¿Qué tan seguros estamos en la red?



**TEMA**

**“Delitos informáticos”**

**Materia:** Programación III

**Trabajo final**

**Carrera:** Desarrollo de software.

**Instituto:** Alfredo Coviello.

**Año**: 2022

**Profesor:** Ing. Carla Arias Acuña

**Alumnos:**

* Santiago David Viva
* David Olivera
* Mateo Chávez

# Resumen

Nuestro proyecto trata de una página web de ciberseguridad que les informa a los usuarios todos los tipos de robos de datos que pueden sufrir por medio de la tecnología, informa también las leyes que hay para frenar estos tipos de delitos, como así también los tipos de delitos que hay y como prevenirlos.

**Palabras Clave**

● Seguridad, dato, web.

# Introducción

Nuestro proyecto ***“¿Qué tan seguro estamos en la red?”***, consiste en un sitio web, página web informativa para concientizar a la sociedad sobre los delitos informáticos que pueden sufrir.

El sitio web fue creado con el fin de mejorar y prevenir el mal uso que muchas veces les damos a nuestra computadora, por ejemplo, como navegar por sitios desconocidos, abrir correos spam y dar datos personales a personas que no conocemos.

# Problemática

Actualmente se registran miles de robos informáticos en el mundo perjudicando a personas y grandes empresas que sufren pérdidas millonarias. Muchas veces estos delitos se producen por la falta de conocimiento en el uso de la tecnología. Existen diferentes maneras de estafas informáticas una de ellas es la suplantación de identidad para robar datos personales, como el Phising o el Carding otro método muy utilizado es la ingeniería social.

# Desarrollo

Para prevenir estos tipos de robos, en la página que hemos creado explicamos algunos consejos que realizó un grupo de expertos de Internexa para un uso seguro de internet y evitar fraudes y otros delitos informáticos, creamos también un ítem donde explicamos las leyes que nos protegen y donde comunicarnos en un caso que suframos algún delito.

# Consejos para evitar robos y fraudes informáticos

1. ***Evita dar información confidencial por Internet****.*

Las fechas de cumpleaños, fechas de vacaciones, componentes del grupo familiar, etc. son datos que suelen usar los hackers para empezar a realizar un perfil que los lleva a datos más importantes cómo contraseñas de sitios, tarjetas de crédito o información de la empresa para la que trabajas.

1. ***En las redes sociales evita dar números telefónicos, publicar claves bancarias, y dar direcciones de ubicación.***

Al igual que el punto anterior, esta información al momento de caer en las manos de los hackers puede ser mal intencionada.

1. ***Evita tener archivos en los dispositivos con las claves de acceso.***

Si bien es cierto hay muchos sitios que piden cambiar cada cierto tiempo las claves de acceso, hay que evitar tener las claves por escrito en algún dispositivo electrónico o visibles dentro del campo de tu cámara web.

1. ***Utiliza claves distintas para cada servicio y cámbialas con regularidad.***

Se recomienda no repetir las claves en diversas plataformas y cambiarlas por lo menos cada tres meses.

1. ***Crea contraseñas difíciles de adivinar, combinando números, letras mayúsculas y minúsculas y caracteres especiales***.

Usa tu creatividad y añadí dificultad a tus claves, no uses información personal como fechas de cumpleaños, tu nombre o el de tu núcleo familiar.

1. ***Evita instalar programas si desconoces el fabricante***.

Si no estás 100% seguro del origen de un archivo o programa, no lo instales en ninguno de los dispositivos que uses.

1. ***Evita conectarte a redes públicas.***

Aunque suene atractivo, el conectarse en redes públicas nos puede provocar más de un mal rato, es mejor no hacerlo.

1. ***Utiliza aplicaciones de seguridad en los dispositivos, como antivirus y/o un firewall.***

Estas aplicaciones te ayudan a mantener segura tu información frente a virus o intrusiones no deseadas. Mantenerlas actualizadas para su mejor desempeño.

1. ***Evita ingresar a páginas gratis para bajar música, películas, videos o imágenes.***

Por muy atractivo que sea la oferta o promoción, el riesgo que se corre puede ser mayor a la satisfacción que se pueda lograr. Es mejor no hacerlo.

1. ***Cuando tomes fotos en lugares de trabajo o estudio, evita exponer los logos.***

Algo tan simple puede significar una mayor seguridad, hay que ser cuidadoso con las fotos que publicamos en espacios públicos.

Los expertos advierten que hoy en día, conectarse a Internet es una acción más que cotidiana, pero los ciberdelincuentes están a la espera y aprovechan cada descuido, sea humano o técnico. Con estos simples consejos podes hacer una diferencia en la seguridad de tus datos y de tu familia. La seguridad cibernética comienza con vos.

# Leyes

Hay una falta de información general sobre este tema, por lo que describimos algunas leyes argentinas y artículos del Código Penal que te serán de utilidad. A nivel mundial, cuando se habla de “delito informático” se implican actividades criminales que los países han tratado de encuadrar en figuras de carácter tradicional, tales como robos, hurtos, fraudes, estafas y sabotajes. En algunos países, como Argentina, esto generó que no se creen nuevas leyes, sino que se fueran modificando.

De manera general, podríamos decir que existen cuatro leyes que se encargan de enmarcar distintas figuras delictivas del mundo digital:

1. Ley de Protección de ***Datos Personales (Ley 25326):*** Se caracteriza por definir principios generales relativos a la ***protección de datos***. Esto abarca desde derechos de los titulares hasta las figuras de usuarios y responsables de archivos, registros y bancos de datos. El control, las sanciones, la acción de protección de los datos personales e inclusive el spam están vinculados a esta Ley.
2. Ley de [***Propiedad Intelectual (Ley 11.723):***](http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm) Establece el régimen legal de la propiedad intelectual, es decir, actúa sobre las obras científicas, literarias y artísticas. Además, comprende los “escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto”.
3. Ley de [***Delitos Informáticos (Ley 26.388):***](http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm) Esta no es una ley especial que regula este tipo de delitos en un cuerpo normativo separado del Código Penal con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el Código.

*Principalmente incluye temas como*:

* Distribución y tenencia con fines de distribución de pornografía infantil.
* Violación de correos electrónicos.
* Acceso ilegítimo a sistemas informáticos.
* Daño informático y distribución de códigos maliciosos.
* Interrupción de comunicaciones o DoS.

4. Ley de [***Grooming (Ley 26.904):***](http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm)Esta ley sancionada en noviembre de 2013, tras una intensa campaña de organizaciones a favor, pena un delito que sigue en alarmante aumento. Según su Artículo 1°, que se incorporó como artículo 131 al Código Penal: “Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma”.

Ahora bien, si en algún momento deseas participar en un proceso legal como perito informático, o si simplemente quieres saber la situación legal en el país, seguramente las siguientes temáticas y artículos del [Código procesal penal](http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/383/texact.htm#9) te sean de utilidad:

## Con respecto a la facultad de ordenar las pericias

Art. 253: “El juez podrá ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinente a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica”. Calidad habilitante

Art. 254: “Los peritos deberán tener título de tales en la materia a que pertenezca el punto sobre el que han de expedirse y estar inscriptos en las listas formadas por el órgano judicial competente. Si no estuviere reglamentada la profesión, o no hubiere peritos diplomados o inscriptos, deberá designarse a persona de conocimiento o práctica reconocidos”.

## Incapacidad e incompatibilidad

Art. 255: “No podrán ser peritos: los incapaces; los que deban o puedan abstenerse de declarar como testigos o que hayan sido citados como tales en la causa; los que hubieren sido eliminados del registro respectivo por sanción; los condenados o inhabilitados”. Excusación y recusación

Art. 256: “Sin perjuicio de lo dispuesto en el artículo anterior, son causas legales de excusación y recusación de los peritos las establecidas para los jueces. El incidente será resuelto por el juez, oído el interesado y previa averiguación sumaria, sin recurso alguno”. Obligatoriedad del cargo

Art. 257: “El designado como perito tendrá el deber de aceptar y desempeñar fielmente el cargo, salvo que tuviere un grave impedimento. En este caso, deberá ponerlo en conocimiento del juez, al ser notificado de la designación. Si no acudiere a la citación o no presentare el informe a debido tiempo, sin causa justificada, incurrirá en las responsabilidades señaladas para los testigos por los Art. 154 y 247. Los peritos no oficiales aceptarán el cargo bajo juramento”. Nombramiento y notificación

Art. 258: “El juez designará de oficio a un perito, salvo que considere indispensable que sean más. Lo hará entre los que tengan el carácter de peritos oficiales; si no los hubiere, entre los funcionarios públicos que, en razón de su título profesional o de su competencia, se encuentren habilitados para emitir dictamen acerca del hecho o circunstancia que se quiere establecer. Notificará esta resolución al ministerio fiscal, a la parte querellante y a los defensores antes que se inicien las operaciones periciales, bajo pena de nulidad, a menos que haya suma urgencia o que la indagación sea extremadamente simple. En estos casos, bajo la misma sanción, se les notifica que se realiza la pericia, que puedan hacer examinar sus resultados por medio de otro perito y pedir, si fuere posible, su reproducción”. Facultad de proponer

Art. 259: “En el término de tres (3) días, a contar de las respectivas notificaciones previstas en el Art. anterior, cada parte podrá proponer, a su costa, otro perito legalmente habilitado, conforme a lo dispuesto en el Art. 254”. Directivas

Art. 260: “El juez dirigirá la pericia, formulará concretamente las cuestiones a elucidar, fijará el plazo en que ha de expedirse el perito y, si lo juzgare conveniente, asistirá a las operaciones. Podrá igualmente autorizar al perito para examinar las actuaciones o para asistir a determinados actos procesales”.

## Conservación de objetos

Art. 261: “Tanto el juez como los peritos procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse. Si fuere necesario destruir o alterar los objetos analizados o hubiere discrepancias sobre el modo de conducir las operaciones, los peritos deberán informar al juez antes de proceder”. Ejecución Peritos nuevos

Art. 262: “Los peritos practicarán unidos el examen, deliberarán en sesión secreta, a la que solo podrá asistir el juez, y si estuvieren de acuerdo redactarán su informe en común. En caso contrario, harán por separado sus respectivos dictámenes. Si los informes discreparen fundamentalmente, el juez podrá nombrar más peritos, según la importancia del caso, para que los examinen e informen sobre su mérito o, si fuere factible y necesario, realicen otra vez la pericia”.





# Conclusiones

En conclusión, lo que queremos transmitir es concientizar a las personas de usar de forma correcta el internet y proteger nuestros datos personales para no lamentarnos luego de futuras estafas. Es muy importante usar correctamente el internet y saber que sitios son seguros y cuáles no. Como también es muy importante saber que no debemos brindar información personal por vía telefónica ni por correo electrónico a personas desconocidas.

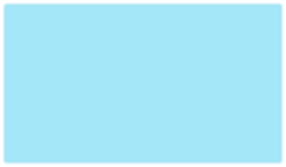
# Sitio Web

Nuestro sitio web del proyecto, fue creado con el editor de código VISUAL STUDIO CODE en donde utilizamos HTML5, CSS3 Y JAVASCRIP.T

HTML5 utilizamos para estructurar y desplegar nuestro sitio web, página web ya que es fundamental para crear sitios web, páginas en internet.

CSS3 utilizamos para darle el diseño a nuestra página web creando una pagina completamente responsive, compatible con todos los dispositivos ya sea celular, tablets o computadoras.

JAVASCRIPT utilizamos para añadir características interactivas a la página que creamos.



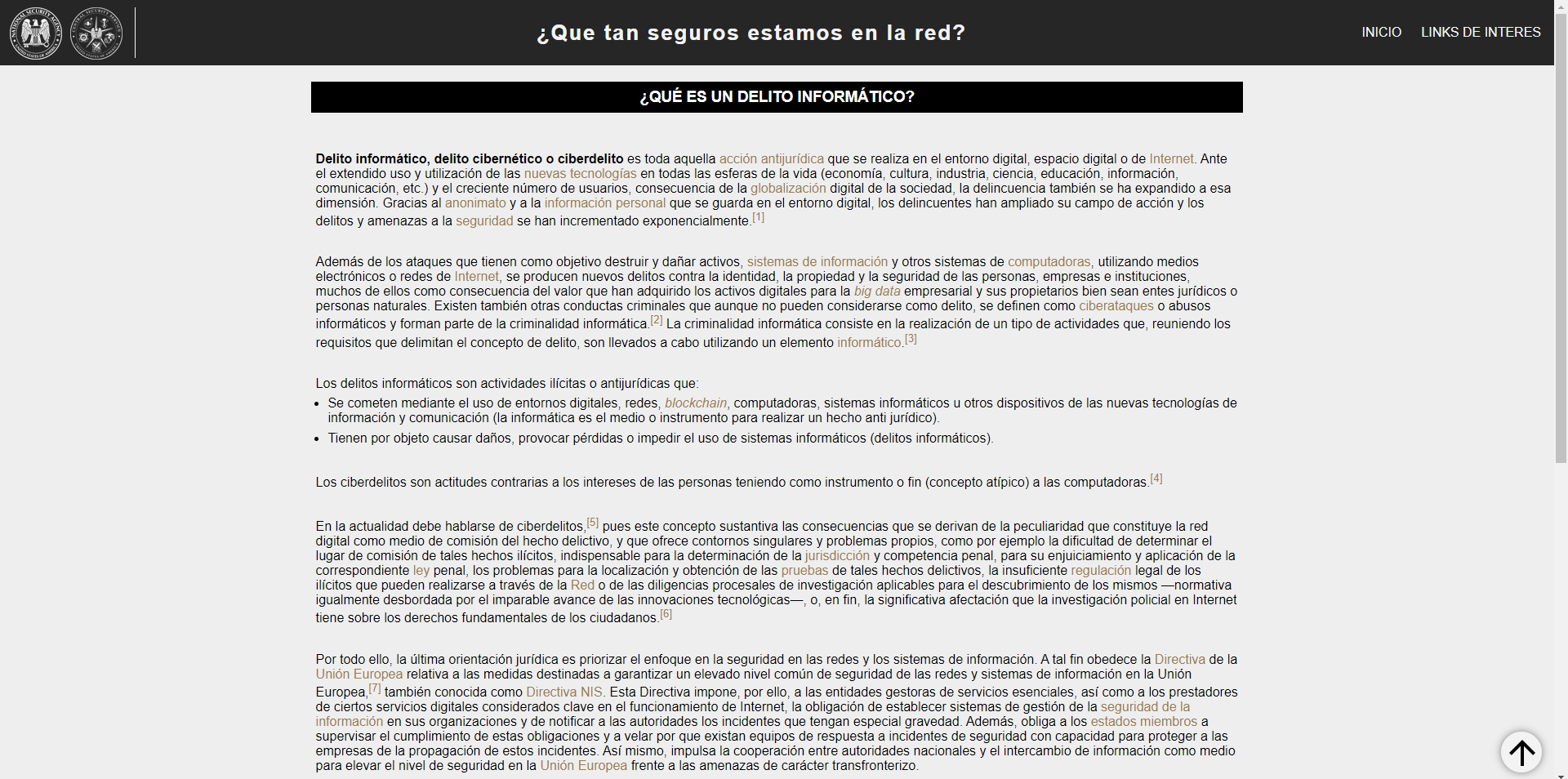
El sitio web de nuestro proyecto:





 Como se puede apreciar en la imagen, el sitio es completamente responsive, por lo que se puede visualizar comodamente tambien desde el celular.

Primer item del sitio.



Código fuente index de la página.

<https://github.com/SantDV/parking>



