Buenas prácticas de Seguridad
Junta de Castilla y León

marzo 2020

Buenas prácticas en el acceso a los sistemas de información

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: Bloquea tu equipo al ausentarte temporalmente de tu puesto con *Ctlr+Alt+Supr* o *Windows+L*; 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.

Autenticación
Proceso para verificar la identidad de una entidad que puede ser una persona, un dispositivo o un proceso automático.

Certificado digital
Fichero, generado por una autoridad de certificación de confianza. Permite confirmar la identidad de un usuario (de persona) o sitio web (de servidor) en una red compartida.

Políticas de acceso
Establecen permisos a nivel de organización, ejecutan actuaciones masivas y aplican actualizaciones críticas de forma completa.

Servicio de directorio
Herramienta para la gestión de la información sobre recursos y usuarios en una red de ordenadores.

Acceso remoto
Tipo de modalidad no presencial de trabajo.

El uso de medios digitales deberá realizarse conforme a lo indicado en la **política de seguridad** de la ACCyL y la política de uso de los **servicios de comunicaciones e informática**

Junta de Castilla y León
Consejería de Fomento y Medio Ambiente
Dirección General de Telecomunicaciones y Transformación Digital