“Tu puesto de trabajo y el equipo informático”

" 8 Consejos prácticos sobre seguridad"

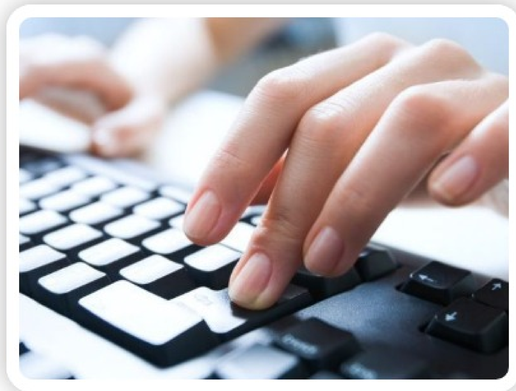
1 Mantén tu **mesa limpia** de papeles y no dejes información confidencial a la vista en tu mesa de trabajo. Cuando hayas acabado con ella, guárdala en un lugar seguro.

No **dejes documentos en la bandeja de la impresora o escáner**
Si tienes que eliminar **documentación confidencial** recuerda utilizar **la destructora de papel** para evitar que se pueda recuperar por un usuario no autorizado.



“Implanta una política de mesas limpias y comprueba que se aplica periódicamente”

2 **Configura el bloqueo del ordenador**



“Te levantas un momento de la mesa, te entretienes en otra cosa, y sin darte cuenta, le has dado a cualquier persona que pase por delante, acceso a tu ordenador, a sus datos y a la red de la organización”

Si el sistema después de un tiempo sin actividad por tu parte, no se bloquea la pantalla y exija identificarse para volver a usarlo, **contacta con cibercentro.**

3 **Reinicia o apaga tu equipo informático periódicamente** para permitir la actualización automática de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.



4 **Usa contraseñas seguras**. Nunca las compartas o las pongas a la vista.

¿Cómo cambiar la contraseña?



“Si a ti te resulta difícil recordarla ¿cuánto más le costará adivinarla a un posible intruso?

5 **No permitas que el navegador guarde o recuerde tus credenciales de acceso corporativo.** Desactiva también la opción auto-completado de formularios

“Tu puesto de trabajo y el equipo informático”

"8 Consejos prácticos sobre seguridad"

6

Utiliza siempre **recursos que la organización pone a tu disposición** para el **almacenamiento de la información.**



Evita almacenar información en dispositivos personales o soportes de los que no se haga copia y carezcan de las medidas de seguridad adecuadas (tales como CDs, DVDs, memorias USB, listados, etc.)



INFO GobBox

Recuerda que tienes a tu disposición **servicios de almacenamiento** de datos que te permite **compartir de forma segura con acceso externo**

7

Haz un **borrado seguro** de la información una vez que ésta ya no sea necesaria.







8

En caso de que **sufra o detecte algún incidente o debilidad** que afecte a la seguridad de la información de los sistemas o de las comunicaciones del Gobierno de Canarias, comuníquelo a **CiberCentro** a través de cualquiera de las siguientes vías



CONTACTO

SÍRVETE

Normativa de seguridad

Para saber más