ABRIL 2020

Buenas prácticas en el acceso a los sistemas de información

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

El acceso a los sistemas de información incluye tanto el acceso al propio puesto de usuario como a todos aquellos sistemas de información, aplicaciones, recursos y dispositivos auxiliares al equipo principal. Se garantizan las mismas condiciones de seguridad independientemente de la forma de acceso, sin merma de las funcionalidades que se requieran según el nivel de seguridad del sistema accedido.

Identificación: Para acceder a los sistemas de información -tanto en modalidad presencial como no presencial- se te proporciona una cuenta digital única y diferenciada, con credenciales estándar u otro factor añadido, certificado digital, etc.

Cuenta: Tus credenciales -normalmente usuario y clave- de acceso a cuentas, son personales e intransferibles, no las debes compartir con terceros. Utiliza únicamente aquellas que te han sido proporcionadas para acceder a tu equipo y sistemas.

Contraseñas: Sigue las buenas prácticas en la generación de contraseñas y claves de acceso. Sobre todo, si vas a acceder desde ubicaciones diferentes a tu puesto habitual.

Vigencia de acceso: Modifica periódicamente las contraseñas de acceso según el procedimiento adecuado, sobre todo cuando no caducan regularmente. En especial, al iniciar una nueva modalidad de acceso remoto a tu puesto de trabajo.

Accesos: No compartas las cuentas de entrada a las aplicaciones a las que tengas acceso para tu trabajo. Cada persona es responsable de las acciones que se realicen con las cuentas que se le hayan proporcionado.

Permisos: Tienes privilegios de acceso a la información y uso de otros recursos, son permitidos según tus credenciales. No dejes que un tercero acceda a estos con tus permisos, pues debe disponer de los suyos propios.

Bloqueo y apagado: Bloqueo y apagado: Bloquea tu equipo al ausentarte temporalmente de tu puesto con Ctlr+Alt+Supr o Windows+L (Ctlr+Alt+Fin para equipo remoto); al finalizar la jornada apaga tus dispositivos. En especial, aquellos que son móviles y los utilizados en acceso remoto y teletrabajo.

Programas autorizados: No instales clientes de terceros o aplicaciones cuyo uso no está aprobado expresamente por la organización.

Copias: No apuntes en papel ni pósit elementos como nombres de usuario, contraseñas de acceso e información confidencial o sensible. Ten especial cuidado con aquella información de acceso que pueda quedar fuera de las instalaciones habituales si trabajas a distancia.

Incidentes: Si sospechas que tus cuentas han sido comprometidas o que alguien ajeno accede a tus cuentas, cambia inmediatamente la clave mediante Ctlr+Alt+Supr > Cambiar una contraseña y pon incidencia en tu CAU.

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 en el acceso a los sistemas de información.