

Protección de la identidad y privacidad digital

Un compromiso personal y empresarial



MATEOS CONSULTORES / ARTÍCULO / Eslin Valle

Vivimos una época donde lo **“digital”** es toda la tecnología capaz de crear, transmitir, procesar y almacenar información, ejemplo de ello son las redes sociales, correos electrónicos, sistemas empresariales, dispositivos móviles, asistentes virtuales y más, desde el momento en que usamos una aplicación, iniciamos sesión en una cuenta o realizamos una videollamada, estamos dejando un rastro que nos representa en el mundo digital. Eso que dejamos no es solo información; es parte de lo que nos representa en línea y elementos de la identidad digital.

En palabras simples:

La identidad digital es el conjunto de datos que permiten que una persona, empresa o dispositivo sea reconocida dentro de un sistema digital. Incluye cosas tan cotidianas como el nombre de usuario y correo electrónico, pero también datos más sensibles como huellas digitales, ubicación, contraseñas o incluso los permisos para acceder a cuentas de banco. Entonces también se puede decir que la identidad digital es un **“Yo virtual”**, y como tal, debe protegerse con el mismo cuidado que tu identidad física.

Diversos organismos internacionales coinciden en este concepto. Por ejemplo:

- La norma ISO/IEC 24760-1:2019 lo define como el conjunto de características que describen a una entidad en un entorno digital, y que permiten identificarla de forma única.
- El NIST, el instituto de estándares de EE.UU., dice que es la representación digital de una persona en cualquier interacción electrónica.
- En Europa, el reglamento eIDAS regula cómo deben gestionarse esas identidades electrónicas cuando se usan para firmar, autenticar o validar transacciones digitales.

¿Y la privacidad digital?

Tiene que ver con el control, es el derecho y deber que tenemos todas las personas a decidir qué datos compartimos, con quién, para qué y por cuánto tiempo. Es proteger nuestra información personal o profesional del uso indebido, del espionaje, de los abusos de las plataformas y de los delincuentes digitales.

Existen bases legales internacionales que velan por este derecho; por ejemplo:

- El GDPR (General Data Protection Regulation), ley europea de protección de datos, establece que toda persona debe saber de forma clara cómo se usan sus datos, debe poder dar o negar su consentimiento, y tiene derecho a que su información sea eliminada si así lo desea.
- La norma ISO/IEC 29100 recomienda que las organizaciones diseñen sus sistemas teniendo la privacidad en mente desde el inicio.
- La OCDE (Organización para la Cooperación y el Desarrollo Económicos), en sus lineamientos sobre privacidad, habla de la importancia de respetar la autodeterminación informativa: el derecho a controlar tu propia información.

¿Cuáles son los peligros que corren la identidad y privacidad digital?

Las amenazas más comunes son:

- Suplantación de identidad: un atacante puede utilizar credenciales robadas para hacerse pasar por una persona, acceder a sus servicios financieros o realizar actividades ilegales en su nombre.

Identidad y privacidad digital

Un compromiso personal y empresarial

- Exposición no autorizada de datos personales: filtraciones de datos pueden revelar información crítica como ubicación, historial médico, hábitos de consumo o preferencias políticas.
- Seguimiento sin que te des cuenta (vigilancia o perfilamiento): Muchas plataformas digitales recolectan información sobre lo que se hace en línea, qué sitios visitas, qué productos ves, con quién hablas, qué te interesa, incluso si no se concedió directamente o sin saber que lo estaban haciendo. Con esa información crean un “perfil”, una especie de retrato digital de tus hábitos, gustos y comportamientos. Luego, ese perfil se puede usar para mostrarte publicidad muy específica o incluso para influir en tus decisiones, sin que seas plenamente consciente de ello.

Estas situaciones no solo afectan la seguridad personal, sino también la salud mental, la reputación y la autonomía del individuo en entornos digitales.

Riesgos para las empresas:

En el sector empresarial, los riesgos se amplifican debido al volumen y la sensibilidad de los datos que se manejan, y por la exposición de las identidades digitales de empleados, socios, clientes y proveedores. Algunos de los principales desafíos incluyen:

- Accesos indebidos a sistemas internos debido a credenciales comprometidas, que pueden derivar en robo de propiedad intelectual, manipulación de información o interrupción operativa.
- Ataques de ingeniería social dirigidos a empleados (phishing, pretexting) que aprovechan identidades digitales para ejecutar fraudes o espionaje corporativo.
- Falta de políticas claras sobre el uso de datos personales de colaboradores y clientes, lo que puede generar sanciones legales por incumplimiento de normativas como el GDPR o leyes locales de protección de datos.
- Pérdida de confianza y reputación ante brechas de privacidad o fugas de información.

Estas amenazas impactan no solo en la operación una empresa, sino también en su valor de marca, relaciones comerciales y cumplimiento legal.

Aquí un ejemplo.

Edgar es gerente administrativo en una empresa de salud, su identidad digital está compuesta por credenciales, permisos y accesos que lo identifican en los sistemas corporativos. Un día recibe un correo falso, supuestamente del área de sistemas de su empresa pidiéndole actualizar su contraseña, y sin sospechar, entrega sus credenciales a un atacante.

Con esta identidad digital comprometida, el intruso accede a datos clínicos, financieros y personales de cientos de pacientes. Días después, parte de esta información es publicada. Edgar, sin saberlo, fue la puerta de entrada a una de las peores violaciones de privacidad que su empresa ha vivido.

Consecuencias:

- Para Edgar: Su reputación laboral queda en entredicho, aunque fue víctima, la investigación interna lo somete a estrés emocional y presión. Sus credenciales personales son revocadas, y debe cambiar cuentas, correos y dispositivos asociados.
- Para la empresa: Además de enfrentar posibles sanciones legales por violación a la privacidad de los datos de salud (protegidos por ley), debe afrontar demandas civiles, pérdida de confianza de pacientes, y una crisis reputacional que afecta su posición en el sector.

¿Cómo podemos proteger la identidad y privacidad digital?

Conocer qué es la identidad y la privacidad digital no basta, entender su valor es solo el primer paso. Lo verdaderamente importante es tomar conciencia de lo fácil que es perderlas y lo difícil que puede ser recuperarlas una vez que han sido vulneradas.

Identidad y privacidad digital Un compromiso personal y empresarial

En el entorno digital, la tecnología avanza constantemente, pero los errores humanos siguen siendo el punto más débil, miedo, confianza excesiva, prisas, falta de conocimiento... son esos momentos en que bajamos la guardia los que más nos exponen, por eso, más allá de saber qué hacer, necesitamos comprender por qué debemos hacerlo.

¿Qué podemos hacer a nivel personal?

Protegernos no requiere ser expertos en informática, basta con adoptar hábitos conscientes y reconocer que cada dato que entregamos tiene un valor. Aquí algunas reflexiones prácticas:

- Cuida lo que compartes: En redes sociales, formularios, suscripciones o conversaciones en línea. Recodar que no todo lo que se sabe, hace o piensa debe ser público, aprender a decir “no” también en lo digital.
- Desconfiar sanamente: Si algo parece sospechoso, probablemente lo es, correos urgentes, enlaces dudosos o premios inesperados suelen ser la puerta de entrada para robar tus datos.
- Hazlo incómodo para los atacantes: Usar contraseñas distintas y difíciles, y activar una segunda verificación cuando sea posible (como un código por mensaje o una app). No es molesto, es inteligente.
- Actualiza tus dispositivos: las actualizaciones corrigen errores que podrían ser usados por cibercriminales, ignorarlas es como dejar una puerta abierta sin darse cuenta.
- Pensar dos veces antes de publicar: Ubicación, rutina, emociones o fotos de familiares son piezas de un rompecabezas digital que otros pueden armar sin permiso.

En resumen: Mantener en privado lo que es tuyo y conocer los límites de exposición digital. Porque una vez que algo se filtra, ya no hay botón de “deshacer”.

¿Y qué deben hacer las empresas?

Para las empresas, proteger la identidad y privacidad digital de sus empleados, clientes y socios no es solamente una cuestión técnica o de cumplimiento legal, es, ante todo, una **responsabilidad estratégica**.

Muchas empresas cometen el error de pensar que adquirir tecnología o difundir un par de boletines informativos basta para estar protegidas. Pero la realidad es que la ciberseguridad no se compra en una caja ni se garantiza con un software, sino que debe planearse como parte de una estrategia integral que responda al contexto, al nivel de exposición, y a la cultura organizacional propia.

Proteger datos e identidades implica mirar más allá de cualquier sistema o infraestructura y preguntarse:

- ¿Qué información es realmente crítica para nosotros?
- ¿Quién accede a ella, cómo y por qué?
- ¿Estamos preparados para responder si esa información se filtra, se altera o se pierde?
- ¿Nuestra gente entiende el valor de los datos que maneja?

Estas preguntas ayudan a construir una estrategia de protección realista, sostenible y alineada a los riesgos específicos de cada entorno empresarial.

Algunas acciones recomendadas:

- Invertir en tecnología especializada, como herramientas de gestión de identidades (IAM), cifrado de datos, monitoreo de accesos y sistemas de prevención de fugas (DLP), pero siempre como parte de una arquitectura planificada, no como soluciones aisladas.
- Apoyarse en expertos en privacidad y ciberseguridad que acompañen la creación de políticas, evaluaciones de riesgo y planes de respuesta a incidentes. Ninguna empresa debería enfrentar amenazas modernas con estrategias improvisadas.

Identidad y privacidad digital

Un compromiso personal y empresarial

- Formar una cultura de protección de la información, donde todos los colaboradores comprendan que la seguridad no es exclusiva del área de TI. Capacitar va más allá de enseñar qué hacer; implica construir conciencia sobre el impacto de lo que se hace.
- Diseñar procesos seguros desde el inicio, incluyendo la privacidad como un componente esencial del diseño de productos, servicios y plataformas.
- Actualizar marcos de cumplimiento y demostrar trazabilidad: conocer las leyes no basta, las empresas deben ser capaces de demostrar responsabilidad, previsión y ética en el tratamiento de los datos.

En definitiva, vivimos conectados, pero no siempre conscientes. En el entorno digital no basta con estar presentes: Debemos estar atentos, informados y decididos a cuidar aquello que no se ve, pero que nos representa.

Nuestra identidad y nuestra privacidad no son simples datos, sino reflejos de quiénes somos, de lo que valoramos y de lo que hacemos, proteger lo digital no es solo una cuestión técnica, ni una tarea exclusiva de los expertos. Es una práctica cotidiana, una responsabilidad compartida y, sobre todo, una forma de cuidado, hacia nosotros mismos, a quienes confían en nosotros, las leyes y hacia el entorno laboral.

Actualmente los clics dejan más huella que las palabras, cuidar la identidad y privacidad digital no es exageración: es sentido común, ética y responsabilidad.