POLÍTICA DE CONTROL DE ACCESOS

Un control de acceso efectivo a los sistemas de información es fundamental para preservar la seguridad y, especialmente, la confidencialidad de la información. **CLÍNICA BEIMAN** ha definido la siguiente política, que fija las reglas de acceso para los sistemas, equipos e información en base a los requerimientos legales y de seguridad de la organización, asegurando la protección de la información y, en particular, de los datos de carácter personal, mediante el empleo de normas y buenas prácticas en la selección, uso y conservación de las credenciales y otros mecanismos de acceso a los recursos.

- Como norma general, los usuarios únicamente dispondrán de acceso a la información, equipos, aplicaciones y otros recursos que precisen para el desarrollo de sus funciones, siguiendo el principio de "mínimo privilegio". Cualquier modificación respecto a los permisos inicialmente asignados, requerirán la autorización de los responsables de área.
- Para los sistemas de información, cada usuario estará identificado de manera inequívoca con una cuenta de acceso. Esta cuenta es personal e intransferible permitiendo que los sistemas mantienen la autenticidad y la trazabilidad de las acciones realizadas. Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- El acceso a la red de la organización y a los sistemas de información, se encontrará protegido de modo que se asegure que sólo los usuarios autorizados pueden acceder a los mismos, requiriéndose para ello que los usuarios se identifiquen y se autentiquen mediante el uso de una contraseña o clave, que cumpla con los requisitos de complejidad necesarios.
- **CLÍNICA BEIMAN** ha definido una Política de Contraseñas que especifica las características que estas deben de tener para garantizar un nivel de seguridad adecuado, y en el que se especifican las medidas o pautas que los usuarios deben considerar para un uso seguro de las mismas.
- Los sistemas están configurados para que: la contraseña no sea visible en la pantalla durante el inicio de sesión, se bloquee la cuenta de usuario si se ingresa una clave incorrecta de manera reiterada, y para que se bloqueen los equipos tras un periodo de inactividad, mediante protector de pantalla que requiera una nueva autenticación del usuario.
- Los usuarios son responsables del uso y custodia de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la empresa. En ningún caso deberán de ser comunicadas a otros usuarios o personas, ni se registrarán o escribirán en ningún formato para evitar accesos no autorizados a los sistemas, o que se pueda suplantar la identidad del usuario.
- Los responsables de sistemas o de la configuración e instalación de los equipos, deberán asegurarse que las claves creadas por los fabricantes de software o hardware, serán cambiadas durante la instalación inicial.
- En el caso de que sea necesario su almacenamiento, los responsables de sistemas de la organización garantizarán que estas se conservan cifradas, o de manera que no puedan ser conocidas o accedidas por nadie.
- Ante una baja o ausencia temporal del usuario, el responsable del departamento podrá solicitar al responsable del sistema la cesión de clave o datos a la persona designada por él, para lo cual existirá autorización expresa, y deberán de quedar evidencias al respecto.
- Se realizan revisiones periódicas y programadas de los derechos de acceso, privilegios o permisos de los usuarios verificando que estos disponen de acceso a las utilidades, recursos o sistemas que precisan para el desarrollo de sus funciones, y que se cumple el principio de "mínimo privilegio".

En caso de que necesite más información al respecto, o detecte alguna desviación o incumplimiento de esta política, puede ponerse en contacto con los responsables definidos a tal efecto. Especialmente, no dude en comunicar cualquier incidencia que perciba o sospeche como puede ser que su contraseña ha podido ser conocida por otros usuarios, que sospecha que su identificador de acceso está siendo utilizado por otras personas, o que dispone de acceso a más información o recursos de los que necesita para el desarrollo de sus funciones.

BENJAMÍN RUIZ CARMONA
Dirección