IMPAR T.V S.A.S.

ELEMENTOS DE SEGURIDAD EN LA WEB

La red mundial Internet y sus elementos asociados son mecanismos que ofrecen amplias posibilidades de comunicación, interacción y entretenimiento, tales como multimedia, foros, chat, correo, comunidades y bibliotecas virtuales, accesibles a todo tipo de público. Sin embargo, estos recursos deben estar acompañados de mecanismos que protejan y reduzcan los riesgos de seguridad distribuidos y potencializados a través del servicio de Internet.

UFINET, como proveedores de servicios de telecomunicaciones, están convencidos de que las relaciones con los clientes se deben fortalecer desde una comunicación asertiva, clara y orientada a proporcionar herramientas y consejos prácticos para la protección adecuada de los equipos de cómputo y los servicios asociados a Internet. Por esta razón, ponemos a disposición de nuestros clientes y la comunidad conceptos teórico–prácticos que pueden evitar o reducir los riesgos al interactuar en la red.

CONCEPTOS GENERALES DE SEGURIDAD

- **Confidencialidad:** La información solo puede ser conocida por individuos autorizados.
- **Integridad:** Garantía de que la información no ha sido alterada, borrada, reordenada o copiada sin autorización.
- **Disponibilidad:** La información debe poder recuperarse y estar disponible cuando se requiera.
- **Seguridad de la Información:** Conjunto de acciones y directrices para alcanzar la confidencialidad, integridad y disponibilidad, así como la continuidad de las operaciones ante eventos que puedan interrumpirlas.
- **Activo**: Recurso de la empresa que tiene valor, tangible (servidores, equipos de comunicación) o intangible (información, políticas, procedimientos).
- **Vulnerabilidad:** Debilidad o fallo de seguridad en un sistema o aplicación.
- **Amenaza**: Evento o situación con potencial de causar daño a un sistema.
- **Riesgo:** Hecho potencial que, de ocurrir, impacta negativamente la seguridad, los costos o el alcance de un proceso.

ELEMENTOS DE PROTECCIÓN

- **Firewall:** Filtra paquetes de entrada y salida en un sistema conectado a Internet o a una Intranet.
- **Antivirus:** Detecta, controla y elimina virus y otros códigos maliciosos como troyanos, gusanos (worms), rootkits, adware y backdoors.

- **Antispam:** Filtra y bloquea correos no solicitados.
- **Criptografía:** Ciencia de cifrar y descifrar información para evitar su interceptación.
- EDR (Endpoint Detection and Response): Sistemas de protección avanzada para detectar y responder a incidentes en equipos de usuario.
- Autenticación de Múltiples Factores (MFA/2FA): Refuerza el control de acceso más allá del uso de contraseñas.

AMENAZAS TÉCNICAS DE SEGURIDAD

- **Spam:** Envío de correos no solicitados.
- **Ingeniería social:** Manipulación de personas para obtener información.
- **Código malicioso:** Programas diseñados para dañar o robar información (troyanos, spyware, ransomware, exploits).
- **Hoax:** Correos con información falsa distribuidos en cadena.
- **Suplantación (Spoofing):** Hacerse pasar por un servicio o persona legítima.
- **Phishing:** Creación de sitios o correos falsos para robar información personal o financiera.
- **Smishing:** Phishing mediante mensajes SMS.
- **Vishing:** Phishing mediante llamadas de voz.
- **Pharming:** Redirección fraudulenta de sitios web legítimos a páginas falsas.

INTERNET SANO Y NORMATIVIDAD

En Colombia, la Ley 679 de 2001 y el Decreto 1524 de 2002 establecen medidas para prevenir y contrarrestar la pornografía y explotación sexual infantil.

Actualmente, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) promueve la estrategia En TIC Confío, que fomenta el uso seguro y responsable de Internet.

- **Canales de denuncia vigentes:**
- **Policía Nacional – CAI Virtual:** https://www.adenunciar.policia.gov.co/
- **Fiscalía General de la Nación:** https://www.fiscalia.gov.co
- **ICBF – Línea 141:** atención a casos de violencia y explotación infantil.

TIPS DE SEGURIDAD

- **Protección infantil:** Nunca alojar ni compartir material que involucre menores en contextos sexuales.
- **Antivirus y software**: Mantener programas de seguridad actualizados.
- **Contraseñas:** Usar claves seguras (mínimo 12 caracteres) y habilitar autenticación de múltiples factores.

- **Correo electrónico:** No responder mensajes sospechosos ni abrir enlaces dudosos.
- **Redes sociales:** No divulgar información sensible ni aceptar solicitudes de desconocidos.
- **Phishing y fraudes:** Validar direcciones web y nunca ingresar datos desde enlaces recibidos.

MECANISMOS DE SEGURIDAD EN UFINET

- **Autenticación y autorización:** Control de acceso a los diferentes servicios de red.
- **Firewall perimetral:** Primera capa de protección en la red de la compañía y de sus clientes.
- **Antivirus corporativo:** Protección activa en servidores y estaciones de trabajo.
- **Antispam:** Filtros de correo electrónico para reducir mensajes basura.
- Filtrado de URLs: Bloqueo de sitios no seguros y de contenidos ilegales.
- **Seguridad en CPE:** Dispositivos de cliente configurados con medidas básicas de seguridad.
- **Políticas de actualización:** Aplicación continua de parches y configuraciones seguras en la infraestructura.