Difusión medidas

Instrucciones:
Esta ficha nos permitirá definir una campaña de difusión de las medidas de ciberseguridad entre nuestros empleados.

1. **Usar contraseñas seguras y únicas**
   - Nuestros empleados deberán crear contraseñas difíciles de conseguir y que no sea la misma que la que usan para el acceso a otras plataformas digitales.
   - Reduce el riesgo de que, si una cuenta es vulnerada, el atacante acceda a otras.

2. **Cerrar la sesión de trabajo**
   - Cada vez que abandonamos nuestro equipo informático debemos cerrar la sesión en nuestro equipo
   - Reduce el riesgo de que nuestro equipo sea accedido en un momento en el que dejamos de trabajar con él por otra persona con fines fraudulentos o peligrosos.

3. **Activar la autenticación en dos pasos (2FA - Doble Factor de Autenticación)**
   - El acceso a nuestro equipo o cuentas de correo debería hacerse introduciendo usuario y contraseña e incorporando un según código que recibiremos por SMS o mediante herramientas como Google Authenticator. Esto se conoce como autenticación de doble factor.
   - Añade una capa extra de seguridad, incluso si la contraseña es robada.

4. **Mantener el sistema operativo y software actualizados**
   - Tener el sistema operativo y los programas que utilicemos actualizados a las últimas versiones que siempre aportan las últimas medidas de protección.
   - Evita que cibercriminales aprovechen fallos de seguridad ya descubiertos.

5. **Usar una red Wi-Fi segura**
   - Acceder a **r**edes i**n**alámbricas que se consideren seguras puesto que si no podemos estar entregando nuestros datos a un tercero. Esto es especialmente importante para los teletrabajadores.
   - Evita que terceros intercepten la información enviada desde tu red doméstica.

6. **Seguridad física de los dispositivos**
   - No permitir el acceso a nuestro equipamiento manteniéndolo en lugares seguros. Es muy importante también para los teletrabajadores.

- Evitamos el acceso a personal no autorizado.

7. **Utilizar una VPN**
   - Cuando estamos desarrollando nuestro empleo como teletrabajadores resulta vital que la comunicación con nuestra empresa se haga de manera segura. Para ello lo más adecuado es crear una Red Privada Virtual (VPN) que hace que la información que enviamos por Internet se envíe cifrada y no se pueda extraer sin conocer las contraseñas utilizadas para cifrarlo.
   - Ocultamos nuestra información en Internet incluso aunque estemos usando una red inalámbrica insegura.

8. **Tener un antimalware actualizado**
   - Cada equipo debería tener instalado un programa de detección y protección ante malware. Malware son programas que se instalan en los equipos para atacarlos de maneras muy diferentes.
   - Protege el equipo contra ataques que puedan robar o destruir datos.

9. **Cifrar archivos sensibles**
   - Tener la información crítica en nuestro equipo guardada con alguna técnica de cifrado que impida acceder a ella sin conocer la clave usada para cifrar.
   - Si te roban el equipo, los datos permanecen inaccesibles.

10. **Hacer copias de seguridad periódicas**
    - Debemos tener una política de realizar copias de seguridad de nuestra información crítica de manera periódica.
    - En caso de ataque (por ejemplo, ransomware que realiza un secuestro de información que se libera tras un pago), puedes recuperar la información.

11. **Evitar hacer clic en enlaces o archivos sospechosos**
    - No debemos acceder a enlaces web o archivos que recibamos por correo electrónico que resulten sospechosos puesto que su ejecución puede conllevar la instalación de un malware o el robo de información.
    - Es una de las formas más comunes de ataque por la curiosidad del usuario de acceder al enlace.