Internet y nuevas tecnologías

Roberto Plá
Coronel de Aviación
http://robertopla.net/

CULTURA DIGITAL

CRITERIO Y DEPENDENCIA

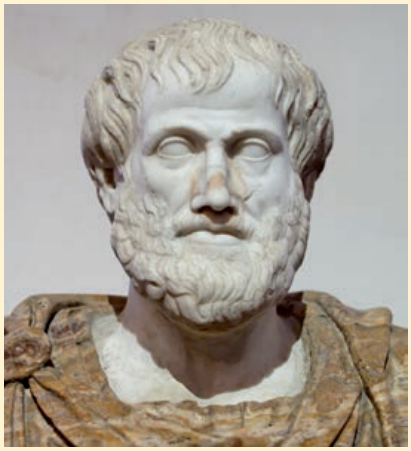
Se habla de una dependencia generalizada de internet y del cambio que ha producido en nuestra cultura la disponibilidad de una fuente ilimitada de información a la que concedemos el mismo valor que antaño a la letra impresa. He leído incluso afirmaciones sobre el efecto devastador que Google ha tenido sobre la memoria de los más jóvenes que no necesitan recordar lo que en cualquier momento pueden buscar en la red.

Toda esta visión, un tanto apocalíptica, puede parecernos exagerada, pero podríamos hacer un poco de examen interior planteándonos algunas de las siguientes cuestiones.

¿Qué haces si al salir de casa adviertes que te has dejado tu móvil? Quizás vuelves a por él o quizás piensas que no lo necesitas porque no te va a llamar nadie.

Si surge una discusión entre amigos sobre quién era o es Carroggio, y tu opinión es diferente, ¿admites que alguno está equivocado y lo dejas ahí, o buscas la respuesta en internet?

¿Consultas la guía telefónica en papel o buscas los teléfonos en la red?, ¿tienes los números de teléfono apuntados en un cuaderno de papel o solo en la agenda del teléfono u ordenador?



Cuando no sabes como ir a un sitio, ¿preguntas a alguien o lo miras en el navegador+GPS?

¿Consultas en internet las críticas de un hotel o restaurante antes de visitarlo?

Estas preguntas no tienen respuestas correctas o incorrectas. Es bueno usar la tecnología que el progreso pone a nuestro alcance y todos preferimos pasar por el supermercado y la panadería antes que correr para cazar nuestra cena y luego amasar el pan de mañana.

Pero al mismo tiempo, es bueno no pecar de ingenuos. Aunque no seamos cazadores, el ejercicio físico es un requisito para la salud, como evitar los alimentos excesivamente procesados o con numerosos aditivos.

En la época de los teléfonos con acceso a internet, ¿qué necesita nuestra mente para mantenerse en forma?

Pues en primer lugar, un criterio. La evaluación para la toma de decisiones basada en la veracidad y congruencia de la información que nos llega por cualquier medio, la lógica que nos permite advertir sesgos informativos, falacias o sofismas que sin embargo se nos presentan como dogmas y la moral para discernir lo bueno de lo malo y la honradez que nos impulsa a elegir la verdad y la bondad, eso lo tenemos que aportar nosotros ahora como siempre. Y es el bagaje que debemos transmitir a nuestros hijos, alumnos o subordinados: que sean cuales sean los medios que usemos para informarnos, y sea cual sea la cantidad de información buque que recibamos, el criterio es patrimonio y responsabilidad de nuestra condición humana, lo que realmente nos hace personas libres.

CIBERGUERRA

HISTORIA DE LA CIBERGUERRA

En la historia son importantes las primeras veces. Los inventores, los pioneros figuran en los libros de historia como los primeros que realizaron una acción o descubrieron una evidencia. Los exploradores y muchas de las figuras históricas deben su renombre a haber sido los primeros que llegaron a un sitio o hicieron algo concreto.

Fabricar una máquina de vapor, hablar por radio o volar en un medio más pesado que el aire son hitos históricos y las fechas en las que se realizaron por primera vez figuran en los libros de historia. La historia es el relato de los hechos verídicos –yo añadiría que relevantes– ocurridos en el devenir de la humanidad. Y todo relato debe tener un principio y esa es la razón por la que las primeras veces son tan importantes. Así que ¿quién inventó la ciberguerra?, ¿en qué momento la curiosidad, el vandalismo, las travesuras o los fallos provocados pasaron de ser una peculiaridad de chicos traviesos para pasar a considerarse una amenaza y una oportunidad entre las técnicas bélicas?

Por regla general, el cine de ficción no es fuente de la historia. La clave está en la palabra 'ficción'. Sin embargo el cine tuvo un importante papel en el nacimiento de la ciberguerra. Nos lo cuenta en su libro "Dark Territory" Fred Kaplan, un afamado escritor norteamericano, ganador del premio Pulitzer y especialista en relaciones internacionales y política estadounidense.

Según es conocido, uno de los entretenimientos favoritos del presidente Reagan era ver películas. En junio de 1983 se

encontraba en Camp Davis y disponía de una copia de la película "Juegos de Guerra" que se estrenaría ese mismo fin de semana en los Estados Unidos. En la película, Mathew Broderic representaba el papel de un quinceañero especialmente hábil con los ordenadores, David Lightman, que utilizaba un marcador automático para encontrar líneas telefónicas que le dieran acceso remoto a sistemas informáticos, y que creyendo haber encontrado un sistema repleto de juegos de estrategia, se introduce en el ordenador principal del NORAD, el Mando Norteamericano de Defensa Aeroespacial, donde, creyendo que está probando un nuevo juego, está a punto de desencadenar la tercera guerra mundial.

El argumento dejó impresionado al presidente. En la siguiente reunión del Consejo de Seguridad Nacional en la Casa Blanca, Reagan preguntó a sus consejeros por la película, y como ninguno la había visto les hizo un resumen de su argumento entre miradas escépticas y suspiros condescendientes de los asistentes, acostumbrados a algunas divagaciones y circunloquios del anciano presidente. Tras la exposición se dirigió directamente al general John Vessey, jefe de la Junta de Jefes de Estado Mayor y le preguntó directamente: ¿algo como ésto podría ocurrir realmente?, ¿podría alguien introducirse en nuestros ordenadores más sensibles? El general, como disciplinado y leal soldado no dudó un momento la respuesta y dijo: "Lo averiguaré".

Una semana después se presentó en la Casa Blanca con una respuesta sorprendente e inquietante: la realidad superaba ampliamente a la ficción. Como consecuencia de esa pregunta presidencial, se desarrollaron memorandos e informes, se reunieron grupos de trabajo y comisiones de expertos y después de muchos estudios y reuniones, se confeccionó una directiva de seguridad nacional con el título "National Policy on Telecomunications and Automated Information Systems Security", clasificada como confidencial, y registro NSDD-145, que el presidente Reagan firmó el 15 de septiembre de 1984 y que fue el primer documento en el que se consideraba la intrusión en sistemas informáticos como una amenaza para la seguridad del estado.

No obstante una serie de circunstancias, entre las cuales figura el escaso desarrollo y acceso público de las redes de ordenadores en aquella época, así como cuestiones de política y burocracia gubernamentales, hicieron que esta directiva no tuviera muchos efectos prácticos hasta una docena de años después, cuando durante la administración Clinton se produjeron una cadena de incidentes informáticos. Pero esa es otra historia. Y quien desee conocerla con detalle, debe leer el libro de Kaplan, aún no traducido al español, pero fácil de adquirir por internet.

REDES

LOS PELIGROS DE LA WIFI PÚBLICA

Los usuarios de terminales móviles usamos para conectarnos a internet tarifas que normalmente establecen un límite de datos. Pasado ese límite el acceso a la red se encarece bastante, o la velocidad se reduce. Por eso andamos buscando siempre conectarnos a través de redes inalámbricas que nos permitan ahorrar nuestro cupo de datos. Cuando estás en casa y es tu propia red doméstica la que te proporciona esa conexión puedes estar tranquilo siempre que tu router esté adecuadamente protegido con un protocolo de seguridad y unas claves adecuadas.

Pero en la calle o en lugares públicos, no se debe sucumbir a la tentación de conectarse a cualquier red disponible.

En primer lugar hay que saber quien y por qué nos está ofreciendo la posibilidad de conectarnos a su red. Hay que tener en cuenta que la conexión tiene un coste y aplicando la máxima de que "nadie regala nada", descubriremos que ante la demanda y debido a las preferencias de los clientes por los lugares con conexión, muchos establecimientos de hostelería ofrecen conexiones gratuitas a sus clientes.

Como la puerta del establecimiento no cierra el paso a las ondas, este tipo de puntos de acceso suelen tener un nombre y una clave que solo se proporciona a los clientes, para evitar que en la puerta se acumulen los "gorrones" que se enganchan a la red sin realizar consumiciones. En este caso está claro que el interés comercial del establecimiento procurará que el servicio sea bueno y seguro para fidelizar a sus clientes con un servicio de calidad.

En la Oficina de Seguridad del Internauta (OSI) del INCIBE (Instituto Nacional de Ciberseguridad de España) entre otros muchos e interesantes consejos, nos recomiendan comprobar el nombre de la red con el personal del local. Un avispado puede llegar a un bar y configurar en su teléfono un punto de acceso con un nombre parecido o igual al del local. Si otros clientes se conectan a internet a través de ese dispositivo, creyendo que lo hacen a través de la red del local, están ofreciendo todos sus datos no cifrados al propietario del dispositivo que puede hacer un uso malicioso de ellos o aún peor, puede encontrar la forma de acceder a nuestro propio teléfono y robar información contenida en el mismo sin necesidad de que nosotros la enviemos por la red. Fotos, cuentas bancarias, cuentas en redes sociales,... ¿Cuántas cosas pueden hacer por nosotros las aplicaciones que residen en nuestro teléfono?

Comprobado que la red es la propia del local, hay que tener en cuenta que algunas de ellas exigen el registro para dar acceso a internet, y si en el registro se incluye la necesidad de dar nuestra dirección de correo electrónico eso puede llevarnos a ser blanco de futuros y fastidiosos envíos de publicidad. Que haya que registrarse no impide que algún delincuente lo haga con malas intenciones y en vez de consultar el tiempo se dedique a 'explorar' las entradas a los dispositivos de los usuarios más incautos.

En definitiva, público quiere decir público. No quiere decir ni discreto ni seguro ni íntimo; son palabras y conceptos diferentes. Muchas aplicaciones no se caracterizan por su fuerte seguridad, muchas comunicaciones no son cifradas y por tanto el uso de las redes públicas debe reducirse en la medida de lo posible y usarse para consultar información, como leer la prensa o los blogs que leemos a diario, pero hay que evitar introducir contraseñas, usar la mensajería, operar con cuentas sensibles como bancos o sistemas de pago a menos de que estemos seguros, con conocimiento de causa de la robustez de su protección. •