

Guía de Ciberseguridad para nuevos profesionales del SAS

Para que puedas hacer un uso seguro de los recursos informáticos que te han asignado, y de la información sensible a la que tienes acceso (datos personales y de salud), dedica unos minutos a leer esta breve guía que hemos preparado.

Ciberseguridad Básica

- 🟢 **Familiarízate** con la Política de Seguridad TIC y el Código de Conducta. Son de obligado cumplimiento.
- 🟢 **Conciénciate y fórmate**. Tus conocimientos y habilidades en ciberseguridad mejorarán.
- 🟢 ¿Algo sucedió? **¡Notifica cualquier problema de ciberseguridad!**



Equipamiento Tecnológico, Aplicaciones, Sistemas y Servicios

Acceso (Contraseñas)

- 🟢 Asegúrate de que son robustas. Conforme a las normas y procedimientos establecidos (mira nuestra recomendaciones).
- 🟢 ¡Cámbiala! Cada 6 meses, sin esperar a que te avisemos.
- 🟢 Jamás la compartas, sin excepción.

Uso

- 🟢 ¡Sé responsable! Sólo para fines profesionales. No son para uso personal. Y no prestes nada.
- 🟢 ¡No te la juegues! Los programas piratas, sin licencia o no autorizados están terminantemente prohibidos.
- 🟢 Una acción sencilla: Bloquea o cierra tu sesión. ¡Ah! Y apaga tu equipo al finalizar tu jornada laboral, salvo en aquellos casos autorizados para que quede encendido.



Información y Datos Personales

Trabajamos con información especialmente sensible: datos personales y de salud de nuestros usuarios y profesionales, investigaciones médicas, nuevos medicamentos, etc. Para ello considera:

- 🟢 **Confidencialidad y secreto profesional**. Evita cualquier situación delictiva como manipular, destruir, robar, revelar o usar información sin autorización.
- 🟢 **Protégelos**, tanto en soporte informático como en papel.



Correo Electrónico y Navegación Segura

- 🟢 **Haz buen uso y utilízalo**. Únicamente para fines profesionales y para nada más. Consúltalo frecuentemente durante tu jornada laboral para no demorar tu trabajo.
- 🟢 **No bajes la guardia y desconfía**. Sólo estando alerta podrás reducir la probabilidad de caer en una trampa de phishing (correos fraudulentos).
- 🟢 **Actúa con prudencia**. Para ello, sigue estas reglas:
 - 🕒 N.º 1. **No pulses nunca en los enlaces** de estos correos maliciosos o no deseados (spam).
 - 🕒 N.º 2. **No abras ni descargues los archivos adjuntos** (malware) de estos mensajes.
 - 🕒 N.º 3. **No respondas** a estos correos electrónicos ni lo reenvíes.
 - 🕒 N.º 4. **No proporciones jamás nombres de usuario, contraseñas y otros datos personales**.
 - 🕒 N.º 5. Si te llega algún correo sospechoso de phishing, **reporta** en ayudaDIGITAL y a la dirección de correo **abuse@juntadeandalucia.es**.
- 🟢 **Navega de forma segura**. Evita visitar web sospechosas y descargar archivos de sitios no confiables.



Proceso Disciplinario. Responsabilidades y Otras Conductas.

- 🟢 **¡No te arriesgues!** El uso irregular, ilícito o ilegal de los recursos TIC y la información, además de ser un delito, dará lugar a la exigencia de las responsabilidades legales que correspondan.



¡Gracias por haber leído esta guía!

Esperamos que te haya resultado útil y te ayude a comprender la importancia de la ciberseguridad para tu trabajo diario.

lajunta.es/sasayudaDIGITALciberseguridad

