Consideraciones de Ciberseguridad para el Trabajo Remoto

Recomendaciones para los usuarios:

1. **Siga las políticas y utilice herramientas aprobadas:**
   En caso de que su institución cuente con políticas de seguridad y herramientas aprobadas adaptadas para el trabajo remoto, utilícelas! Utilice solamente aquellas herramientas, plataformas y dispositivos autorizados por la Dirección de TIC, ante la duda, consulte!

2. **Contraseñas seguras y autenticación de doble factor:**
   Cuide que todas las cuentas de los funcionarios que estén asociadas a las herramientas de trabajo remoto (Gmail, Outlook, Hotmail, etc.), ya sean personales o corporativas, cumplan los siguientes requisitos:
   - Utilizar contraseñas seguras: al menos 12 caracteres; utilizar mayúsculas, minúsculas, números, símbolos, etc., evite contraseñas fáciles de adivinar, etc.
   - Habilitar autenticación de doble factor. Outlook, etc.)
     Tutoriales:
     - Guia - Autenticacion_Doble_Factor.pdf
     - Google (Gmail, GDocs, etc.): Guía
     - Outlook: Guía
     - Facebook: Guía

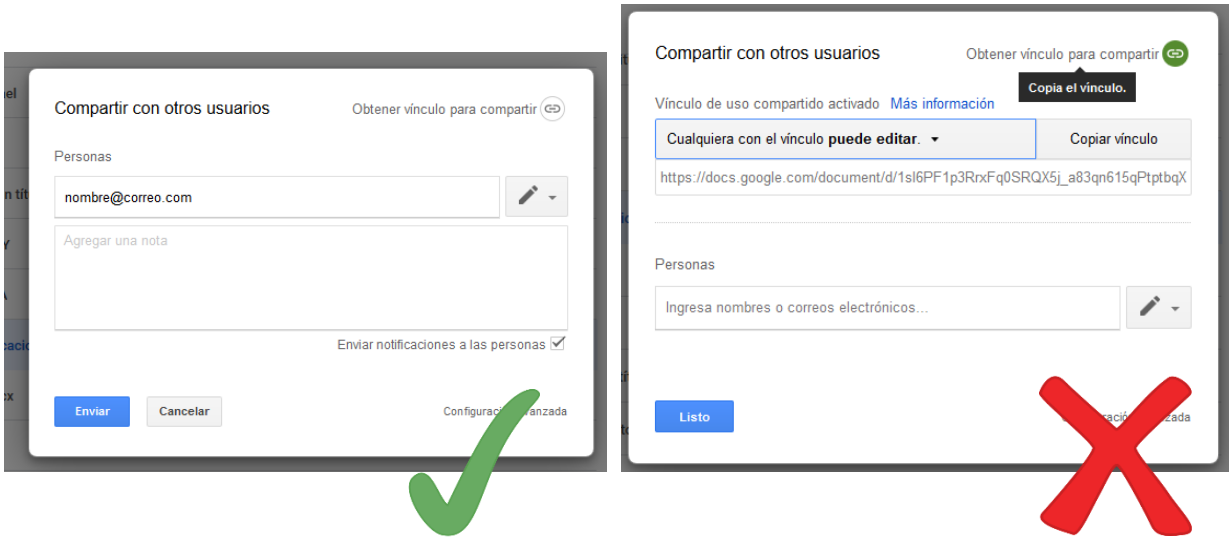
3. **Cifre toda información sensible:**
   En caso de necesidad de compartir información sensible, recuerde cifrarla antes de subirla a Internet. Esto puede ser realizado incluso con herramientas simples como un archivo comprimido con contraseña[1]. La contraseña debe ser enviada a la/s persona/s con quien se desea compartir el archivo por un medio distinto al que se envió el archivo.
   - Guía - Archivo comprimido con contraseña

   Para almacenar archivos sensibles en un dispositivo personal, cífrelos. Puede utilizar técnicas simples como comprimir el archivo con una contraseña. También existen herramientas específicas gratuitas; algunos antivirus cuentas con funcionalidad de cifrado

   - AES Crypt
   - AxCrypt
   - Bitlocker
   - AeroDocs
   - FileVault
   - VeraCrypt

4. **Cuide con quién comparte la información:**
   Si utiliza una herramienta de compartición de archivos como por ej. Google Drive, utilice la opción de compartir el enlace con usuarios específicos. Evite compartir los archivos en modo público o sin autenticación.

[1] Esta técnica no es suficientemente segura para información altamente sensible o secreta; para compartir este tipo de información, evalúe utilizar herramientas específicas más avanzadas que la Dirección de TIC le indique (aplicaciones de cifrado punto a punto).



5. **Utilice antivirus:**
   Todo funcionario que trabajará remotamente desde un dispositivo, ya sea personal o corporativo, debe contar con un antivirus. Existen alternativas gratuitas de uso personal, tales como Windows Defender, Avast, Kaspersky, Comodo, entre otros.

6. **Mantenga sus dispositivos actualizados**:
   Asegurese que todos los dispositivos, tanto personales como institucionales, que utilice para trabajar remotamente, deben estar siempre actualizados, con todos los parches de seguridad instalados.

7. **Conectese a redes seguras**:
   Evite conectarse a redes wifi inseguras. En lo posible, utilice siempre una VPN. Existen alternativas gratuitas como Hotspot Shield,ProtonVPN, Kaspersky VPN, TunnelBear, entre otros.

8. **Cuidado con el phishing**:
   En caso de que reciba alguna comunicación (correo, llamada, mensaje) sospechoso que le solicite hacer click en un enlace desconocido, abrir archivos adjuntos sospechosos y/o revelar alguna información sensible, contacte a la persona que dice haber enviado esa comunicación a través de alguno de los mecanismos de mensajería, para asegurar que la comunicación sea legítima.

9. Cuando retome las actividades laborales de manera normal luego del período indicado, asegúrese de eliminar la información sensible (archivos, datos, conversaciones) de sus dispositivos y cuentas personales, asegurando que todo registro de dicha información quede únicamente en los dispositivos autorizados por su institución.

Para los administradores de TIC:

1. Establezca lineamientos y herramientas simples y seguras para el trabajo remoto de los funcionarios de su institución.

2. Para la administración remota de un servidor o sistema interno de su red, evite publicarlo a Internet, utilice un cliente VPN.
   Tutoriales:
   - Configurar OpenVPN con pfSense: Guía
   - Instalación servidor OpenVPN: Guía
   - Guía completa OpenVPN: Guía

3. Si va a publicar un servicio o plataforma a Internet, utilice contraseñas robustas para todas las cuentas asociadas (al menos 12 caracteres; utilizar mayúsculas, minúsculas, números, símbolos, etc., evite contraseñas fáciles de adivinar). En caso de publicar un sistema web interno, asegúrese que éste no tenga vulnerabilidades o que las mismas se encuentren mitigadas o controladas.
   - Criterios mínimos de seguridad del software: Guía

4. Asegúrese de que todos los funcionarios conozcan los canales de comunicación para reportar problemas o evacuar dudas de seguridad.

Adoptemos entre todos estas medidas básicas para asegurar que el trabajo remoto no sea una razón para reducir los niveles de seguridad!