
legitec
legislación y tecnología

¿Quién os habla?

Manuel Moreno Aliaga

Director de consultoría de LEGITEC
CISA, CISM, L.A. ISO27001
Ing. T. Informática, especializado en Seguridad del la Información y Protección de Datos.

Somos LEGITEC

Legislación y tecnología

Es una organización de ámbito nacional especializada en ofrecer servicios de **consultoría, auditoría y formación sobre normativa del sector de las nuevas tecnologías.**

Consultoría, Auditoría y formación relacionada con

Legislación y Tecnología

Experiencia de 20 años en el sector.
Servicio en Murcia, Madrid, Alicante, Córdoba y Sevilla.
Abogados Especialistas en Nuevas Tecnologías.
Informáticos especializados en Seguridad de la Información y cumplimiento normativo.
Auditores CISA, CISM por ISACA, ISO27001…
Procedimientos certificados en ISO9001 e ISO27001.

Gracias por estar aquí

Teniendo en cuenta que estamos hasta los webinars ;)

Teletrabajo

Videoconferencias

La NUBE

E-commerce

ERTEs

Educación y formación

Desescalada

CIBERSEGURIDAD

legitec
legislación y tecnología

“Toda persona tiene derecho a saber porqué, quién, para qué y cómo son tratados sus datos personales y decidir sobre su tratamiento”.

Principios de la protección de datos

Licitud, lealtad y transparencia

Limitación de la finalidad

Minimización de datos

Exactitud

Limitación del plazo de conservación

Seguridad adecuada (Confidencialidad, Integridad y Disponibilidad)

Responsabilidad DEMOSTRABLE

El principio de **responsabilidad activa:**

La necesidad de que el responsable del tratamiento aplique medidas apropiadas a fin de **garantizar y poder demostrar** que el tratamiento es conforme con el Reglamento ante los interesados y ante las autoridades de supervisión. Exige una actitud consciente, diligente y proactiva.

Protección de datos desde el diseño y por defecto:

Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales.

TELETRABAJO

@legitec

GESTIONA EL TELETRABAJO EN TU ORGANIZACIÓN

Equipo de trabajo listo

Usuario específico y sin permisos de administrador.No dejes tu equipo desatendido. El sistema operativo debe estar actualizado a la última versión disponible. El antivirus debe estar activo y actualizado.

Política de mesas limpias

Cuida tu entorno de trabajo.
Mantenlo ordenado y limpio.

No te conectes a redes wifi públicas

Es mejor que te conectes con los datos de tu móvil

Asegura la wifi y tu router

Cambia la contraseña por una más larga y compleja.
Cambia la identificación de la red (SSID) y ocúltala.
Activa el cifrado WPA2-AES.
Limita el número de equipos conectados...

Mientras trabajas:

- Nunca envíes datos sensibles por email.
- No navegues por sitios ajenos a la organización o a tu trabajo.
- Cuidado con el Phishing.
- Desactiva las macros por defecto en documentos Office.
- Mantente alerta ante cualquier situación extraña.

Autorización

Diseña un protocolo de actuación autorizando el teletrabajo de forma temporal

Cuida la información

No dejes información accesibles por terceros, pueden acceder a información que no deben, perderla, romperla, ...

Discos externos y USB

Puede ser una buena idea tenerlo en un disco duro externo, pero en ese caso asegura que lo tienes cifrado

Red Privada Virtual

La conexión debe hacerse mediante VPN para asegurar que el canal de comunicación esté cifrado.

Haz copias de seguridad

Debes asegurar que el lugar donde haces copias es distinto al original (de disco duro a disco externo) y que está protegido (cifrado) y correctamente custodiado.

Si usas móvil:

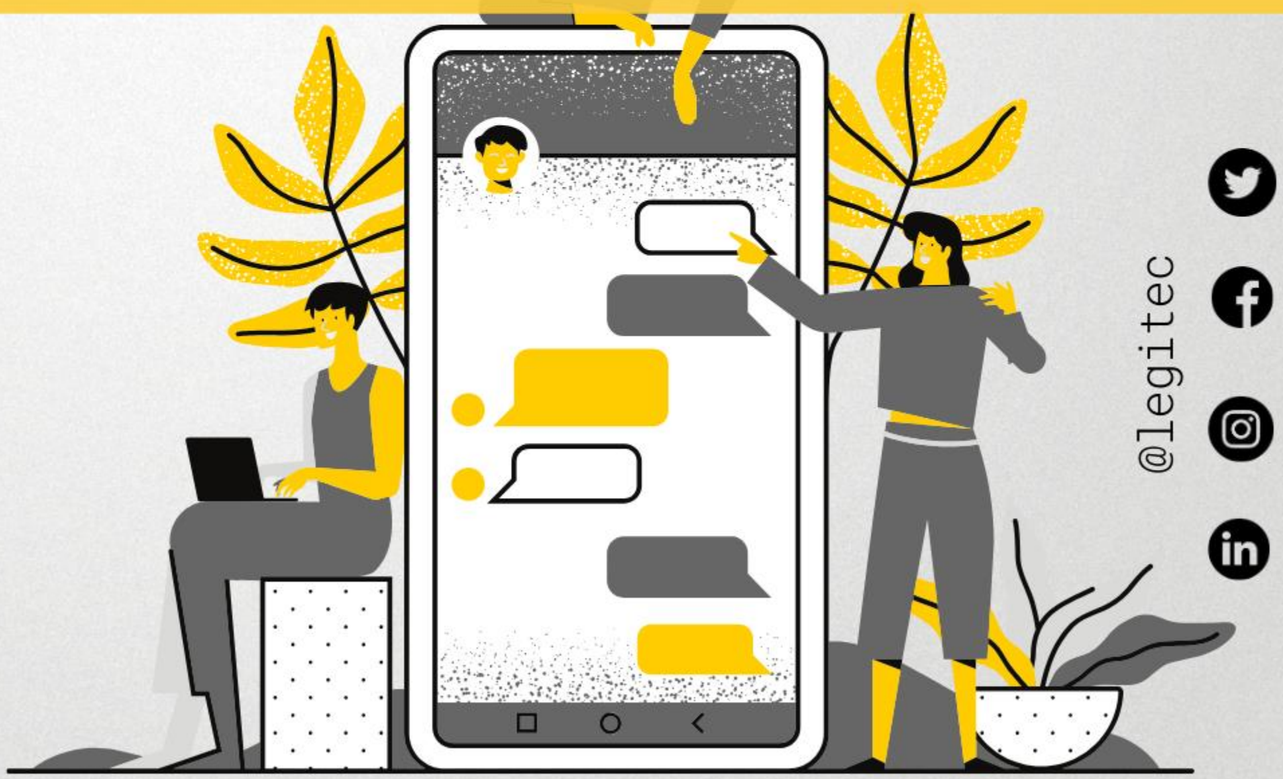
- Activa un método de desbloqueo seguro.
- Elimina la previsualización de los mensajes cuando el móvil está bloqueado.
-Deshabilita la wifi y bluetooth cuando no se utilice.
- Mantenlo actualizado, no pospongas ninguna actualización

Sigue estas pautas y disfruta de un entorno de trabajo seguro

Información en la nube

Lo normal es que se acceda a ella mediante herramientas o vía web con https. Si no asegura una comunicación cifrada no debería utilizarse.

¿ES POSIBLE ACCEDER AL CORREO ELECTRÓNICO DEL EMPLEADO EN SITUACIÓN DE ERTE?



No debe existir ninguna expectativa de privacidad.

La forma más efectiva de evitar esa percepción de privacidad es establecer protocolos que dejen constancia de en qué circunstancias y cómo se podría acceder o redireccionar el correo de un trabajador, dejando claro que se considera una herramienta de trabajo, prohibiendo su uso para fines particulares, y, como tal, podrá ser revisado en caso de incidencias o por ausencia o baja del trabajador, o ser desviado a un responsable o a otro compañero, con la finalidad de no dejar las tareas desentendidas

Habrá que hacer análisis de proporcionalidad… y

Qué medios de grabación se van a poder utilizar.

Dónde van a conservarse estas grabaciones y durante cuánto tiempo.

Cómo se van a solucionar las incidencias que sucedan durante el examen.

Cómo garantizar la adecuada transparencia.

Ya se han producido denuncias

¿Y a los empleados?

¿Y a nosotros en este evento?

legitec
legislación y tecnología

¿La fiebre es un dato personal?

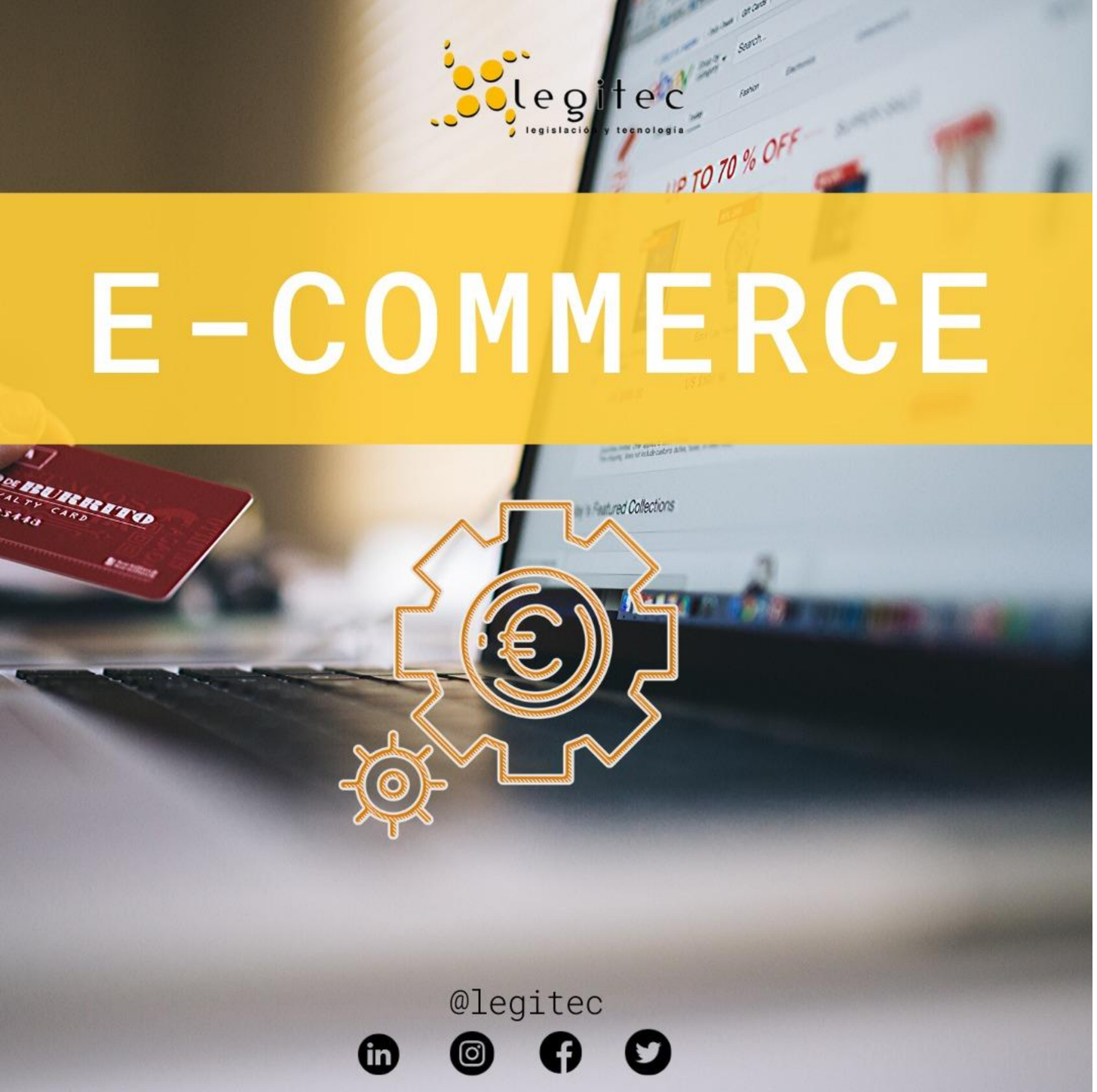
si tomamos la temperatura de nuestros trabajadores , clientes, visitantes, etc. -con la intención de detectar posibles indicios de padecer una enfermedad- estamos tratando un dato personal de salud.

Haciendo el correspondiente **examen de ponderación** podríamos salvar el escollo de la prohibición de tratar datos de salud.

- El consentimiento no vale.
- Interés legítimo tampoco
- ¿PRL?.. A veces, pero ¿y clientes/visitantes?
- ¿Interés general por salud pública? Si lo establecen las autoridades sanitarias, sí.

Deben realizar, con carácter previo, un análisis de riesgos y evaluación de impacto para valorar las medidas de seguridad utilizadas, los datos tratados y la proporcionalidad del tratamiento en sí.

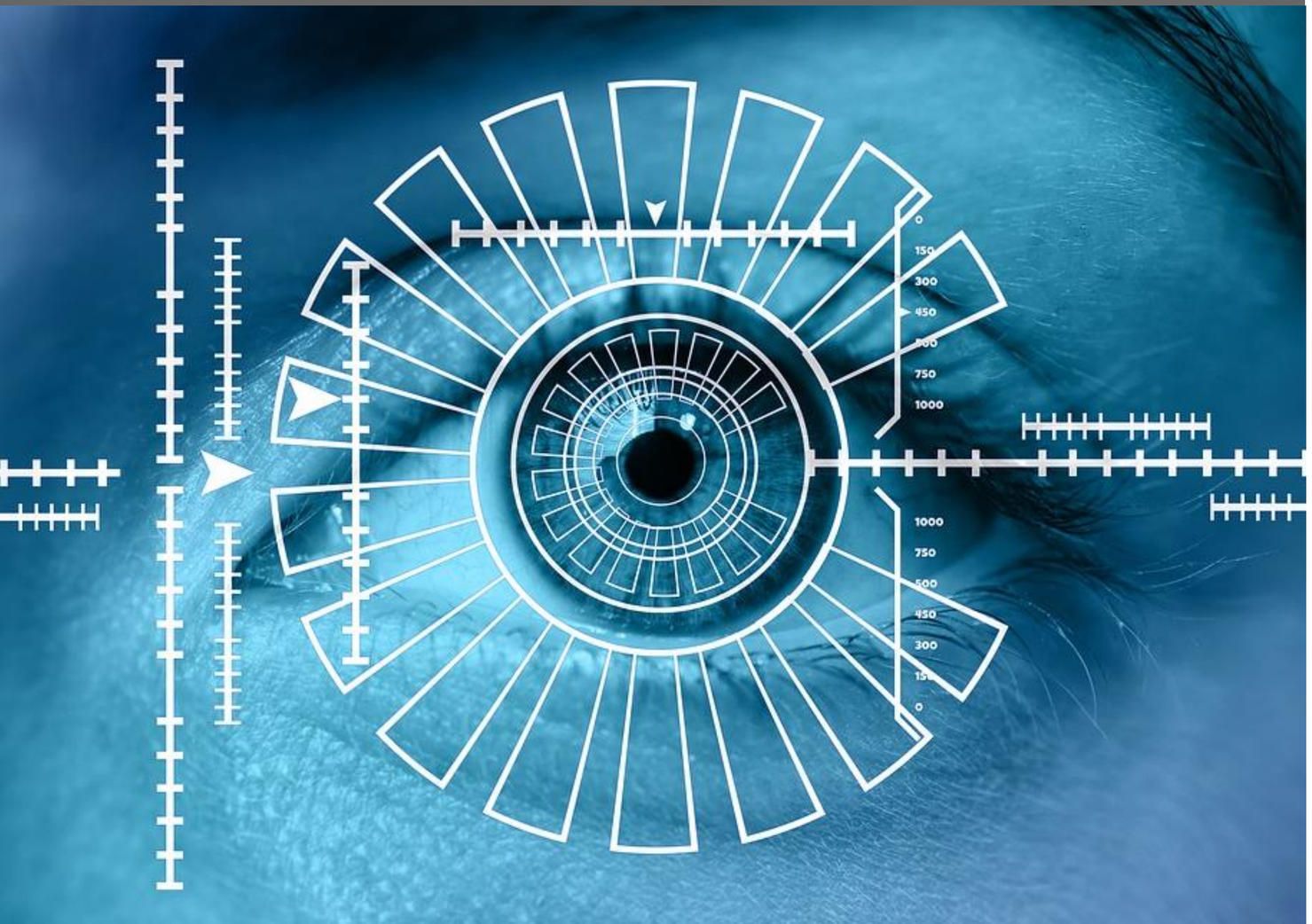
Mucho cuidado con usarlas en empresa



A Vender por internet como sea…

- Protección de datos
- LSSI
- Consumidores y usuarios
- Propiedad Intelectual e industrial
- Cookies

DECÁLOGO:
LA EMPRESA CIBSERSEGURA



1. Política, normativa y cumplimiento legal (concienciación)
2. Control de acceso
3. Copias de seguridad (3x2x1+1)
4. Protección antimalware
5. Actualizaciones
6. Seguridad de la red
7. Información en tránsito
8. Gestión de soportes
9. Registros de actividad
10. Continuidad de negocio

¿Dudas?

Legitec, Consultores y Auditores

Asesórese por verdaderos profesionales en Protección de Datos y Seguridad de la Información

¡Muchas Gracias!

mmoreno@legitec.com

https://legitec.com

+34 968 902 975