Seguridad Informática en Bibliotecas

Téc. Cristina González Pagés
Asesora Técnica y Editora Web
Biblioteca Médica Nacional

26 de abril 2016

Seg. Informática VS Seg. de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

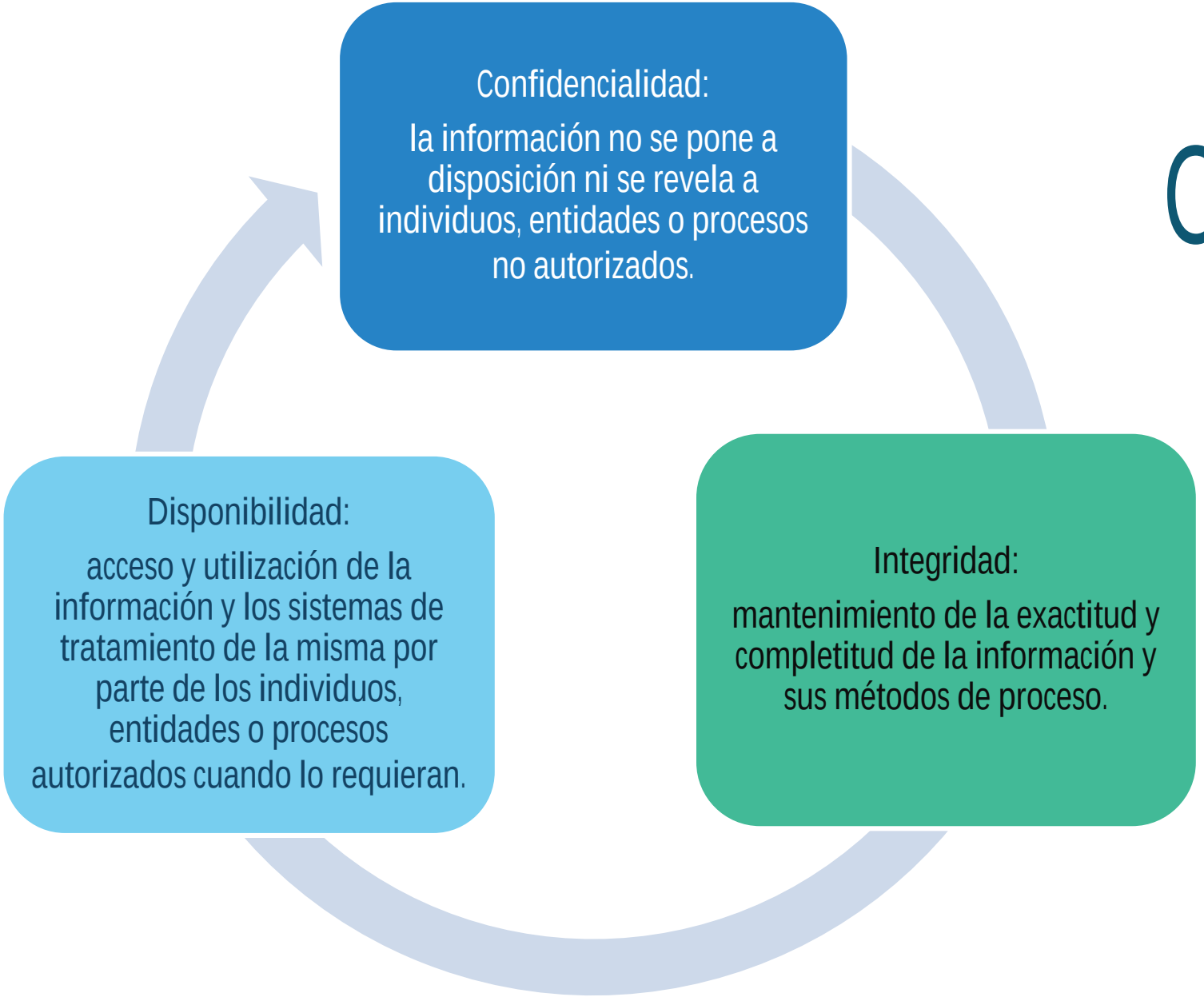
Sistema de Gestión de Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

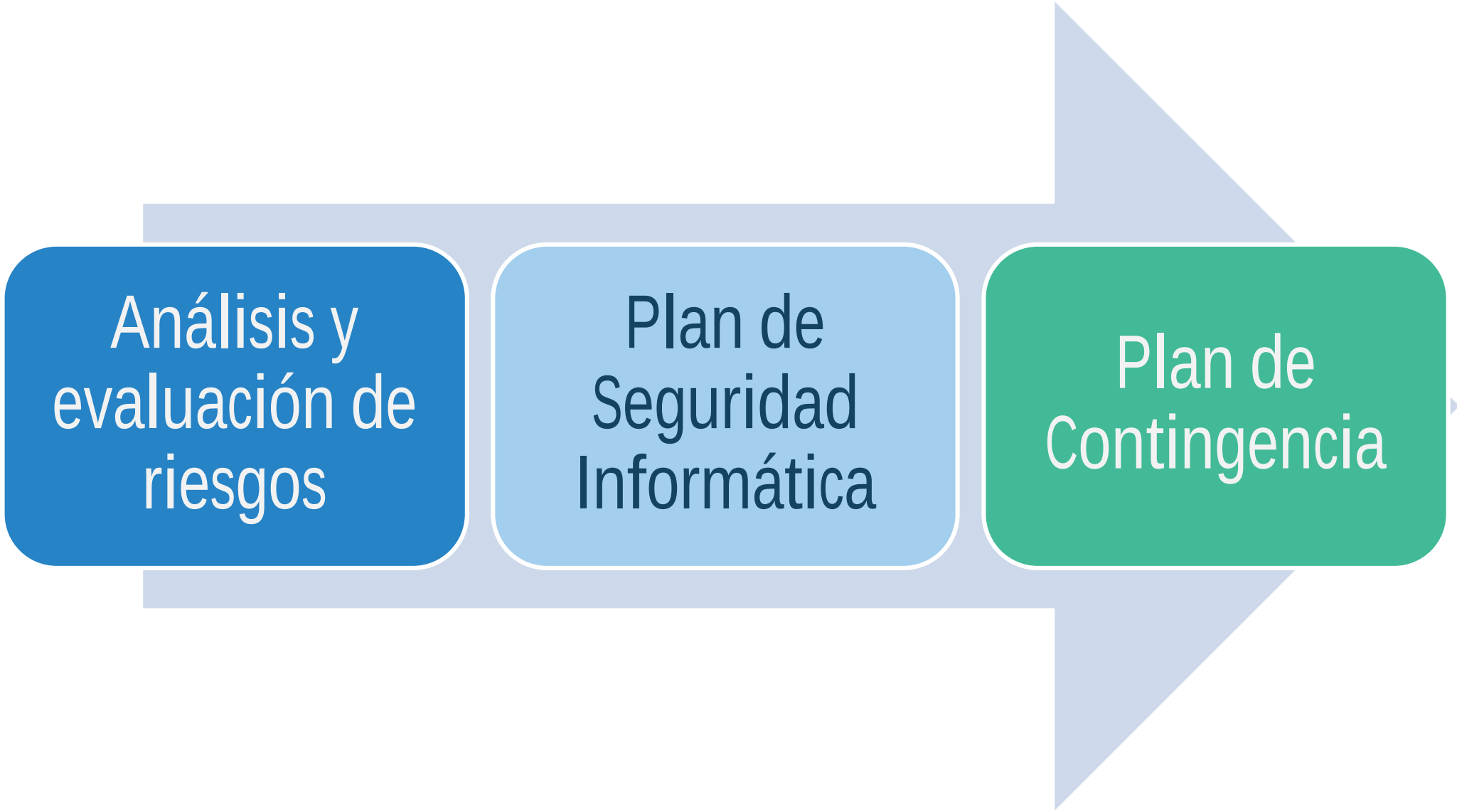
Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Ciclo de Vida C-I-D



Factores de ÉXITO

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités a distintos niveles (operativos, de dirección, etc.) con gestión continua de no conformidades, incidentes de seguridad, acciones de mejora, tratamiento de riesgos...
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.


Análisis y evaluación de riesgos
Plan de Seguridad Informática
Plan de Contingencia

Dirección de Informática y Comunicaciones MINSAP

http://www.di.sld.cu/

Seguridad de la Información desde nuestro puesto de trabajo

ESCRITORIOS LIMPIOS

Proteger la información confidencial en papeles y medios removibles

- ✓ **Guarde bajo llave** en gabinete o mobiliario seguro, cuando no se esté utilizando la información.
- ✓ Deje su lugar de trabajo en orden, **apague los equipos y guarde en un lugar seguro los documentos** al finalizar la jornada laboral.
- ✓ **No deje accesibles documentos** impresos que contengan datos confidenciales.
- ✓ **Retire los documentos de las impresoras** inmediatamente una vez impresos.

PANTALLAS LIMPIAS

Estaciones de trabajo y equipos portátiles protegidos

- ✓ **Cierre la sesión al ausentarse** o dejar de utilizar un sistema informático.
- ✓ Si debe abandonar, aunque sea momentáneamente, su puesto de trabajo, **bloquee su computador con un protector de pantalla** que solicite el ingreso de una contraseña.
  - Tecla Windows + L
  - Control + Alt + Supr

CREACIÓN DE CLAVES ROBUSTAS

- ✓ **No utilice** palabras comunes, de diccionario, ni nombres de fácil deducción por terceros, **no las vincule** a un dato personal.
- ✓ **No utilice** como contraseña su nombre de usuario ni derivados del mismo.
- ✓ Las contraseñas se deben construir utilizando como **mínimo 8 caracteres:**

  Donde debe incluir **al menos** una mayúscula, una minúscula y un número.
  Ejemplo: A23J77c31
- ✓ **Use claves distintas** para equipos y/o sistemas diferentes.
- ✓ Elija una **clave que no pueda olvidar**, para evitar escribirla en alguna parte.

NORMAS DE USO DE CLAVES

- ✓ Cuide que **nadie observe** cuando escribe su clave.
- ✓ **No escriba la clave** en papeles, post-it, ni en archivos sin cifrar.
- ✓ **No comparta su clave** con otra persona.
- ✓ **No pida la clave** de otra persona.
- ✓ **No habilite** la opción de "recordar claves" en los programas que utilice.
- ✓ **No envíe su clave por correo** electrónico ni la mencione en una conversación.
- ✓ **Cámbiela regularmente** o con la frecuencia establecida por la Unidad de Infraestructura TIC.
- ✓ Recuerde que los **intentos fallidos bloquean su cuenta** y los únicos encargados de desbloquear son Soporte TIC.

10 Consejos para Navegar seguros por Internet

1. Evitar los enlaces sospechosos: evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa, provienen de un remitente desconocido o remiten a un sitio web poco confiable.

2. No acceder a sitios web de dudosa reputación: a través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario – como descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc.

3. Actualizar el sistema operativo y aplicaciones: el usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

4. Descargar aplicaciones desde sitios web oficiales: muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema.

5. Utilizar tecnologías de seguridad: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante la principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

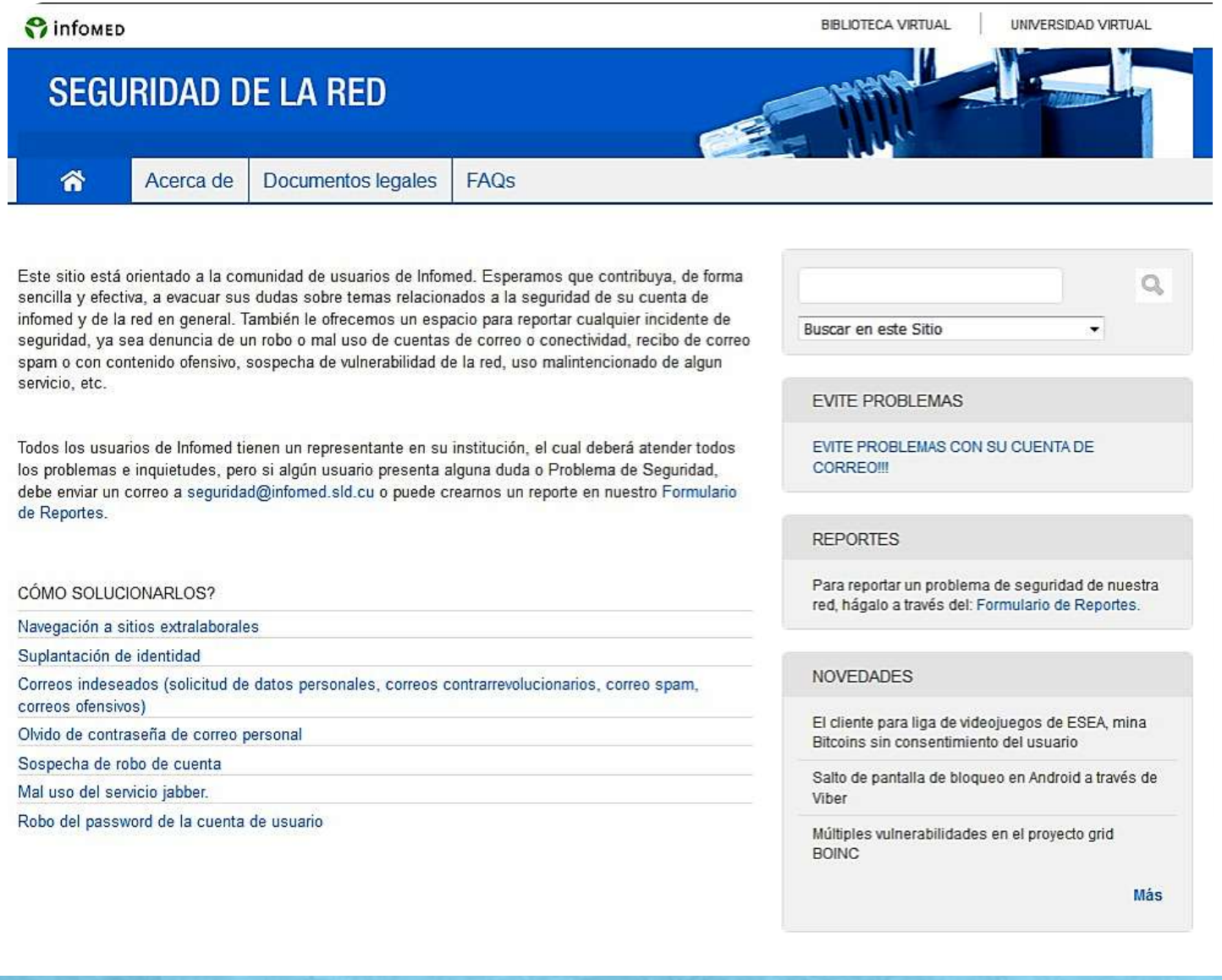
6. Evitar el ingreso de información personal en formularios dudosos: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. De esta forma, se pueden prevenir ataques que intentan obtener información sensible a través de la simulación de una entidad de confianza.

7. Tener precaución con los resultados arrojados por buscadores web: suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras muy utilizadas por el público, como temas de actualidad, noticias o temáticas populares. El usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado.

8. Aceptar sólo contactos conocidos: tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.

9. Evitar la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web).

10. Utilizar contraseñas fuertes : muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres.

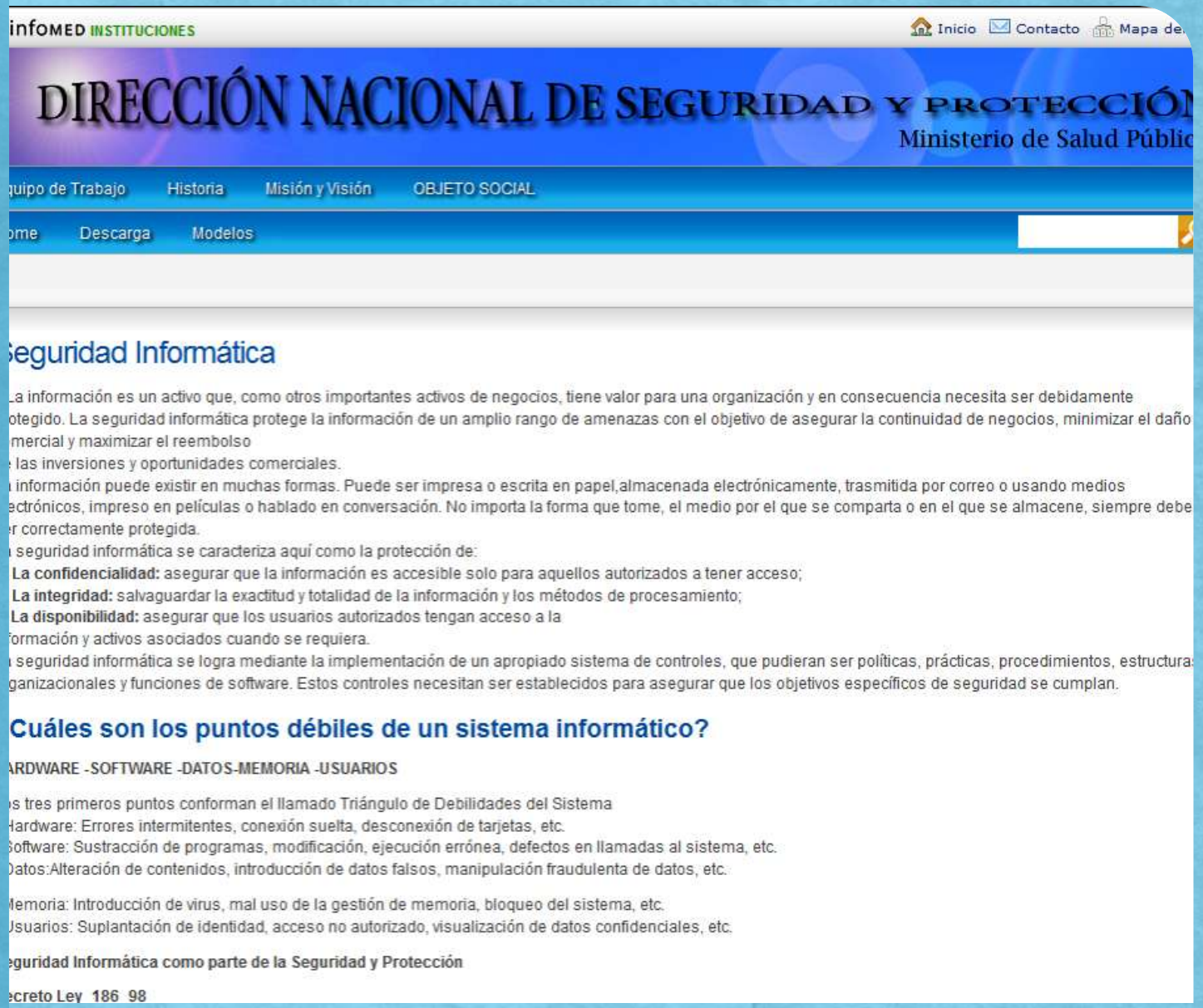


Seguridad de la RED INFOMED

http://infocert.sld.cu/

Dirección Nacional de Seguridad y Protección MINSAP

http://instituciones.sld.cu/dnspminsap/



Respuesta a Incidentes de Seguridad Informática en Cuba

https://www.cucert.cu/index.php

Bibliografía

- CITMATEL. Curso de “Seguridad Informática”. Marzo 2016