D I G I T A L I Z A C I O N

FORO EVALUABLE 2

A L U M N O C E S U R 2 4 / 2 5

Alejandro Muñoz de la Sierra

PROFESOR

Raúl Moreno Luque

introdu

Introducción

En la actual era digital, la información destaca como uno de los activos más preciados. Desde datos financieros hasta los hábitos de consumo, las empresas manejan un flujo constante de información a escala global, lo que inevitablemente incrementa los riesgos. No sorprende, por tanto, que los ciberdelincuentes hayan fijado su atención en este valioso tesoro digital.

Las cifras hablan por sí mismas. Según proyecciones de NTT DATA, se prevé que los ciberataques se dupliquen en 2024 en comparación con el año anterior, pudiendo ocasionar pérdidas de alrededor de 10.000 millones de euros a las empresas (fuente: elderecho.com). Adicionalmente, el informe “Cost of Data Breach” de IBM indica que el costo promedio de una filtración de datos ya se sitúa en torno a los 4,88 millones de dólares, un aumento del 10 % con respecto al año previo (ibm.com). Ante esta situación, fortalecer la seguridad es más que aconsejable; es imprescindible. Igualmente, deberíamos reflexionar sobre cómo estamos gestionando nuestra presencia digital, tanto a nivel corporativo como individual.

1.Medidas clave para una protección eficaz

Para abordar eficazmente estos riesgos, un simple antivirus resulta insuficiente. Las empresas necesitan implementar un enfoque integral y meticulosamente diseñado. Algunas medidas esenciales abarcan el cifrado de datos sensibles, tanto en reposo como en tránsito, y el establecimiento de controles de acceso sólidos, como contraseñas robustas combinadas con autenticación multifactor (MFA).

Las redes deben estar segmentadas y protegidas mediante firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS). Es crucial, además, mantener el software actualizado para mitigar posibles vulnerabilidades. La creación de copias de seguridad regulares y la implementación de un plan de recuperación ante desastres son también fundamentales para responder rápidamente ante cualquier eventualidad.

No menos importante resulta el factor humano. Muchos ataques tienen su origen en un simple clic en un correo electrónico fraudulento. Por ello, la formación del personal en ciberseguridad es tan vital como la tecnología utilizada. Modelos como el “zero trust” –que asumen que ningún acceso es confiable sin verificación previa– están ganando terreno como referencia. A esto se suma la aplicación de la inteligencia artificial para identificar patrones inusuales mediante herramientas como SIEM o UEBA.

La conclusión parece obvia: la inversión en seguridad digital puede representar un costo, sí, aunque este resulta significativamente menor que las consecuencias de una brecha de datos.

2. Dilemas éticos: ¿qué pasa con nuestros datos personales?

Paralelamente, somos testigos de un debate cada vez más intenso en torno a la recopilación y el uso de nuestros datos personales. Gigantes tecnológicos como Google, Meta o Amazon rastrean continuamente nuestra actividad en línea, desde nuestras búsquedas hasta nuestras compras y nuestras interacciones. Esta información alimenta algoritmos que nos ofrecen anuncios “relevantes” o sugerencias personalizadas. Sin embargo, no todos se sienten cómodos con esta dinámica.

De acuerdo con una encuesta realizada en territorio español, un 75 % de los ciudadanos manifiesta seria preocupación sobre el uso que empresas y gobiernos hacen de sus datos, y un 70 % se opone a que su información se utilice para entrenar inteligencia artificial. En los Estados Unidos, otro estudio (Pew Research) revela que el 81 % de las personas temen que sus datos sean utilizados de maneras con las que no están de acuerdo.

La inquietud está justificada. El escándalo de Cambridge Analytica en 2018 demostró el potencial de uso opaco, incluso manipulador, de los datos. Hoy, se exige mayor transparencia. En Europa, el Reglamento General de Protección de Datos (RGPD) impone normas claras: la obtención de consentimiento explícito, la recopilación exclusiva de los datos necesarios y la garantía de derechos como el acceso, la rectificación o el borrado.

A pesar de ello, persiste la paradoja de la privacidad: a menudo aceptamos términos y condiciones sin leerlos detenidamente. Por ello, además de. En el contexto actual, donde las leyes son cruciales, también lo son las buenas prácticas. Las empresas, por ejemplo, deberían adoptar principios como el diseño enfocado en la privacidad desde el inicio (privacy by design), llevar a cabo auditorías periódicas y proporcionar alternativas viables a quienes prefieran no compartir su información personal. Paralelamente, los usuarios podemos emplear herramientas de protección: navegadores con seguridad reforzada, bloqueadores de rastreo, contraseñas únicas, entre otros. En resumidas cuentas, el equilibrio entre innovación, utilidad y respeto a la privacidad es fundamental.

3. ¿Quién controla nuestros datos? El papel de las grandes plataformas

Las grandes tecnológicas acumulan enormes volúmenes de información sobre nuestras vidas. Cada búsqueda, uso de una aplicación o compra en línea deja una huella digital. En teoría, estas empresas deberían salvaguardar nuestra información y actuar responsablemente con ella. No obstante, en la práctica, la situación es más compleja.

La Comisión Federal de Comercio (FTC) de EE. UU. ha señalado que el modelo de negocio de muchas de estas compañías se basa en la recopilación masiva de datos con fines publicitarios (r3d.mx). Según Lina Khan, presidenta de la FTC, esta vigilancia puede comprometer nuestra privacidad y libertades fundamentales.

A nivel legal, se han dado pasos significativos. En Europa, el RGPD y la reciente Ley de Servicios Digitales (DSA) establecen normas estrictas. Meta, sin ir más lejos, fue sancionada con 1.200 millones de euros en 2023 por transferir ilegalmente datos de usuarios europeos (infobae.com), constituyendo la mayor multa de este tipo hasta la fecha.

A pesar de estos progresos, la confianza pública sigue siendo limitada. Según Pew Research, el 77% de los estadounidenses opina que los directivos de redes sociales no asumen la responsabilidad cuando cometen errores. Esto demuestra que, además de leyes, son necesarios vigilancia, exigencia y una sólida cultura ética.

Algunas empresas han empezado a reaccionar, ofreciendo controles de privacidad más claros, opciones para eliminar datos o sistemas de autenticación más seguros. Sin embargo, el debate continúa abierto. La responsabilidad debe ser compartida: las plataformas deben mejorar su gobernanza, los usuarios exigir transparencia real y los gobiernos establecer límites y garantizar su cumplimiento.

0 2
C O N C L U S I O N E S

La economía digital actual gira en torno a los datos. Son el motor de la innovación, pero también una vulnerabilidad si no se gestionan correctamente. Por ello, las organizaciones deben priorizar la ciberseguridad, desde el cifrado y las copias de seguridad hasta la formación interna y la planificación ante incidentes.

Pero la seguridad no lo es todo. La ética es igualmente importante. La gestión masiva de datos personales tiene un impacto real en nuestras vidas, y solo mediante prácticas transparentes, respeto a la privacidad y leyes efectivas se podrá mantener la confianza de los usuarios.

Finalmente, las grandes plataformas, con su inmenso poder, no pueden seguir operando sin rendir cuentas. Se requiere una mayor responsabilidad por parte de ellas, así como de los usuarios y los gobiernos. En última instancia, proteger nuestros datos no es solo una cuestión técnica, sino también de valores: solo así podremos construir un ecosistema digital más seguro, justo y sostenible.

R E F E R E N C I A S

https://elderecho.com/los-ciberataques-a-empresas-en-2024-duplicaran-las-cifras-registradas-en-2023#:~:text=La%20estimaci%C3%B3n%20de%20ciberataques%20que,este%20a%C3%B1o%2C%20seg%C3%BAn%20NTT%20DATA

https://www.ibm.com/es-es/reports/data-breach#:~:text=La%20adopci%C3%B3n%20de%20la%20IA,4%2C88%20millones%20de%20d%C3%B3lares

https://www.ibm.com/es-es/reports/data-breach#:~:text=La%20adopci%C3%B3n%20de%20la%20IA,4%2C88%20millones%20de%20d%C3%B3lares

https://elderecho.com/el-75-de-los-espanoles-siente-gran-preocupacion-por-el-uso-que-entidades-publicas-y-privadas-hacen-de-su-informacion-personal#:~:text=El%2075,hacen%20de%20su%20informaci%C3%B3n%20personal

https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/#:~:text=%2A%2070,people%20are%20not%20comfortable%20with

https://r3d.mx/2024/10/04/ftc-senala-a-plataformas-digitales-por-vigilar-a-usuarios-para-monetizar-sus-datos-personales/#:~:text=Otro%20dato%20importante%20que%20revel%C3%B3,mayor%20parte%20de%20sus%20ingresos

https://www.infobae.com/america/mundo/2023/05/22/la-union-europea-multo-a-facebook-en-casi-usd-1300-millones-por-no-proteger-los-datos-de-sus-usuarios/#:~:text=El%20gigante%20estadounidense%20de%20las,por%20este%20tipo%20de%20infracciones