



# EL PUESTO DE TRABAJO

## Medidas de protección

El **puesto de trabajo** es el lugar en el que realizamos nuestras tareas diarias en la empresa y es un punto clave en la seguridad de la información. **Son varios los riesgos a los que se expone el puesto de trabajo:**

- Información en papel al alcance de cualquiera.
- Falta de confidencialidad de los medios de comunicación tradicionales.
- Accesos no autorizados a los dispositivos, infecciones por malware, robo de información.

Es necesario que apliquemos un **conjunto de medidas de seguridad** que nos garanticen que la información está correctamente protegida.



### Contrato de confidencialidad

Como empresa contratada, colaborador o empleado tendremos que firmar estos acuerdos **si vamos a tratar información confidencial.**



### Mesas limpias

Al acabar la jornada se debe **guardar la documentación que se encuentre a la vista**, evitando que miradas indiscretas puedan derivar en una fuga de información, además del robo de documentos que pueden contener información confidencial.



### Antivirus y firewall

Tanto el antivirus como el *firewall* o cortafuegos son las herramientas de seguridad que protegen al equipo del software malicioso. **Ambas deben estar siempre activadas**, ya que son complementarias.



### Uso adecuado de Internet y sistemas corporativos

Los dispositivos y recursos que la empresa ofrece están pensados para que sean utilizados para los fines de la organización. **No deben ser usados para cuestiones personales o en circunstancias que puedan afectar a la seguridad de la empresa.**



### Bloqueo de sesión

Todos los dispositivos empleados en el trabajo **deben estar bloqueados cuando no se están utilizando**. Al terminar la jornada dejaremos **siempre los equipos apagados** y si fueran portátiles o móviles, bajo llave.



### Documentación sensible

Es común que en ciertas situaciones algunos empleados hagan uso de información sensible. Cuando este tipo de documentación se encuentra en formato físico, **debe quedar guardada en un lugar seguro al finalizar la jornada laboral.**



### Uso seguro de dispositivos extraíbles

Debido a su uso generalizado tenemos que **minimizar las situaciones de riesgo** como robo, manipulación, extravío e infección por virus. Una buena práctica consiste en cifrar la información e informar de forma inmediata al responsable en caso de pérdida o robo.



### Software legítimo y actualizado

Es obligatorio el uso de software legal. El uso de «programas pirata» podría conllevar sanciones económicas y penales. Además, todos los sistemas de la empresa deben estar actualizados.



### Cómo y cuándo reportar un incidente de seguridad

Una vez identificado el incidente que hemos sufrido: **acceso no autorizado a sistemas o información, denegación de servicio, infección por malware, robo de información de la empresa, etc.**

Pondremos en conocimiento al responsable de la empresa para aplicar las medidas de seguridad más adecuadas.

Si necesitamos apoyo en la resolución del incidente, podemos **ponernos en contacto con la Línea de Ayuda en Ciberseguridad** que ofrece INCIBE por medio del teléfono gratuito 900 116 117 y del correo electrónico [incidencias@incibe-cert.es](mailto:incidencias@incibe-cert.es)

En caso de que el incidente suponga un delito es recomendable **interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.**