



A este texto legal si no hay mucho que hacerle, no hay frases sarcásticas que valgan, ni la más mínima posibilidad de agregarle humor o irreverencia, porque es duro, denso e impenetrable. Esperamos que nadie argumente que lo que pasa es que estamos alentando a la gente a que no lea los textos legales, porque la verdad es que nadie los lee.

Sin embargo, te sugerimos que apeles a tu sentido común para usar internet y le pegues una ojeada a los temas relevantes del poema de abajo o también puede ser que si quieres, pues lo leas ya que insistes tanto.

RIESGOS RELATIVOS A LA SEGURIDAD DE LA RED Y LAS ACCIONES PARA PRESERVAR LA MISMA Y LAS COMUNICACIONES.

El listado de riesgos debidos a la utilización de nuestros servicios móviles que escapan a nuestros mecanismos de control y a los cuales están expuestos los Suscriptores y/o Usuarios de Virgin Mobile Colombia debido a la naturaleza del medio son:

- Posible infiltración en las comunicaciones al utilizar redes de datos públicas como Internet, para transferir información.
- Robo o fuga de información al enviar datos a través de redes públicas como Internet.
- Robo o fuga de información por la falta de conocimiento y/o por el buen uso que se le dé al dispositivo móvil.
- Daño intencional del móvil y/o alguno de sus componentes de software por la utilización de software no licenciado o por el envío y/o recepción de información a través de redes de datos públicas.
- Problemas de desempeño del equipo móvil y/o alguno de sus componentes de software debido a la administración que se le dé a la información almacenada en él.
- Actividades de espionaje debido al uso que se le dé al dispositivo móvil o al intercambiar datos a través de redes públicas como Internet.



- Uso indebido de las facilidades de software y/o de la información provista por el móvil debido a la no disponibilidad o falta de configuración de las facilidades de control de acceso disponibles en el dispositivo móvil.
- Uso del medio de comunicación para la transmisión de información con fines malintencionados.
- Fomento y/o recepción de mensajes no esperados o de origen desconocido.
- No disponibilidad del servicio de telefonía móvil y/o de valor agregado por motivos de "fuerza mayor".
- Pesca de información, se utilizan mensajes de correo electrónico "engañosos" y sitios Web falsos para pedir información personal a los usuarios. Se pueden reconocer porque ofrecen promociones para recargas. Por eso debes recordar que ese procedimiento sólo se hace a través de Servicio en Línea.
- Correos electrónico que parecen provenir de una compañía reconocida y son fraudulentos. Estos correos deben eliminarse de inmediato porque un simple clic puede producir la instalación de un virus que graba tus actividades en el teclado y con esto obtener tus datos bancarios.
- Mensajes de texto en su celular diciendo que gano un premio y que debe responder con sus datos, debe poner mucha atención pues no es más que una nueva técnica usada por los delincuentes para cometer fraudes a su nombre.

Los clientes en red necesitan que se les garantice que los proveedores aplican prácticas adecuadas de seguridad para mitigar los riesgos a los que se enfrentan el cliente y el proveedor (por ejemplo, los ataques distribuidos de denegación de servicio, o DDoS). Por este motivo, hemos expresado muchas de las recomendaciones del informe en forma de listado de cuestiones que puede ser utilizado para ofrecer o recibir aseguraciones.

- Evaluar el riesgo de utilizar servicios en red.
- Comparar las ofertas de los distintos proveedores en red.
- Obtener aseguraciones de los proveedores en red seleccionados.
- Reducir la carga de la aseguración con respecto a los proveedores en red.
- La lista de comprobación de seguridad abarca todos los aspectos de los requisitos en materia de seguridad, incluidas la seguridad física y las implicaciones legales, políticas y técnicas.

