

Contexto de tareas iniciales del Proyecto Desarrollar un Marco de controles de ciberseguridad para gestión y control de funcionamiento de redes IoT.

Bolatti Diego Angelo¹, Scappini Reinaldo¹, Gramajo Sergio¹, Jorge Roa¹, Raúl Montiel¹

¹ Centro de Investigación Aplicada en Tecnologías de la Información y las Comunicaciones de la Universidad Tecnológica Nacional (UTN), Facultad Regional Resistencia (UTN-FRRe).

Calle French 414, Resistencia, Provincia del Chaco, Argentina.

{dbolatti, rscappini, sergiogramajo,sroa, roajorge, raulmontiel}@gfe.frre.utn.edu.ar

Resumen

El objetivo principal de este artículo es presentar un panorama de las tareas preliminares para definir, arquitectura, parámetros, objetivos de control y controles; en el ámbito del proyecto “Desarrollar un Marco de controles de ciberseguridad para gestión y control de funcionamiento de redes IoT”; partiendo del estado del arte de la implementación de seguridad en ámbitos de redes de IoT

a) Contexto

El presente trabajo, está inserto en una línea de I/D presentada en la Universidad Tecnológica Nacional, y homologado con código: SIPPREE008640. Título: “Proyecto Desarrollar un Marco de controles de ciberseguridad para gestión y control de funcionamiento de redes IoT”. Dicho proyecto se lleva a cabo en el ámbito del CINAPTIC Centro de Investigación Aplicada en TIC Universidad Tecnológica Nacional Facultad Regional de Resistencia Chaco Argentina. El objetivo radica en la descripción de normas y tecnologías aplicadas en el ámbito de IoT, y brindar un contexto descriptivo del ámbito de trabajo, a los efectos de una mejor comprensión de los criterios adoptados en la selección de los objetivos de control y controles específicos. Las Redes que conforman la IoT, tienen características específicas que las diferencian de las redes de datos convencionales, y la principal es que el origen de los datos provienen de sensores y acceso inalámbrico mediante un gateway que introduce dichos datos al backhaul de la red del proveedor o eventualmente el camino inicial

hacia la aplicación de proceso de esos datos, también está presente la computación en la nube, paradigma que permite el acceso a la red a un conjunto escalable y elástico de recursos físicos o virtuales compartibles con aprovisionamiento de autoservicio y administración bajo demanda. El sistema de IoT incluye dispositivos de IoT, puertas de enlace de IoT, sensores y actuadores, también incluye aplicaciones y backend que admiten soluciones de IoT. Este conjunto de tecnologías perfectamente integradas, que potencialmente incluyen sensores, puertas de enlace y actuadores, pueden resolver un problema o necesidad específica o pueden usarse para crear funcionalidad adicional en otras soluciones que no sean de IoT. A toda esta infraestructura se denomina ecosistema, y un análisis profundo es esencial para desarrollar nuevas soluciones de ciberseguridad y sus aplicaciones, en particular a sistemas en nuestra región

1. Introducción

La norma ISO 27001 (octubre de 2005) es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

La ISO/IEC 27003, publicada el 1 de febrero de 2010, aunque fue actualizada el 12 de abril de 2017, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según el ciclo de Deming, o ciclo PHVA (acrónimo de Planificar, Hacer, Verificar,

Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002

ISO/IEC 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información originalmente cuenta con 11 dominios, 39 objetivos de control y 133 controles. Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. Esta norma fue revisada en distintas oportunidades, siendo la última en el año 2022

El 16 de febrero de 2022 fue publicada por la actualización de ISO 27002, norma diseñada para uso por parte de las organizaciones como referencia para la selección de controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la información (SGSI) con base en la norma certificable ISO/IEC 27001.

Se trata de la tercera versión de la norma ISO 27002, que tuvo su primera versión en 2.005 y la segunda en 2.013, con lo cual se establece un ciclo de actualización de versiones cada 8/9 años. Actualmente se encuentra disponible únicamente en idioma inglés.

Cambios en controles de seguridad: La norma ISO 27002:2013 contenía 114 controles (divididos en 14 dominios). La versión 2022 se modernizó y contiene 93 controles, divididos en 4 cláusulas que se enfocan hacia el contexto de aplicación.

Con respecto del término "Dominio": la norma ISO 27001, no utiliza el término "dominio de control" de la misma manera que algunas otras normas o marcos de seguridad. En su lugar, utiliza el concepto de "cláusulas de control" y "controles" en el contexto de la seguridad de la información. Este nuevo enfoque conlleva también la desaparición del concepto "objetivo de control", aunque se incluye un atributo que permite la clasificación específica del control en uno o más de 15 categorías, pero también en el año 2022 Se publica ISO/CEI 27400:2022; Ciberseguridad — Seguridad y privacidad de IoT

— Directrices. la organización en el tema IoT, y proporciona pautas sobre riesgos, principios y controles para la seguridad y privacidad de las soluciones de los conjuntos de controles críticos de ciberseguridad son acciones prioritarias que forman colectivamente un enfoque de defensa en profundidad y las mejores prácticas que mitigan los ataques más comunes contra los sistemas y las redes, el desafío de nuestro proyecto es establecer conforme los estándares y normas establecidas, un conjunto implementable utilizando soluciones no propietarias, y que además se adapte a las necesidades locales.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

En un anterior proyecto de investigación, "Análisis y Aplicaciones de Internet de las Cosas y Smart Cities basados en Telecomunicaciones y Seguridad" [1], acordamos atender sus objetivos sin perder generalidad, Durante 2019 los estudio preliminares y revisión de bibliografía se concretaron en la presentación de trabajos a diversos congresos, [2], [3], [4], [5] y un reporte técnico generando la necesidad de contar con una plataforma de ensayos y simulación que permita la prueba y validación de conceptos propuestos en el Technical Report "Proposal of an Intelligent Anomaly Detection System for IoT"[6], presentado ante la ITU y se puede resumir en la Figura 1; que muestra la arquitectura IoT estudiada. Existe bastante consenso en el hecho de ubicar monitores de tráfico en la capa de dispositivos, o lo más próxima posible a dicha capa. Nuestro grupo desarrolló un monitor que trabaja bajo este concepto (Figura 2) y se pueden ver los detalles en la publicación [7].

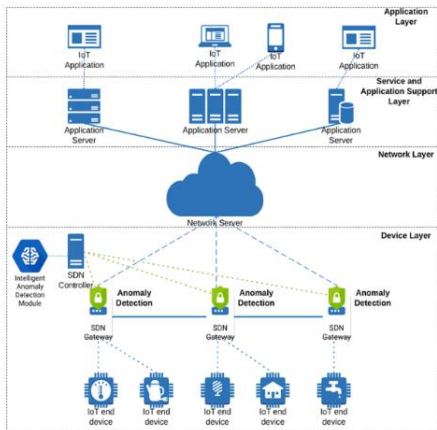


Figura 1 - Arquitectura IoT propuesta [propia]

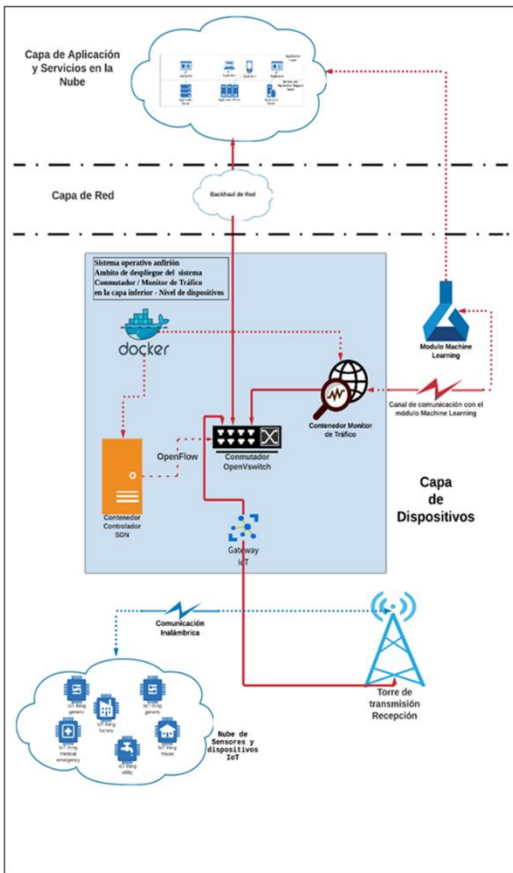


Figura 2 - Esquema del ámbito de desarrollo para el sistema de Conmutación y Monitoreo de Tráfico [propia]

2.1. Criterios generales (descripción de las principales fuentes seleccionadas)

A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) según

la norma ISO 27001, debemos considerar como eje central de este sistema la Evaluación de Riesgos. Este capítulo de la Norma permitirá a la dirección de la empresa tener la visión necesaria para definir el alcance y ámbito de aplicación de la norma, así como las políticas y medidas a implantar, integrando este sistema en la metodología de mejora continua, común para todas las normas ISO.

Lo primero, es elegir una metodología de evaluación del riesgo apropiada para los requerimientos del negocio. Existen numerosas metodologías estandarizadas de evaluación de riesgos. En este trabajo aplicamos la metodología sugerida en la Norma.

Las fases de esta metodología se muestra en la Figura 3:



Figura 3 - metodología de evaluación del riesgo [ISO 27001]

ISO/IEC 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la

información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

Acerca de la ISO 27400; este documento proporciona pautas sobre riesgos, principios y controles para la seguridad y privacidad de las soluciones de Internet de las cosas (IoT). Términos y definiciones Para los fines de este documento, se aplican los términos y definiciones dados en ISO/IEC 20924, ISO/IEC 27000, ISO/IEC 29100, ISO 31000 y siguientes:

- b) Computación en la nube paradigma para permitir el acceso a la red a un conjunto escalable y elástico de recursos físicos o virtuales compartibles con aprovisionamiento de autoservicio y administración bajo demanda. Ejemplos de recursos incluyen servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento[8] y [9]
- c) Servicio de almacenamiento en la nube una o más capacidades ofrecidas a través de la computación en la nube invocadas usando una interfaz definida[10]
- d) Dispositivo de iot entidad de un sistema de IoT que interactúa y se comunica con el mundo físico mediante la detección o actuación
- e) Desarrollador de dispositivos IoT entidad que crea un dispositivo IoT final ensamblado “final” en esta definición significa la etapa de entrega
- f) Plataforma de iot. infraestructura que permite la implementación, gestión y operación de dispositivos IoT
- g) Sistema de iot. Sistema que proporciona funcionalidades de Internet de las cosas. El sistema de IoT incluye dispositivos de IoT, puertas de enlace de IoT, sensores y actuadores. a la entrada: En el contexto de este documento, esto también incluye aplicaciones y backend que admiten soluciones de IoT.
- h) Solución de IO. Conjunto de tecnologías

perfectamente integradas, que potencialmente incluyen sensores, puertas de enlace y actuadores. Estos pueden resolver un problema o necesidad específica o pueden usarse para crear funcionalidad adicional en otras soluciones que no sean de IoT.

- i) Ecosistema. infraestructura y servicios basados en una red de organizaciones y partes interesadas. Nota 1 a la entrada: Las organizaciones pueden incluir organismos públicos.

3. MÉTODO DE TRABAJO:

Selección de fuentes confiables: Seleccionar fuentes de información confiables y autorizadas es esencial. Esto puede incluir bases de datos académicas, sitios web de instituciones educativas, publicaciones científicas, gobiernos y organizaciones internacionales, entre otros.

Uso de palabras clave: Identificar palabras clave relevantes relacionadas con el tema de investigación facilita la búsqueda. Estas palabras clave se utilizan para realizar consultas en motores de búsqueda y bases de datos.

Registro de resultados: Es importante llevar un registro de los resultados de la búsqueda, incluyendo enlaces a las fuentes relevantes, resúmenes y datos de referencia. Esto ayuda a mantener organizada la información recopilada.

Evaluación de la calidad de la información: Se debe evaluar críticamente la calidad y la relevancia de la información encontrada. No todas las fuentes en línea son confiables, por lo que es esencial verificar la credibilidad de las fuentes antes de utilizar la información en la investigación.

4. RESULTADOS OBTENIDOS / ESPERADOS

Con lo expuesto buscamos mostrar en forma estructurada las tareas iniciales en el ámbito del proyecto mencionado en el título.

Antes que nada, SIEMPRE se debe tener clara cuál es la meta que está definida en el objetivo del proyecto que es: **proponer el desarrollo de**

un marco de controles factible de implementación a empresas, organismos e instituciones gubernamentales de la región donde se encuentra ubicada nuestra Facultad Regional.

Con las premisas y método de trabajo buscamos:

- La definición taxativa de los aspectos de ciberseguridad a ser preservados en entornos IoT.
- Definición de Cláusulas de control (ex Dominio de control).
- Dentro del dominio, los objetivos de control y sus correspondientes controles específicos.

A futuro, se espera obtener como resultado, un conjunto de buenas prácticas para brindar seguridad conforme a las normas, pero que sean de aplicación específica para organizaciones públicas y privadas pertenecientes a la región de influencia de nuestra Universidad; permitiendo a las mismas ejecutar las acciones pertinentes, en un ciclo continuo tal como muestra en la Figura 4.

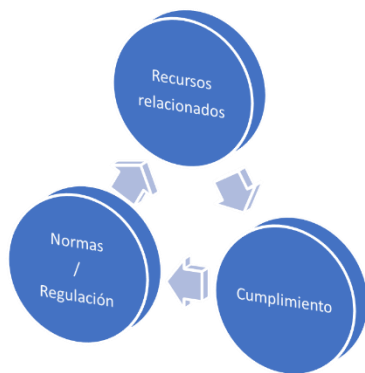


Figura 4 – Ciclo de implementación [propia]

5. BIBLIOGRAFÍA

[1] Sergio Gramajo; Reinaldo Scappini; Diego Bolatti; Ricardo Calcagno Frameworks de Internet de las Cosas y Ciudades Inteligentes basadas Telecomunicaciones y Seguridad. JATIC 2019 - IV Jornadas Argentinas de Tecnología, Innovación y Creatividad. REPORTE BREVE DE INVESTIGACIÓN. IV Workshop de Creatividad e Innovación en Informática (IV W - INF) Internet of Things (IoT) y wearables technologies. Tema (IA, IoT, smartcities).

Universidad CAECE - Mar del Plata, Buenos Aires, Argentina. 7 y 8 de noviembre de 2019

- [2] Carlos Ivan Piasentini, Jose Statkiewicz, Diego Bolatti, Reinaldo Scappini, Sergio Gramajo. Smartcities con LoRaWAN. El Caso de Monitoreo de Condiciones Ambientales de Lagunas en Tiempo Real. CACIC 2019. Congreso Argentino de Ciencias de la Computación. Workshop Arquitectura, Redes y Sistemas Operativos (WARSO). Universidad Nacional de Rio Cuarto. Rio Cuarto, Córdoba. 14 al 18 de octubre de 2019.
- [3] Federico Aguirre; Lucas Ibañez Claudio Basilio; Sergio Gramajo. Framework IoT para escenarios de multipropósitos. El caso de monitoreo de Shelters de Fibra Óptica. JATIC 2019 - IV Jornadas Argentinas de Tecnología, Innovación y Creatividad. CASO, EXPERIENCIA O INTERVENCIÓN. IV Workshop de Creatividad e Innovación en Informática (IV W - INF). Aplicaciones Creativas e innovadoras en Informática. Universidad CAECE - Mar del Plata, Buenos Aires, Argentina. 7 y 8 de noviembre de 2019.
- [4] Monzón German, Todt Carolina Mariana, Bolatti Diego Angelo, Gramajo Sergio, Scappini Reinaldo. Modelo de Seguridad IoT. CACIC 2019. Congreso Argentino de Ciencias de la Computación. Workshop Seguridad Informática (WSI). Universidad Nacional de Rio Cuarto. Rio Cuarto, Córdoba. 14 al 18 de octubre de 2019.
- [5] Federico Aguirre, Lucas Ibañez, Claudio Basilio, Sergio Gramajo. Framework IoT aplicado a Monitoreo de Precipitaciones de la Provincia del Chaco. CACIC 2019. Congreso Argentino de Ciencias de la Computación Tack Gobierno Digital y Ciudades Inteligentes. Universidad Nacional de Rio Cuarto. Rio Cuarto, Córdoba. 14 al 18 de octubre de 2019.
- [6] Diego Bolatti; Sergio Gramajo; Reinaldo Scappini; Ricardo Calcagno. Analysis and Applications of Internet of Things and Smart Cities based on Telecommunications and Security - UTN Facultad Regional Resistencia. Technical Report in International Telecommunication Union (ITU). ITU-T SG20RG-LATAM (Study Period 2017) Contribution 13. Date: 2019-09-02. Source: Universidad Tecnológica Nacional. AI/Question: QALL/20. Meeting: 2019-09-11 Access: <https://www.itu.int/md/T17-SG020RG.LATAM->

C-0013/en

- [7] Bolatti, D.A., Todt, C., Scappini, R., Gramajo, S. (2022). Network Traffic Monitor for IDS in IoT. In: Rucci, E., Naiouf, M., Chichizola, F., De Giusti, L., De Giusti, A. (eds) Cloud Computing, Big Data & Emerging Topics. JCC-BD&ET 2022. Communications in Computer and Information Science, vol 1634. Springer, Cham. https://doi.org/10.1007/978-3-031-14599-5_4.
- [8]] Recomendación UIT-T Y.3500 <https://www.itu.int/rec/T-REC-Y.3500-201408-I/es>
- [9] ISO/IEC17788:2014,3.2.5] <https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en>