DATOS PERSONALES SENSIBLES

Si bien toda la información que identifica o puede usarse para identificar a una persona debe estar protegida contra el acceso no autorizado, existe un estándar más alto cuando se trata de datos confidenciales. Los datos sensibles son información que, si se divulga públicamente, tiene el potencial de provocar un daño significativo, como discriminación, robo de identidad o fraude financiero. A continuación, se muestran algunas pautas a seguir cuando se trata de datos confidenciales.

SEPA POR QUÉ LO TIENE

- Conozca y documente las razones por las que necesita datos confidenciales antes de recopilarlos
- No recopile datos sensibles que no necesite
- Pregunte a su abogado de grupo si necesita consentimiento antes de recopilar datos confidenciales
- No utilice datos sensibles para propósitos nuevos o diferentes sin consultar con su abogado de grupo.
- Complete una DPIA antes de implementar o cambiar cualquier proveedor, herramienta o proceso que use o recopile datos confidenciales

FÍSICAMENTE SEGURO

- Almacene los datos confidenciales en un lugar seguro con acceso limitado
- No deje los datos confidenciales en su escritorio o de otro modo desatendidos
- Revise los archivos con regularidad y sepa qué tipos de datos confidenciales tiene
- No comparta los datos confidenciales con nadie que no esté autorizado para tenerlos o que no necesite conocerlos.
- No haga copias innecesarias de datos sensibles
- Elimine los datos confidenciales triturando
- No tome fotografías de su espacio de trabajo si se pueden ver datos confidenciales

ASEGÚRELO ELECTRÓNICAMENTE

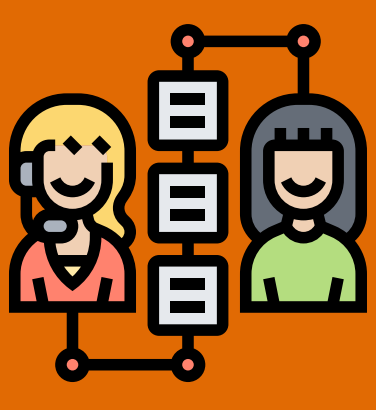
- Almacene, transfiera y procese datos confidenciales únicamente en dispositivos, software, servidores y sitios web aprobados por TI.
- No guarde ni acceda a datos confidenciales en dispositivos personales a menos que estén aprobados previamente por TI.
- Utilice contraseñas seguras o cifrado al transferir o almacenar datos confidenciales
- No comparta ni ponga a disposición sus credenciales de inicio de sesión o claves de cifrado
- No almacene datos personales en su disco duro o escritorio
- Limite los permisos y el acceso a datos confidenciales siempre que sea posible
- No acceda a datos confidenciales desde una conexión Wi-Fi pública no segura

MINIMIZAR LA RETENCIÓN

- No guarde datos sensibles de forma indefinida
- Asignar un período de retención a todos los datos confidenciales cuando se reciben
- No realice copias de seguridad de datos confidenciales en ningún dispositivo o sitio a menos que haya sido aprobado previamente por TI.

INFORMAR PROBLEMAS

- Esté atento a la actividad sospechosa
- No responda a las solicitudes de datos sensibles por correo electrónico o por teléfono a menos que haya confirmado la legitimidad de la solicitud por otros medios.
- Utilice la página de eventos notificables para informar cualquier problema, inquietud o violación de datos confidenciales
- No se demore en reportar incidentes que involucren datos sensibles



SOMOS RPM Y NUESTRO ÉXITO DEPENDE DE QUE CADA UNO DE NOSOTROS SIGA EL CAMINO CORRECTO Y ADOPTE NUESTRO VALOR DE 168® PARA TOMAR LAS DECISIONES CORRECTAS.

CONTÁCTENOS: DATAPROTECTION@RPMINC.COM