



EMPLEADOS

Protección del puesto de trabajo

básico



Normativa de protección del puesto de trabajo.

Informas al personal sobre la normativa de protección del puesto de trabajo y otra normativa asociada llevando a cabo auditorías periódicas para asegurar su cumplimiento.



Sistema operativo actualizado.

Mantienes actualizados los sistemas operativos de los equipos de los usuarios.



Antivirus actualizado y activo.

Mantienes el antivirus actualizado y activo en todos los equipos de los usuarios.



Deshabilitar por defecto los puertos USB.

Deshabilitas por defecto los puertos USB y los habilitas para el personal que necesite dicha funcionalidad.



Seguridad de impresoras y equipos auxiliares.

Verificas la seguridad de las impresoras y equipos auxiliares conectados a la red o que puedan almacenar información (cortafuegos, contraseñas,...).



Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas.

Solicitas al personal informático la instalación de software específico o el cambio de configuración del equipo si es necesario para el desempeño de tu trabajo.



Política de mesas limpias.

Tu mesa de trabajo se encuentra despejada sin documentación confidencial ni dispositivos extraíbles al alcance de otras personas.



Dstrucción básica de documentación mediante mecanismos seguros.

Utilizas las destructoras de papel para eliminar la información confidencial.



No abandonar documentación sensible en impresoras o escáneres.

Recoges inmediatamente aquellos documentos enviados a imprimir y guardas la información una vez escaneada.



EMPLEADOS

Protección del puesto de trabajo

básico



No revelar información a usuarios no debidamente identificados.

Conoces la existencia y peligros de la ingeniería social y la información que no debes desvelar.



Obligación de confidencialidad.

Aceptas y cumples la política de confidencialidad que firmaste al incorporarte al puesto de trabajo.



Uso de contraseñas.

No publicas ni compartes tus claves. Tampoco las anotas en documentos ni en cualquier otro tipo de soporte. Usas contraseñas robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.) Cambias la contraseña periódicamente.



Obligación de bloqueo de sesión y apagado de equipo.

Bloqueas la sesión al ausentarte del puesto de trabajo y apagas el equipo al finalizar la jornada laboral.



Uso adecuado de Internet.

Conoces y aplicas la normativa relativa al uso de Internet.



Uso de portátiles y dispositivos móviles propiedad de la empresa.

Conoces y aceptas la normativa aplicada al uso de portátiles y dispositivos móviles propiedad de la empresa antes de usarlos como herramienta de trabajo.



Obligación de notificar incidentes.

Notificas cualquier incidencia de seguridad (virus, pérdida de información o de dispositivos, etc.).



EMPLEADOS

Protección del puesto de trabajo



Destrucción avanzada de documentación mediante mecanismos seguros.

Destruyes la información confidencial de forma segura teniendo en cuenta el método apropiado para cada soporte de almacenamiento.



Bloqueo programado de sesión.

Programas un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo.



Uso de los medios de almacenamiento.

Conoces y aplicas las políticas relativas al almacenamiento seguro de la información.



Cifrado de la información confidencial.

Conoces y aplicas la normativa relativa al cifrado de la información.

avanzado