2. CÓMO COMPARTIR SUS CONTRASEÑAS DENTRO DE SU ORGANIZACIÓN

TERRE DES HOMMES - LAUSANNE

1. Resumen ejecutivo 1
2. Cómo compartir sus contraseñas dentro de su organización 2

1. Resumen ejecutivo

1.1. Objetivos del tutorial

Después de leer este documento, usted conocerá las buenas prácticas relativas a cómo compartir de manera segura sus contraseñas dentro de la organización.

¿Por qué es importante la manera en la que comparte sus contraseñas de Terre des hommes?

Tener buenas prácticas al momento de compartir una contraseña garantiza que se mantenga la seguridad en el acceso a las aplicaciones dentro de la organización.

1.2. Resumen del documento

Cómo compartir sus contraseñas con seguridad
Comparta sus contraseñas con el debido cuidado, caso por caso, y únicamente si es necesario hacerlo. *No envíe contraseñas o credenciales para el inicio de sesión a través de redes WIFI públicas o no seguras.* *Envíe las contraseñas y las credenciales para acceder a los datos a través de diferentes canales.*

2. Cómo compartir sus contraseñas dentro de su organización[1]

1) **Comparta las contraseñas con el debido cuidado, caso por caso, y únicamente si es necesario.**

   A pesar de que se trata de un consejo para la protección de datos muy enfatizado, todavía hay muchas personas que no siguen este consejo. La verdad es que es poco práctico en el ambiente moderno. En el lugar de trabajo, existen abundantes razones por las que los compañeros de trabajo o socios podrían necesitar compartir las credenciales de inicio de sesión (por ejemplo, las cuentas de Kobo para la recolección de datos móviles). Usted no debe dar sus contraseñas sin reservas; más bien, determine cuándo otra persona requiere legítimamente acceso a su información profesional o cuenta y otorgue el acceso caso por caso. Si otra persona necesita acceso para un propósito único y aislado, puede cambiar su contraseña cuando la tarea haya finalizado y esta persona ya no necesite el acceso.

2) **No envíe contraseñas o credenciales para el inicio de sesión a través de redes WIFI públicas o no seguras.**
   Nunca envíe información de cuentas y contraseñas a través de una conexión inalámbrica abierta (insegura). Si lo hace, estaría transmitiendo a todas las personas dentro del radio de su señal inalámbrica, que puede ser de varios cientos de pies, toda su información profesional e información de cuenta. Estas personas podrían usar esta información para comprometer sus cuentas y robar sus datos de trabajo, o cometer fraude en su nombre.

3) **Envíe las contraseñas y las credenciales para acceder a los datos a través de diferentes canales.[2]**

   Por razones de seguridad, asegúrese de enviar la contraseña a través de un canal diferente al que usará para enviar las credenciales de inicio de sesión y el enlace a los datos, para no arriesgarse a lo que los hackers tengan acceso a estos directamente.

   Por ejemplo, puede enviar la información para el inicio de sesión a través de un correo electrónico y la contraseña a través de Skype/mensaje de texto.
   Este es el mismo concepto que utilizan los bancos cuando envían una tarjeta de débito en un sobre y un código temporal en otro sobre separado, y los envía por correo en diferentes envíos.

[1] Fuente : https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe
[2] Fuente: « Manejo de datos responsable de Oxfam. »