Perfiles Biográficos Digitales: Un Modelo Conceptual de la Exposición en Redes Sociales

Román Pablo Zenobi[1] y María Luciana Roldán[12][0000-0002-4786-5592]

[1] Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina
rozenobi@hotmail.com
[2] Instituto de Desarrollo y Diseño (CONICET/UTN), Santa Fe, Argentina
lroldan@santafe-conicet.gov.ar

Abstract. Una Red Social Digital es un grupo de personas que están conectadas entre sí por medio de una plataforma de software que brinda el soporte para que cada una tenga definido su perfil y se comunique con otras. El perfil que una persona define en dicha Red Social Digital se denomina "perfil biográfico digital". La vulnerabilidad respecto de su privacidad puede ser desconocida por los usuarios, por no ser conscientes de los riesgos a los que se exponen, por el supuesto de estar respaldados por una plataforma "con condiciones establecidas de cuidado de privacidad". La exposición en un perfil biográfico digital conlleva una gran responsabilidad, debiendo ser cada persona el custodio de su privacidad. El objetivo de este trabajo es proponer un modelo conceptual de perfiles biográficos digitales, factores de incremento de exposición, y formas de mitigación asociadas, que sirva de base para la implementación de herramientas informáticas de concientización de usuarios. El modelo propuesto puede ser usado como una estrategia de protección de la exposición de las personas en redes sociales digitales, que permita mitigar ataques que comprometan su privacidad y la de su entorno.

Keywords: Privacidad, Redes Sociales Digitales, Exposición, Vulnerabilidad.

1 Introducción

Cada persona en su vida tiene un perfil psicológico dado por su personalidad, que la identifica y hace única en relación con otras personas. En informática, cuando se habla de una Red Social Digital (RSD) se hace referencia a un grupo de personas que están conectadas entre sí por medio de una plataforma de software que oficia de mediadora y brinda el soporte para que cada individuo tenga definido su perfil y pueda entablar comunicación con otros seres humanos. Ese perfil que una persona define en dicha RSD se denomina "perfil biográfico digital" o simplemente "perfil digital".

Como indica el autor Andy Stalman [1], "las redes sociales son un amplificador de lo que las personas ya somos como sociedad, en el sentido de que nuestra forma de actuar en nuestra vida física o terrenal debería ser la misma con la que nos desarrollamos, también de manera digital. Es decir, son las mismas personas, pero amplificando su vida en redes sociales digitales". Por ende, las personas deben ser conscientes de que

las redes sociales digitales también implican la amplificación de su nivel de exposición, aumentando así la vulnerabilidad de sufrir ataques a su privacidad y la de su entorno. El autor recalca que estamos presenciando el nacimiento de un nuevo hombre, cuyo desafío es aprender a vivir entre dos mundos: el online y el offline.

En el mundo digital, en el que las redes sociales son una de las plataformas más utilizadas para interactuar entre pares, las personas se exponen. Se denomina "exposición" a la forma en que sus características personales, su perfil biográfico, su privacidad y cuestiones propias de su vida son mostradas a otros, dejándose accesibles para que desde una plataforma de RSD otros sujetos puedan conocerlas. Cuando una persona se encuentra expuesta en una RSD, es posible que "alguien" encuentre la forma de sacar provecho de la información que la persona ha compartido. Esta persona malintencionada podría seguir una serie de pasos que le permitan revelar el grado de exposición que tiene usuario en sus redes sociales digitales y concretar un ataque a su privacidad.

La problemática expuesta en relación con la privacidad en redes sociales digitales constituye la motivación del trabajo. Muchas personas desconocen cómo configurar apropiadamente la privacidad en sus perfiles biográficos en redes sociales, emplean las configuraciones por defecto, y no son conscientes de qué aspectos de su vida privada quedan expuestos en las plataformas de redes sociales de las que son usuarios. Las grandes empresas que están detrás de las redes sociales descargan en el usuario la responsabilidad de controlar la privacidad de sus perfiles. La inadecuada exposición en los perfiles biográficos no solo puede representar una vulnerabilidad para cada individuo, sino también para las organizaciones o empresas en las que los individuos participan. Es necesario, que desde las organizaciones a las que pertenecen los individuos, ya sea en el ámbito laboral, educativo, privado o público, se ofrezcan herramientas para la capacitación y concientización de los usuarios de redes sociales digitales.

La situación de vulnerabilidad respecto de su privacidad puede ser desconocida por parte de los usuarios, en cuanto a no ser conscientes de los riesgos a los que se exponen, ya que suponen que están respaldados por una plataforma de RSD "con ciertas condiciones en cuanto al cuidado de privacidad". Sin embargo, son las personas los principales custodios de su información personal, ya que son los dueños de ésta, y, por lo tanto, son los principales interesados en proteger algo tan valioso como su privacidad.

El objetivo de este trabajo es proponer un modelo conceptual de perfiles biográficos digitales, publicaciones y atributos expuestos, factores de exposición y de mitigación asociadas, que sirva de base para la implementación de herramientas informáticas de concientización de usuarios. El modelo propuesto busca ser usado como una estrategia de protección de la exposición de las personas en redes sociales digitales, que permita mitigar ataques que comprometan su privacidad y su entorno.

El resto de este trabajo se organiza de la siguiente manera. En la sección 2 se presentan algunos antecedentes y trabajos relacionados que sirven de contexto de la propuesta. En la sección 3 se presenta el modelo conceptual de perfil biográfico digital. En la sección 4 se presentan métricas para el cálculo de nivel de exposición. En la sección 5 se presentan ejemplos que instancian los conceptos que intervienen en el modelo y se calcula la exposición. Finalmente, en la sección 6 se presentan las conclusiones y cuál es la idea de trabajo a futuro en el desarrollo de una herramienta de concientización.

2 Antecedentes y trabajos relacionados

En la historia del desarrollo de las Redes Sociales Digitales, han ocurrido sucesos impactantes que constituyen ejemplos en donde la privacidad de los usuarios no ha sido cuidada por las plataformas en las que dichas redes se despliegan.

En el mundo de las redes sociales consideradas “laborales”, LinkedIn es la plataforma estrella para tal fin. Millones de usuarios arman sus perfiles profesionales, al estilo Curriculum Vitae digital y generan contactos con pares vinculados por sus especialidades y disciplinas de trabajo. En ese sentido, existe un perfil digital para cada usuario, donde el objetivo es dar a conocer sus antecedentes profesionales y laborales. En este caso, un usuario, mediante una RSD profesional, no sólo puede exponer su propia información personal sino también la de su entorno laboral. Es común que los usuarios comenten en dichos perfiles cuál es su trabajo actual, puesto, tareas, tecnologías usadas y vínculos internos dentro de su lugar de empleo. Como se menciona en [2], las empresas deben diseñar una estrategia para mitigar la exposición de información confidencial por parte de sus empleados, en el uso que ellos hacen de sus redes sociales. En ese sentido, se destaca la necesidad de construir una política de uso de redes sociales y que sea comunicada de manera periódica. En este trabajo, el autor menciona que la conducta o comportamiento de una persona en las redes sociales, la forma en cómo se expone, puede superar los límites de su propia privacidad y llegar a la confidencialidad de su trabajo dentro de la organización en la que se inserta.

En el año 2012, LinkedIn reconoció que la empresa sufrió un acceso no autorizado y, en consecuencia, se produjo la filtración de aproximadamente 6,5 millones de credenciales de usuario. En respuesta a este ataque, la acción tomada por la plataforma fue el reseteo de claves de aquellas cuentas que habían sido comprometidas. Esto fue confirmado por la misma red social en un comunicado oficial [3]. Posteriormente, en 2016 se descubrió que un mayor número de credenciales de usuarios había sido expuesto en Internet. Aproximadamente, más de 100 millones de datos de cuentas de perfiles habían sido filtrados y publicados. Al identificar los usuarios comprometidos, la empresa les pidió que reseteen sus contraseñas y, además, promovió al uso del Doble Factor de Autenticación y la construcción de contraseñas robustas. Se puede observar que las medidas tomadas por la empresa consistieron en el traslado de la responsabilidad de la seguridad de los perfiles a cada uno de los usuarios.

Por otro lado, la red social Facebook es, tal vez, el exponente principal del tipo de plataformas en las cuales los usuarios crean sus perfiles y comparten con otras personas, creando sociedades digitales. En el año 2014, se produjo un hecho que puso en cuestión hasta qué punto los datos que brindan los usuarios quedan protegidos y no son usados para otros fines. La consultora Cambridge Analytica fue acusada de haber obtenido información de millones de usuarios de Facebook sin permiso, es decir violando las políticas de uso de la red social [4]. Para ello diseñaron una aplicación para que usuarios la usen para responder una serie de preguntas a cambio del pago de algunos dólares y de esa manera conocer un poco más sobre sus conductas y preferencias. Hasta ese punto, se habían conseguido aproximadamente 270000 perfiles de usuarios con su consentimiento para hacer el test de referencia. Esta aplicación necesitaba que se inicie sesión en Facebook y que se le otorguen ciertos privilegios. Lo que pasó realmente es

que uno de los permisos que pedía la aplicación era el acceso a los datos de los "amigos" de los perfiles aceptados en primera instancia. Eso produjo una recopilación total de información de 50 millones de perfiles, cuando éstos en su mayoría no habían brindado la aprobación para eso. La información que se obtuvo fue enviada a la consultora Cambridge Analytica, pero no sólo para fines académicos (como había sido informado a los usuarios) sino para ser usada para otras cuestiones, por ejemplo, para campañas políticas. El descubrimiento de estos hechos llevó a que la opinión pública e instituciones de gobierno cuestionaran la falta de transparencia que implica el uso de los datos sin permiso de los perfiles de los usuarios. Este suceso puso en el ojo de la mira a esta red social, por lo que dicha plataforma revisó y actualizó sus condiciones de uso y privacidad de los datos de usuarios.

En agosto de 2016, WhatsApp [5] hizo un cambio en la política de privacidad agregando que la plataforma podría compartir información de los usuarios de WhatsApp con Facebook, según se cita: "Como parte de la familia de empresas de Facebook, WhatsApp recibe información de esta familia de empresas y comparte información con ellas. Podemos usar la información que recibimos de ellas, y ellas pueden usar la información que compartimos con ellas, para ayudar a operar, proveer, mejorar, entender, personalizar y comercializar nuestros Servicios y sus ofertas, así como ofrecer servicios de ayuda para nuestros Servicios... Facebook y las demás empresas de la familia de Facebook también pueden usar nuestra información para mejorar tus experiencias con sus servicios...". Este cambio de política hizo que la Agencia Española de Protección de Datos (AEPD) impusiera una multa a las dos plataformas por considerar que las condiciones establecidas de privacidad no se ajustan a la normativa vigente [6]. Para el caso de WhatsApp, dicha agencia consideró a esta política como una intención de brindar datos de los usuarios a Facebook sin su aprobación previa, y por el lado de Facebook, se consideró la intención de usar esa información para sus propios usos y beneficios.

Existen en la literatura, trabajos que abordan la historia de cómo se ha llegado a la situación de hoy en donde existe un sobre-exposición de la privacidad de las personas. Rosenblum y colab. [8] relatan cómo comenzó a producirse a nivel global a través de la propagación y adopción de las RSDs. Estos autores referencian que en los albores de las comunicaciones digitales, era posible expresarse mediante blogs, realizar algunas videoconferencias con la webcam, y hacer uso de emoticones para mostrar los sentimientos. En esos inicios, los perfiles de una persona en esos sitios webs se circunscribían únicamente a su nombre, edad, ciudad, correo electrónico y alguna imagen identificatoria. Posteriormente, las redes sociales como Facebook y MySpace (precursoras en los inicios), propiciaron el gran salto, es decir, lograr que cada usuario cree su propio perfil, indique sus preferencias de exposición, mostrando lo que, en principio, quedaba en el plano de las redes sociales humanas convencionales. Se podría decir que ese "pequeño salto" para las redes sociales digitales fue un "salto al vacío" para la privacidad de las personas, dando paso a la problemática de la exposición, y surgiendo el concepto de la "intimidad online". Los mismos autores remarcan en su trabajo, que la privacidad implica confidencialidad y que el usuario sea el único dueño de su perfil y por ende administre los permisos en el mayor nivel de granularidad posible. Esto es, al mayor detalle, tópico por tópico de su espacio de perfil. Ante el desafío actual, se menciona la

necesidad de trabajo colaborativo entre expertos en ciencias sociales, las comunidades de seguridad, la industria y las regulaciones a fin de tomar decisiones sobre la manera de aplicar seguridad en los mecanismos y políticas que permitan preservar la privacidad en las redes sociales digitales.

Choi y colab. [9] analizan el fenómeno de las redes sociales y presentan un esquema de "audiencia" en torno a un usuario de una RSD con los siguientes roles de participantes: "Usuario objetivo", "Amigos diseminadores", "Amigos del usuario objetivo" y "Amigos en común". En base a ese esquema, diferencian en la "audiencia" entre sólo posteo (Posting Only) y posteo con etiquetado (Posting with Tagging). En ese trabajo se evidencia el poder de "propagación" del perfil del Usuario objetivo entre los distintos usuarios y roles que se conectan. Se hace la distinción con el modo de propagación en donde los usuarios "etiquetan" a otros usuarios en las publicaciones de los perfiles. En esos casos, se amplía la exposición porque explícitamente los usuarios son nombrados por las etiquetas.

Para comprender el contexto que presentan las redes sociales digitales, es interesante el trabajo de Srivastava y Geethakumari [10], donde se afirma que las redes sociales digitales se movieron desde un fenómeno de nicho hacia una adopción masiva por la población de usuarios. Esto significa que, en la última década, se usaron a las redes como plataformas para que los usuarios puedan comunicarse entre sí, intercambiar información, expresar sus sentimientos y construir relaciones con otros miembros de Internet. Los autores presentan los resultados de una encuesta en la que se indagó sobre el nivel de conocimiento que tienen las personas sobre cómo una red social puede exponer la privacidad y hasta qué punto los usuarios conocen ese nivel de exposición. Lo que se obtuvo como información de interés, es que un 88% de ese grupo de personas frenarían el uso de una red social si encuentran que sus datos personales sensibles son usados de una manera no esperada por ellos. En contraposición, por medio de otra pregunta, en su mayoría (63,3%) los usuarios comentaron que el proceso de ajustar la privacidad de un perfil de una red social les genera una pérdida de tiempo y además es complejo o difícil de entender. Otro resultado relevante de este trabajo es el de "cálculo de la sensibilidad". La sensibilidad es la propiedad de la información que la convierte en privada. Empleando este concepto, se espera que, a mayor nivel de privacidad requerida, la sensibilidad de la información se incrementa. Por ende, es la información sensible, la que debe ser fuertemente protegida por parte de los usuarios. En relación a ello, los autores, identificaron y categorizaron los atributos de los perfiles que hacen a la sensibilidad de la información.

3 Modelo conceptual

En esta sección se presenta un modelo conceptual (Fig. 1) para publicaciones en perfiles biográficos digitales. El modelo permite identificar los principales conceptos y relaciones para comprender el dominio de la privacidad en redes sociales y sirve de base para la implementación de herramientas informáticas de concientización de usuarios.

Se parte del concepto de *Red Social Digital*, que refiere a un grupo de personas que están conectadas entre sí por medio de una plataforma de software que oficia de mediadora y brinda el soporte para que cada individuo tenga definido su *Perfil Biográfico Digital* (PBD) y pueda entablar comunicación con otros individuos en la red. Este perfil

constituye la configuración inicial que un *Usuario* (persona) crea para empezar a utilizar las funcionalidades de la plataforma de RSD. Contar con un *Perfil Biográfico Digital* es el primer paso para comenzar a adquirir exposición.

Un *Usuario* de una red social digital presenta algún tipo de relación con otro/s *Usuario/s* de la misma red, y, en consiguiente puede generar interacción y compartir contenido como si fueran "conocidos". Dependiendo de la RSD, esta relación se conoce con el término de *contacto*. En el caso de Facebook, los contactos son llamados "Amigos". Para el caso de Instagram, un contacto es llamado "Seguidor" (o "Follower"). En ese sentido, un determinado usuario tendrá un número de "Seguidores" y un número de "Seguidos" ("Following"). Para el caso de Instagram, el tipo de Contacto es unidireccional. Si un usuario A solicita seguir a un Usuario B, y si el Usuario B acepta, no significa que ese Usuario B puede ahora ver los contenidos del Usuario A, es decir el Usuario A se convierte en *Follower* del Usuario B. Por otro lado tiene que haber un pedido del Usuario B para seguir al usuario A, y la aceptación correspondiente, para que el Usuario B se transforme en *Follower* del Usuario A, y así emparejar el acceso. Para la red LinkedIn, los contactos son llamados "Conexiones". Un usuario puede optar por conectarse con otro usuario para convertirse en *contacto*, comenzar a interactuar directamente, y ver los contenidos publicados. En la Fig. 1 se simplifican todas estas variaciones considerando un RSD genérica, y estableciendo una relación entre usuarios indicando los roles *seguidor* y *seguido.* En cada *PBD*, un usuario comienza a efectuar publicaciones (*Publicación*). Las mismas se clasifican en tipos (*TipoPublicación*) y tienen una propiedad denominada *Ubicación* que indica el lugar o sección que tiene la publicación en el *PBD.*

Esta clasificación de tipo de publicaciones se presenta en la Tabla 1, y se define el correspondiente tipo como especializaciones del concepto *TipoPublicación* en la Fig. 1.

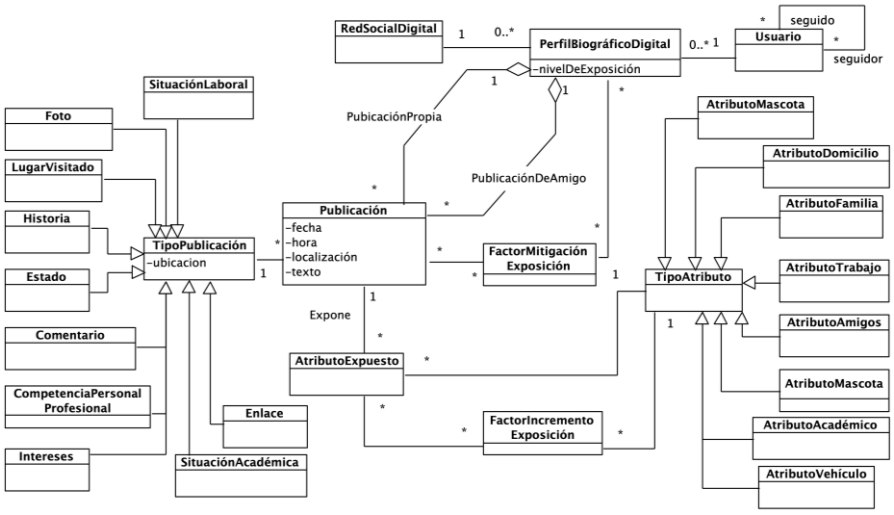

Figura 1. Modelo conceptual de Perfil Biográfico Digital.

Tabla 1. Tipos de publicaciones y sus atributos.

TipoPublicación	Ubicación
1. Comentario	1.1. Muro / Página central perfil
	1.2. En otro tipo de publicación (fotos)
2. Foto	2.1. Portada
	2.2. Perfil
	2.3. En muro / página central perfil
3. Enlace	
4. Intereses	4.1. Personales
	4.2. Laborales
5. LugarVisitado	
6. Historia	
7. Estado	
8. SituaciónLaboral	8.1. Actual
	8.2. Antecedentes
9. SituaciónAcadémica	9.1. Nivel de estudios
	9.2. Institución educativa
10. CompetenciaPersonalProfesional	

En la Tabla 1 también se presentan los posibles valores que puede tomar la propiedad *Ubicación* según el tipo de publicación que se trate. Puede observarse que para ciertos tipo de publicaciones el valor de la ubicación no es relevante.

Cada Publicación en un PBD puede implicar la exposición de ciertos atributos o de aspectos del PBD (representado por *AtributoExpuesto*, Fig. 1). Por ejemplo, cuando un usuario publica la foto de portada de un perfil, se estará efectuando una cierta exposición dependiendo de qué se identifique en esa foto.

En el modelo conceptual se describe que un *AtributoExpuesto* es de cierto tipo (*TipoAtributo*). El tipo de atributo indica a qué conjunto de aspectos relativos al usuario o su perfil biográfico digital corresponde un atributo. Por ejemplo, el nombre de la mascota del usuario, la raza, la veterinaria en donde es asistido, etc. corresponden al tipo *AtributoMascota;* el nombre de los hijos, la escuela a la que asisten, si tiene pareja o su estado civil, datos sobre sus padres, etc. corresponden al tipo *AtributoFamilia*. Para catalogar los posibles tipos de atributos que pueden ser expuestos, se propone una tipificación de los tipos mismos. Esta tipificación se explicita en la primera columna de la Tabla 2. Se debe considerar que para una Publicación, se pueden tener más de un tipo de atributo expuesto.

Vale aclarar que, en el alcance de este trabajo, no es de interés conocer qué datos privados son expuestos (o podrían ser expuestos) en una publicación, es decir, conocer el valor de un atributo expuesto. Lo que es de interés es qué tipo de datos son expuestos (o podrían ser expuestos) en una publicación por el usuario de una RSD, ya que el objetivo final del modelo conceptual es generar herramientas para alertar a un usuario sobre qué tipos de datos podría dar a conocer con una potencial publicación, y crear conciencia de si es realmente su voluntad hacerlo.

Por otro lado, un tipo de atributo puede verse potenciado por diversos factores que generen un incremento en la exposición propia de ese tipo de atributo. En la Fig. 1 esto es representado por el concepto *FactorIncrementoExposición* (FIE).

Tabla 2. Tipos de atributos y sus Factores de Incremento de Exposición.

Tipo de Atributo	Factor de Incremento de Exposición
1. Datos de Domicilio (Casa, Departamento, Oficina de Trabajo, Locación temporal) representado por *Atributo-Domicilio*	1. Existencia de puertas y/o ventanas 2. Tipo de puertas y ventanas 3. Existencia de sensores de alarmas 4. Existencia de cámaras de seguridad 5. Tipo de habitación: dormitorio, comedor, living, patio. 6. Cantidad de habitaciones 7. Tipo / Estilo de mobiliario: por semejanza en distintas fotos, se puede inferir la cantidad de habitaciones del domicilio. 8. Logos / Marcas en objetos y/o prendas de vestir depositadas en la habitación.
2. Datos de Vehículos. Representado por *AtributoVehículo*	1. Marca, modelo, color. 2. Patente / Dominio. 3. Rasgos particulares únicos (calcomanías, marcas, rayones, choques, etc.). 4. Referencias a ciudades / locaciones / empresas en el caso de un vehículo de flota laboral. 5. Lugar de estacionamiento. Ej.: una playa de estacionamiento particular. 6. Zonas aledañas al lugar de estacionamiento. 7. Puntos de referencias (negocios, casas, otros vehículos)
3. Datos de Familia. Representado por *AtributoFamilia*	1. Cantidad de integrantes y posible parentesco. a. Identificación de menores. 2. Fechas y/o acontecimientos particulares (cumpleaños, casamientos, etc.) 3. Locaciones relacionadas a la familia (casas de padres, vecinos, etc.) 4. Mascotas de familia 5. Vehículos de familia 6. Locaciones relacionadas a la familia
4. Datos de Amigos. Representado por *AtributoAmigos*	1. Cantidad de amigos. 2. Rangos etarios. 3. Viviendas y locaciones relacionadas. 4. Familiares y/o contactos de los amigos. 5. Vehículos de amigos 6. Mascotas de amigos 7. Lugares de uso común como clubes, negocios, etc. 8. Eventos / Acontecimientos (cumpleaños, encuentros, aniversarios).
5. Datos de Mascotas. Representado por *AtributoMascota*	1. Cantidad y tipo con raza. 2. Rasgos distintivos únicos: collar, cadenitas, colgantes, tapados, ropa especial. 3. Locaciones de las mascotas. 4. Conductas relacionadas al paseo de las mascotas. 5. Personas con mayor afinidad a las mascotas.
6. Datos de Trabajo. Representado por *AtributoTrabajo*	1. Nombres de otros empleados de la misma empresa y sector. 2. Presentaciones con información corporativa. 3. Escritorio de la computadora, evidenciado los programas que se usan. 4. Espacios físicos de la empresa y/o usuarios. 5. Software institucional de uso entre empleados. Ej.: G-Suite, MS Teams, Cisco. 6. Plataformas de correo electrónico. 7. Interfases de desarrollo de software. 8. Marca y modelo de la computadora. 9. Sistema Operativo. 10. Navegador de Internet: URL de páginas abiertas 11. Estructura de las páginas web, secciones 12. Contactos vinculados / corporativos 13. Aplicaciones instaladas y/o en ejecución 14. Disposición de las oficinas, escritorios.

	15. Tipos de computadoras y posición según pasillos, ventanas. 16. Personas en la misma locación trabajando: cantidad, ubicaciones, posible identificación de sector. 17. Personal relacionado: mantenimiento, limpieza, etc. 18. Posición de máquinas de impresión, escáneres, trituradoras de papel, máquinas de café, etc. 19. Ubicación de cámaras de seguridad y sensores de alarma / incendio. 20. Ubicación de puertas, ventanas y sistema de control de acceso físico. Ejemplo: presencia de vigilancia y uso de tarjeta magnética para aperturas de puertas.
7. Datos de Académicos (*Atributo-Académico*)	1. Nombre y locación de institución educativa. 2. Nombres de profesores y alumnos. 3. Disposición física de las aulas. 4. Ubicación de las aulas. 5. Nombres de personal perteneciente a la institución educativa. 6. Ubicaciones físicas de las distintas dependencias de la institución: Secretarías, Alumnado, Dirección, etc. 7. Datos presentados en los pizarrones de las aulas. 8. Disposición de las puertas de ingreso y ventanas. 9. Existencia de guardias de seguridad. 10. Existencia de control de acceso con molinete u otro sistema. 11. Existencia y ubicación de cámaras de seguridad.

En la Tabla 2, esto es detallado en la segunda columna, catalogándose de esta manera un conjunto de posibles factores de incremento de la exposición por tipo de atributo.

Cada tipo de atributo expuesto implica un incremento en el nivel de exposición que tendrá el perfil de la red social. Por ejemplo, cuando en la foto de portada que selecciona un usuario (instancia de *Publicación*, cuya propiedad *ubicación* toma valor *Portada*), se exponen datos relativos a familia (en este caso, el tipo de atributo expuesto es *AtributoFamilia*). Pero además, frecuentemente se está frente a otros Factores de Incremento de Exposición, cuando se pueden identificar por medio de esa foto otros aspectos como nombre de los menores en la familia, cantidad de integrantes, etc. para obtener información adicional del grupo familiar (instancias de *FactorIncrementoExposición*). En conclusión, desde una determinada publicación seleccionada por el usuario, la misma puede incrementar su nivel de exposición por intermedio de estos factores adicionales, que son pertenecientes de manera inherente al tipo de atributo expuesto utilizado. El concepto *Atributo Expuesto* agrega (reúne) todos *los Factores de Incremento de la exposición* que pueden existir para ese tipo de atributo expuesto en la publicación.

Además de los Factores de Incremento de Exposición, existen otros factores que impactan sobre las publicaciones del usuario, atenuando o mitigando los efectos de la exposición. Éstos se denominan Factores de Mitigación de la Exposición (FME), representado en el modelo conceptual con el concepto *FactorMitigaciónExposición*, y como puede observarse en la Fig. 1, se relaciona directamente con *Publicación* o *con el Perfil Biográfico Digital*. Por ejemplo, publicar una foto y que ésta sólo sea accesible por los “amigos” del usuario, es una forma de mitigar una exposición. Este tipo de mitigaciones actúan a nivel de Publicación en general y a nivel del perfil biográfico del usuario, siendo configuraciones propias de cada plataforma.

Para minimizar la exposición en una publicación, se debe alcanzar una solución de compromiso que tienda a anular a los factores de incremento de exposición, para balancearlos con los factores de mitigación y lograr una exposición adecuada. Una buena

práctica para lograr una adecuada exposición es que el usuario al momento de hacer una publicación o configuración favorezca a los factores que atenúan la exposición y minimice los factores de incremento de exposición.

Adicionalmente, el modelo conceptual planteado, permite a partir del concepto Perfil Biográfico Digital calcular lo que se denomina una *Exposición en cadena*. Así, observando los diferentes tipos de atributos expuestos en diferentes publicaciones de un perfil, podría inferirse información del usuario más amplia, que abarque diversos tipos de atributos con varios factores de incremento de la exposición. Un ejemplo de exposición en cadena es el siguiente: un usuario publica una foto con su grupo de amigos, mencionando los nombres de cada uno de ellos. Posteriormente, pasado un tiempo, publica una nueva foto mostrando una locación de un club, en donde hará un deporte en particular. Luego de esa publicación, a un tiempo posterior, genera una nueva fotografía de una cena con el mismo grupo de amigos en donde se puede apreciar y se menciona el lugar. Con esas tres fotos, correspondientes a Atributos Expuestos de su Perfil Biográfico Digital, dicha persona está brindando información valiosa para un atacante. Entonces, el atacante conocerá: el grupo de amigos con sus nombres, el horario y lugar de las fotos, el deporte que practican con sus amigos, el hábito de cenar luego de la actividad deportiva con sus amigos.

El modelo además, permite inferir para un PBD la condición de *SujetoExpuestoPasivo*. En este caso, a través de la presencia de instancias de publicaciones con alta exposición realizadas por amigos de un PBD, sería posible inferir que un usuario tiene cierto nivel de exposición debido a publicaciones en donde se encuentra arrobado o etiquetado.

4 Métricas propuestas para cuantificar la exposición de un perfil biográfico

En el modelo conceptual para PerfilBiográficoDigital se definió el atributo *nivel de exposición* (*nivelDeExposición*). Para calcular el valor de este atributo se definen un conjunto de métricas que se basan en los conceptos representados.

1) Métrica para calcular el valor de exposición de un atributo *i* en una publicación *p*

$$VE\_ip = AtributoExpuesto\_i * Sumatoria(FIE\_ip)/Cantidad\ total\ de\ FIE\ para\ el\ tipo\ de\ atributo\ de\ i.$$

AtributoExpuesto_i toma valor 1 o 0, si hay presencia o no de ese tipo de atributo en la publicación *p*. Se calcula como la sumatoria de todos los factores de incremento de la exposición que posee el atributo expuesto, dividido la cantidad de factores de incremento de la exposición posibles por tipo de atributo.

Se supone que si se calcula esta métrica es porque la publicación *p* expone el atributo *AtributoExpuesto_i* . Caso contrario el valor de la métrica es 0. Interpretación: se obtiene un valor entre 0 y 1, cuanto más cercano a 1, mayor es la exposición del tipo de atributo expuesto.

2) Métrica para calcular el valor de exposición en una publicación *p*

*VE_p = FME_p * Sumatoria(*VE*_ip) / Cantidad total de TipoAtributo*

FME_p toma valor 1 o 0 si un factor de mitigación es aplicado o no para la publicación *p*. Este valor de mitigación es aplicado como producto a una sumatoria. La sumatoria se calcula sobre los resultados obtenidos en el cálculo de todas las métricas *VE_ip* para todos los atributos expuestos *i* por la publicación *p*, obteniéndose un valor de exposición para la publicación. Si existe mitigación, el valor de *VE_p* se anula, sino, será mayor a cero. Dado que los tipos de atributos posibles de encuentran tipificados, se conoce la cantidad total de ellos. Dividiendo la sumatoria por esta cantidad, se obtiene un valor entre 0 y 1.

Interpretación: cuanto más cercano a 1 sea el valor de *VE_p* más aspectos de privacidad del usuario son expuestos en la publicación.

3) Métrica para calcular el nivel de exposición de un PBD *pbd*

VE*_ pbd = FME_pbd * (Sumatoria(VE_p) + Sumatoria(VE_pp))*

FME_pbd toma valor 1 o 0 si un factor de mitigación es aplicado o no para al perfil biográfico digital. Este valor de mitigación es aplicado como producto a la suma de dos sumatorias. La primera sumatoria se calcula sobre los resultados obtenidos en el cálculo de todas las métricas *VE_p* para todas las publicaciones *p* de un perfil biográfico digital *pbd*, obteniéndose un valor de exposición para el *pbd*. La segunda sumatoria, se calcula sobre los resultados obtenidos en el cálculo de todas las métricas *VE_p* para todas las publicaciones *pp* de los amigos del perfil biográfico digital *pbd* en los cuales ha sido etiquetado, obteniéndose un valor de exposición para el *pbd* como sujeto expuesto pasivo. Si existe mitigación a nivel del PBD, el valor de *VE_pbd* se anula (o disminuye), sino, será mayor a cero. Dado que la cantidad de publicaciones de un perfil es variable, la interpretación de esta métrica es: el valor de *VE_pbd* puede ser 0, si se aplica correctamente mitigación, o mayor a 0 si no se aplica mitigación, siendo más alto cuando más publicaciones con exposición existen.
Podría proponerse una variación de esta métrica si se considera que existen más de un nivel de mitigación posible *FME_pbd*, pudiendo tomar valores entre 0 y 1.
La métrica *VE_pbd* es la que se emplea para calcular el *NivelExposición* de un PBD. Se pueden definir rangos para indicar niveles de exposición Alto, Medio, y Bajo.

5 Caso de estudio

A continuación se desarrolla un caso de estudio en la red social Facebook donde se aplican los conceptos definidos (Fig. 2). Se considera un PBD que contiene una publicación del tipo *Foto*, cuyo valor de atributo *ubicación* es el Muro del usuario. Se presenta además el diagrama de objetos para este PBD basado en el modelo conceptual. A partir de la fotografía se pueden identificar los siguientes tipos de atributos expuestos: *ADomicilio1:AtributoDomicilio* (valor igual a 1) y *AVehiculo1:AtributoVehiculo* (valor igual a 1).

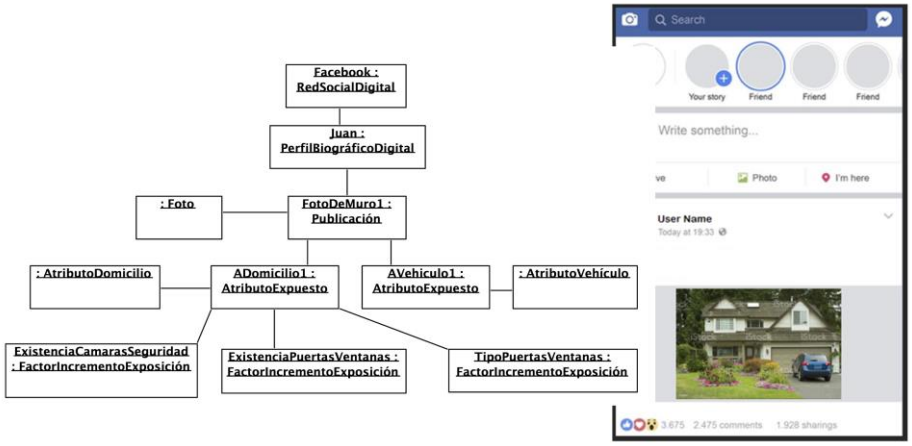

Figura 2. Instancias intervinientes en una publicación en Facebook con foto en muro. Fuente[1]

A continuación, en la Fig. 3 se identifica los factores de incremento de la exposición que pueden identificarse para el atributo expuesto *ADomicilio1* (*AtributoDomicilio*).
FIE_ ADomicilio1_1: Existencia de Cámaras de Seguridad (Descripción: se detectan dos cámaras de seguridad en el frente de la casa)
FIE_ ADomicilio1_2: Existencia de Puertas y Ventanas (Descripción: se detectan 5 ventanas y 2 puertas (un portón incluido).
FIE_3_ADomicilio1_3: Tipo de Puertas y Ventanas (Descripción: se detectan puertas/portón de madera. Además se distinguen materiales de puertas y ventanas, tipo de portón, la inexistencia de rejas y/o celosías, entre otra cosas).

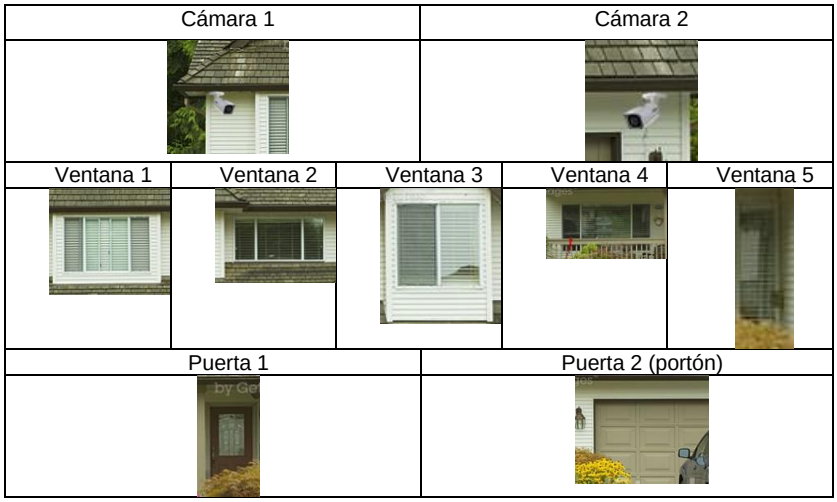

Figura 3. Ejemplo de Factores de incremento de exposición en la publicación.

[1] Fuente foto: Hermosos Casa Y Jardín Foto de stock y más banco de imágenes de Coche - Coche, Camino de entrada, Casa - iStock (istockphoto.com)

Por otro lado, para el atributo expuesto *AVehiculo1* (de tipo *AtributoVehiculo*) se identifican los factores de incremento de exposición: *FIE_ AVehiculo1_1*: Marca, color y modelo, y *FIE_ AVehiculo1_2*: Patente / Dominio (Fig. 4).

Figura 4. Ejemplo de Factores de incremento de exposición en la publicación.

A continuación, se aplican las métricas definidas para el caso de estudio:

- Métrica para calcular el valor de exposición de atributo "ADomicilio1:AtributoDomicilio" en la publicación *FotoDeMuro1*.

VE_AtributoDomicilio_FotoMuro1 = ADomicilio1:AtributoDomicilio * Sumatoria(*FIE_i_AtributoDomicilio_FotoMuro1)/Cantidad total de FIE para tipo de atributo de AtributoDomicilio* = 1 * 3 / 8 **= 0,375**

- Métrica para calcular el valor de exposición de atributo "AVehiculo1:AtributoVehiculo" en la publicación *Foto de muro 1*.

VE_AtributoVehiculo_FotoMuro1 = AVehiculo:AtributoVehiculo * Sumatoria(*FIE_i_AtributoVehiculo_FotoMuro1*) / *Cantidad total de FIE para el tipo de atributo AtributoVehiculo* = FotoMuro1 = 1 * 2 / 7 **= 0,285**

- Métrica para calcular el valor de exposición en la publicación *FotoMuro1*

Para el cálculo se considera que *FME_FotoMuro* es 1, es decir, que la foto se publicó de manera pública, sin restricción de acceso. Se emplean además, los resultados de las métricas calculadas previamente.

*VE_FotoMuro1 = FME_FotoMuro1 * (VE_AtributoDomicilio1_FotoMuro1 + VE_AtributoVehiculo_FotoMuro1) / Cant. total TipoAtributo*
*= 1 * (* 0,375 + 0,285*) / 7* = 0,66 / 7= **0,09**

6 Conclusiones y trabajos a futuro

En este trabajo se presentó un modelo que identifica los principales conceptos que intervienen al analizar la exposición de usuarios en una red social digital. Para mejorar el modelo propuesto, un trabajo a futuro es incorporar un conjunto de restricciones OCL (Object Constraint Language) que permitan validar diferentes modelos de instancias, y agregar consultas sobre dichos modelos, por ejemplo, para inferir la existencia de *Exposición en cadena* en un PBD, o cuando un usuario es un *Sujeto Expuesto Pasivo*.

A continuación, se enumeran las líneas de trabajo futuras para este proyecto:

- Desarrollar una prueba de concepto o prototipo, y llevar a cabo experiencias con perfiles biográficos reales.

- Estudiar la posibilidad de integrar la herramienta en navegadores, o a las plataformas de redes sociales digitales, como herramienta de concientización tanto para uso individual, como por organizaciones.
- Definir reglas que automaticen la detección de factores de exposición o usuarios expuestos pasivos.

La herramienta se piensa como un complemento a agregar a los navegadores de internet como una extensión. Esta herramienta al momento de que el usuario ingrese a la RSD (Facebook, Instagram o LinkedIn) y decida efectuar una publicación, podrá ser usada antes para analizar y conocer el nivel de exposición que dicho elemento tiene para con su privacidad y la de su entorno. En una primera versión de la herramienta, la aplicación será sólo para el análisis de tipos de publicaciones "fotos". Una versión avanzada de tal aplicación será la posibilidad de subir una determinada foto y por medio de una tecnología de reconocimiento de imágenes, detectar y categorizar a la publicación según el atributo expuesto correspondiente: AtributoFamilia, AtributoDomicilio, etc. y presentar al usuario los posibles Factores de Incremento de la exposición, a fin de que el usuario realice un checklist, obtenga un nivel estimado de exposición para la potencial publicación y decida si desea proseguir o no con la publicación. Además se espera implementar características basadas en el modelo conceptual para conocer el nivel de exposición del PBD completo.

Referencias

1. Stalman, A.: Humanoffon. Ediciones Deusto (2016).
2. Wu He.: A review of social media security risks and mitigation techniques. In: Journal of Systems and InformationTechnology Vol. 14, pp. 171 – 180 (2012).
3. LinkedIn Blog Page, https://blog.linkedin.com/2016/05/18/protecting-our-members, last accessed: 2020/05/23.
4. Infobae Homepage, https://www.infobae.com/america/tecno/2018/03/20/7-datos-para-entender-el-escandalo-de-facebook-y-cambridge-analytica/, last accessed: 2020/05/23.
5. WhatsApp Homepage, https://www.whatsapp.com/unsupportedbrowser?doc=privacy-policy&version=20160825, last accessed: 2020/05/23.
6. AEPD Homepage, https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar, last accessed: 2020/05/23.
7. Twitter Blog Page, https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html, last accessed: 2020/06/21.
8. Rosenblum D.: What Anyone Can Know: The Privacy Risks of Social Networking Sites. In: IEEE Security & Privacy, vol. 5, no. 3, pp. 40-49 (2007).
9. Choi, B. C. F., Jiang, Z. (Jack), Xiao, B., & Kim, S. S.: Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding. In: Information Systems Research, pp. 675–694 (2015).
10. Srivastava A., Geethakumari G.: Measuring privacy leaks in Online Social Networks. In: 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2095-2100 (2013).