JORNADA DE CIBERSEGURIDAD Y SOCIEDAD

6 de octubre de 2023
Facultad Regional Santa Fe

UNIVERSIDAD TECNOLÓGICA NACIONAL

AJEA
Actas de Jornadas y Eventos Académicos de UTN

UTN SANTA FE

Facultad Regional Santa Fe -UTN
I Jornada de Ciberseguridad y Sociedad : Facultad Regional Santa Fe -UTN / compilación de María Luciana Roldán ; editado por María Luciana Roldán. - 1a ed. - Ciudad Autónoma de Buenos Aires : Universidad Tecnológica Nacional, 2023.
Libro digital, PDF/A

Archivo Digital: descarga y online
ISBN 978-950-42-0233-2

1. Ciberdelitos. 2. Ingeniería. I. Roldán, María Luciana, comp. II. Título.
CDD 607.2

ISBN 978-950-42-0233-2

JORNADA DE
CIBERSEGURIDAD Y
SOCIEDAD

Jornadas de Ciberseguridad y Sociedad

6 de octubre de 2023

Facultad Regional Santa Fe
Asociación Civil "Consumidores de la Era Digital" (CED)

Libro de actas
Publicado en diciembre de 2023

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Resumen

La primera edición Jornada de Ciberseguridad y Sociedad surge como continuación de una serie de charlas y actividades en común que habían sido organizadas entre el Departamento de Ingeniería en Sistemas de Información de la Facultad Regional Santa Fe, Universidad Tecnológica Nacional y la Asociación Civil "Consumidores de la era digital", a principios del año 2023.

De esta manera, con el objetivo de abordar los desafíos actuales en el ámbito de la ciberseguridad y su impacto en la sociedad surge la idea de llevar adelante la Jornada de Ciberseguridad y Sociedad. Esta jornada abordó la temática de la ciberseguridad desde diferentes puntos de vista: el legal, el técnico y el de la ingeniería social, procurando destacar la importancia de valorar la actuación humana en el diseño de los sistemas de seguridad tecnológica. Con ese objetivo, el programa de la jornada incluyó una variedad de charlas a cargo de expertos destacados en el campo de la ciberseguridad, ciberdelitos, ingeniería social y la tecnología.

Además, se realizó un llamado a presentación de trabajos, invitando a la comunidad educativa a presentar resultados de investigación y experiencias, en relación a temáticas como la protección de datos personales, la prevención del ciberdelito, la utilización de técnicas de manipulación psicológica y social de delincuentes para cometer ciberdelitos, la seguridad en las redes sociales y la privacidad en línea.

Mediante esta jornada se busca ampliar la mirada de quienes diseñan y operan sistemas tecnológicos en la prevención de riesgos asociados a fraudes y otros delitos, destacando la importancia de la seguridad en línea, incorporando herramientas y análisis provenientes de la ciberseguridad en el mundo digital actual, las tecnologías asociadas, las leyes y jurisprudencia actuales para defender al consumidor, responsabilidades empresariales, etc.

La jornada se desarrolló de manera híbrida, teniendo lugar en el Auditorio Cruz del Sur de la UTN FRSF, y fue transmitida a través de internet para los asistentes virtuales. Contó con la participación de más de 70 inscriptos y 10 expositores. Además, se contó con más de 130 reproducciones de la charla "Ciberseguridad, una oportunidad para todos" que fue realizada de forma totalmente abierta a la comunidad.

Quienes organizamos la jornada esperamos que esta propuesta de acercamiento de una organización de la sociedad civil a la Universidad, sirva para que podamos ofrecer a la sociedad de la que todos formamos parte mejores servicios, más seguros, más amigables, que permitan sostener un ambiente de negocios saludable, donde las empresas puedan desarrollarse y competir, sin que los consumidores tengan que asumir riesgos que no les corresponden, sino que, por el contrario, puedan acceder a bienes y servicios en libertad y con seguridad.

The first edition of the Cybersecurity and Society Day is a continuation of a series of talks and common activities that had been organized between the Department of Information Systems Engineering of the Santa Fe Regional Faculty, National Technological University and the Civil Association "Consumers of the digital era", at the beginning of 2023.

In this way, with the aim of addressing current challenges in the field of cybersecurity and its impact on society, the idea of carrying out the Cybersecurity and Society Day arised. This conference addressed the topic of cybersecurity from different points of view: legal, technical and social engineering, trying to highlight the importance of valuing human performance in the design of technological security systems. With that objective, the day's program included a variety of talks by leading experts in the field of cybersecurity, cybercrimes, social engineering and technology.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

In addition, a call for papers was made, inviting the educational community to present research results and experiences, in relation to topics such as the protection of personal data, the prevention of cybercrime, the use of psychological and social manipulation techniques. criminals to commit cybercrimes, security on social networks and online privacy.

This conference seeks to broaden the perspective of those who design and operate technological systems in the prevention of risks associated with fraud and other crimes, highlighting the importance of online security, incorporating tools and analyzes from cybersecurity in today's digital world. the associated technologies, current laws and jurisprudence to defend the consumer, business responsibilities, etc.

The day was developed in a hybrid way, taking place in the "Cruz del Sur" Auditorium of the UTN FRSF, and was transmitted over the internet for virtual attendees. It had the participation of more than 70 registrants and 10 key note speakers. In addition, there were more than 130 reproductions of the talk "Ciberseguridad, una oportunidad para todos", which was transmitted completely open to the community.

Those of us who organized the event hope that this proposal to bring a civil society organization closer to the University will help us to offer the society of which we are all part better, safer, friendlier services that allow us to sustain an environment of healthy business, where companies can develop and compete, without consumers having to take risks that do not correspond to them, but, on the contrary, can access goods and services freely and safely.

Organización

Universidad Tecnológica Nacional, Facultad Regional Santa Fe (UTN FRSF)

Asociación Civil "Consumidores de la Era Digital" (CED)

Lugar

Auditorio "Cruz del Sur", Facultad Regional Santa Fe, Universidad Tecnológica Nacional.

Mención

El Honorable Concejo Municipal de la Ciudad de Santa Fe de la Vera Cruz, declaró su beneplácito a la Jornada de Ciberseguridad y Sociedad, organizada por el Departamento de Ingeniería en Sistemas de Información de la U.T.N. F.R.S.F. y Asociación Civil Consumidores de la Era Digital, realizada el 6 de Octubre del corriente.

Hizo entrega del reconocimiento la concejal ***Valeria López Delzar***.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Temas de interés

- Ciberdelitos, ingeniería social y tecnología
- Protección de datos personales
- Prevención del ciberdelito
- Seguridad en redes sociales y privacidad en línea
- Gestión de la Seguridad de los sistemas de información
- Identidad Digital. Autenticación de Personas.
- Concientización y capacitación
- Informática forense
- Inteligencia Artificial aplicada a ciberseguridad
- Gobernanza de la ciberseguridad. Políticas. Estrategias
- Gestión de incidentes de seguridad
- Desarrollo seguro de aplicaciones
- Prevención, detección y recuperación de incidentes
- Herramientas para la gestión y administración de la ciberseguridad
- Ciberseguridad en entornos de infraestructura crítica
- Ciberseguridad en entornos de nube (Cloud)

Auspiciantes

BancoBica PILAY JERÁRQUICOS Salud

Chairs

Dra. Luciana Roldán (CONICET / UTN)

Abg. Marcelo Gelcich (CER)

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Comité Organizador

Dra. Luciana Ballejos

Dra. Milagros Gutiérrez

Mg. Marcela Vera

Ing. Matías Orué

Comité de Programa

Ing. Sofía Lottersberger (UTN FRSF)

Ing. Alejandro Tóffolo (UTN FRSF)

Dra. Beatriz Parra de Gallo (UCASAL)

Dra. Laura Spina (UTN FRSF)

Dra. Luciana Roldán (CONICET / UTN)

Ing. Alejandra Giménez (INICIACTIVA)

Ing. Paula Yanotti (UTN FRSF)

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Índice

Keynotes

Trabajos

Keynotes

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Keynote

Ciberseguridad: ¿Cómo protegernos de las amenazas actuales?

Pese a los denodados esfuerzos del personal de las organizaciones, lamentablemente los incidentes de ciberseguridad continúan creciendo permanentemente, impactando de manera negativa no sólo en la operatoria de las organizaciones, sino también en los costos de remediación, pérdida de imagen reputacional y en algunos casos sanciones económicas o legales impuestas por los entes reguladores. Esta situación no es ajena a nuestro país, donde se reportaron en los últimos meses, numerosos casos de organizaciones que han sufrido ataques de ciberseguridad, tanto obras sociales, como empresas agroexportadoras, empresas de seguros, y varios organismos del estado nacional, organismos públicos provinciales, entre otros.

Es fundamental que tanto las organizaciones públicas como privadas lleven adelante un programa de prevención de riesgos de seguridad de la información, que le permita proteger la información propia así como la de terceros que tenga en custodia. Este programa debe ser apoyado por la dirección y llevado a cabo por especialistas con conocimiento en buenas prácticas de seguridad de la información, con una revisión y actualización permanentes. Si la empresa no cuenta con los mismos internamente, es fundamental buscar el asesoramiento externo especializado, que la ayude a definir e implementar un programa de prevención adaptado a sus necesidades. A modo de guía inicial, en dicho programa integral deberían existir mínimamente las siguientes actividades: Concientizar e involucrar a la dirección, Identificar regulaciones y definir marco referencial, Designar un responsable y empoderarlo, Organizar la implementación, Identificar los riesgos, Priorizar los riesgos en base a su nivel, Definir e implementar un plan de acción basado en los riesgos, y Definir un esquema de Mejora continua.

Independientemente de las acciones llevadas a cabo por las organizaciones, cada uno de nosotros como usuarios de la tecnología debemos tomar acciones para protegernos de los riesgos a los que estamos expuestos. En la charla se presenta un conjunto de recomendaciones que se agrupan en los siguientes dominios: Navegación y hábitos seguros, Control de acceso, Identificación de mensajes fraudulentos, y Equipos seguros.

Disertantes:
Alejandra Gimenez y Claudio Ballhorst (INICIACTIVA)

CV de los disertantes:

Ing. Alejandra Giménez. CEO y fundadora de la consultora INICIACTIVA de la ciudad de Santa Fe, con mas de 15 años en el mercado.
Ingeniera en Sistemas de Información, egresada de la Universidad Tecnológica Nacional, Facultad Regional Santa Fe. Consultora especializada en aspectos de Gobierno y Gestión de la Seguridad de la Información y Ciberseguridad, con foco en la prevención, y en normas de Sistemas de Gestión de la Calidad ISO 9001 y CMMI. Auditor Líder ISO/IEC 27001 e ISO 9001 (IRCA), Cyber Security Foundation Professional Certificated (Certiprof). Conferencista en numerosas jornadas y eventos relacionados a la Seguridad de la Información. Profesional matriculada en el Colegio de Ingenieros Especialistas de Santa Fe Distrito I.

Ing. Claudio Ballhorst. Ingeniero en Sistemas de Información egresado de Universidad Tecnológica Nacional, Facultad Regional Santa Fe. Posgrado en Dirección Estratégica de Sistemas. Perito Informático del Superior Tribunal de la Provincia de Entre Ríos. Más de 20 años de experiencia en proyectos de Seguridad de la Información e Infraestructura. Consultor especializado en seguridad de la información y ciberseguridad en IniciACtiva. Conferencista en numerosas Jornadas y Eventos relacionados a la Seguridad de la Información y Ciberseguridad.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Keynote

Ciberseguridad Financiera: Un Desafío Apasionante y un Futuro de Oportunidades

Iniciando con un recorrido por la historia y la evolución de los principales ataques a la ciberseguridad en la historia de la informática, se presenta la estrategia de seguridad por capas, enfocada al riesgo, con el objetivo de proteger los sistemas informáticos de amenazas y brechas, garantizar el uso adecuado de recursos y aplicaciones del sistema, gestionar la recuperación pertinente del sistema a partir de un incidente de seguridad y cumpliendo con los marcos legales. En la charla se presenta una introducción a los principales marcos de gestión de la ciberseguridad y a los desafíos que se tienen respecto de la ciberseguridad. Además, se mencionan las herramientas que hoy en día ayudan a hacer frente a los desafíos. Para finalizar se presentan las oportunidades que existen para quienes deseen aventurarse a la ciberseguridad como carrera.

Disertante:
Diego Real (Banco Bica)

CV del disertante:

Diego Real. Ing. en Sistemas de Información egresado de UTN FRSF, Licenciado en Seguridad de la Información (Fundación Libertad), Gerente de Ciberseguridad de Banco Bica con más de 15 años de experiencia en la función. Previamente cumplió diferentes funciones en el área de tecnología, siendo desarrollador en sistemas IBM AS/400, analista y desarrollador en sistemas Visual Basic y administrador de Bases de Datos, lo cual le ha permitido conocer las distintas facetas del ámbito de la tecnología, y trabajar formando parte y liderando distintos equipos de trabajo.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Keynote

Ciberseguridad e Ingeniería Social

A partir de la pandemia surgió la necesidad de digitalizar muchos procesos y servicios, lo cual significó una oportunidad para los ciberdelincuentes ¿Cuáles son las estrategias emplean los ciberdelincuentes para hacer caer a sus víctimas en estafas? Se presenta en esta charla la fisonomía de un ataque y las principales formas de mitigar las ciberestafas.

Disertante:
Maximiliano Macedo

CV del disertante:
Maximiliano Macedo es Analista en Informática Aplicada egresado de la Facultad de Ingeniería y Ciencias Hídricas de la Universidad Nacional del Litoral, Perito en informática Forense, Matriculado en el Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación (COPITEC) Matrícula L-342. Posee más de 15 años de experiencia en proyectos de Seguridad de la Información. Co-fundador de ODILA: Observatorio de Delitos Informáticos de Latinoamérica. Es docente en materia de Evidencia Digital e Investigación de Delitos Informáticos para distintas Universidades, integrantes del Ministerio Público Fiscal y diversas Fuerzas de Seguridad Provinciales y Nacionales. Es conferencista en numerosas Jornadas, Congresos y Eventos relacionados al Derecho, la Seguridad de la Información y la Informática Forense, nacionales e internacionales.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Keynote

Ciberseguridad, una oportunidad para todos

Partiendo de analizar cómo la tecnología nos une y cómo la innovación digital impacta en todas las industrias y en la vida personal, se destaca la importancia de la ciberseguridad. A medida que el mundo digital continúa creciendo, la superficie de ataque se amplía, expandiéndose para incluir todo lo que pueda conectarse y comunicarse. Esto incluye redes, datos y contenido, personas, dispositivos y sistemas. La falta de profesionales con conocimientos en el área de ciberseguridad será uno de los retos más importantes para las empresas. Y una gran oportunidad para quienes se están formando y puedan ingresar a esta industria. En la charla se presentan los posibles caminos a seguir y las oportunidades para los jóvenes profesionales que buscan realizar carrera en la industria de la ciberseguridad.

Disertantes:
Claudia Suarez y Ángel Dituro (FORTINET)

CV de los disertantes:

Angel Dituro se desempeña como Systems Engineer de cuentas del Interior de Argentina para la empresa Fortinet, acompañando al área comercial en el desarrollo de arquitecturas estratégicas relacionadas a ciberseguridad en las organizaciones. Ha transitado un camino por diferentes fabricantes de tecnología y empresas integradoras dentro de rubros como networking, seguridad, telefónica, aportando desde diferentes roles, algunos más técnicos, otros liderando proyectos y finalmente en pre-venta técnica-comercial. También ha liderado equipos de trabajo donde se articulan esfuerzos público - privados para la organización de eventos masivos. Actualmente también se desempeña como profesor de la materia Arquitectura de Ciberseguridad en el Instituto de Ciberdefensa de las FF.AA.

Claudia Suarez es Ingeniera Electrónica egresada de la Universidad Tecnológica Nacional Facultad Regional Buenos Aires. Ha realizado una maestría en Gestión de las Comunicaciones y Tecnologías de la Información - Universidad Católica Argentina y la fundación EOI de Madrid, España. Es docente en la UTN FRBA, y actualmente se desempeña en la empresa Fortinet como Major Account Manager (Gerencia Enterprise / Service Providers).

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Keynote

Ciberseguridad: Aspectos Legales

Quienes se encargan de los aspectos técnicos de la ciberseguridad no deben perder de vista los aspectos legales y sociales que también están involucrados. En esta charla se aborda la normativa vigente en el país en materia de ciberseguridad. Se explicaron las figuras penales más relevantes relacionadas a la materia, tales como las estas informáticas, el daño informático y el acceso indebido a sistemas informáticos; así como la incorporación de las mismas al Código Penal Argentino mediante la Ley 26.388. Se analizan sintéticamente las principales amenazas y los ataques de ciberseguridad con mayor ocurrencia en el territorio nacional durante el último año. Se explica la importancia de los datos personales y de la toma de conciencia respecto a la huella digital que se deja como usuario de las diversas aplicaciones y plataformas. Además, se destaca el rol de la legislación como elemento de prevención y como herramienta de acción posterior a la ocurrencia de incidentes de ciberseguridad.

Se aborda además el tema de la responsabilidad bancaria que tienen las entidades financieras en general respecto de ciertas maniobras asociadas a la ciberdelincuencia. Los canales electrónicos que se utilizan para transacciones comerciales y financieras hoy ofrecen grandes posibilidades para mejorar la economía, al tiempo que representan riesgos muy importantes. El aumento de los delitos de estafas o fraudes digitales es una muestra de lo segundo. Los sistemas de ciberseguridad de las empresas se enfocan en proteger los activos más importantes frente a las amenazas más poderosas: ej. ramsonwares, mientras que la protección del consumidor suele ocupar los últimos puestos en el ranking de prioridades. Lo mismo ocurre con la capacitación de usuarios: se privilegia a los usuarios internos de la organización, mientras que, con el usuario externo se realizan campañas genéricas de difusión, sin segmentación ni aspiraciones de comunicación efectiva.

Los sistemas de validación de identidad suelen ser robustos, sin embargo, las malas prácticas de los usuarios son las que los exponen a los más graves riesgos, los cuales hoy son conocidos y, en su mayoría, pueden ser neutralizados. La ley prevé un reparto de riesgos para el caso: el uso de la firma electrónica (la más difundida por su ductilidad) expone a la empresa a tener que probar que la persona de su cliente fue la que operó el usuario electrónico cuando éste desconoce la firma electrónica que se le asigna, según la Ley de Firma Digital art. 5 (Ley 25.506).

En este escenario, ante ciber incidentes que causan daños a usuarios financieros digitales, las empresas deben responder ante los usuarios conforme la responsabilidad objetiva de seguridad (deber de resultado) dado que la actividad comercial/financiera en la web resulta riesgosa (un riesgo mayor a la actividad comercial no virtual) y siendo que se obtiene un provecho de la misma, no siendo justo trasladar los riesgos y retener los beneficios.

Por su parte, los diseñadores de sitios web deben estar conscientes que, mientras que en la realidad no virtual, las leyes de causalidad suelen ser las de la física, en los ecosistemas digitales son los desarrolladores los “creadores de causalidad”, es decir, que son quienes asignan las consecuencias a los hechos que ocurren en la web, lo cual puede representar una causa específica de responsabilidad civil (en la medida del aporte de “causalidad adecuada”): para la empresa titular del servicio tanto como para el diseñador.

Se recomienda a los usuarios perjudicados analizar los elementos del caso a la luz de las obligaciones legales del proveedor (ej. requisitos mínimos de seguridad del BCRA), los estándares regulatorios de la actividad en la web (ej. Ley 25.506) y los deberes del proveedor de diligencia especial en la prevención del daño. A los proveedores de servicios financieros en la web, se les recomienda una comunicación fluida con cada usuario, que permita perfilarlo y acotar los niveles de riesgos a los que se lo expone, evitando exposiciones de riesgos innecesarias, y, además, tener procedimientos adecuados para dar cuenta de una actuación diligente frente a ciber incidentes, de modo que se pueda probar en juicio que el riesgo presentado en cada caso no estaba comprendido en el ámbito de previsión de ocurrencia o actuación posible.

Disertantes:
Mariana Oroño y Marcelo Gelcich

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

CV de los disertantes:

Mariana L. Oroño. Abogada (Universidad Nacional del Litoral), Presidente de la Comisión de Derecho Informático del Colegio de Abogados de Santa Fe, Diplomada en Derecho Informático (Universidad de Palermo) y en Ciberdelitos (Universidad de Palermo), Especialista en Investigación en Ciberdelitos (Universidad Siglo 21), Socia titular en los Estudios Jurídicos Oroño Abogados y Oroño-Kiener Abogados, de la ciudad de Santa Fe.

Marcelo G. Gelcich. Abogado (Universidad Nacional del Litoral), Magister en Asesoramiento Jurídico de Empresa (Universidad Austral), Especialista en Derecho Administrativo (Universidad Nacional del Litoral), Coordinador General Jurídico de la Secretaría de Comercio Interior y Servicios de la provincia de Santa Fe, Diplomado en Derecho del Consumidor (Univ. Nacional Del Sur) ex delegado local de Proconsumer desde 2005 a 2020.

Trabajos de Investigación

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Definición de esquema de asignación de permisos

Definition of a permission assignment scheme

Presentación: 6/10/2023

Juan Carlos Ramos
Departamento de Ingeniería en Sistemas de Información (Universidad Tecnológica Nacional, Facultad Regional Santa Fe)
jramos@frsf.utn.edu.ar
María Luciana Roldán
INGAR, Instituto de Desarrollo y Diseño (CONICET/UTN)
lroldan@santafe-conicet.gov.ar

Resumen

Uno de los problemas más desafiantes en la gestión de redes grandes y sistemas de información es la complejidad de la administración de la seguridad. El control de acceso basado en roles (RBAC) (también llamado "seguridad basada en roles") se ha convertido en el modelo predominante para el control de acceso avanzado porque reduce este costo. El valor de negocio de RBAC resulta de integrar seguridad y políticas de accesos con una vista organizacional de requerimientos de accesos. Esta integración es habilitada por tecnología, pero es además es una iniciativa que permite alinear políticas, procesos y responsabilidades organizacionales. En este trabajo se estudia la propuesta de RBAC y se define un esquema de implementación de permisos inicial para el manejo de usuarios y roles en un sistema de información ejemplo, basado en el estándar RBAC.

Palabras clave: Control de acceso, Roles, Políticas de acceso

Abstract

One of the most challenging problems in managing large networks and information systems is the complexity of security management. Role-based access control (RBAC) (also called "role-based security") has become the predominant model for advanced access control because it reduces this cost. The business value of RBAC results from integrating security and access policies with an organizational view of access requirements. This integration is enabled by technology, but it is also an initiative that allows aligning policies, processes, and organizational responsibilities. In this work, the RBAC proposal is studied, and an initial permissions implementation scheme is defined for the management of users and roles in an example information system.

Keywords: Access control, Roles, Access Policies

Introducción

Los sistemas de información deben contar con, además de un mecanismo de autenticación, con un mecanismo de autorización a los usuarios (asignación de permisos y privilegios), el cual permite garantizar que éstos tengan los permisos correctos para realizar las actividades que le corresponden según su rol en el sistema.

Un estándar sobre esquema de asignación de permisos de acceso es el denominado **RBAC** (Rol-Based Access Control), (INCITS 359, 2004). Está comprobado [publicaciones] que modelo disminuye los costos de gestión de usuarios en un sistema de información. Existen otros modelos de control de acceso denominado 'Control de Acceso Discrecional' (Discretionary Access Control), (Gasser, 1988) en el que se incluyen mecanismos como 'Listas de Acceso' (Capability/Access List), 'Owner/Group/Other' y ACL (Access Control List), en el que se identifica a los usuarios individuales o grupos de usuarios que pueden acceder a un archivo. [ver si se pueden mencionar diferencias, ventajas desventajas]

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

El valor de negocio de RBAC resulta de integrar seguridad y políticas de accesos con una vista organizacional de requerimientos de accesos. Esta integración es habilitada por tecnología, pero es además es una iniciativa de negocio que bien direccionada permite alinear políticas, procesos y responsabilidades organizacionales.

El potencial real de RBAC reside en la capacidad para gestionar permisos de acceso, o simplemente permisos, a través de muchas aplicaciones, redes y plataformas. Es decir, es posible con un mismo proceso RBAC controlar el acceso a una red corporativa, y además, por ejemplo, gestionar las tarjetas de acceso a edificios. De hecho, RBAC ofrece beneficios a toda la organización no tan solo a una aplicación específica.

Para que la implementación de RBAC en una organización sea exitosa, se necesita encontrar una manera de determinar el mínimo o más simple conjunto de roles que provea a los usuarios con todos los derechos de accesos y activos que ellos requieren, pero no más. Lo expresado está basado en el Principio de Mínimo Privilegio (Bishop, 2002).

En este trabajo se estudia la propuesta de RBAC y se define un esquema de implementación de permisos inicial para el manejo de usuarios y roles en un sistema de ejemplo.

Desarrollo

El modelo RBAC incorpora el concepto de "rol" entre un sujeto (usuario/sistema) y el objeto protegido (dato o función), desacoplando los permisos entre el sujeto y el objeto correspondiente. En este modelo, un rol dado es el que tiene los permisos requeridos para ese rol, pudiendo ese rol corresponder a más de un usuario o sujeto.

El modelo central incluye cuatro elementos básicos: el usuario (*User*), roles (*Rol*), sesión (*Session*), y permisos (*Permissions*). Los permisos se establecen entre Operaciones (*Operations*) y Objetos (*Objects*).

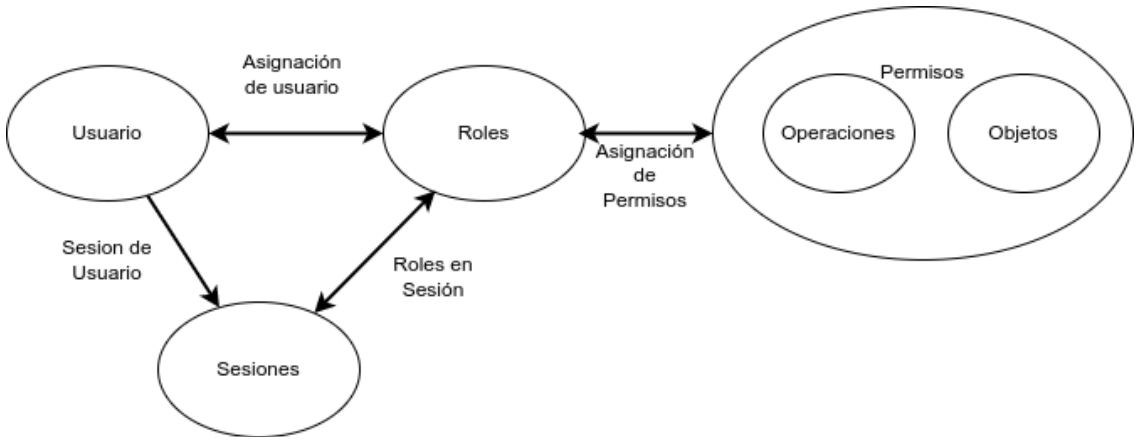

Figura 1: Principales conceptos que intervienen en el modelo RBAC (INCITS 359, 2004)

Un rol representa un conjunto de relaciones muchos a muchos entre usuarios individuales y permisos. Cada sesión (*Session*) es un mapeo entre un usuario y un subconjunto de roles activos que son asignados al usuario en un momento determinado. Un usuario puede tener muchas sesiones, y cada sesión tiene un subconjunto de roles asignados.

La idea básica de este modelo es asignar:

1. permisos a roles, y luego
2. los roles son asignados a usuarios.

De esta manera, en una sesión, los usuarios pueden obtener los permisos de acceso a través de sus roles. La relación entre los elementos es: un usuario puede tener múltiples roles, un rol puede ser asignado a múltiples usuarios; un rol puede tener múltiples permisos, un permiso puede ser asignado a múltiples roles.

Un "rol" es una función laboral dentro del contexto de una organización con cierta semántica asociada en relación con la autoridad y responsabilidad conferida al usuario asignado a tal rol.

El permiso es una aprobación para realizar una operación sobre uno o más objetos protegidos.

La Figura 1 ilustra las relaciones de asignación de usuario (UA) y asignación de permiso (PA). Las flechas indican una relación de muchos a muchos (por ejemplo, se puede asignar un usuario a uno o más roles y se puede asignar un rol a uno o más usuarios). Esta configuración proporciona una gran flexibilidad y granularidad en la asignación de permisos a roles y usuarios a roles. Esto evita que a un usuario se le pueda otorgar más acceso del necesario a los recursos.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Cada sesión es una asignación de un usuario a posiblemente muchos roles, es decir, un usuario establece una sesión durante la cual activa algún subconjunto de roles que se le asignan. Cada sesión está asociada a un único usuario y cada usuario está asociado a una o más sesiones. Los permisos disponibles para el usuario son los permisos asignados a los roles que están actualmente activos en todas las sesiones del usuario.

Definición de roles

Un rol es distinto al trabajo de un empleado, título o posición, dado que un empleado puede tener muchos roles, así como también dos empleados con el mismo título o posición pueden tener diferentes roles. Hay dos enfoques que suelen aplicarse en la definición de roles: definir roles de negocio y definir roles técnicos. El proceso de refinar y redefinir roles de negocio existentes para hacerlos utilizables para RBAC se denomina definición de roles "top-down". El enfoque alternativo denominado "bottom-up" asigna permisos de accesos concretos a empleados que pueden ser agrupados en roles. Una combinación de enfoques bottom-up y top-down (híbrido) es más efectivo en la definición de roles.

La definición de roles incluye dos subtareas: definir los permisos para el rol, y definir los usuarios a los que se da membresía en el rol.

Definición de Permisos de roles

Es clave en la definición de permisos aplicar el principio de "mínimo privilegio" (least-privileges)(Bishop, 2002).

Para cada usuario se deben identificar cuáles funciones o tareas representa en cada rol que tiene, a fin de describir el rol en términos de negocio, y determinar cuáles individuos cumplen con esos roles.

Un conjunto simple de roles debe representar responsabilidades para una función o tarea y definir un conjunto de permisos de acceso requeridos para poder realizar estas responsabilidades.

Definir miembros de Roles

El proceso de asignación más simple es disponer de una lista de individuos que cumplimentan los roles y asignarlos. Pero, si se quiere automatizar la asignación de roles, debe disponerse de un conjunto de reglas que mapeen usuarios a roles basadas en atributos de los usuarios.

Los sistemas de RRHH o directorios empresariales describen cada identidad mediante atributos tales como el código de trabajo, título del trabajo, centro de costo y clasificación de seguridad. Se pueden definir nuevos atributos no registrados actualmente para cada usuario los cuales deberían ser capturados e ingresados para los usuarios en el futuro. Basados sobre lógica booleana simple se pueden usar estos atributos para definir un conjunto de reglas de membresía para cada uno de los roles.

Estas reglas pueden no ser infalibles, y por esta razón presentar "falsos negativos" (alguien es excluido de un rol cuando en realidad le corresponde, otorgándole menos privilegios del que debería) y "falsos positivos" (alguien recibe un rol superior al que le corresponde, otorgándole más privilegios del que debería). De estos, el primero se puede resolver manualmente, en tanto que el segundo presenta un problema de seguridad (no cumple con el principio de mínimo privilegio).

La habilidad de las reglas de membresía de evitar falsos negativos se llama "cobertura" (*coverage*) (Qubera, 2011); un 100% de cobertura significa que se es capaz de identificar automáticamente para cada rol todos los usuarios que deben ser asignados. Por otra parte, la capacidad de evitar falsos positivos es llamada "precisión" (*accuracy*) de la regla; un 100% de *accuracy* significa que no se identificó ningún usuario que no debería ser asignado al rol.

Definición de Restricciones adicionales a RBAC

El modelo RBAC considera la inclusión de restricciones para "separación de funciones" (segregation-of-duties, SoD). Las reglas estáticas de SoD (SSD) especifican que dos roles conflictivos específicos no pueden ser asignados al mismo usuario. Por ejemplo, un empleado de 'Cuentas a Pagar' no puede además procesar 'Cuentas a Cobrar', y el mismo individuo no puede ingresar y aprobar cheques recibidos. SSD define y ubica restricciones sobre el espacio total de permisos del usuario. La política de SSD es complementaria y debe ser utilizada al momento de asignar roles.

SSD reduce la cantidad de permisos potenciales que pueden ser disponibles a un usuario mediante la definición de restricciones a ser aplicadas al momento de asignar roles.

La Separación de Funciones Dinámicas (Dynamic Separation of duty (DSD)) son incorporadas para limitar los permisos que están disponibles para un usuario. Pero lo hacen un contexto diferente a SSD: establece restricciones sobre los roles que pueden ser activados con o entre sesiones de usuario. Esto permite definir que un usuario tiene diferentes niveles de permisos en diferentes tiempos. Estas propiedades aseguran que los permisos no persisten más allá del tiempo necesario para realizar la función requerida. Los usuarios son

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

autorizados a uno más role (SSD) pero están restringidos a ser activados simultáneamente. Por ejemplo: un usuario que está autorizado a tener roles 'Cajero' y 'Supervisor de Cajeros', si el usuario está en rol 'Cajero' no puede cambiar al rol Supervisor de Cajeros hasta tanto no salga de su rol Cajero.

Asignación de roles a usuarios

Hay tres formas de proveer roles a usuarios:

1) Si las reglas de membresía son completamente seguras (sin falsos positivos) el proceso de provisión de roles puede hacerse automático. El sistema RBAC agrega o actualiza usuarios en el directorio, los evalúa de acuerdo a las reglas de membresía, y si ellos caen dentro de un criterio, le asigna el rol y provee de los recursos de IT.

2) Si las reglas de membresía son razonables, pero no enteramente confiables, se puede generar un workflow de requerimiento de acceso condicional, donde un gerente de seguridad de la información revisa y aprueba los roles asignados antes de que sean efectivamente asignados al usuario.

3) Si las reglas de membresía tienen una confiablidad baja, todas las asignaciones serán realizadas mediante un workflow de asignación manual en forma discrecional.

Implementación RBAC en un caso de estudio

Para ilustrar y generar una prueba de concepto del modelo RBAC estudiado, vamos a tomar como caso de aplicación un 'Sistema de Pedido de Compras (SPDC)' ficticio. El objetivo del sistema es permitir que los refrentes de las diferentes áreas de la organización realicen 'pedidos de compra' de diferentes elementos.

En primer lugar, se propone un modelo de clases UML que sirve de base para la implementación del modelo RBAC en un sistema real.

Figura 2: Modelo de clases RBAC Base

A partir de esta primera conceptualización, se refina el modelo en el modelo de la Figura 3.

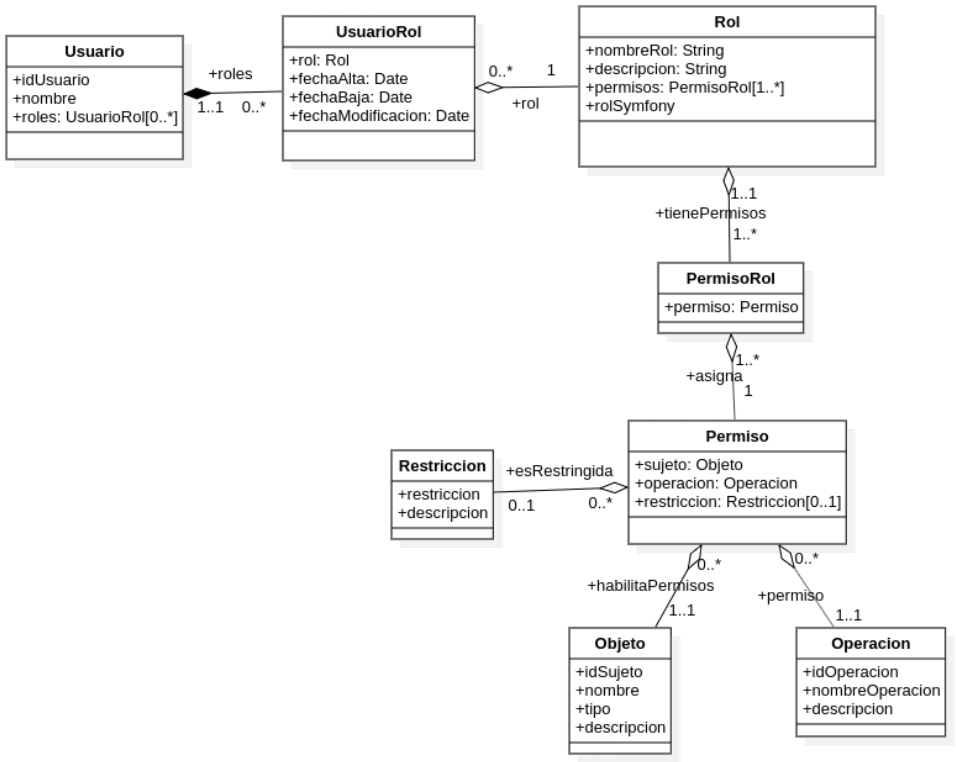

Figura 3: Diagrama de clases que especifica el diseño del modelo RBAC

Las transformaciones necesarias del modelo base consisten principalmente en transformar las asociaciones de 'muchos a muchos' y explicitar los 'Objetos' y 'Operación' que conforman cada 'Permiso'.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

En esta conceptualización se considera al concepto de sesión que incluye el estándar RBAC como un aspecto dinámico que se presenta al momento de que un usuario selecciona un rol, por tal motivo, se deja dicha funcionalidad a nivel de implementación del esquema.

Para considerar el tratamiento de la 'Separación de Funciones' (SoD) estática (SSD) y dinámica (DSD) se propone la siguiente solución:

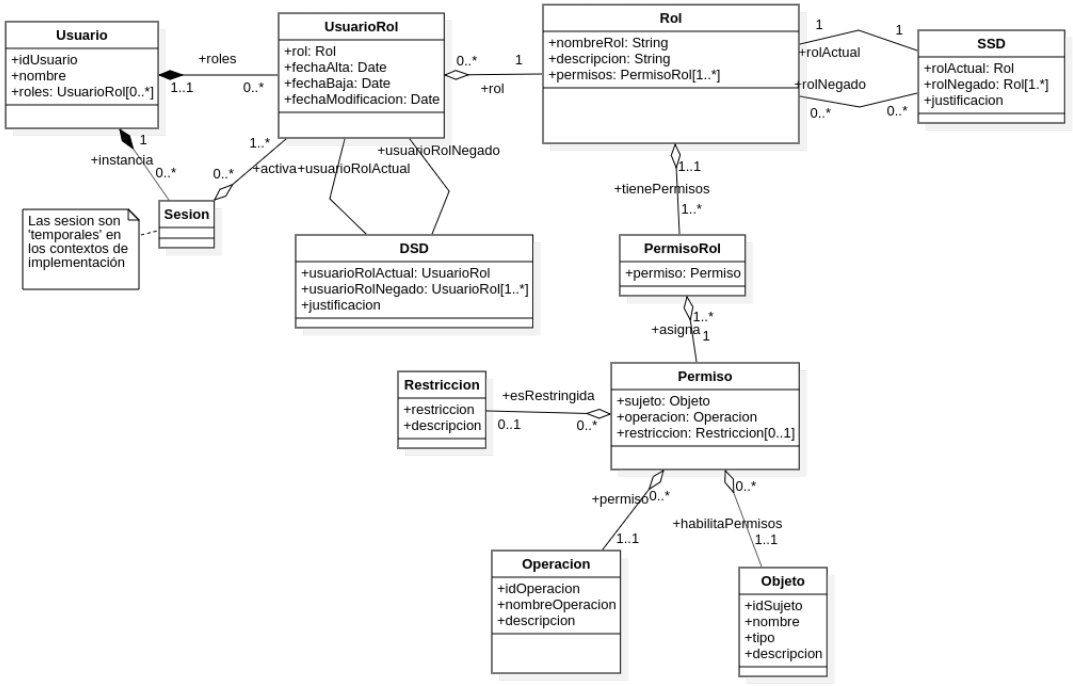

Figura 4 – Modelo RBAC extendido incluyendo SSD y DSD

Identificación de roles en el sistema

De acuerdo con lo planteado por el modelo RBAC, para materializarlo en el SPDC, el primer paso es definir los "roles" para dicho sistema. Se definen a continuación los "Roles Administrativos".

Los roles propuestos para este caso son:

- *Administrador SPDC*: tiene privilegios para realizar ABMC (Altas, Bajas, Modificaciones, Consultas) de todos las entidades propias del sistema, como así también de realizar todas las operaciones disponibles sobre éstas.
- *Referente de Área*: tiene privilegios para realizar ABMC de las "solicitudes de Compra" que pertenezcan a su área. Tiene privilegios para poder consultar los datos relacionados a una solicitud de compra.
- *Evaluador Técnico*: tiene privilegios para observar Solicitudes de Compra que involucren artículos que deban ser evaluados antes de poder hacer el pedido correspondiente.
- *Evaluador Presupuestario*: tiene privilegios para observar Solicitudes de Compra que involucren a sus áreas dependientes en cuanto al presupuesto asignado y que no se sobrepasen. Accede a funciones propias del evaluador presupuestario.
- *Superusuario*: en todo sistema habrá un 'super usuario' que tiene permiso para cualquier función del sistema. Puede trabajar sobre las entidades propias del sistema y las complementarias. Por ejemplo: las entidades de definición de permiso no están habilitadas para un 'Administrador Compras' (Administrador 'sistema').

Para este sistema se definen, entre otros, las siguientes Entidades (Objetos):

- Artículo
- Rubro
- Proveedor
- Período de Compra
- Solicitante
- Solicitud de compra
- Tipo de Unidad
- Unidad Administrativa

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

A continuación, se presenta un modelo conceptual de las entidades y objetos que intervienen en el SPDC, sobre los cuales se aplicarán ciertos permisos que darán lugar a la definición de los roles apropiados para el sistema.

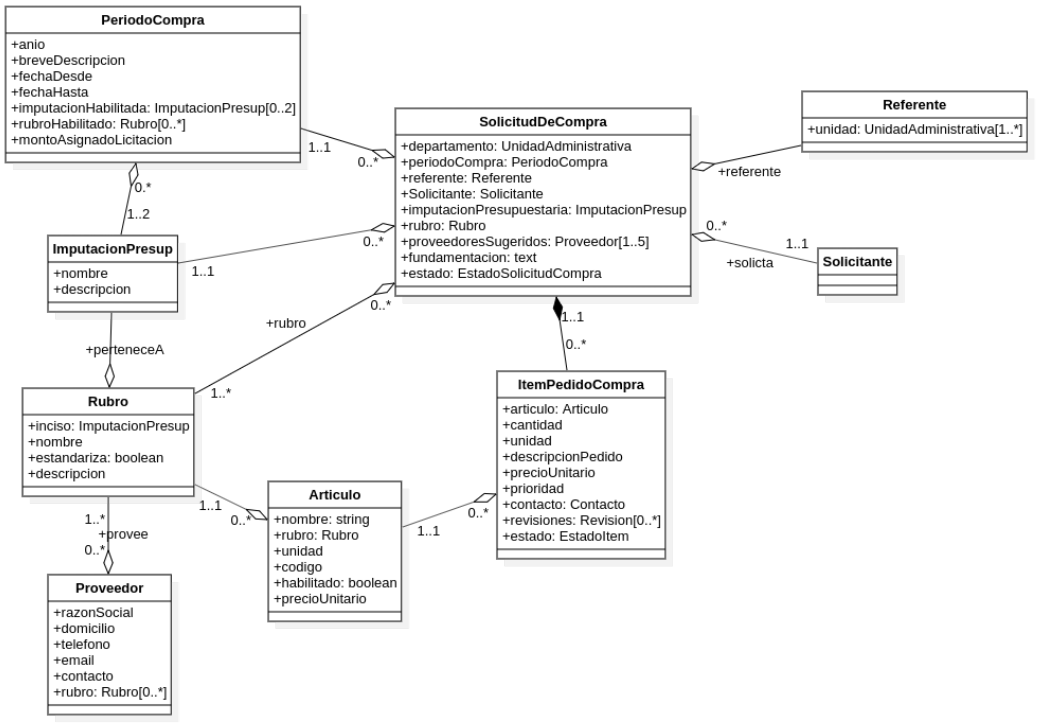

Figura 5: Modelo de clases que presenta entidades que intervienen en el SPDC

Para poder aplicar RBAC es necesario definir las *operaciones* que se pueden aplicar sobre una *entidad (objeto)*. Las principales son:

Tabla 1: Definición de posibles de operaciones sobre objetos/entidades

Operación	**Descripción**
Agregar	Agregar una instancia de una entidad.
Modificar	Modificar una instancia de una entidad.
Borrar	Borrar una instancia de una entidad.
Consultar	Consultar una/s instancia/s de una entidad.
Ejecutar	Ejecutar una función
Acceder	Acceder a una opción de menú. (es equivalente a 'Ejecutar')

Luego, los 'Permisos' sobre un 'Objeto' se dan estableciendo la relación 'Objeto / Operación' permitidos. A modo de ejemplo se indican en la Tabla 2 un subconjunto de permisos para el sistema.

Tabla 2: Definición de permisos sobre objetos/entidades

Objeto	**Operación**	**Permiso**
Articulo	Agregar	Agregar_Articulo
	Modificar	Modificar_Articulo
	Borrar	Borrar_Articulo
	Consultar	Consultar_Articulo
Rubro	Agregar	Agregar_Rubro
	Modificar	Modificar_Rubro
	Borrar	Borrar_Rubro
	Consultar	Consultar_Rubro
SolicitudDeCompra	Agregar	Agregar_SolicitudDeCompra
	Modificar	Modificar_SolicitudDeCompra
	Consultar	Consultar_SolicitudDeCompra
	Borrar	Borrar_SolicitudDeCompra

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Definición de Roles y Permisos para el sistema

Luego del análisis de los roles identificados en el sistema y los permisos requeridos, se procede a definir el mapeo entre los Usuarios-Roles y Permisos requeridos basados en el modelo RBAC.

Tabla 3: Roles y permisos por Objeto

Rol	Descripción	Permiso	Objeto
Superusuario	Administra el sistema. Puede realizar ABMC de todas las entidades, y funciones de administración.	Por definición tiene TODOS los PERMISOS sobre TODAS las entidades propias del sistema. No es necesario explicitarlas unas por una.	Todos
Referente de Área	Es la persona/usuario que puede realizar 'Solicitudes de compra' como referente de un área concreta por la que es responsable.	Agregar_SolicitudDeCompra	SolicitudDeCompra
		Modificar_SolicitudDeCompra	SolicitudDeCompra
		Consultar_SolicitudDeCompra	SolicitudDeCompra
Evaluador Técnico	Es la persona/usuario que puede evaluar una solicitud de compra con artículos que pertenecen a los rubros que él evalúa.	Consultar_SolicitudesDeCompra	SolicitudDeCompra
		ConsultarItemPedidoDeCompra	ItemPedidoCompra
		Agregar_ObservaciónItemSolicitud	ItemPedidoRevisión
		Consultar_ObservacionItemSolicitu	ItemPedidoRevision
Evaluador Presupuestario	Usuario director de área tiene permisos para consultar y evaluar los presupuestos de las áreas controladas.	Consultar_SolicitudesDeCompra	SolicitudDeCompra
		ConsultarItemPedidoDeCompra	ItemPedidoCompra
		Agregar_RevisionPresupuestaria	RevisiónPresupuestaria
		Consultar_RevisionPresupuestaria	RevisionPresupuestaria

Vale aclarar que todos los permisos no asignados, son negados.

A las definiciones de 'Objeto', 'Operaciones', y 'Permiso' se agrega el concepto de 'Restricción'. Una restricción define los diferentes tipos de restricciones que se pueden aplicar a una operación sobre un objeto.

Tabla 4: Tipos de restricciones

Restricción	Descripción
SOLO_LAS_PROPIAS	Puede aplicar la operación, pero SOLO para aquellas instancias en las que está relacionado directamente (sea el dueño de la instancia).
INSTANCIAS_HABILITADAS	De las instancias existentes, sólo puede aplicar el permiso sobre las instancias indicadas.
SOLO_LAS_DEL_AREA	Sólo puede acceder a las instancias del sujeto que pertenecen al área a la pertenece el usuario con este rol.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Cada una de estas restricciones brindan información que deben ser complementadas con procesos. Por ejemplo, deben existir procesos implementados que permitan obtener cuáles son las entidades de las que un sujeto/usuario es dueño o propietario. Además, es necesario contar con procedimientos para conocer cuáles son las ´instancias habilitadas´ de una entidad para un usuario. Por otro lado, el modelo debería ser enriquecido con mapeos que permitan establecer cuál es el ´área del usuario´. Estas necesidades se deben resolver implementando funciones complementarias en el código de acuerdo a lo requerido en cada caso. Y contar con algún mecanismo que permita disparar estas reglas de verificación cuando sea necesario.

Conclusiones

Se estudió el modelo RBAC y trabajó en el diseño de un modelo específico para un sistema de compras genérico. Esto significó llevar adelante las actividades de análisis necesarias para la identificación de usuarios, entidades, permisos, y roles requeridos.

Además, se definieron algunas restricciones para hacer más específicos los permisos a activar en determinadas sesiones, dependiendo de las relaciones del usuario con respecto a la propiedad o no sobre entidades del sistema.

Como trabajos a futuro se extenderá el modelo de diseño incluyendo la posibilidad de 'herencia de roles", así también como también la implementación de un proceso de asignación automática de roles.

Referencias

ANSI INCITS 359. (2004). *Role Based Access Control*
M. Gasser. (1988). *Building a Secure Computer System*, Van Nostrand Reinhold
M. Bishop. (2002). *Computer Security – Art and Science, (13.2.1 – Principle of Least Privilege)*, Addison Wsley
Qubera Solutions, Inc. (2011). *Implementing Role-Based Access Controls in the Enterprise*
Novell. (2007). *Smart Implementation of Role-based Access Control*.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

Perfiles Biográficos Digitales: Identificación de Atributos de Exposición y su Mitigación en Redes Sociales

Digital Biographical Profiles: Identification of Exposure Attributes and their Mitigation in Social Networks.

Presentación: 6/10/2023

Zenobi Román Pablo
Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina
rozenobi@hotmail.com

Roldán María Luciana
Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina
Instituto de Desarrollo y Diseño (CONICET/UTN), Santa Fe, Argentina
lroldan@santafe-conicet.gov.ar

Resumen

Una Red Social Digital es un grupo de personas que están conectadas entre sí por medio de una plataforma de software, la cual brinda el soporte para que cada persona tenga definido un 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 identificar los atributos de un perfil biográfico digital que contribuyen a elevar la exposición de la privacidad de las personas y plantear una serie de medidas de mitigación y buenas prácticas para una adecuada protección de la exposición en redes sociales.

Palabras clave: Privacidad, Redes Sociales Digitales, Exposición, Vulnerabilidad

Abstract

A Digital Social Network is a group of people who are connected with others through a software platform, which provides support for defining their profile and communicating with other ones. The profile that a person defines in a Digital Social Network is called “digital biographical profile”. The vulnerability regarding their privacy may be unknown to users as they are not aware of the risks to which they are exposed, due to the assumption of being supported by a platform "with established conditions of privacy". Exposure in a digital biographical profile entails a great responsibility, and each person must be the guardian of their privacy. The objective of this work is to identify the attributes of a digital biographical profile that contribute to increasing the exposure of people's privacy and propose a series of mitigation measures and good practices for adequate exposure.

Keywords: Privacy, Digital Social Networks, Exposure, Vulnerability.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

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 (Stalman, A., 2016), "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

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

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.

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 Wu He. (2012), 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. (Twitter, 2020). 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. (Infobae, 2018). 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.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

En agosto, publicado en (WhatsApp, 2016) se 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. (AEPD , 2018). 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 sobreexposición de la privacidad de las personas. En Rosenblum (2007), los autores 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.

En Choi et al. (2015), los autores 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 (2013), 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

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

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.

Desarrollo

- Atributos de Exposición

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 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.

Tabla 1: Tipos de publicaciones y su ubicación

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	

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

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. 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.

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 y de qué manera se puedan efectuar una mitigación y adecuación para proteger la exposición que afecte la privacidad de los usuarios. La idea es generar herramientas para alertar a los usuarios sobre qué tipos de datos podría dar a conocer con una potencial publicación, y advertir y crear conciencia, de manera de exponer lo que realmente quieren mostrar.

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. Esto es representado por el concepto *FactorIncrementoExposición* (FIE).

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

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 *AtributoDomicilio*	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. 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.
7. Datos de Académicos (*AtributoAcadémico*)	1. Nombre y locación de institución educativa. 2. Nombres de profesores y alumnos.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

	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. 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.

En la Figura 1 se puede ver un ejemplo de publicación de una foto en un perfil biográfico digital y cómo se identifican cada uno de los atributos que favorecen a la exposición.

Figura 1: ejemplo de publicación de una foto en un perfil biográfico digital e identificación de los atributos que favorecen a la exposición.

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). 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.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

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, a partir del concepto Perfil Biográfico Digital, se puede 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.

A partir de lo mencionado, se deriva el concepto de *Sujeto Expuesto Pasivo*. Este concepto representa al sujeto que sin haberlo hecho explícitamente en su propio perfil, posee un alto nivel de exposición. En este caso se debe a que, a través de instancias de publicaciones con alta exposición realizadas por amigos del sujeto en un PBD, es posible inferir información personal o privada debido a publicaciones en donde se encuentra arrobado o etiquetado.

- Mitigación y buenas prácticas

Como una regla de oro en relación con las Redes Sociales Digitales, cuando un usuario decida crear un perfil y publicar información, en primer lugar, debe saber que ya está ingresando a una plataforma de acceso público. Esto significa que su perfil estará en Internet y la superficie de exposición y posterior ataque será más alta en dicho ambiente. Por lo anterior mencionado, la clave está en cómo minimizar la exposición y tomar las medidas adecuadas para que la información compartida en las Redes Sociales Digitales esté protegida y se tenga control sobre la privacidad.

Como primera medida de mitigación, se debe proteger el dispositivo sobre el que se accede al perfil de la red social y el inicio de sesión concreto a la plataforma. Vale considerar que la Seguridad Informática actúa por capas, colocando medidas de seguridad en diferentes niveles, para proteger desde diferentes posiciones, de tal manera que, si un atacante logra superar una barrera, todavía existen otras que debe superar.

En base a lo anterior, el concepto de capas de seguridad aplicará a la protección del acceso a la Red Social para el usuario. Las siguiente capas de seguridad deben ser consideradas:

1) Seguridad a nivel de dispositivo:
   A. Contar con el sistema operativo vigente, con soporte y actualizado. Constatar que las últimas actualizaciones hayan sido aplicadas.
   B. Aplicaciones de uso actualizadas y con sus versiones actualmente soportadas por el fabricante.
   C. Inicio de sesión al Sistema Operativo con credenciales. Esto puede incluir usuario / contraseña, PIN, acceso biométrico y patrón.
   D. Bloqueo de sesión cuando el equipo queda desatendido. Al alejarse de la computadora, notebook o al dejar el celular, hay que asegurar de que se bloquea el dispositivo.
   E. Evitar escribir las contraseñas de acceso al dispositivo y/o plataformas en papeles o lugares visibles como ayudas memoria.

2) Seguridad de la Plataforma de Red Social:

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

A. Habilitar el Múltiple Factor de Autenticación (MFA) para el inicio de sesión. Este mecanismo agrega factores adicionales a la contraseña para confirmar la identidad de los usuarios.
B. Definir distintas contraseñas para cada Red Social. Es importante no repetir las contraseñas y no emplear patrones repetidos como, por ejemplo, mes del año, número de día, año, etc.
C. Considerar el uso de una plataforma de Gestión de Contraseñas. Estos programas permiten armar una biblioteca de todas las contraseñas de los sistemas con los que se opera. Sólo se debe usar una contraseña maestra junto con MFA para acceder a este servicio. Luego, dentro se podrá consultar por las contraseñas según cada sistema. Además, ofrecen herramientas para generar contraseñas robustas.
D. Evitar almacenar las contraseñas de inicio de sesión en el navegador web del dispositivo. Con cada intento de acceso se deberían de aplicar las credenciales.
E. Cerrar la sesión de la Red Social cuando se deja de usar la misma en el dispositivo.

3) Seguridad a nivel de "uso" de las Plataformas de Redes Sociales

Por otro lado, para mitigar la exposición de un perfil, se deben aplicar una serie de prácticas que ayudan a la "limpieza" de la exposición de un perfil en una red social digital. Con estas prácticas, lo que se busca es controlar los factores de exposición que posee el perfil. Este concepto se denomina también "sanitización" y hace referencia a articular las medidas y cambios necesarios para lograr un nivel de exposición adecuado.

Es importante mencionar que la exposición no se puede eliminar completamente y que, una vez que se publica información, ya no se tiene control de su ciclo de vida. En el caso de buscar la "máxima sanitización" posible, entonces se debería eliminar el Perfil completo de la Red Social.

Por lo tanto, considerando un perfil biográfico digital, se deben tener en cuenta las siguientes prácticas de sanitización:

A. Los "contactos" / "amigos" que están en Facebook, no necesariamente son los mismos que están en Instagram. Por eso, cobra importancia hacer una revisión completa de cada uno de los contactos que están en la red social y tomar acciones pertinentes.
B. De la revisión de cada perfil de las redes sociales, poner el foco en identificar los atributos de exposición del perfil y desde ese punto identificar los Factores de Incremento.
C. Como resultado del punto anterior, proceder a eliminar información con exposición detectada. Aprovechar la situación de detección de exposición no adecuada para generar un proceso de concientización sobre el tema a los usuarios. Es decir, a los propios contactos de la red social. Una forma de mitigación efectiva es reemplazar aquellas publicaciones que tenían esa exposición por mensajes de buenas prácticas y/o recomendaciones sobre cómo prevenir una exposición proclive a ataques.
D. Realizar una búsqueda del nombre del usuario en cada una de las redes sociales, usando un buscador. Considerando sus motores de búsqueda, se mostrarán los resultados en donde haya alguna mención sobre el usuario. Esto evidenciará, por ejemplo, aquellas fotos en que la persona fue "mencionada" / "arrobada". En este punto, aparecen los Sujetos Expuestos Pasivos. El mismo usuario puede ser un Sujeto Expuesto Pasivo, así como también, se puede descubrir que otras personas también están siendo expuestas, tal vez, sin consentimiento.

Un factor importante para mencionar es el comportamiento de los usuarios de las redes sociales digitales. Independientemente de las medidas de seguridad que cada plataforma implemente y de las configuraciones de privacidad efectuadas en los perfiles biográficos digitales, en última instancia está el comportamiento del usuario como único dueño de la exposición que desea realizar.

Conclusiones

Cada una de las personas dueñas de un perfil biográfico digital, son las propietarias de sus publicaciones y, por ende, son quienes deciden qué y cómo exponer la información. Si bien una herramienta informática podría

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

ayudar a mostrar qué nivel de exposición tiene una determinada publicación, la decisión final la tendrá cada usuario. Por lo dicho anteriormente, es clave trabajar en un proceso de concientización hacia las personas, relacionado al cuidado de la exposición en las redes sociales digitales y los posibles ataques y consecuencias que un inadecuado uso de la información puede producir en los usuarios y su entorno.

Este trabajo propone una capa de concientización para los usuarios de redes sociales que permita tener conocimiento del nivel de exposición de sus publicaciones, logrando que preservar la privacidad del usuario en el nivel deseado. Para ello se identificaron una serie de atributos de exposición frecuente, los cuales, en conjunto, con las medidas de sanitización prepuestas, contribuyen al fortalecimiento de las acciones que posibilitan la protección de los perfiles biográficos digitales.

Como un punto de partida para un programa de concientización para los usuarios, y un trabajo a futuro, se requiere realizar una encuesta a una determinada muestra para indagar sobre los comportamientos presentes en las Redes Sociales Digitales. La encuesta deberá indagar sería sobre el conocimiento de las personas de las Políticas de Privacidad de cada una de las plataformas. Es decir, si conocen de su existencia y si las tienen en cuenta para leer o si se omiten directamente.

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

1. Desarrollar una herramienta que se integre a los navegadores web y permita determinar y alertar a los usuarios de una posible exposición inadecuada cuando está subiendo una foto a un perfil biográfico digital. En un trabajo relacionado, se propuso un modelo conceptual que incorpora los principales aspectos que intervienen en el dominio de una herramienta de tales características.
2. Validar la herramienta como elemento de concientización tanto para uso individual, como por organizaciones.
3. Definir reglas que automaticen la detección de factores de exposición o usuarios expuestos pasivos.
4. Se explorará la posibilidad de emplear tecnologías de reconocimiento de imágenes.

La herramienta futura 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. A sí mismo, 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.

Referencias

Stalman, A. (2016). Humanoffon. Ediciones Deusto.

Wu He. (2012). A review of social media security risks and mitigation techniques. Journal of Systems and InformationTechnology, 14, 171-180.

LinkedIn. Protecting our members. (2016, 18 mayo). https://blog.linkedin.com/2016/05/18/protecting-our-members.

Infobae. (2018, 20 marzo). 7 claves para entender el escándalo de Facebook y Cambridge Analytica. infobae. https://www.infobae.com/america/tecno/2018/03/20/7-datos-para-entender-el-escandalo-de-facebook-y-cambridge-analytica

Política de privacidad de WhatsApp. (s. f.). https://www.whatsapp.com/legal/privacy-policy

AJEA – Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1300.2023

La AEPD sanciona a WhatsApp y Facebook por ceder y tratar, respectivamente, datos personales sin consentimiento. (s. f.). AEPD. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar

An update on our security incident. (s. f.). https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.

Rosenblum, D. (2007). What anyone can know: the privacy risks of social networking sites. IEEE Security & Privacy, 5(3), 40-49. https://doi.org/10.1109/msp.2007.75

Choi, B. C. F., Jiang, Z., Xiao, B., & Kim, S. S. (2015). Embarrassing exposures in online social networks: An Integrated perspective of privacy invasion and relationship bonding. Information Systems Research, 26(4), 675-694. https://doi.org/10.1287/isre.2015.060

Srivastava, A. P., & Geethakumari, G. (2013). Measuring privacy leaks in Online Social Networks. International Conference on Advances in Computing, Communications and Informatics (ICACCI). https://doi.org/10.1109/icacci.2013.6637504

DOI: https://doi.org/10.33414/ajea.1300.2023

JORNADA DE CIBERSEGURIDAD Y SOCIEDAD