Analítica en seguridad y privacidad

Características generales | Características del Equipo de Investigación | Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Analítica en seguridad y privacidad**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**Seguridad y privacidad**
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	**GRADIANT (Centro Tecnológico de Telecomunicaciones de Galicia)**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Juan González Martínez**	TELÉFONO	+34 986120430
ROL EN EL EQUIPO	Director del área de de Seguridad y Privacidad	MAIL	jgonzalez@gradiant.org
WEB DEL EQUIPO	https://www.gradiant.org/tecnologias/seguridad-y-privacidad/		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Citexvi	CENTRO	Campus Universitario de Vigo
TIPO DE VÍA	Rúa	NOMBRE DE LA VÍA	Fonte das Abelleiras
NÚMERO	s/n	CIUDAD	Vigo
PROVINCIA	Pontevedra	CÓDIGO POSTAL	36310

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Sara Campos Márquez
MAIL	gradiant@gradiant.org
TELÉFONO	+34 986120430
WEB	www.gradiant.org

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Citexvi	CENTRO	Campus Universitario de Vigo
TIPO DE VÍA	Rúa	NOMBRE DE LA VÍA	Fonte das Abelleiras
NÚMERO	s/n	CIUDAD	Vigo
PROVINCIA	Pontevedra	CÓDIGO POSTAL	36310

Analítica en seguridad y privacidad

Características generales | Características del Equipo de Investigación | Características de la Investigación

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Lilian Adkinson Orellana	Ingeniería de Telecomunicación Máster en Ingeniería Telemática Máster en Innovación Industrial y Optimización de Procesos

TRAYECTORIA PROFESIONAL

Lilian Adkinson Orellana es Ingeniera de Telecomunicación por la Universidad de Vigo, con la especialidad de Telemática. Posee además el Máster en Ingeniería Telemática y el Máster en Innovación Industrial y Optimización de Procesos, ambos por la misma Universidad. En 2009 se incorporó a Gradiant como investigadora y actualmente es la responsable de la línea de Analítica en Seguridad y Privacidad, la cual forma parte del área de Seguridad y Privacidad del centro. Durante su trayectoria profesional ha coordinado y participado en más de 20 proyectos de I+D relacionados con la seguridad y privacidad, machine learning, arquitecturas orientadas a servicios, tecnologías cloud e interfaces de usuario avanzadas. Además, durante su trayectoria ha recibido diversos premios tecnológicos y ha publicado varios artículos científicos en diferentes congresos internacionales.

WEB Y REDES SOCIALES

MIEMBROS DEL EQUIPO

Sestelo Pérez, Marta	Pintos Castro, Borja	López Román, Iago
Martínez Villanueva, Nora	Alonso Valderrey, Borja	Gómez Rodríguez, Iván
Elkortbi Martínez, Sara	Ortega Fernández, Inés	Pérez López, Roi
Sotos Martínez, Eva		

Analítica en seguridad y privacidad		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
ATAQUES Y DEFENSA ANTE AMENAZAS	Desarrode herramientas de detección de amenazas Detección de anomalías Detección y monitorizado de ataques Identificación y localización del atacante Filtraciones de Información
EVALUACIÓN DE SISTEMAS Y CIBERRIESGOS	Estudio de patrones Recolección de información sobre amenazas Detección temprana de ciberriesgos Inteligencia de Seguridad
INFRAESTRUCTURAS CRÍTICAS	Detección de amenazas
PROCESADO DE DATOS	Análisis de datos a gran escala
MÉTRICAS	Métricas Evaluación y métricas de privacidad Implementación de métricas de seguridad y privacidad en TIC Validación de métricas
PRIVACIDAD	Privacidad Tecnologías de potenciadores de la privacidad (PET) Sanitización y anonimización de datos Privacidad en Cloud
SISTEMAS FIABLES Y ACTUALIZABLES	Seguridad / Privacidad mediante el diseño Diseño de requisitos de seguridad
ÁREAS DE INTERÉS	Cloud Computing Data mining

Analítica en seguridad y privacidad		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS
PUBLICACIONES AÑO 2020
Adkinson Orellana L., Dago Casas P., Sestelo M., Pintos Castro B. A New Approach for Dynamic and Risk-Based Data Anonymization. Publication presented at 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020). Advances in Intelligent Systems and Computing, vol 1267. Springer, Cham. (2021)
PUBLICACIONES AÑO 2018
Martínez-Álvarez, R. P., Giraldo-Rodríguez, C., & Chaves-Diéguez, D. Large scale anomaly detection in data center logs and metrics. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (p. 37). ACM. (2018)
PUBLICACIONES AÑO 2015
Rodríguez Silva, D. A., González Castano, F. J., Adkinson Orellana, L., Pedrero López, B. (2015, May). Cloud Spreadsheets supporting Data Processing in Encrypted Domain. Publication presented at Proceedings of 5th International Conference on Cloud Computing and Services Science (CLOSER 2015)
Gürses, S., Troncoso, C. & Diaz, C. Engineering privacy by design reloaded. in Amsterdam Privacy Conference 1–21 (2015).
PUBLICACIONES AÑO 2013
Rodríguez Silva, D. A., Adkinson Orellana, L., Nuñez Taboada, D. M., González Castaño, F. J. (2013, May). PaaS Federation Analysis for Seamless Creation and Migration of Cloud Applications. Publication presented at Proceedings of 3rd International Conference on Cloud Computing and Services Science (CLOSER 2013).
Rodríguez Silva, D. A., Adkinson Orellana, L., Fernández Díaz, V., González Castaño, F. J. (2013, May). Towards Virtualization of Rich Applications for Distribution under a SaaS Model. Publication presented at Proceedings of 3rd International Conference on Cloud Computing and Services Science (CLOSER 2013).
PUBLICACIONES AÑO 2012
Rodríguez Silva, D. A., Adkinson Orellana, L., González Castano, F. J., Armino Franco, I., González-Martinez, D. (2012, June). Video surveillance based on cloud storage. Publication presented at 2012 IEEE Fifth International Conference on Cloud Computing (CLOUD 2012).
PUBLICACIONES AÑO 2011
Rodríguez Silva, D. A., González Castano, F. J., Adkinson Orellana, L., Fernández Cordeiro, A., Troncoso Pastoriza, J. R., & González Martınez, D. (2011, May). Encrypted domain processing for cloud privacy. Publication presented at Proceedings of 1st International Conference on Cloud Computing and Services Science (CLOSER 2011
Adkinson Orellana, L., Rodríguez Silva, D. A., Gonzalez Castano, F. J., Gonzalez Martinez, D. (2011, May). Sharing Secure Documents in the Cloud-A Secure Layer for Google Docs. Publication presented at Proceedings of 1st International Conference on Cloud Computing and Services Science (CLOSER 2011)
PUBLICACIONES 2010
Adkinson Orellana, L., Rodríguez Silva, D. A., Gil Castiñeira, F., Burguillo Rial, J. C. (2010, May). Privacy for google docs: Implementing a transparent encryption layer. Publication presented at 2nd Cloud Computing International Conference (CloudViews 2010)

Analítica en seguridad y privacidad

Características generales | Características del Equipo de Investigación | **Características de la Investigación**

PROYECTOS RELEVANTES
CLOUD ME UP (2010-2013): El objetivo es disponer de una plataforma cloud capaz de escalar recursos y aprovisionar servicios automáticamente. Se diseñó e implementó la capa de seguridad necesaria para ofrecer un servicio de reconocimiento de formas en la nube.
HIGEA (2012-2014): Creación de una aplicación orientada a la gestión de información clínica en la nube que almacene de forma segura datos médicos. Para garantizar la seguridad de la información en la nube, se cifrará el contenido de la base de datos asociada a la aplicación clínica, y se desarrollarán los mecanismos de seguridad necesarios para que dicha aplicación pueda realizar consultas eficientes sobre la base de datos como si su contenido estuviese en claro.
SIXIC (2012-2014): El proyecto surge de la necesidad de garantizar la seguridad en el sistema de gestión de crónicos planteado en el proyecto. Se ofrecerán diferentes capas de seguridad (biometría, cifrado, comunicaciones seguras) sobre la infraestructura cloud que servirá de soporte a la red social de gestión de crónicos del proyecto. La infraestructura cloud gestionará datos multimedia (entre otros tipos de datos), que se utilizarán para proveer al sistema de un control de acceso basado en reconocedor de locutor.
PRIPARE (2012-2015): Definición de metodologías de diseño que incluyan implícitamente aspectos relacionados con la privacidad y la seguridad en el diseño de sistemas TIC. La labor de Gradiant en este proyecto se centra principalmente en la creación de enlaces entre la investigación a nivel académico y las necesidades de la industria y la identificación de lagunas donde hace falta más investigación, o es necesaria una labor de transferencia de conocimiento para adecuar la investigación a los requisitos de producción.
SCAPE (2012-2017): El objeto de este proyecto es investigar tecnologías que permitan ofrecer mecanismos avanzados de seguridad en la nube. El proyecto se compone de tres subproyectos: SafeGDocs (SP1), que permite cifrar documentos en el SaaS de Google Docs mediante una extensión de Firefox; Criptonube (SP2), que permite gracias al uso de criptoprocesadores ofrecer un entorno seguro de ejecución dentro un proveedor cloud no confiable; y CloudSeep (SP3), que permite procesar datos de forma segura en un cloud utilizando técnicas de procesado de señal en el dominio cifrado.
WITDOM (2015-2017): El proyecto está dedicado a generar herramientas para la privacidad y seguridad de operaciones realizadas en entornos cloud. La labor de Gradiant cubre la definición de métricas de privacidad, el diseño de mecanismos de anonimización de datos y la implementación de herramientas para brokering de Clouds dependiendo de sus políticas de privacidad.
PRACTICIES (2017-2019): Prevención y detección en materia de radicalización basada en procesado de lenguaje natural. La tecnología permitirá complementar las herramientas de identificación o detección temprana y monitorización de situaciones sospechosas.
INFINITECH (2019-2022): Aplicación de técnicas de anonimización en entornos big data en los que se procesan datos de servicios financieros y seguros. Gradiant es socio del proyecto y proporciona una herramienta de anonimización que se utilizará en dos de los pilotos.
IRMAS (2017-2020): Protección de sistemas de información basado en el análisis de datos; Sistemas de control de acceso avanzado y verificación de identidad; Protección y compartición segura de activos digitales basada en el uso de tecnologías criptográficas hardware y software.
IRMAS 2.0 (2020-2023): Este proyecto se crea como continuación/consolidación del proyecto IRMAS, con el fin de trabajar en el diagnóstico y en la solución de problemas de seguridad de los sistemas de Seguridad de la Información, a través de la creación de diversos proyectos e iniciativas. En concreto, las actividades de innovación de este proyecto se organizan en tres áreas o líneas de trabajo, protección de la información, protección contra el fraude digital y ciberinteligencia.
REDBEE (2018-2019): El objetivo del proyecto es la detección, categorización y predicción automática de los ciberataques recibidos en una red de honeypots SSH, con el fin de obtener información representativa para un analista de seguridad. La herramienta realiza una categorización de los ciberataques basada en técnicas de Machine Learning no supervisadas. Incluye además un módulo de predicción de ciberataques basado en su evolución temporal. Con el desarrollo de este proyecto, Gradiant obtuvo el premio a la mejor solución del reto IN1 del programa de transferencia de las Jornadas Nacionales de Ciberseguridad
PERSIST (2020-2023): proyecto orientado a los supervivientes de cáncer colorrectal o de mama, financiado por la comisión europa y coordinado por Gradiant, en el que se desarrollan métricas para evaluar el nivel de privacidad de los datos, entre otros.
BIECO (2020-2023): BIECO es un framework holístico que proporcionará estos mecanismos para ayudar a las empresas a entender y gestionar mejor sus riesgos de ciberseguridad y las amenazas a las que están expuestas por el simple hecho de formar parte de la cadena de valor TIC. El framework, compuesto por un conjunto de herramientas y metodologías, se enfrentará a los retos asociados con la gestión de vulnerabilidades, resiliencia y auditoría de sistemas complejos.

Analítica en seguridad y privacidad

Características generales | Características del Equipo de Investigación | Características de la Investigación

PROYECTOS RELEVANTES

ÉGIDA (2020-2022): ÉGIDA nace como una red formada por 78 investigadores, de los cuales el 27% son doctores, con más de 15 años de experiencia en el ámbito de la seguridad y privacidad de sistemas e información, distribuida en 4 centros de trabajo ubicados en Galicia, Andalucía y País Vasco. Actualmente, los miembros de ÉGIDA facturan más de 9,7 millones de euros de euros en esta tecnología Cervera, lo que supone en promedio el 14% de sus ingresos anuales totales. En el proyecto se trabajará en 4 líneas tecnológicas: criptografía aplicada, protección de la identidad y privacidad, tecnologías para el desarrollo de sistemas de información seguros y seguridad en sistemas distribuidos. Además de estas cuatro actividades técnicas, ÉGIDA cuenta con otras dos actividades transversales, una orientada a la mejora de las capacidades investigadoras y otra relacionada con el impacto de la red.

CONGALSA 4.0 (2020-2022): el objetivo principal del proyecto es acometer un proceso de reorientación continua de toda la organización hacia la fábrica inteligente a través de un Gemelo Digital integral, uniendo producción y costes. El proyecto incluye el diseño e implementación de algoritmos basados en la detección de anomalías asociadas a posibles incidentes de seguridad, con el fin de identificar de forma temprana indicadores de que los sistemas industriales pueden haber sido comprometidos por un ciberataque.