **soluciones locales** habitualmente van a requerir un proceso de **instalación, configuración y puesta en producción**.
- El **cumplimiento normativo, los costes y la seguridad** de cada solución harán decantar la balanza hacia la nube, hacia en entorno local (onPremise) o una solución híbrida.
  - En una solución local, a mayor número de servicios, mayor complejidad.
  - En una solución de nube los servicios se aprovisionan y se despliegan en conjunto, sin incrementar la complejidad.

Facilidad y agilidad de puesta en marcha

- Aspecto **clave** ante la emergencia Covid-19.
- El teletrabajo debe estar **habilitado en cuestión de horas** o días.
- En muchas ocasiones **no será posible iniciar un proceso de contratación** para la adquisición de hardware, software o servicios profesionales.
- Se deberá encontrar una solución cuyo **tiempo de puesta en producción sea el mínimo** posible.
- Todo ello sin dejar de lado, otro aspecto clave: **la seguridad.**

Coste de la solución

- En la mayoría de los casos, el **coste será el elemento fundamental** de toma de decisión.
  - Solución de nube o local.
  - Solución temporal o permanente.
  - Pago por uso, pago por reserva de recursos (EA) o licenciamiento tradicional de software.
  - Solución para todos los empleados o para una parte de ellos.
- Todas estas cuestiones **tendrán un impacto directo** en el coste de la solución seleccionada.

Sidertia

Seguridad

- La **falta de previsión** y la necesidad de una solución rápida puede hacer que expongamos innecesariamente a la organización a un **alto riesgo de seguridad**.
- La solución seleccionada deberá cumplir con unos **mínimos de seguridad**:
  - Autenticación de **doble factor**.
  - Canales de **acceso remoto cifrado** con algoritmos fuertes.
  - Control de usuarios basado en **roles**.
  - Registro de accesos y **auditoría**.
  - Capacidad de **cifrado** de documentos **en tránsito y en reposo**.
  - Control de la seguridad basado en **directivas**.
  - **Con soporte** de fabricante o proveedor de servicios.

OBJETIVO: Seleccionar la mejor solución para cada caso

- La decisión debe **girar en torno a la seguridad**.
- Estamos permitiendo el acceso a la red local y/o documentación sensible y por tanto a **posibles intrusiones no autorizadas**.
- Se deben **evitar soluciones gratuitas sin soporte** o de procedencia desconocida.
- Despliegues rápidos y masivos pueden forzar a que **no se adopten las medidas de seguridad adecuadas** y necesarias para el teletrabajo.
  - Enfoque tradicional de funcionalidad frente a seguridad.
  - Imprevisión y descontrol.

Soluciones existentes para cada necesidad

- **Acceso remoto** a los servidores y estaciones de trabajo de la organización
  - Servidores VPN.
  - Servidores VDI.
  - Acceso remoto a escritorios físicos.
  - Publicación de aplicaciones remotas.
- **Compartir y colaborar** en documentos entre usuarios.
  - Correo electrónico.
  - Gestores documentales.
  - Almacenamiento compartido en la nube.
- **Comunicación y mensajería instantánea.**
  - Correo electrónico.
  - Chat de texto.
  - Mensajes de voz y video.
- **Videoconferencia y reuniones virtuales.**
- **Espacios de trabajo "modern workplace"**
  - Acceso desde cualquier sitio, en cualquier momento y desde cualquier dispositivo.
  - Gestión remota de dispositivos móviles y portátiles.
  - Acceso condicional a servicios.
  - Aplicaciones para dispositivos móviles y tablets.
  - BYOD controlado y seguro.

EL CORREO ELECTRÓNICO COMO HERRAMIENTA FUNDAMENTAL.

Sidertia.Sistemas

EL CORREO ELECTRÓNICO COMO HERRAMIENTA FUNDAMENTAL

- A pesar de los años y la introducción de otras herramientas de colaboración, el correo electrónico sigue siendo la **pieza clave de la comunicación** de las organizaciones.
- Se trata de un servicio **critico** y el principal vector de **introducción de malware**.

EL CORREO ELECTRÓNICO COMO HERRAMIENTA FUNDAMENTAL

- Se deben **revisar y reforzar** las medidas de seguridad en el teletrabajo.
  - En instalaciones locales, se recomienda habilitar el acceso Web al correo a través de **proxy con inspección de tráfico y detección de intrusión**.
  - En suscripciones de nube, se recomienda **habilitar MFA** y controlar el acceso al correo desde **dispositivos y orígenes autorizados**.
- En ambos casos:
  - **Reforzar las medidas de detección** de malware, SPAM y Phishing.
  - Revisar y actualizar los **planes de contingencia** en caso de incidentes de seguridad o caída del servicio.

Sidertia

COMPARTICIÓN Y EDICIÓN DE DOCUMENTOS CORPORATIVOS.

Sidertia.Sistemas

COMPARTICIÓN Y EDICIÓN DE DOCUMENTOS CORPORATIVOS

- Acción habitual en cualquier entorno de trabajo.
- Antes de compartir información sensible será necesario tomar algunas medidas:
  - **Revisar y reforzar los permisos** y el control de acceso a los almacenes de datos.
  - Habilitar el **registro y la auditoría** de la solución.
  - Limitar mediante directivas la **compartición con usuarios externos** o anónimos.
  - Los usuarios deben **compartir únicamente lo necesario** en cada momento.
  - Establecer niveles de criticidad de la información y **etiquetas de sensibilidad**.
  - Aplicar mecanismos de **derechos de información** y cifrado.
  - En el caso de soluciones de nube:
    - Debe ser una **solución corporativa**, controlada por la organización.
    - **No se recomienda utilizar servicios gratuitos** de almacenamiento en la nube. Estos servicios están destinados a usuarios finales y no a organizaciones.
    - Se debe **limitar el acceso de aplicaciones** de terceros a la información contenida.

Sidertia

MENSAJERÍA INSTANTÁNEA Y REUNIONES VIRTUALES.

Sidertia.Sistemas

MENSAJERÍA INSTANTÁNEA Y REUNIONES VIRTUALES

- Servicio **muy utilizado** en estos días.
- Se trata de un servicio con **altos requerimientos** de capacidad y rendimiento.
  - Habitualmente se contrata como servicio de nube.
- Muchas aplicaciones ofrecen videollamadas y mensajería, pero **no todas son seguras o confiables**.
- Las organizaciones deben seleccionar **soluciones corporativas**, en ningún caso hacer uso de aplicaciones gratuitas.
  - Las soluciones corporativas permiten aplicar **directivas de seguridad y control.**
- Algunas medidas recomendables:
  - Controlar y limitar el acceso externo y el acceso de invitados.

Sidertia

MEDIDAS DE SEGURIDAD A ADOPTAR DURANTE EL TELETRABAJO EN PEQUEÑOS ORGANISMOS Y AYUNTAMIENTOS.

Sidertia.Sistemas

MEDIDAS QUE PUEDEN ADOPTAR LOS USUARIOS EN SUS DOMICILIOS

- Preferiblemente hacer uso de una **conexión por cable y deshabilitar la WiFi** mientras se está teletrabajando (si es posible).
- En caso de no ser posible utilizar una conexión por cable:
  - Uso de protocolos seguros de WiFi (WPA2+AES).
  - Cambiar la clave WiFi predeterminada por una de alta complejidad y longitud.
  - Cambiar la contraseña predeterminada de acceso administrativo al router por una de alta complejidad y longitud.
  - Deshabilitar WPS
  - Desconectar otros dispositivos de la red WIFI. (equipos con sistemas operativos obsoletos, móviles personales, dispositivos electrónicos).
  - Ocultar el SSID de la red a la que se conectan los dispositivos.
  - Crear una red WiFi específica para conectar los dispositivos de trabajo o aquellos dispositivos personales que vayan a ser usados para teletrabajar.
  - NUNCA hacer uso de redes WiFi compartidas.
- Habilitar un espacio de trabajo adecuado en las instancias de la casa que impidan la obtención de información por agentes externos.

MEDIDAS QUE PUEDEN ADOPTAR LOS USUARIOS EN SUS DOMICILIOS

- Crear una **cuenta local sin privilegios** para uso exclusivo del teletrabajo, sobre todo en equipos no pertenecientes a la organización.
- Generar cuentas **diferenciadas** de las cuentas profesionales habituales.
- Establecer siempre **contraseñas complejas** y de una longitud mayor a 8 caracteres para cualquier tipo de servicio.
- **Bloquear la sesión** cuando no esté en uso.
- Evitar navegar por **paginas web de dudosa seguridad o poco confiables**.
- Atender a alertas y comportamientos anómalos. **Avisar de inmediato al soporte técnico** de la organización.

MEDIDAS ADICIONALES

- Comprobar e instalar las últimas actualizaciones de seguridad.
  - Sistema operativo.
  - Productos y aplicaciones.
  - Drivers o controladores.
- Implementar siempre que sea posible un doble factor de autenticación (2FA).
  - Tokens físicos de acceso.
  - Aplicaciones de autenticación
  - Mensajería SMS.
  - Certificados.
  - Smartcards.
  - Biometría.

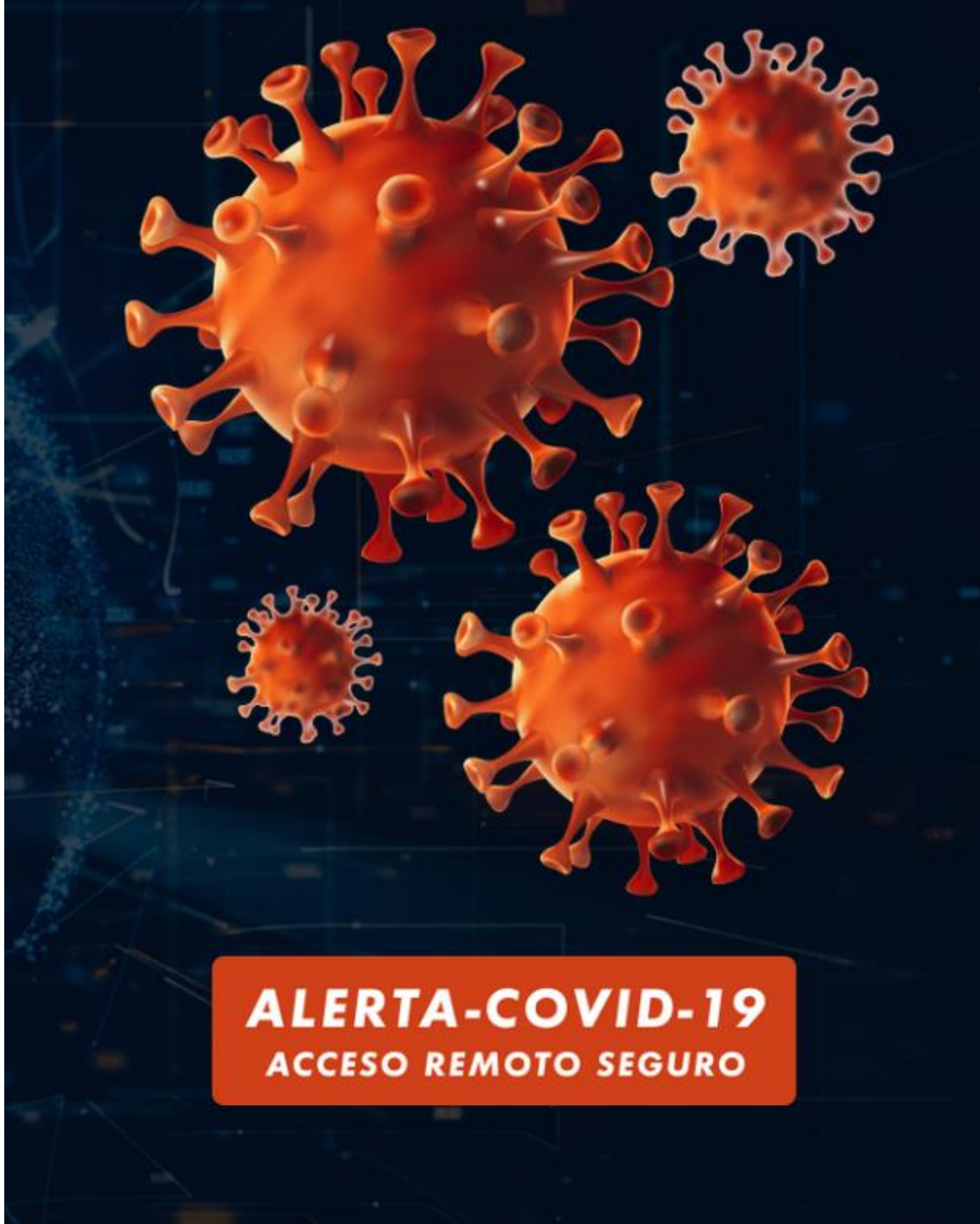
MEDIDAS ADICIONALES

- Limitar al máximo las funcionalidades de los servicios y aplicaciones utilizados, sobre todo en los accesos remotos a equipos de la organización.
- Evitar el uso de soluciones no corporativas y/o personales de correo para el intercambio de datos del organismo (Gmail, Outlook, Hotmail, etc.).
- Evitar soluciones no seguras para el almacenamiento de datos, de dudosa confianza, o que no garantizan 100% la seguridad de los datos almacenados.
- Aplicar medidas de seguridad adicionales sobre la información compartida (cifrado de ficheros).

Sidertia

MEDIDAS DE SEGURIDAD A ADOPTAR DURANTE EL TELETRABAJO

- Sidertia Solutions ha elaborado una guía rápida de **DIEZ MEDIDAS DE PREVENCIÓN DE INCIDENTES** de seguridad.
- https://www.sidertia.com/soluciones-de-acceso-seguro/



Sidertia

MEDIDAS DE SEGURIDAD A ADOPTAR DURANTE EL TELETRABAJO

1. Auditoría

Activa las **Auditorías de los sistemas de acceso perimetral.** Debes saber quien se conecta, a qué hora y desde que dirección IP.

2. Backup

Revisa tus **planes de copia de seguridad** y realiza **test de recuperación** de servicios completos.

3. Parches

Actualiza todos los sistemas y equipos cliente con los últimos **parches de seguridad**, especialmente aquellos expuestos a Internet y en el teletrabajo.

4. Ancho de Banda

Incrementa tu **ancho de banda** para garantizar las **conexiones concurrentes** de las **sesiones de teletrabajo**.

CCN-CERT centro criptológico nacional

Sidertia

MEDIDAS DE SEGURIDAD A ADOPTAR DURANTE EL TELETRABAJO

5. Acceso

Limita el acceso de **teletrabajo** a las localizaciones conocidas. Si no tienes sede en Asia, nadie debería poder conectarse desde allí.

6. ENS

Aplica las medidas de seguridad necesarias tomando el **ENS (Esquema Nacional de Seguridad)** como referencia.

7. Redundancia

Refuerza la disponibilidad de tu **infraestructura de teletrabajo**. **Implementa redundancia**.

8. MFA

Implementa doble factor de autenticación de los usuarios que realicen **teletrabajo**

CCN-CERT centro criptológico nacional

MEDIDAS DE SEGURIDAD A ADOPTAR DURANTE EL TELETRABAJO

9. Contingencia

Diseña un **plan de contingencia y continuidad de negocio** en caso de algún incidente **grave de seguridad**

10. MONITOR

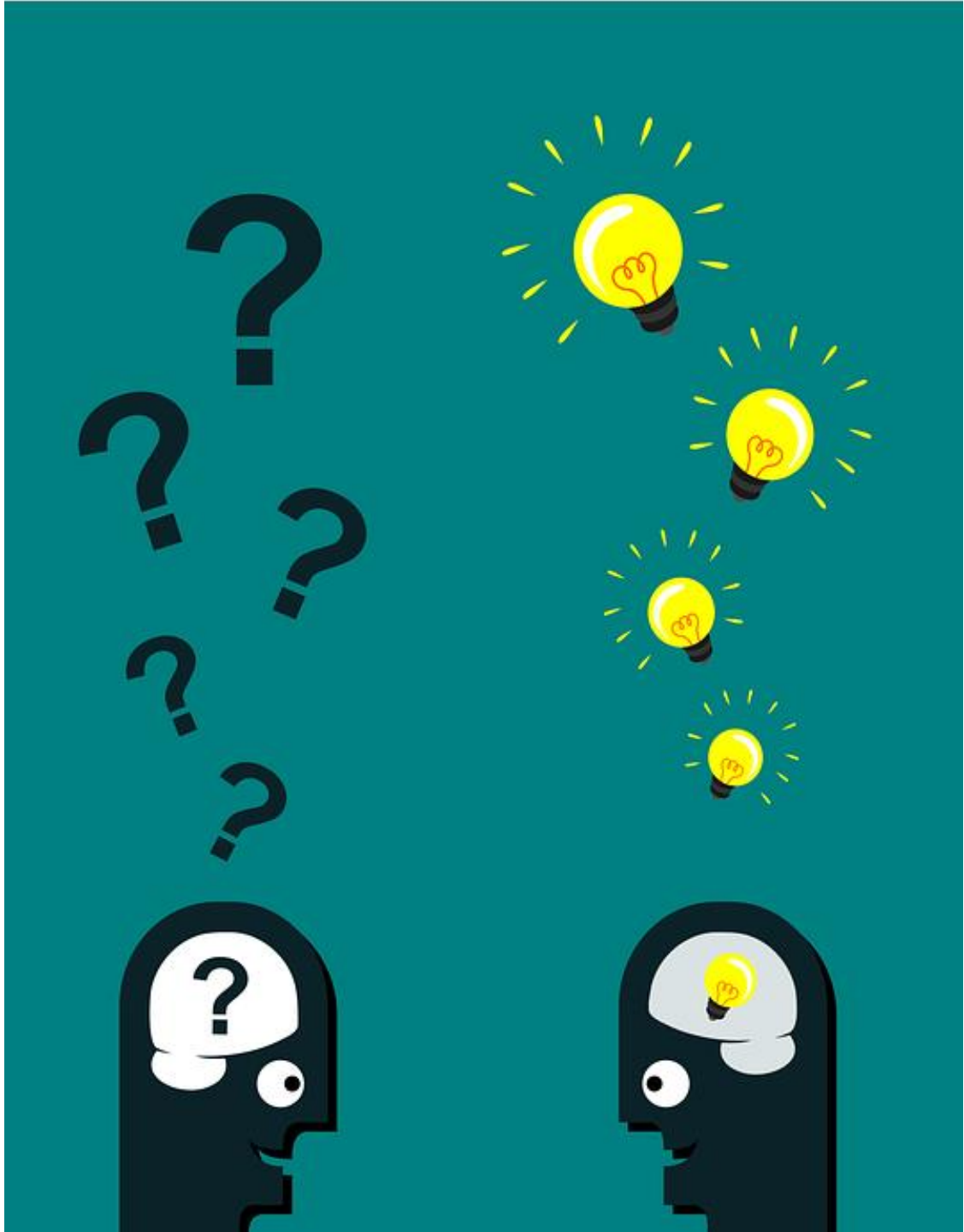
Monitoriza de forma **proactiva y contínua** la seguridad de tu **infraestuctura de teletrabajo**.

CONCIENCIACIÓN DE LOS USUARIOS

- **Ninguna de estas medidas son efectivas si los usuarios no están concienciados con los riesgos y la seguridad.**
  - Identificación de correos anómalos o fuera de lo común.
  - Comprobación de los ficheros descargados.
  - Actualización del sistema operativo y de las aplicaciones.
  - Desconfiar de ofertas, premios, suscripciones gratuitas o correos que no se han solicitado.
  - Los usuarios deben estar formados en el uso seguro de la tecnología.

ANTE LAS DUDAS

- Preguntar.
- Informarse.
- Realizar pruebas.



Muchas gracias

Sidertia Solutions

www.sidertia.com

info@sidertia.com

+34 91 400 64 47