SEGURIDAD EN LA WEB.

- **ELEMENTOS DE PROTECCIÓN:**
  - Firewall
    Elemento de protección que sirve para filtrar paquetes (entrada o salida) de un sistema conectado a una red, que puede ser Internet o una Intranet. Existen firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.

  - Anti-virus
    Programa capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos (Troyanos, Works, Rootkits, Adware, Backdoor, entre otros).

  - Anti-spam
    Programas capaz de detectar, controlar y eliminar correos spam.
  - Criptografía
    Es el arte cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos, evitando la interceptación de éstos.

- **AMENAZAS TÉCNICAS DE SEGURIDAD.**

  - Spam
    Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

  - Ingeniería social
    Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesario para superar las barreras de seguridad.

  - Código Malicioso

Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Ejemplo: Troyanos, Works, Spyware, Rootkits, Adware, Backdoor, Cookies, Dialers, Exploit, Hijacker, keyloggers, Pornware, etc.

- Hoax
  Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam. Algunos de los Hoax más conocidos son correos con mensajes sobre virus incurables, temática religiosa, cadenas de solidaridad, cadenas de la suerte, Regalos de grandes compañías, entre otros.

- Suplantación:
  El atacante se hace pasar por algún servicio, correo, programa original.

- **FRAUDES.**

  - Phishing
    Es la capacidad de duplicar una página Web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada.

    Se tienen dos variantes de esta amenaza:

  - Vishing
    Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).

  - Smishing
    Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

  ¿Cómo funcionan?
  - A través de Sitio Web

En primera instancia los atacantes crean un sitio Web similar al original, trascribiendo textos, pegando las mismas imágenes y los mismos formularios para digitar los datos. Una vez creado el sitio, lo publican en la Web con un alias parecido al sitio original.

Ej: Reemplazando un simple de caracteres, usando un dominio real como prefijo:

- Sitio oficial:
  www.sitioReal.com
- Sitio falsos:
  www.sitioReal.com.sitio.com
- Variaciones:
  www.sitioReal-account.com
  www.sitioReal.actualiza.com

- **TIP DE SEGURIDAD.**

- Pornografía Infantil:
  Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

- Control de virus y códigos maliciosos:
  Mantenga siempre un antivirus actualizado en su equipo(s), procure correr éste periódicamente, de la misma manera, tenga en su equipo elementos como anti-spyware y bloqueadores de pop-up (ventanas emergentes).

  Evite visitar páginas no confiables o instalar software de dudosa procedencia.
  La mayoría de las aplicaciones peer-to-peer contiene programas espías que se instalan sin usted darse cuenta.
  Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.

Si sus programas o el trabajo que realiza en su computador no requieren de pop-up, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos. Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

- Correo electrónico:
  - No publique su cuenta de correo en sitios no confiables.
  - No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
  - No divulgue información confidencial o personal a través del correo.
  - Si un usuario recibe un correo con una advertencia sobre su cuenta bancaria, no debe contestarlo.
  - Nunca responda a un correo HTML con formularios embebidos.
  - Si ingresa la clave en un sitio no confiable, procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.

- Control de Spam y Hoax:
  - Nunca hacer click en enlaces dentro del correo electrónico aun si parecen legítimos.
  - Digite directamente la URL del sitio en una nueva ventana del browser
  - Para los sitios que indican ser seguros, revise su certificado SSL.
  - No reenvié los correos cadenas, esto evita congestiones en las redes y el correo, además el robo de información contenidos en los encabezados.
  - Control de la Ingeniería social:
  - No divulgue información confidencial suya o de las personas que lo rodean.
  - No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.
  - Utilice los canales de comunicación adecuados para divulgar la información.
- Control de phishing y sus modalidades:
  - Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.
  - Para los sitios que indican ser seguros, revise su certificado SSL.
  - Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.
- Robo de contraseñas:
  - Cambie sus contraseñas frecuentemente, mínimo cada 30 días.
  - Use contraseñas fuertes: Fácil de recordar y difícil de adivinar.

- Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 10 caracteres, combinada con números y caracteres especiales.
- No envié información de claves a través del correo u otro medio que no esté encriptado.

- **MECANISMOS DE SEGURIDAD**

Cuenta con sistema de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente).

DIALNET DE COLOMBIA cuenta con diferentes protecciones para controlar el acceso a los servicios de Internet tales como los mecanismos de identificación y autorización respecto a los servicios.

Para proteger las plataformas de los servicios de Internet, DIALNET DE COLOMBIA ha implementado configuraciones de seguridad base en los diferentes equipos de red, lo que comúnmente se llama líneas base de seguridad, además del establecimiento de medidas de seguridad a través de elementos de control y protección como:

- Firewall:
  A través de éste elemento de red se hace la primera protección perimetral en las redes de DIALNET DE COLOMBIA y sus clientes, creando el primer control que reduce el nivel de impacto ante los riesgos de seguridad.
- Antivirus:
  Tanto las estaciones de trabajo como los servidores de procesamiento interno de información en DIALNET DE COLOMBIA son protegidos a través de sistemas anti códigos maliciosos.
- Antispam:
  Todos los servidores de correo poseen antispam que reduce el nivel de correo basura o no solicitado hacia los clientes, descongestionando los buzones y el tráfico en la red.
- Filtrado de URLs:
  Los clientes pueden realizar filtrado de URL a través de sus navegadores Web, se sugiere instalar además sistemas parentales. DIALNET DE COLOMBIA cuenta con varios mecanismos capaces de realizar el bloqueo de URLs, entre ellos se encuentran los sistemas DNS y una herramienta para todo el tráfico hacia Internet, el objetivo principal de bloquear las que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales.

- Seguridad a nivel del CPE:
  Los dispositivos de conexión final ubicados en las premisas de los clientes cuentan con elementos bases para la autenticación y autorización, con ello cuenta con sistema de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente).