Jadue Andrade Sarah

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Amenaza | Descripción breve de la Amenaza | Probabilidad (1-10) | Justificación de la probabilidad, Posibilidad o Frecuencia de Ocurrencia de la Amenaza | Impacto (1 a 10) | IT1 | Ctrls. Preventivos | Ctrls. Correctivos | IT2 |
| 1 | Uso no autorizado del dispositivo | El dispositivo puede ser usado por personas diferentes al usuario sin su consentimiento | 6 | En un entorno de trabajo con muchas personas es frecuente que se dejen los dispositivos a fácil alcance de otros | 5 | 30 | Poner una contraseña, PIN o configurar la autenticación biométrica | Revisar el registro del dispositivo para asegurarse que no se haya comprometido ninguna información sensible | 12 |
| 2 | Perdida de información | Los contactos, registros de llamadas, SMS y otra información puede ser modificada y sustraída por un Malware | 5 | Al navegar en internet es común que se descarguen aplicaciones o que se redireccione a paginas fraudulentas | 7 | 35 | Utilizar un software anti malware y antispyware | Eliminar aplicaciones sospechosas  Reiniciar de fabrica las configuraciones | 21 |
| 3 | Vigilancia de los movimientos del usuario | El dispositivo puede grabar audio, imágenes o enviar la posición GPS si se usa un malware | 4 | Al navegar en internet es común que se descarguen aplicaciones o que se redireccione a paginas fraudulentas | 8 | 32 | Utilizar un software anti malware y antispyware | Eliminar aplicaciones sospechosas  Reiniciar de fabrica las configuraciones | 12 |
| 4 | Comunicación insegura | Uso de redes inseguras para la comunicación | 7 | Las redes inseguras pueden ser vulneradas y los usuarios pueden correr riesgos | 6 | 42 | Evitar la conexión a redes libres de contraseñas o a redes que no conozca  No llevar encendido el WIFI todo el tiempo | Cambiar la configuración para no conectarse automáticamente a la red | 24 |
| 5 | Robo del dispositivo | El dispositivo es sustraido para el uso de otras personas | 7 | Es común en nuestro entorno con la inseguridad sufrir un robo | 8 | 56 | Evitar el uso del celular en zonas inseguras  Utilizar manos libres para contestar llamadas | Rastrear el dispositivo  Bloquear el dispositivo  Eliminar los datos del dispositivo | 40 |
| 6 | Distribución de información | La información del dispositivo puede ser enviada a otros con malas intenciones | 6 | Datos confidenciales son buscados para poder poner el usuario en situaciones de riesgo o que afecten su posición | 7 | 42 | Revisar las aplicaciones instaladas y los permisos que tienen  No navegar en sitios web sospechosos | Bloquear sitios web fraudulentos  Eliminar apps sospechosas | 21 |
| 7 | Conexión a redes maliciosas | Las conexiones a WIFI libres pueden ser usadas para acceder al dispositivo | 7 | Las redes abiertas son carnada para acceder a usuarios ingenuos | 6 | 42 | Evitar la conexión a redes libres de contraseñas o a redes que no conozca  No llevar encendido el WIFI todo el tiempo | Cambiar la configuración para no conectarse automáticamente a la red | 18 |
| 8 | Configuración incorrecta de aplicaciones | Aplicaciones gratuitas que pueden contener código malicioso con permisos para acceder a funciones del dispositivo | 8 | Es común modificar las configuraciones de seguridad del dispositivo para poder instalar apps que no están disponibles en la región y garantizar permisos sin pensarlo | 7 | 56 | Revisar las apps que se instalan  Solo garantizar permisos a las que se tenga total confianza  No permitir la instalación de fuentes desconocidas | Eliminar apps desconocidas  Reiniciar a configuración de fabrica | 35 |
| 9 | Acceso a los datos en la nube | Archivos como fotos, documentos y otros asociados a la cuenta del usuario pueden ser sustraídos o modificados | 6 | Con la cuenta del usuario vinculada a su espacio en la nube es sencillo acceder a todos los datos por medio de aplicaciones que no solicitan inicio de sesión | 5 | 30 | Protreger el dispositivo con contraseña  No dejar sesiones iniciadas  Proteger el acceso a las apps | Revisar que no se haya perdido o modificado información  Cambiar contraseña | 15 |
| 10 | Mal uso de información sensible almacenada | Información como números de tarjetas de crédito, contraseñas, etc pueden ser utilizadas por alguien no autorizado | 4 | La posibilidad de recordar contraseñas y vincular tarjetas de crédito a las cuentas hace que sea un riesgo tenerlas sin protección | 8 | 32 | Proteger el acceso a las apps que manejan esta información  No almacenar contraseñas en el navegador | Eliminar las contraseñas guardadas  Cambiar las contraseñas | 8 |