SEPTIEMBRE 2020

Buenas prácticas de seguridad orientadas al puesto despejado

Información proporcionada por el Servicio de Seguridad de la Información, D. G. de Telecomunicaciones y Transformación Digital (C. Fomento y Medio Ambiente)

Seguridad de la Información de Castilla y León

La política de *mesas limpias* se orienta a evitar tener accesible en el puesto de usuario la información, tanto confidencial como habitual, que no debiera estar visible y disponible para terceros. Especialmente debemos cuidar estas actuaciones cuando nuestro puesto de trabajo se oriente en un espacio público a la atención al ciudadano, o bien nos encontremos en una de las modalidades de trabajo a distancia.

MESA LIMPIA Y ORDENADA: evita dejar elementos y objetos visibles encima de tu mesa cuando no estás trabajando con ellos. Ordena el material de uso habitual de forma que tenga un fácil acceso, respecto al que no es tan utilizado.

MATERIAL Y DOCUMENTOS: utiliza las cajoneras para aquellos documentos y útiles con los que no estás trabajando en el momento; al finalizar la jornada, recuerda no dejarlos accesibles.

ACCESO CONTROLADO: los archivadores, armarios o salas que contengan informacion confidencial como por ejemplo datos personales, debes mantenerlos cerrados, sobre todo fuera del horario de trabajo.

ORIENTACIÓN DE PANTALLA: intenta posicionar tu pantalla de modo que solo tú leas el contenido, con especial cuidado si hay ventanas o cristaleras a tu espalda. Si atiendes al ciudadano, no deben ver el contenido personas no relacionadas con tu actividad del momento.

BLOQUEO DE PUESTO: al ausentarte, aunque sea de forma temporal, bloquea tu puesto de usuario de modo que no quede accesible para cualquier persona. Cierra tu sesión si compartes el dispositivo.

SESIONES DE USUARIO: en aquellos sistemas y aplicaciones que manejan información confidencial o sensible, cierra tu sesión cuando no vayas a estar presente de forma continuada.

APAGADO DEL EQUIPO: apaga tus dispositivos de trabajo al finalizar tu jornada laboral, verificando que no quedan encendidos y con tu cuenta de usuario abierta.

DISPOSITIVOS MÓVILES: aquellos dispositivos móviles como portátiles y teléfonos inteligentes deben estar vigilados por sus propietarios, no dejándolos desbloqueados y sin prestar atención a los mismos.

ELEMENTOS EXTRAÍBLES: igualmente, no te olvides que un dispositivo de memoria extraíble puede contener información sensible o confidencial. Sigue las mismas recomendaciones que con los documentos. Y cifra la información según su nivel de confidencialidad.

NOTAS: no llenes tu escritorio de notas que contengan contraseñas o información sensible. Intentar esconderlas tampoco es una solución aconsejable.

Si eres empleado público de la Junta de Castilla y León el uso de medios digitales deberá realizarse conforme a la **política de seguridad** de la ACCyL, así como la política de uso de los **servicios de comunicaciones e informática** para todo usuario de los mismos.

Descubre más conceptos sobre buenas prácticas de seguridad orientadas al puesto despejado.