TRABAJO FINAL DE TITULACIÓN

Desarrollo de un observatorio tecnológico enfocado a la Seguridad de la Información para Instituciones de Educación Superior (IES)

Propuesta de artículo presentado como requisito parcial para aprobar el título:

Maestría en Auditoría en Tecnología de la Información

Por los estudiantes:

Danny Vivanco Toala
Ingrid Chilán González

Bajo la dirección de:
Antonio Cevallos Gamboa

Universidad Espíritu Santo
Facultad de Ingeniería en Sistemas Telecomunicaciones y Electrónica.
Guayaquil - Ecuador

Febrero 2019

Desarrollo de un observatorio tecnológico enfocado a la Seguridad de la Información para Instituciones de Educación Superior (IES)

Development of a technological observatory focused on Information Security for Higher Education Institutions (IES).

Ingrid CHILÁN GONZÁLEZ[1]
Danny VIVANCO TOALA [2]
Antonio CEVALLOS GAMBOA[3]

Resumen

El objetivo del estudio de esta investigación, es el desarrollo de un observatorio tecnológico, orientado hacia la seguridad de la información para instituciones de educación superior. Para ello, mediante la revisión de la literatura y casos de éxito, se realizó un análisis de las múltiples funcionalidades que estos brindan y sus principales características para aportar al conocimiento. Además, mediante la entrevista a los informantes claves, se pudo validar la arquitectura desarrollada y la relevancia de este en el contexto ecuatoriano. Así también, el análisis de los resultados obtenidos de las encuestas realizadas a los informantes claves, donde todos coinciden que están "de acuerdo o totalmente de acuerdo" con la propuesta planteada del Observatorio Tecnológico. Se concluye, que el desarrollo de un observatorio tecnológico en seguridad de la información, se constituye en una herramienta relevante para la gestión del conocimiento, difusión, colaboración y soporte en el ámbito académico-científico.

Palabras clave: Seguridad de la Información, Observatorio tecnológicos, Instituciones de Educación Superior.

Abstract

The objective of the study of this research is the development of a technological observatory, oriented towards information security for higher education institutions. To do this, by reviewing the literature and success cases, an analysis was made of the multiple functionalities that these provide and their main characteristics to contribute to knowledge. In addition, through the interview with key informants, it was possible to validate the architecture developed and the relevance of this in the Ecuadorian context. Also, the analysis of the results obtained from the surveys made to key informants, where all agree that they are "in agreement or totally in agreement" with the proposed proposal of the Technological Observatory. It is concluded that the development of a technological observatory on information security is an important tool for knowledge management, dissemination, collaboration and support in the academic-scientific field.

Key words: Information Security, Technological Observatory, Higher Education Institutions

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail correo ichilan@uees.edu.ec.
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail correo dvivancot@uees.edu.ec.
[3] PhD (c) en Ciencias de la Dirección, MSIG, MBA, Ingeniero en Sistemas; Profesor Principal; Decano de la Facultad de Ingeniería en Sistemas, Telecomunicaciones y Electrónica en la Universidad Espíritu Santo - Ecuador; email: acevallos@uees.edu.ec.

INTRODUCCIÓN

Leite y Albuquerque (2019) señalan, que la evolución de la tecnología y la influencia del Internet, han impactado no solo a los técnicos informáticos, académicos o empresarios, sino también a la sociedad en general, ya que cada vez utilizamos los servicios en línea, para acceder a la información. Además está sujeto a varias formas de amenazas que afectan la seguridad de las personas mediante la explotación de vulnerabilidades. Asimismo, Mihai-Ştefan (2018) considera que los datos estadísticos a finales del 2017, habrían sido aproximadamente 4,15 millones de usuarios en Internet, con un incremento aproximado de 1 millón de usuarios por año, de un estimado de 7.63 mil millones de la población mundial, donde se evidencia que cada vez existen más usuarios conectados al Internet.

Según A Da Veiga y JHP Eloff (2007) indican que la seguridad de la información involucra en su trascendencia a la tecnología, los procesos y las personas, así como los procedimientos técnicos basados en políticas de acceso tales como contraseñas, biometría, y firewalls, ya que en la actualidad no son suficientes para mitigar las amenazas en cuanto a la seguridad de la información. Por otro lado Cárdenas, Martínez, y Becerra (2016) analizan, la evolución desde la seguridad física orientada a la protección de ordenadores y dispositivos de almacenamiento de información, a través de mecanismos y acciones que buscan la prevención y detección de vulnerabilidades, pasando por la seguridad de los sistemas y redes de tecnología de la información.

De acuerdo a Ramirez y Mejia (2015), señalan que a partir de un estudio realizado en México, la fuga de información a través del correo electrónico se encuentra situada con un 19.2% de incidencia, el cual es el principal riesgo para las empresas, así también, el robo de información vía dispositivos de memoria portátiles con el 13.6 %, y por último la sustracción de información en dispositivos móviles, laptops y tabletas con el 12.8%. Por otro lado, el 50% de las empresas en Ecuador presentan alguna brecha de seguridad en los últimos 12 meses, y de estas, el 20% no se pudo determinar el impacto de dicha brecha, ya que no cuentan con un proceso de gestión de incidentes (DELOITTE, 2017).

Borbúa, Chicango, y Herrera (2017) mencionan que el acceso al internet, ha registrado un incremento de usuarios durante los últimos 5 años, es decir, los datos revelan que en el año 2012, los usuarios de internet en Ecuador fueron el 22,5% de la población ecuatoriana y en el 2015 los usuarios que tuvieron acceso fueron el 32,8%. Por otro lado, Álvarez (2018) menciona, los riesgos de Ciberseguridad aumentan continuamente en los países de América Latina y del Caribe. Así pues algunos de ellos ya tienen una estrategia en operación, como Colombia, Jamaica, Panamá y Trinidad y Tobago. Además Henriques, Mendonça, Poleto, Camara, y Cabral (2018), mencionan que en el año 2017, el mercado global de Ciberseguridad tuvo daños relevantes en cuanto a pérdida de información, sistemas informáticos intervenidos por virus ransomware, entre otros, lo cual se cuantificó en pérdidas una cantidad USD 103.84 mil millones.

Respecto a las necesidades de seguridad, existe instituciones como European Network and Information Security Agency [ENISA] que señalan, cómo se creó el concepto de un equipo de respuesta ante incidentes de seguridad, Computer Security Incident Response Team [CSIRT], con la finalidad de atender las incidencias de seguridad relacionadas con la información, los cuales se emplean para mitigar y minimizar los riesgos en cuanto al número de respuestas necesarias que ofrecen los CSIRT's, asimismo, respecto a la implementación de un CSIRT, se enfocaría como relevante los siguientes puntos: el análisis del alcance del equipo que coordina y responde los incidentes, y los diferentes tipos de vulnerabilidades encontradas para crear una taxonomía y clasificación de incidentes dentro de la organización (Centro Criptológico Nacional, 2011; ENISA, 2006; Martins et al., 2011).

Por otro lado en Ecuador ya existe el Centro de Respuesta a Incidentes Informáticos del

Ecuador [ECUCERT], así como otros pertenecientes a entidades privadas tales como el Centro de Operaciones de Ciberseguridad [CSOC] de Telconect y CSIRT-CEDIA, los cuales son equipos conformados para responder a incidentes de seguridad informática, igualmente, son los encargados de la Gestión de incidentes y vulnerabilidades (CSIRT-CEDIA, 2019; CSOC, 2019; ECUCERT, 2019).

Por otra parte, la creación de Observatorios nace como un instrumento de análisis de varios temas o problemas de cualquier actividad, es decir, tienen como finalidad la evaluación y seguimiento de las diversas problemática de orden social. Además están destinados a captar, organizar, evaluar y procesar información para poder difundir conocimientos, mediante un portal o un sitio web, donde se especifiquen teléfonos y correos electrónicos, de tal manera que se puedan orientar a las instituciones del sector público o privado (Angulo, 2009; Diaz, 2013; DiFranzo et al., 2014; Phélan, 2007).

En cuanto a De la Vega (2007) señala, que en Francia en el año de 1990 se creó el primer observatorio de ciencia y tecnología en el mundo y ese modelo de organización se ha multiplicado en varios países. Por otro lado Torres y Martínez (2014) señalan, que el Observatorio Tecnológico aplicado desde la Universidad de San Buenaventura en Colombia, trabaja con el fin de potencializar el desarrollo tecnológico en entidades de diferentes sectores generando impactos económicos y sociales en beneficio del conocimiento, sin embargo en Ecuador el observatorio tecnológico gestiona, analiza y difunde información como estudios a los ciudadanos sobre tecnología de información y comunicación (OTIC, 2017).

De modo similar, Gonzalez, Marin, y Salinas (2013) señalan, que los Observatorios tecnológicos deben ser implementados y puestos a disposición de los investigadores para identificar problemáticas. No obstante, Moyares y Infante (2016) definen, el contexto de la educación superior, como un proceso basado en sistematización, que incluyen las actividades de gestión de tecnologías, permitiendo la anticipación a la ocurrencia de los riesgos y la eficaz toma de decisiones que garantizan la competitividad de la universidad. Del mismo modo, Sáez, Antolín, y Ricau (2009) mencionan que la competitividad de las empresas siempre están buscando la innovación tecnológica mediante la gestión de información en el ámbito científico y tecnológico.

Por otro lado Sanz, De Felippo, García, y García (2011) analizan, las limitaciones que existen en las actividades de una universidad. Entre ellas, el hecho que en algunos solo analizan determinados campos científicos, que incluyen un periodo temporal limitado, lo cual produce un enfoque inconcluso al mostrar únicamente una dimensión de las actividades de una universidad, es por ello que recientemente crearon un observatorio en la Universidad de España [IUNE], financiado por el Ministerio de Educación, convirtiéndose así en su fuente oficial de la información de las actividades de Investigación, Desarrollo e Innovación [I+D+i] del sistema universitario español.

El Observatorio de Seguridad de la Información [OSI] es un referente mundial al servicio de los ciudadanos, empresas y administraciones para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza en la Sociedad de la Información. Es así que, durante el año 2010, el observatorio publicó un total de 15 estudios sobre seguridad de la información y privacidad de los datos personales, dirigidos a ciudadanos y a empresas (INTECO, 2010; OTIC, 2017). Sin embargo, de acuerdo a los estudios antes indicados se puede evidenciar la problemática que no existe un Observatorio de Seguridad de la Información en el Ecuador que pueda aportar con el análisis, difusión y prevención de ataques y vulnerabilidades, que pudiesen existir en los servicios tecnológicos para las Instituciones de Educación Superior [IES]; y este Observatorio a su vez permita generar impactos económicos y posicionarse socialmente dentro de la industria universitaria, aportando con la difusión del

conocimiento, a través de la I+D+i en beneficio de la academia.

Por consiguiente, y de acuerdo a lo antes expuesto, el objetivo de la presente investigación es el desarrollo de un Observatorio Tecnológico [OT], orientado hacia la seguridad de la información para instituciones de educación superior, por lo que, se plantea la necesidad de proponer una arquitectura que permita crear el OT enfocado a la Seguridad de la Información.

MARCO TEÓRICO

En esta sección se abordarán los temas de Seguridad de la Información que involucra Gobernanza de Seguridad de la Información, Gestión de Seguridad de la Información, Equipos de Respuesta ante Incidentes de Seguridad Informática [CSIRT], Equipos de Respuesta ante Emergencias Informáticas [CERT], Ciberseguridad y Observatorios Tecnológicos, donde se detallarán la creación y estudios de los Observatorios Web y Observatorios TIC.

1. Seguridad de la Información

Según Merino y Cañizares (2012), el origen del por qué aplicar seguridad en la información puede estar en las siguientes causas: errores humanos, acciones malintencionadas, falta de control, fallo de los sistemas, carencia de formación y concienciación; lo que puede provocar en una serie de grandes consecuencias como: pérdida documental, pérdida de confidencialidad, indisponibilidad de la información, alto tiempo de recuperación, baja productividad, disminución del nivel de servicio, pérdida reputación y pérdida de oportunidades de negocio.

Por consiguiente, la seguridad de la información ha evolucionado desde la seguridad orientada a la protección de computadoras y dispositivos de almacenamiento de información pasando por la seguridad de sistemas y redes de tecnologías de información, mediante políticas, procedimientos y controles basados en las personas (Cárdenas et al., 2016).

Del mismo modo, Cano y Segurinfo (2009) indica que en Latinoamérica muestra una tendencia en la inversión de seguridad de la información en redes perimetrales, locales y en la protección de datos de clientes, donde muestran a los antivirus, las contraseñas y los firewalls como los mecanismos de seguridad más utilizados seguidos de los sistemas Virtual Private Network [VPN] y proxies. Así también, se muestra un interés por las herramientas de cifrado de datos, certificados digitales y control de contenidos, tres tendencias emergentes ante las frecuentes fugas de información y migración de las aplicaciones web a través de los servicios web (Daltabuit, Hernandez, Mallén, & Vásquez, 2007).

Es así que, la información se ha convertido en un activo importante para las organizaciones, más aún cuando es completa, precisa y actualizada. Así también la información se expresa como un sistema conformado por personas y recursos materiales, la cual se fundamenta en la teoría de la organización, es por ello que deben considerarse las organizaciones como sistemas de información (Martelo, Madera, & Betín, 2015). Los sistemas de información a medida que se consultan, almacenan y generan información se pone en riesgo la integridad de la misma tanto en el interior como en el exterior de la organización (INTECO, 2010).

Es por ello, que la seguridad de la información no es solo emplear nombres de usuarios y contraseñas, sino que requiere de reglamentos y diversas políticas de privacidad y protección de datos que imponen obligaciones para las organizaciones, además de lo indicado debe incluir seguridad del personal, control de acceso a usuarios, seguridad de red y otros aspectos regulatorios. Donde una política es simplemente una regla general para limitar las acciones que pudiesen realizar los empleados de una organización. Del mismo modo, los sistemas de gestión de información definen las políticas como un instrumento de control para establecer límites de comportamiento aceptable, guiar y restringir las decisiones y servir como estándares (Martelo et al., 2015).

1.1 Gobernanza de Seguridad de la Información

Zellhofer (2019) indica que las medidas de seguridad informática aplicadas en una institución con el fin de aumentar la conciencia de seguridad de la información se consideran un paso importante para lograr el cumplimiento de las políticas de seguridad, teniendo en cuenta que los problemas de seguridad de la información se basa en los aspectos técnicos, sociales, psicológicos y de organización, donde se refleja en un marco propuesto de proceso integral de los aspectos antes indicados llamado gobernanza de seguridad de la información. Donde, la gobernanza como concepto aislado representa el proceso de toma de decisiones y el proceso por el que las decisiones son implementadas. Del mismo modo, la gobernanza de seguridad de la información describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización (Cárdenas et al., 2016).

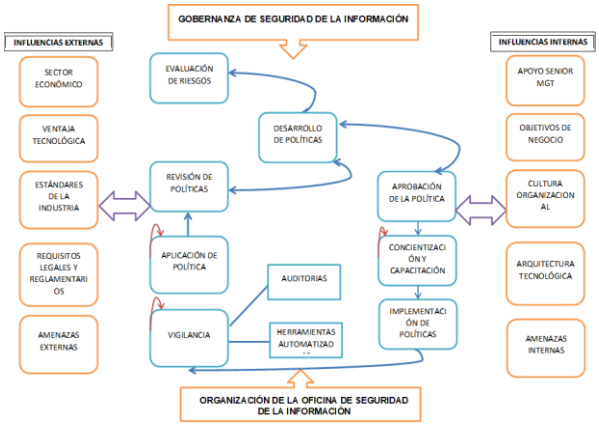


Figura 1: Modelo de proceso integral de la política de seguridad de la información.
Fuente: Elaboración propia adaptado de Zellhofer (2019).

En la Gestión de Seguridad de la Información, Diéguez, Cares, y Cachero (2017) mencionan que el conjunto de buenas prácticas en el tratamiento de los activos de información obliga a las empresas a disminuir la probabilidad de falla o vulneración y este conjunto se derivan de un estándar de seguridad de la información, lo cuales reúnen un conjunto de acciones tendientes al aseguramiento de la información importante de una organización, los cuales se referencian en normas como: ISO 27001, la cual se ha reconocido como el estándar más utilizado en todo el mundo, mientras que la norma ISO/IEC 27001:2013 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información [SGSI] (Cárdenas et al., 2016).

Según Ramirez y Mejia (2015) indica que un CSIRT es un equipo de especialistas en seguridad de la información dedicado a responder incidentes de seguridad de la información. Asimismo, el término CSIRT se suele usar en lugar del término CERT, registrado en EEUU por el CERT/Centro Coordinador [CC], para lo cual se usan las siguientes abreviaturas para el mismo tipo de equipos: Equipo de respuesta a emergencias informáticas [**CERT] o CERT/CC**, **CSIRT**, Equipos de Respuesta a Incidentes [**IRT]**, Equipo de Respuesta de Incidentes Informáticos **[CIRT]** y Equipo de Respuesta a Emergencias de Seguridad [**SERT]** (ENISA, 2006).

Los servicios de un CSIRT están alineados a las necesidades de la población sobre seguridad informática. Del mismo modo, los servicios que un CSIRT podría ofrecer serian muchos, pero hasta ahora ningún CSIRT los ofrece todos. A continuación se muestran de manera general los servicios más conocidos de CSIRT; sin embargo es necesario con métodos de llevar una adecuada gestión de acceso, seguridad en el puesto de trabajo, seguridad en aplicaciones y datos, seguridad en los sistemas y seguridad en las redes de cómputo (Mejía, Muñoz, Ramírez, & Peña, 2016; Ramírez & Mejia, 2015).

Tabla 1: Servicios de un CSIRT

Servicios reactivos	Servicios proactivos	Manejo de instancias
Alerta y advertencias	Comunicados	Análisis de instancias
Tratamiento de incidentes	Observatorio de Tecnologías	Respuesta a las instancias
Análisis de incidentes	Evaluaciones o auditoría de la seguridad	Coordinación de la respuesta a las instancias
Apoyo a la respuesta de incidentes	Configuración y mantenimiento de la seguridad	Gestión de la calidad de la seguridad

Fuente: Elaboración propia adaptado de Ramirez y Mejia (2015)

Tabla 1: Servicios de un CSIRT

Servicios reactivos	Servicios proactivos	Manejo de instancias
Coordinación de la respuesta a incidentes	Desarrollo de herramientas de seguridad	Análisis de riesgos
Respuesta a incidentes	Servicios de detección de intrusos	Continuidad del negocio y recuperación tras un desastre
Respuesta a incidentes en el sitio	Difusión de información relacionada con la seguridad	Consultorio de seguridad
Tratamiento de vulnerabilidad		Sensibilización
Análisis de la vulnerabilidad		Educación/Formación
Respuesta a la vulnerabilidad		Evaluación o certificación de productos

Fuente: Elaboración propia adaptado de Ramirez y Mejia (2015)

Con base al estudio de Andrade y Fuertes (2013) se observó que el proceso de implementación del CSIRT, se conforma de cinco etapas con objetivos y actividades específicas de acuerdo a la Figura 2: **Etapa 1**. Alistamiento y definición de procedimientos., **Etapa 2**. Capacitación y entrenamiento, **Etapa 3**. Gestión de alertas e investigación. **Etapa 4**. Respuesta a incidentes y apoyo a la comunidad. **Etapa 5**. Operación, revisión y mejoramiento continuo.

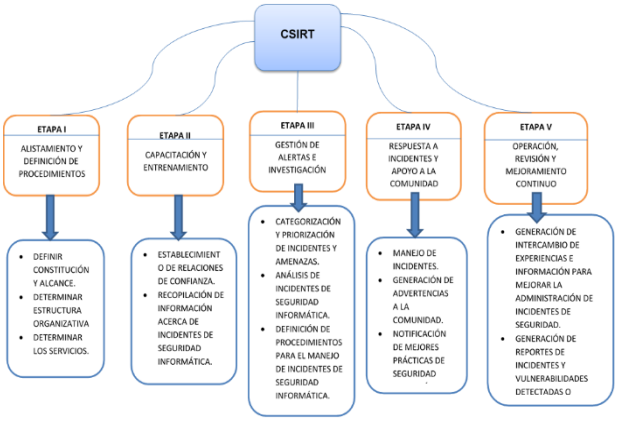


Figura 2: Etapas y actividades para la implementación de un CSIRT.
Fuente: Elaboración propia adaptado de Andrade y Fuertes (2013).

Es la Capacidad de Respuesta a emergencias informáticas. Por lo tanto el CERT es competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas, como es en temas de avances en tecnología, malware, fraudes y protección de datos (INCIBE, 2015). Según Miranda y Ramirez (2016) los resultados que se obtuvieron, revisando los sitios web sobre 10 CSIRTs/CERTs, los cuales se eligieron al azar tomando en consideración que fueran CSIRTs/CERTs formalmente establecidos. Durante el análisis, se buscaron elementos de páginas web oficiales de CSIRTs que se encuentran registrados dentro del portal de FIRST [Improving Security Together], el cual es el foro mundial de respuestas a incidentes y equipos de seguridad, donde se añadieron otras características o sitios que lo complementen, así como seguridad en idioma/tips, blogs, cursos, suscripción a alertas y redes sociales, a continuación se enlistan los resultados que se muestran en la Tabla 2; es así que, se puede indicar que es importante esta comparación porque se evidencia el comportamiento de cada características según el sitio Web de un CSIRT o CERT seleccionado, además, como factor común se tiene que él Acerca de, Eventos y Noticias estarían ubicados en todos los sitios Web de los Centros o Instituciones descritas.

Tabla 2: Cuadro comparativo de CSIRT/CERT

Características-Sitios	INCIBE	UNAM-CERT	INFOTEC	CERT	US-CERT	CERT-EU	NCI	ENISA	TERENA	TF-CSIRT
Acerca de	si	si	si	si	si	si	si	si	si	si
FAQ	si	no	si	si	si	no	no	no	no	no
Misión y Objetivos	si	si	si	si	si	no	si	si	no	no
Contacto	no	si	si	si	si	si	si	si	si	si
Eventos	si	si	si	si	si	si	si	si	si	si

Fuente: Elaboración propia adaptado de Miranda y Ramirez (2016)

Tabla 2: Cuadro comparativo de CSIRT/CERT

Caracterís ticas- Sitios	INCIBE	UNAM-	INFOTE	CERT	US-CERT	CERT-EU	NCI	ENISA	TERENA	TF-
Documentos	si	si	si	si	si	si	no	si	si	no
Herramientas	si	si	si	no	no	si	no	si	no	no
Vulnerabilidades	si	si	no	si	si	si	no	no	no	no
Noticias	si	si	si	si	si	si	si	si	si	si
Indicadores/Estadísticas	no	si	no	no	no	si	no	no	no	no
Enlaces	si	si	si	si	si	si	si	si	si	si
Seguridad en tu idioma	no	si	no	no	si	no	no	no	no	no
Blogs	si	no	no	si	no	no	no	no	no	no
Cursos	no	no	no	si	no	no	no	si	no	si
Reportes de incidentes	si	si	no	si*	si*	no	no	no	no	no
Suscripción a alertas	si	si	no	si	si	si	si	si	si	no
Redes sociales	si	si	si	si	no	no	no	si	si	no

Fuente: Elaboración propia adaptado de Miranda y Ramirez (2016)

En cuanto a Rea, Calvo, y San Feliu (2018), señalan que la ciberseguridad, se sintetiza como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información. Así también en sus inicios, la ciberseguridad era relativamente simple, enfocada a virus y código malicioso. Pero en la actualidad, es una actividad compleja, caracterizada por ataques persistentes a gran escala que permiten entrar en las redes internas empresariales, generando pérdidas económicas, robo de información crítica, caída de los servicios, e incluso llegando hasta la pérdida de la imagen y prestigio de la empresa. Así pues, la seguridad cibernética representa un desafío complejo, para todas las empresas dentro de la Industria, por lo que es aplicada a los sistemas y redes de computadoras, conectados a Internet, que necesitan proteger la información de los ataques cibernéticos (Henriques et al., 2018; Lezzi, Lazoi, & Corallo, 2018; Srinivas, Das, & Kumar, 2019).

2. Observatorios

Los observatorios están dedicados al análisis de varios temas o problemas, y se están empleado para referirse a un portal o sitio web, como un instrumento de análisis de cualquier actividad. Por otro lado, están destinados a captar, organizar, evaluar y procesar información para poder difundir conocimientos. Por lo tanto están compuesto de acuerdo, a las necesidades de cada País, para ejecutar políticas públicas en el componente de seguridad (Angulo, 2009; Diaz, 2013; DiFranzo et al., 2014; OEA, 2013; Phélan, 2007).

Por otro lado Herrera (2005, 2006) señala, que los observatorios latinoamericanos se diferencian entre sí, como su origen, composición, orientación ideológica, sus estructuras y modos de funcionamiento. En particular los aspectos de los medios que analizan, es el instrumental metodológico que emplean y la sistematización de su actividad.

Por otro lado, Aguilar y Rodrigues (2014) mencionan, que los observatorios latinoamericanos en educación surgen como un instrumento capaz de interconectar y dinamizar el intercambio entre investigadores, centros, grupos, laboratorios e instituciones con vocación para la Investigación comparada en Educación. A continuación se analizan la

clasificación de los observatorios en tecnológicos.

2.1 Observatorios Tecnológicos

En Francia el año 1990, se creó el primer observatorio de ciencia y tecnología [OST] en el mundo y ese modelo de organización se ha reproducido en varios países. En efecto para la creación de observatorios de diferentes temas, en la que se puede monitorear de manera sistemática de un sector o problemática. Asimismo, permite el intercambio de información, creación de conocimiento, para la visibilidad de artículos, y difundir información procesada a través de informes (De la Vega, 2007; Moyares & Infante, 2016).

Los Observatorios Tecnológicos apoyan a la vigilancia tecnológica, es decir procesa, gestiona y observa, a su vez son desarrollados con diferentes paradigmas y metodologías. Dado que capturan información externa con el propósito de transformarla en conocimiento. Pues gracias a las características más atrayente es la capacidad que tienen los agentes de adquirir y generar conocimiento con un alto nivel de importancia, al ser actual y novedoso. Asimismo, con la integración de una herramienta de información se entrega informes, resúmenes y alertas que permiten a la toma decisiones (Brown, Hall, & Harris, 2014; Hadfeg, Morales, & Moreno, 2015; Moreno, Carrasco, Rosete, & Delgado, 2013; Moyares & Infante, 2016).

El Observatorio de Tecnología de la información y Comunicación [OTIC], dado que es la unidad técnica que integra las principales estadísticas y estudios del sector de las TIC. De hecho, a partir de los observatorios TIC nacionales e Internacionales en Colombia, es necesario identificar los ejes de acción de cada uno de ellos. Así también, es un espacio en el cual se trabajan proyectos relacionados con el uso de implementación, aplicación y apropiación de las TIC, con el fin de potencializar el desarrollo tecnológico en entidades de diferentes áreas generando impactos económicos y sociales. Si bien, es un espacio que recopila, consolida, gestiona y promociona información integral del sector y las convierte en publicaciones para el apoyo al diseño de políticas públicas en América Latina. Además, ayuda a las empresas de los diferentes tipos de industrias, así como las Instituciones de Educación Superior, para que sean más competitivas, en innovación tecnológica tanto interna como del entorno para generar conocimiento a la sociedad (OTIC, 2017; Sáez et al., 2009; Torres & Martínez, 2014).

Booth, Hall, Gibbins, y Galanis (2014), señalan, que el observatorio web fue concebido como un entorno global de recursos y análisis de datos abiertos, con todo utilizan procesos analíticos innovadores para congregar puntos de vista de los datos observados. Por ende, utilizan la web como una plataforma para la publicación de datos interactivos. Así también, DiFranzo et al. (2014) mencionan, que al realizar metadatos más explícitos y fácilmente indexados por los motores de búsqueda y otros agentes para la comunidad científica, se podrían identificar mejor las oportunidades.

De acuerdo a González, Bonacic, y Fernández (2015), mencionan, que el observatorio web en tiempo real son sistemas capaces de controlar de forma automática la información de cualquier tema o redes sociales. Por otro lado. Tinati, Wang, Brown, Tiropanis, y Hall (2015), señalan, que la estructura se compone de dos grupos principales que pertenecen ya sea a los sistemas concebidos y desarrollados. Por otra parte, Diaz (2013), asevera que el método de análisis, para dar sentido a la cantidad de contenido generado por los usuarios es la web social.

Por otro lado la importancia de los Observatorios Tecnológicos aplicados desde una Institución de Educación Superior [IES], aportan a la ciudadanía en la difusión e intercambio de la información y conocimiento para la investigación de algún tema. Por consiguiente los referentes teóricos de los observatorios tecnológicos varían de los diferentes autores consultados. En la tabla 1 se presenta un análisis de los observatorios implementados en el sector de la Educación Superior que representan casos de éxito (Gonzalez et al., 2013; Moyares & Infante, 2016; Torres & Martínez, 2014).

Tabla 3: Observatorios tecnológicos en el sector de Educación Superior.

Componentes		OT1 Observatorio IUNE	OT2 Red de observatorios de las universidades cubanas	OT3 Observatorio de la red de macro-universidades públicas de América Latina y el	OT4 Observatorio Virtual de Transferencia de Tecnología (OVTT)
País		España	Cuba	España	España
Objetivo		Seguimiento de la actividad científica de 73 universidades españolas	Compilador de 23 observatorios de universidades cubanas especializados en áreas temáticas	Análisis de la situación de la educación superior de América Latina y el Caribe	Impulsar la transferencia de conocimientos, tecnología, innovación y emprendimiento en Iberoamérica
Herramientas tecnológicas	**Herramientas de búsqueda y**	Web of Science y Red OTRI	Directorios, Bases de datos y Archivo documental	Catálogo de postgrado, de tutores y de líneas de investigación	Meta buscador Observa Sistema de alertas de VT
	Herramientas colaborativas		Foro, blogs, RSS, etiquetado y marcadores sociales		RSS, Redes sociales y Redes de investigadores
Cartera de productos		Nivel medio de análisis, en los informes, ofrece a sus usuarios finales, los datos primarios de análisis	Alertas tecnológicas, foro de discusión para el intercambio de temas de interés entre los usuarios	libros, revistas, líneas de investigación, servicios de información	Publican a sus usuarios productos que incluyen un estándar bajo y medio de análisis

Fuente: Elaboración propia adaptado de Moyares y Infante (2016)

Tabla 3: Observatorios tecnológicos en el sector de Educación Superior.

Componentes	OT1 Observatorio IUNE	OT2 Red de observatorios de las universidades cubanas	OT3 Observatorio de la red de macro-universidades públicas de América Latina y el	OT4 Observatorio Virtual de Transferencia de Tecnología (OVTT)
Metodología de trabajo	Caracterización de la actividad científica de las universidades a partir de indicadores bien definidos	Está establecido que cada observatorio funcione a partir de las orientaciones de una hora de ruta que rige el ME	Captura de información y consulta. Cada universidad ingresa sus datos al sistema	funciona a partir de tres ejes de actividad: Contenidos, Herramientas y acciones

Fuente: Elaboración propia adaptado de Moyares y Infante (2016)

2.2 Observatorios Tecnológicos: Arquitectura

Existen muchas arquitecturas de observatorios tecnológicos, construidos de unas series de pasos y conjuntos de módulos que soportan su funcionamiento, para el apoyo de la toma de decisiones. En la figura 3 se muestra una arquitectura basada en un Sistema Multi Agente [SMA], está compuesto por una capa cliente y una capa para el SMA. En la capa cliente está la interfaz gráfica. La capa del SMA está compuesta por un repositorio y cuatro tipos de agentes: agente personal (AP), agente de confianza (AC), agente analista (AA) y agente fuente de datos (AFD) (Espino, Suárez, Bustamante, Férnandez, & Dapena, 2014; Moreno et al., 2013).

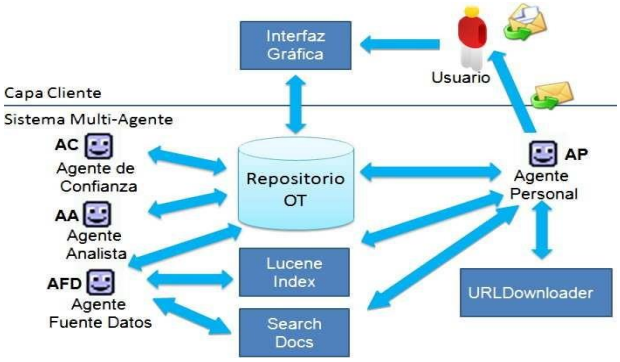


Figura 3. Arquitectura del sistema OT basada en un Sistema Multi-Agente.
Fuente: Moreno, et (2013).

Del mismo modo, el Observatorio Web Southampton [SUWO], proporcionan acceso a fuentes controlables y visualizaciones de datos. En efecto se muestra la figura 4, que es un enfoque de desacoplado con el fin de ofrecer reconfiguración y escalabilidad para el análisis, el almacenamiento y visualizaciones en la portal web. Así pues se integran mediante la API del observatorio web. Es decir, la arquitectura está asociada con un conjunto de datos y otras visualizaciones separadas y operando de una manera distribuida (A Da Veiga & JHP Eloff, 2007; Ramine, Xin, Thanassis, & Hall, 2015; Tinati, Wang, Tiropanis, & Hall, 2015)

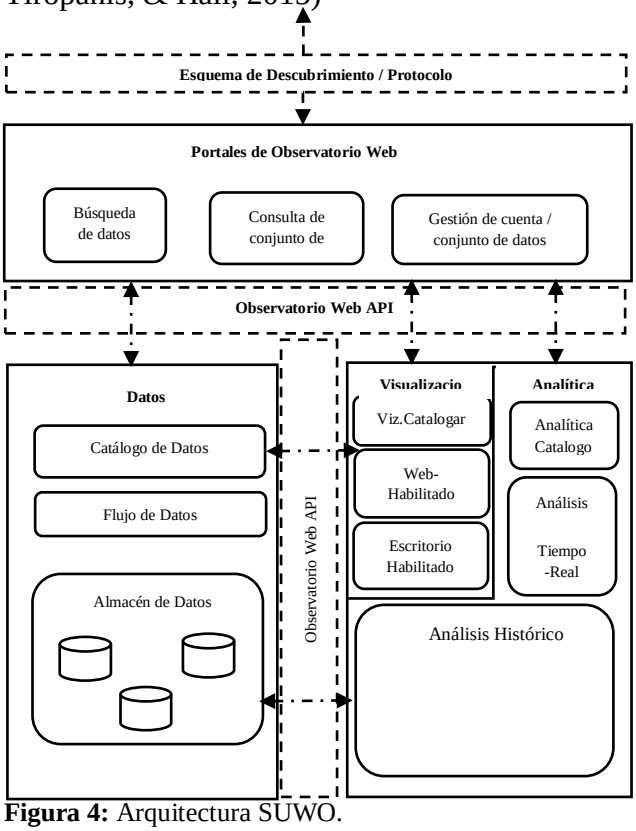


Figura 4: Arquitectura SUWO.
Fuente: Elaboración propia adaptado de Ramine et al. (2015)

En cuanto a Matray et al. (2007) el Observatorio Virtual de Medición de Redes [nmVO], consiste en mejorar investigación en la red, a través de la medición de datos disponibles. Por lo tanto proporciona un marco adecuado para la red con las herramientas de datos y análisis asociados a la infraestructura ETOMIC [European Traffic Observatory Measurement Infrastructure]. Así también, permiten ejecutar consultas simples y complicadas que se almacenan en el servidor, por ende, no hay necesidad de transferir datos masivos no procesados a través de la red. En definitiva el servicio web habilitado de la arquitectura [nmVO] se muestra en la Figura 5.

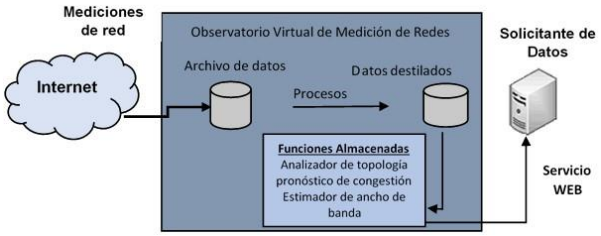


Figura 5: Arquitectura del Observatorio nmVO
Fuente: Elaboración propia adaptado de Matray et al. (2007)

El observatorio de conducta de seguridad es una infraestructura cliente-servidor diseñada para recopilar una amplia gama de datos sobre el comportamiento de los usuarios y las computadoras de cientos de participantes durante varios años. A continuación se ilustra la arquitectura en la Figura 6, donde el flujo de datos resulta de la siguiente manera: Cada cliente y servidor se autentican mutuamente cifrando los números aleatorios para el acceso de los datos. (Forget et al., 2014)

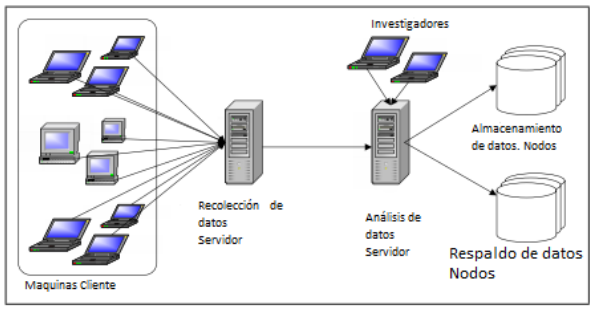


Figura 6: Arquitectura de hardware de alto nivel SBO
Fuente: (Forget et al., 2014)

El proceso que realiza el equipo de la estructura funcional y operativa del Observatorio Tecnológico, se señala en la

Figura 7, el cual es el encargado de realizar investigaciones básicas de evaluación de apropiación y uso de las TIC, asimismo, realiza las propuestas de implementación de acuerdo con dichos estudios, coordina y ejecuta las diferentes labores administrativas propias del observatorio (Torres & Martínez, 2014).

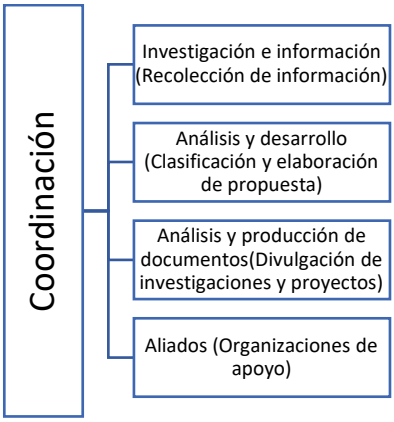


Figura 7. Estructura funcional y operativa del Observatorio TIC
Fuente: Elaboración propia adaptado de Torres y Martínez (2014)

2.3 Observatorios Tecnológicos: Seguridad de la información y Ciberseguridad.

Es un grupo de especialistas dedicados a la comunicación, formación y divulgación en la materia de TIC y las nuevas tecnologías. Por lo tanto, el objetivo de un observatorio es: Observar, analizar, asesorar, detectar ataques, difundir la cultura de la seguridad. Así también, malos hábitos, sistemas de defensa, protección en el mundo TIC y promover mejoras que impulsan la sensibilización a través de una herramienta web. Es decir que incluyan, para la sociedad, los estudiantes y la comunidad académica en general, en los distintos ámbitos de la Ciberseguridad y la seguridad de la información. A continuación se presenta la tabla 4, sobre un análisis de los observatorios, en los que detallan los objetivos y catálogos de productos (CYBERWATCHING, 2019; INCIBE, 2019; INTECO, 2010; IURISCYBER, 2019; OSIC, 2019).

Tabla 4: Observatorios tecnológicos en Seguridad de la Información y la Ciberseguridad

Autores	OBSERVATORIOS	Objetivos	Catálogo de Productos	País
(INCIBE, 2019)	Observatorio en Seguridad de la Información	Desarrollar soluciones innovadoras a través de la I+D+i Potenciar la transferencia tecnológica desde la investigación	Avisos de seguridad Kit de concienciación Cursos y talleres **Herramientas** Políticas de seguridad, Servicio antibotnet, Análisis de riesgo, servicios antiransomware, ciberseguridad	España
OSIC (2019)	Observatorio en Ciberseguridad	Observar y detectar ataques, malos hábitos, sistemas de defensa y protección, en el mundo TIC, en distintos ámbitos de la ciberseguridad y la seguridad de la información.	Formación. Servicios Comunicación dirigida a ciudadanos, instituciones y empresas.	España
(OSALC, 2019)	Observatorio de la ciberseguridad en américa latina y el caribe	Seguridad cibernética Resultado de una gestión entre el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) para presentar una imagen actualizada en seguridad cibernética	Informe para los gobiernos y expertos en seguridad cibernética en sus respectivos países y en todo el hemisferio	Estados Unidos de América

Fuente: Elaboración propia

Tabla 4: Observatorios tecnológicos en Seguridad de la Información y la Ciberseguridad

Autores	OBSERVATORIOS	Objetivos	Catálogo de Productos	País
CYBERWATCHING (2019)	Observatorio I+D de Ciberseguridad	Centro en línea para I + D en ciberseguridad y privacidad en Europa.	Ofrece a los ciudadanos acceso a productos, servicios y software de TIC innovadores y confiables que tienen en cuenta los derechos fundamentales, como la privacidad. Kit de comunicación e Informes	Europa
(IURISCYBER, 2019)	Observatorio de ciberseguridad	Investigar y analizar las problemáticas jurídicas, de las nuevas tecnologías y la cibercriminalidad	Espacio académico único que está en el centro de la discusión de temas innovadores, actuales y de suma importancia para la sociedad.	Colombia
(MIU, 2019)	Observatorio en ciberseguridad	Vincular, en persona o virtualmente, instituciones, empresas y académicos. Por lo tanto, se espera que el Observatorio multiplique los esfuerzos a un gran número de instituciones	Informe sobre el estado del arte de protección de infraestructura crítica en la seguridad Publicaciones: Sector público y privado, investigación nacional e internacional. Programas de formación abiertos al público	EE.UU e Italia
ODILA (2019)	Observatorio de Delitos Informáticos de	Ser una guía para orientar al usuario, brindar información y fomentar la realización de denuncias	Denunciar delitos informáticos. Reportes anuales de delitos denunciados e Incidentes.	España

Fuente: Elaboración propia

METODOLOGÍA

Se realizó una revisión sistemática (artículos científicos, revistas indexadas, libros, entre otras fuentes de información primaria y secundaria), con un tipo de investigación cualitativa, con un alcance exploratorio-analítico para la recolección de la información más relevante sobre la estructura funcional y operativa de los observatorios tecnológicos existentes, de igual forma, mediante la comparación de estudios y observatorios tecnológicos existentes, para encontrar elementos comunes para la propuesta antes planteada, asimismo, a través de entrevista a informantes claves, la cual se establecieron características comunes relevantes, lo que permitió constituir los procedimientos para el desarrollo de la arquitectura del observatorio tecnológico.

Para el estudio se tomó la muestra por conveniencia para la validación del modelo propuesto, realizada a las Empresa TELCONET S.A, DELOITTE, DIRTIC (Dirección de Tecnologías de la Información y Comunicaciones de la Armada del Ecuador), APPLE y la UNIVERSIDAD DE STANFORD, para lograr las entrevistas se seleccionaron 5 informantes claves, con un método de investigación que permite observar la experiencia en, seguridad de la información, Ciberseguridad, gestión de riesgos, Auditoria en tecnología de la información, prevención de ataques, vulnerabilidades e incidentes y respuestas ante incidentes de seguridad [CSIRT]. Para ello, se utilizó como instrumento un cuestionario de preguntas, las cuales fueron validadas en base a la revisión de la literatura de varios autores (Crespo, 2018; ITU, 2018; Vera, 2017).

En cuanto al análisis e interpretación de los resultados de la investigación, la información obtenida de la técnica de recolección de datos, mediante las entrevistas considerando los resultados reflejados de los informantes claves, para luego realizar un rastreo de las entrevistas en profundidad, la cual está orientada a la validación del modelo propuesto, los cuales coinciden que están “de acuerdo o totalmente de acuerdo” con el esquema planteado y la

percepción sobre las capacidades y alcance de un Observatorio Tecnológico en Seguridad de la Información aplicado a las Instituciones de Educación Superior. Para lo cual, es importante destacar también que algunos de los informantes indicaron que la información que llega al observatorio no se coordina sino se redirecciona a los CSIRT, asimismo mencionaron que para la propuesta del desarrollo del observatorio no se debe generar conocimiento sino aportar conocimiento a la academia, ya que, generar conocimiento es investigación para tesis doctoral.

3. DESARROLLO DEL OBSERVATORIO TECNOLOGICO EN SEGURIDAD DE LA INFORMACIÓN

De acuerdo a lo antes expuesto, a continuación se va a detallar el desarrollo de un observatorio tecnológico en seguridad de la información, según los siguientes lineamientos: Arquitectura, Catálogo de Servicios, Equipamiento y Presupuesto.

3.1 Arquitectura

En función de las arquitecturas antes investigadas y del análisis comparativo de los Observatorios Tecnológicos, se estudió los siguientes modelos:

1. Arquitectura basada en Sistema Multi Agente [SMA] realizado para desarrollar un observatorio proactivo, con el objetivo de mantener a los usuarios actualizados, para el apoyo a la toma de decisiones.
2. Observatorio Web Southampton [SUWO], se basa en los principios del Observatorio Web para el acceso a las fuentes controlables y visualizaciones de datos heterogéneas, se distingue de otros observatorios web mediante la adopción de un enfoque desacoplado.
3. Observatorio Virtual de Medición de Redes [nmVO], consiste en mejorar investigación en la red, a través de la medición de datos disponible. Es decir, proporciona un marco adecuado para a red con las herramientas de datos.
4. La Arquitectura de hardware de alto nivel SBO. Es un Observatorio de conducta de seguridad basada en una infraestructura cliente-servidor diseñada para recopilar una amplia gama de datos sobre el comportamiento de los usuarios y las computadoras.

Seguidamente con la investigación se pudo desarrollar el modelo de la presente propuesta, además de las recomendaciones dadas por los informantes claves.

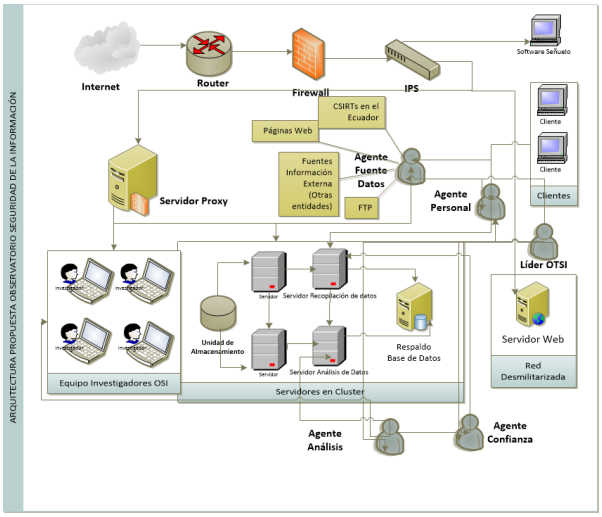


Figura 8. Arquitectura propuesta del Observatorio Tecnológico en SI
Fuente: Elaboración propia

Como puede observarse en la figura anterior, la arquitectura propuesta del OTSI operaría de la siguiente manera, el OTSI debe tener una fuente de comunicación distinta al direccionamiento de red y de Internet que maneja la IES tanto en el área académica como administrativa; así también debe tener un Firewall que se encuentra como primer elemento de seguridad, con el fin de bloquear posibles intrusiones a la red de la organización; un Software de Detección de Intrusos [IPS] que se encuentra después del Firewall, a fin de examinar las firmas de las peticiones y así detectar las posibles amenazas de ataques a la red o modificar las firmas de las peticiones para que no logren su objetivo malicioso; se debe colocar también un software señuelo, para examinar las peticiones clasificadas como sospechosas; además se tendrá un servidor Web dentro de una red desmilitarizada para mantener accesos de redes externas.
Asimismo, se debe contar con un Servidor de recopilación de datos, un servidor de análisis de datos, 02 servidores de contingencia y una unidad de almacenamiento para almacenar la

información y respaldos de la base de datos dentro de un clúster de servidores; los investigadores del OTSI deben contar con reglas sobre la información que entra y sale de la red interna del OTSI, la cual está siendo examinada por un proxy; además, contiene, 01 Líder del Observatorio Tecnológico de Seguridad de la Información [OTSI], 04 agentes que son Personal [AP], Fuente de Datos [AFD], Confianza [AC] y de análisis [AA], en donde el líder OTSI se encarga de coordinar y certificar que las peticiones de los clientes lleguen y sean respondidas por los agentes, asimismo, el AP está a cargo de la gestión de los recursos de la información disponibles, se registra el perfil del usuario, el cual se guarda en el repositorio, para obtener los datos del mismo cuando se autentique en el sistema y permita atender y responder a las necesidades de cada uno; el AFD, esta alerta para atender los pedidos del AP para buscar y descargar del File Transfer Protocolo [FTP] la información que esta indexada a través del FTP; el AC, escucha los mensajes que se envían entre los agentes del OTSI y guarda las trazas, las mismas que el AA las utiliza para determinar que investigadores son especialistas en un tema o cuales están trabajando en temas similares, también el AA puede consultar la cantidad de recursos de información de una temática que ha enviado un AP o la cantidad de mensajes relacionados, ya sean siendo mensajes de recuperación o de contribución de contenido.

El desarrollo del observatorio tecnológico por estar inmerso en el sector académico, podría ser gestionado su financiamiento a través de alianzas estratégicas con otras instituciones de educación superior o entidades públicas o privadas, a fin de generar conocimiento.

Así también esta propuesta se mantendrá en el tiempo, ya que es un servicio que brindaría al resto de Instituciones de Educación Superior para coadyuvar a la investigación y al almacenamiento de información de los distintos casos de incidentes presentados, además estaría orientado como un servicio para las entidades públicas y privadas en el caso de que suscite algún incidente informático.

4.2 Estructura Organizacional OTSI

De acuerdo a la arquitectura propuesta del Observatorio de Seguridad de la Información se propone la siguiente estructura organizacional con la cual funcionaría:

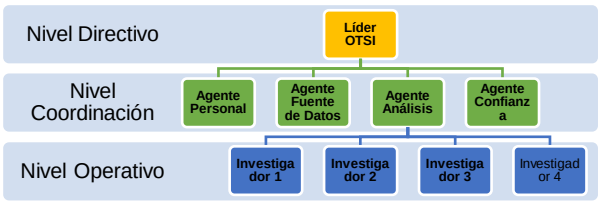


Figura 9. Organigrama del Observatorio SI
Fuente. Elaboración propia

Donde se tienen tres niveles, Nivel Directivo, Nivel Coordinación y Nivel Operativo, para lo cual, el Nivel Directivo se encuentra el Líder OTSI, en el Nivel Coordinación se conforman por los Agentes de Información y el Agente Análisis es el que determina y designa a que investigador le corresponde el tema a investigar.

3.2 Portafolio de Servicios OTSI

Los servicios que el OTSI puede ofrecer, se agrupan en las siguientes tres categorías, servicios reactivos, proactivos y los de gestión de calidad de la información, a través del siguiente portafolio:

Tabla 5: Catálogo Servicios del OTSI

Servicios Reactivos	Servicios Preventivos	Servicios Gestión de Calidad de la SI
Apoyo a la respuesta a incidentes	Evaluaciones de la seguridad de la información	Consultoría de seguridad de la información
Re direccionar los incidentes a los CSIRT	Auditorias en Tecnologías de la Información	Programas de prevención para la SI, talleres, cursos
Recopilación de pruebas forenses	Alertas y advertencias	Evaluación y capacitación a entidades públicas y privadas e Instituciones de Educación Superior

Fuente: Elaboración propia.

Tabla 5: Catálogo Servicios del OTSI

Servicios Reactivos	Servicios Preventivos	Servicios Gestión de Calidad de la SI
Coordinación en el manejo de evidencias	Configuración y mantenimiento de la seguridad de la información	Publicaciones o boletines: semanales, semestrales y anuales a través de la página web OTSI
Coordinación de la respuesta a la vulnerabilidad	Difusión de información relacionada con la SI: Informe de Vulnerabilidades,Informe de incidentes e Informe de seguridad cibernética	Centro de interacción multimedia del OTSI
Asistencia remota a vulnerabilidades e incidentes	Sensibilización de la seguridad de la información	
Seguimiento o rastreo	Planificación de la continuidad de la operación y recuperación tras un desastre	
	Políticas de SI	

Fuente: Elaboración propia.

3.3 Estrategias del Observatorio de Seguridad de la Información

Dentro del catálogo de servicios se realizarán las labores de investigación, análisis, estudio, asesoramiento y divulgación, que atenderán entre otras, a las siguientes estrategias:

Tabla 6: Estrategias del OTSI

Ítem	Estrategia del OTSI
1	Posesionar el OTSI a nivel de las IES, entidades públicas y privadas.
2	Desarrollar soluciones innovadores a través del OTSI.
3	Potenciar la transferencia tecnológica desde la investigación a las IES, entidades públicas y privadas en colaboración con los CSIRT registrados a nivel nacional
4	Identificar, atraer, generar y retener el talento investigador en temas relacionados a seguridad de la información y ciberseguridad a nivel nacional.
5	Elaboración de estudios e informes propios en materia de Seguridad de la Información, Ciberseguridad y Auditoría en TI
6	Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza de la información.
7	Impulso de proyectos de seguridad de la información en materia de Seguridad de la información.
8	Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, sobre seguridad de la información y ciberseguridad.
9	Asesoría a las IES, entidades públicas y privadas en materia de seguridad y confianza de la información.

Fuente: Elaboración propia.

3.4 Equipamiento del Observatorio de Seguridad de la Información

El equipamiento que se muestra en la siguiente tabla, tanto de Hardware como de Software, conformaría la infraestructura del OTSI.

Tabla 7: Equipamiento del OTSI

Cantidad.	Equipos
01	Servicio de Internet con un ancho de banda de 8 MB
01	Firewall capa 3
01	Router capa 3
01	Equipos IPS
06	Laptops core i7 1TB 8 GB de RAM
01	Servidor Web
01	Página Web del OTSI
01	Servidor proxy
02	Servidor para recopilación y análisis de datos
02	Servidor de respaldo
01	Unidad de almacenamiento de 50 TB, tipo de arreglo raid 5

Fuente: Elaboración propia

Por otro lado, para que exista la continuidad del servicio y el equipamiento antes mencionado se ponga a producción, deberá contratarse personal como, el Líder OTSI, agentes de información e investigadores OTSI, de acuerdo al **Anexo B** del presupuesto de la infraestructura tecnológica para la creación del Observatorio de Seguridad de la Información.

Así también, se presenta el presupuesto de la infraestructura arquitectónica de acuerdo al **Anexo C**, donde se detalla el plano propuesto de cómo estarían distribuidas las áreas para la creación del Observatorio de Seguridad de la información.

CONCLUSIONES, LIMITACIONES Y TRABAJOS FUTUROS

De acuerdo a la literatura revisada y analizada se concluye que los observatorios tecnológicos enfocados en seguridad de la información son un grupo de especialistas dedicados a Observar, analizar, asesorar, coordinar, difundir la cultura en seguridad de la información, la protección de la información, así también detectar malos hábitos, lo que permitiría promover mejoras que impulsan la sensibilización a través de las publicaciones o boletines: semanales, semestrales y anuales, además de capacitaciones, seminarios o talleres de prevención para la seguridad de la información.

El desarrollo de un observatorio tecnológico en seguridad de la información, dentro de una institución de educación superior, permitiría mantener una arquitectura sostenible en el tiempo, ya que es un servicio que brindaría al resto de Instituciones de Educación Superior para coadyuvar a la investigación y al almacenamiento de información de los distintos casos de incidentes presentados, además estaría orientado como un servicio para las entidades públicas y privadas en el caso de que suscite algún incidente informático.

Con respecto a la metodología utilizada donde se aplica el tipo de investigación cualitativa con un alcance exploratorio-analítico y en lo concerniente a las entrevistas realizadas a los informantes claves, se destaca la relevancia de la implementación de un Observatorio Tecnológico enfocado a la Seguridad de la Información, marcando un hito a nivel de las Instituciones de Educación Superior.

Según los resultados obtenidos de las encuestas realizadas a los informantes claves, donde todos coinciden que están “de acuerdo o totalmente de acuerdo” con la propuesta planteada de un Observatorio de Seguridad de la Información, la cual permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas. Es importante destacar que algunos de los informantes indicaron que la información que llega al observatorio no se coordina sino se redirecciona a los CSIRT, asimismo mencionaron que para la propuesta del desarrollo del observatorio tecnológico no debe generar conocimiento sino aportar conocimiento a la academia, ya que, generar conocimiento es investigación para tesis doctoral.

Como trabajo futuro se puede indicar que, los observatorios analizados cuentan con una metodología de trabajo implícita, por lo que, a partir de las fuentes analizadas, se recomienda implementar la arquitectura propuesta de un Observatorio Tecnológico en Seguridad de la información en una Institución de Educación Superior y se investigue sobre la legislación y regulación en CSIRT y Ciberseguridad a nivel nacional. Además de analizar el financiamiento de la propuesta para su implementación con la ayuda de entes reguladores, como los proveedores de Servicio de Internet ISP, Ministerio de Educación, Ministerio del Interior e Instituciones públicas y CSIRT del Ecuador.

En general, el aporte de la investigación realizada del desarrollo de un observatorio tecnológico de seguridad de la información, con uno de sus servicios relevantes en la auditoria TI para las empresas públicas, privadas y a la ciudadanía en general como fiscalizadores, permitiría ser un referente en la entidades de educación superior a nivel nacional, a fin de convertirse en una fuente oficial de la información de las actividades de I+D+i, además de aportar conocimiento en la academia.

BIBLIOGRAFÍA

A Da Veiga, & JHP Eloff. (2007). Un marco de gestión de la información de seguridad.

Aguilar, L. E., & Rodrigues, J. A. (2014). LOS OBSERVATORIOS COMO UN RECURSO DE INVESTIGACIÓN, INTERCAMBIOS, PRODUCCIÓN Y DISEMINACIÓN DE CONOCIMIENTO. *Education's Role in Preparing Globally Competent Citizens. BCES Conference Books, 12*.

Álvarez, V. D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista chilena de derecho y tecnología, 7*(1), 1-2.

Andrade, R., & Fuertes, W. (2013). Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: ESPE: Recuperado de: http://ciencia. espe. edu. ec/wp-content/uploads/2013/05/COM61. pdf.

Angulo, N. (2009). ¿ Qué son los observatorios y cuáles son sus funciones? *Innovación Educativa, 9*(47).

Barth, B. (2016). Survey: 48% of organizations attacked by ransomware over 12-month period. *SC Magazine US*.

Booth, P., Hall, W., Gibbins, N., & Galanis, S. (2014). *Visualising data in web observatories: a proposal for visual analytics development & evaluation.* Paper presented at the Proceedings of the 23rd International Conference on World Wide Web.

Borbúa, R. V., Chicango, R. P. R., & Herrera, L. R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO: Revista Latinoamericana de Estudios de Seguridad*(20), 31-45.

Brown, Hall, & Harris, L. (2014). Towards a Taxonomy for Web Observatories. *IW3C2*.

Cano, J. J., & Segurinfo, C. C. (2009). Seguridad de la Información en Latinoamérica Tendencias 20091.

Cárdenas, L., Martínez, H., & Becerra, L. (2016). GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA.

Centro Criptológico Nacional. (2011). GUÍA DE CREACIÓN DE UN CERT / CSIRT

Crespo. (2018). *La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior.* UNIVERSIDAD TÉCNICA DE AMBATO.

CSIRT-CEDIA. (2019). Equipo de respuesta a incidentes de seguridad informática. Retrieved from https://csirt.cedia.org.ec/

CSOC. (2019). Centro de operaciones de Ciberseguridad. Retrieved from https://www.telconet.net/index.php/soluciones/security/csoc

CYBERWATCHING. (2019). Cyberwatching.eu es el observatorio europeo de investigación e innovación en el campo de la ciberseguridad y la privacidad. Retrieved from https://www.cyberwatching.eu/observatory

Daltabuit, E., Hernandez, L., Mallén, G., & Vásquez, J. d. J. (2007). La Seguridad de la Información. 774.

De la Vega, I. (2007). Tipología de Observatorios de Ciencia y Tecnología. Los casos de América Latina y Europa. *Revista española de documentación científica, 30*(4), 545-552.

DELOITTE. (2017). Seguridad de la Información en Ecuador 2017.

Diaz, A. E. (2013). Living Analytics Methods for theWeb Observatory.

Diéguez, M., Cares, C., & Cachero, C. (2017). Metodología para la Selección de Controles de Seguridad de la Información. 6.

DiFranzo, D., Erickson, J. S., Gloria, M. J. K. T., Luciano, J. S., McGuinness, D. L., & Hendler, J. (2014). The web observatory extension: facilitating web science collaboration through semantic markup. *Proceedings of the 23rd International Conference on World Wide Web*, 475-480.

ECUCERT. (2019). Centro de respuesta a incidentes informáticos del Ecuador. Retrieved from https://www.ecucert.gob.ec/

ENISA. (2006). *Como crear un CSIRT paso a paso*. Retrieved from

Espino, M. M., Suárez, A. R., Bustamante, A. C., Férnandez, Y. H., & Dapena, M. D. D. (2014). Un Observatorio Tecnológico proactivo a partir del Modelado Social. *Ciencias de la Información, 45*(1).

Forget, A., Komanduri, S., Acquisti, A., Christin, N., Cranor, L. F., & Telang, R. (2014). *Building the security behavior observatory: an infrastructure for long-term monitoring of client machines.* Paper presented at the Proceedings of the 2014 Symposium and Bootcamp on the Science of Security.

González, I. R., Bonacic, C., & Fernández, Á. (2015). *A real-time web observatory for cycling safety: a tool for supporting research and decision making of people and organizations.* Paper presented at the Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community.

Gonzalez, S., Marin, V., & Salinas, D. J. (2013). OBSERVATORIO DE LAS TECNOLOGÍAS EN LA EDUCACIÓN EN LA PATAGONIA: EL PROCESO DE

ELABORACIÓN Y SELECCIÓN DE INDICADORES.

Hadfeg, F. Y., Morales, A. N., & Moreno, E. M. (2015). Incorporación de Proactividad a los Agentes en un Observatorio Tecnológico. *Lámpsakos*(13), 72-79.

Henriques, Mendonça, Poleto, Camara, & Cabral. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management, 43*, 248-260.

Herrera, D. S. (2005). Tipología de los observatorios de medios en Latinoamérica. *Palabra Clave*(13).

Herrera, D. S. (2006). El porqué de los observatorios de medios latinoamericanos.

INCIBE. (2015). *Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+I en ciberseguridad*. Retrieved from

INCIBE. (2019). OBSERVATORIO EN SEGURIDAD DE LA INFORMACIÓN. Retrieved from https://www.incibe.es/

INTECO. (2010). *Informe anual* Retrieved from

ITU. (2018). *Guía para el cuestionario sobre el Índice Mundial de Ciberseguridad ...*

https://www.itu.int/en. Retrieved from

IURISCYBER. (2019). Observatorio de Ciberseguridad, Prevención y Análisis del Delito Informático-iURiscyber. Retrieved from http://www.urosario.edu.co/Facultad-de-Jurisprudencia/Observatorio-de-Ciberseguridad/Sobre-el-observatorio/

Leite, G. S., & Albuquerque, A. B. (2019). *An Approach for Reduce Vulnerabilities in Web Information Systems*, Cham.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry, 103*, 97-110.

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información tecnológica, 26*(2), 129-134.

Martins, D. J. R., Knob, L. A. D., da Silva, E. G., Wickboldt, J. A., Schaeffer-Filho, A., & Granville, L. Z. (2011). Specialized CSIRT for Incident Response Management in Smart Grids. *Journal of Network and Systems Management*, 1-17.

Matray, P., Csabai, I., Haga, P., Steger, J., Dobos, L., & Vattay, G. (2007). *Building a prototype for network measurement virtual observatory.* Paper presented at the Proceedings of the 3rd annual ACM workshop on Mining network data.

Mejía, Muñoz, Ramírez, & Peña. (2016). Proposal of content and security controls for a CSIRT website. *Springer International Publishing Switzerland*.

Merino, C., & Cañizares, R. (2012). Auditoría de Sistema de Gestión de Seguridad de la Información. *Fundación Confemental*.

Mihai-Ştefan, D. (2018). New Data Protection Regulations and Their Impact on Universities. (1).

Miranda, & Ramirez. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*(17), 01-15.

MIU. (2019). Cybersecurity Observatory. Retrieved from https://www.miuniversity.edu/en/osservatorio-cybersecurity/

Moreno, Carrasco, Rosete, & Delgado. (2013). Apoyo a la toma de decisiones en un Observatorio Tecnológico incorporando proactividad. *Ingeniería Industrial, 34*(3), 293-306.

Moyares, & Infante. (2016). Caracterización de los observatorios como plataformas para la gestión de la vigilancia tecnológica en el sector de la Educación Superior. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento,*, 13 (11), 11-27.

ODILA. (2019). Observatorio de Delitos Informáticos de Latinoamérica. Retrieved from https://www.odila.org/

OEA, E. O. D. L. H. D. S. D. L. (2013). MANUAL DE OBSERVATORIOS NACIONALES.

OSALC. (2019). OBSERVATORIO DE LA CIBERSEGURIDAD EN AMERICA LATINA Y EL CARIBE. Retrieved from http://observatoriociberseguridad.org/graph/countries//selected//0/dimensions/1-2-3-4-5

OSIC. (2019). Observatorio Nacional para la Seguridad de la Información y la Ciberseguridad. Retrieved from https://observatoriociber.org/

OTIC. (2017). El Observatorio de Tecnología de la información y Comunicación Retrieved from https://observatoriotic.mintel.gob.ec/

Phélan, C. (2007). La red observatorios locales de Barcelona, España. Un estudio de casos para diseñar una propuesta nacional. *Fermentum. Revista Venezolana de Sociología y Antropología, 17*(48).

Ramine, T., Xin, W., Thanassis, T., & Hall, W. (2015). Building a Real-Time Web Observatory. *IEEE Internet Computing*.

Ramirez, & Mejia. (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica*(1).

Ramírez, & Mejia. (2015). Propuesta de infraestructura técnica de seguridad para

un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT).

Rea, G. M., Calvo, M. J., & San Feliu, T. (2018). *A prototype to manage cybersecurity in small companies.* Paper presented at the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI).

Sáez, D. D., Antolín, F. M., & Ricau, G. F. (2009). La Vigilancia Tecnológica aplicada al sector de Tecnologías de la Información y la Comunicación: Observatorio Tecnológico del ITI. *Actas de XI Jornadas Españolas de Documentación. Zaragoza, Spain. In XI Jornadas Españolas de Documentación G, 8*, 291-295.

Sanz, C. E., De Felippo, D., García, Z., Carlos , & García, P. (2011). OBSERVATORIO IUNE: UNA NUEVA HERRAMIENTA PARA EL SEGUIMIENTO DE LA ACTIVIDAD INVESTIGADORA DEL SISTEMA UNIVERSITARIO ESPAÑOL.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188.

Tinati, R., Wang, X., Brown, I., Tiropanis, T., & Hall, W. (2015). *A Streaming Real-Time Web Observatory Architecture for Monitoring the Health of Social Machines.* Paper presented at the Proceedings of the 24th International Conference on World Wide Web.

Tinati, R., Wang, X., Tiropanis, T., & Hall, W. (2015). Building a real-time web observatory. *IEEE Internet Computing, 19*(6), 36-45.

Torres, & Martínez. (2014). Análisis y propuesta de implementación de un observatorio TIC para un conjunto de mipymes de la localidad de Usaquén (Bogotá) en la Universidad de San Buenaventura. *Ingenium, 15*, 24.

Vera. (2017). *Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i. .* Universidad Politécnica de Valencia

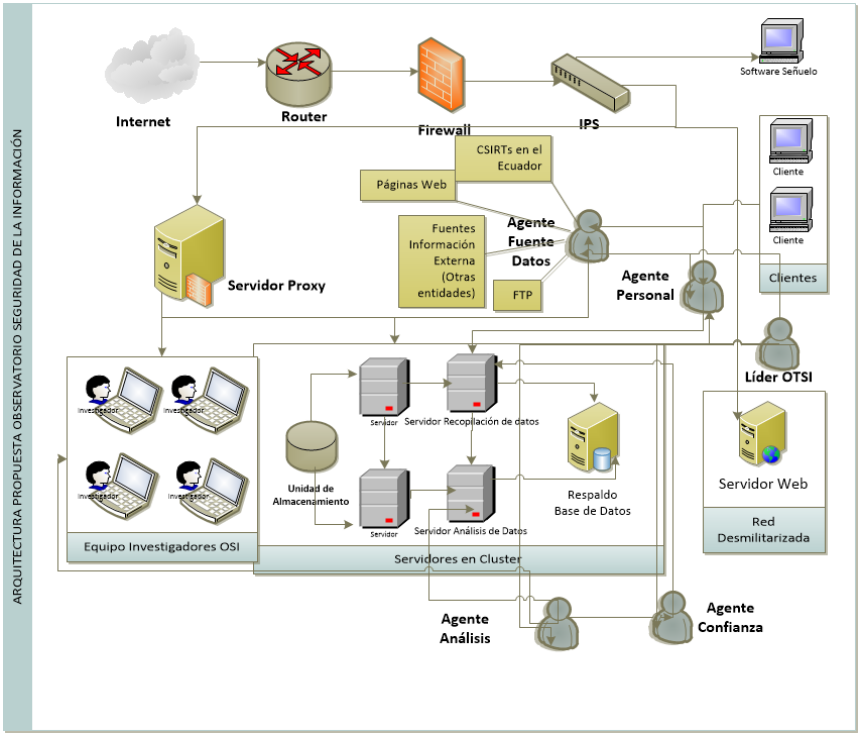
Zellhofer, D. (2019). Information Security Policies in Organizations *Organizing for the Digital World* (pp. 49-62): Springer.

ANEXO A
PROPUESTA DE CREACIÓN DE UN OBSEVATORIO DE SEGURIDAD DE LA INFORMACION PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR

Objetivo General

Crear una propuesta de un Observatorio de Seguridad de la Información, que permita proteger la información y la infraestructura de un equipo de expertos de respuestas ante incidentes de seguridad (CSIRT) para proveer de servicios como alertas y advertencias, tratamiento de incidentes, auditorias de seguridad, publicación de informes y estudios, seguridad en la nube, con lo cual se brindaría un servicio a las Empresas e Instituciones Públicas y Privadas en el Ecuador, a fin de establecer una cultura de seguridad y concientizar a la sociedad para el resguardo de la información.

Arquitectura Propuesta



Explicación de la arquitectura

Como puede observarse en la figura anterior, la arquitectura que debe considerar un observatorio de la seguridad de la información es el siguiente: El OTSI debe tener una fuente de comunicación distinta a direccionamiento que maneja el IES para el área académica y administrativa; Un Firewall se encuentra como primer elemento de seguridad, con el fin de bloquear posibles intrusiones a la red de la organización; Un Software de Detección de Intrusos [IPS] se encuentra después del Firewall, a fin de examinar las firmas de las peticiones y así detectar las posibles amenazas de ataques a la red o modificar las firmas de las peticiones para que no logren su objetivo malicioso; Un software señuelo, para examinar las peticiones clasificadas como sospechosas; Se tendrá el servidor Web dentro de una red desmilitarizada para que puedan ser accedidos de redes externas.

Así también, se debe contar con un Servidor de recopilación de datos, un servidor de análisis de datos y el respaldo de la base de datos dentro de un clúster de servidores; Los investigadores del OTSI que cuenta con reglas sobre la información que entra y sale de la red interna del OTSI, la cual está siendo examinada por un proxy; además, contiene 04 agentes que son Personal, Fuente de Datos, Confianza y de análisis, en donde el Agente de Personal [AP] está a cargo de la gestión de los recursos de la información disponibles, se registra el perfil del usuario, el cual se guarda en el repositorio, para obtener los datos del mismo cuando se autentique en el sistema y permita atender y responder a las necesidades de cada uno; el Agente Fuente de Datos [AFD], esta alerta para atender los pedidos del AP para buscar y descargar del File Transfer Protocolo [FTP] la información que esta indexada a través del FTP; el Agente de Confianza, escucha los mensajes que se envían entre los agentes del OTSI y guarda las trazas, las mismas que el Agente de Análisis [AA] las utiliza para determinar que investigadores son especialistas en un tema o cuales están trabajando en temas similares, también el AA puede consultar la cantidad de recursos de información de una temática que ha enviado un AP

o la cantidad de mensajes relacionados, ya sean siendo mensajes de recuperación o de contribución de contenido.

ENTREVISTA A INFORMANTES CLAVES

A continuación, se presenta las respuestas y comentarios de los informantes claves entrevistados:

ENTREVISTA 1

Entrevistado 1: Ing. Patricio Samaniego **Empresa:** CSIRT- TELCONET

Cargo: Jefe de Ciberseguridad

1. **¿Cree usted que deberíamos desarrollar y aplicar un marco de referencia de mejores prácticas de ciberseguridad en Ecuador como otros países o simplemente aplicar los disponibles?**

Enuncie tres razones a favor de su recomendación.

Ideas relevantes:

   a) **Se requiere adoptar las prácticas internacionales que ya existen, como las que hay en España, por ejemplo.**
   b) Se requiere adecuar las prácticas internacionales a nuestras necesidades y utilizar el marco global que ya existe como IS027001 e IS022301.
   c) Deberíamos desarrollar los propios con base a la situación de la empresa Ecuatoriana y considerando el marco legal que prevalece en el país.
   d) Sí se debe desarrollar, hay talento en el país para hacerlo.

Comentario: Se debe adoptar estándares internacionales, Esquemas de gobernabilidad.

2. **¿Cuáles son nuestras oportunidades para desarrollar talento especializado y proyectos de I + D + i en ciberseguridad?**

Enuncie tres oportunidades y como cultivarlas

Ideas relevantes:

   a) Existe potencial en Ecuador
   b) Se requiere crear áreas especializadas
   c) Se debe invertir para desarrollar al personal interno
   d) Que la asignatura de ciberseguridad sea obligatoria desde la primaria
   e) Intensificar la oferta de carreras en ciberseguridad.

Comentario: El mercado está madurando, se está empezando.

3. **¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?**
   a) Identificación riesgos
   b) Análisis riesgos
   c) Evaluación de riesgos

Comentario: Base de operación y EGSI esquema gubernamental en seguridad de la información

4. **¿Se realizan con frecuencia auditorías de ciberseguridad?**

   a) Evaluaciones sistemáticas de la seguridad de un sistema de información
   b) Evaluar la seguridad de la configuración y el entorno físico del sistema
   c) Procesos de gestión de la información y las prácticas de los usuarios

Comentario: El entrevistado realiza diariamente por contar con CSOC

5. ¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad?

Explicación: Estos incluyen, entre otros, análisis de programas informáticos dañinos o investigaciones sobre criptografía, vulnerabilidades de los sistemas y modelos y conceptos de seguridad. Los programas de desarrollo de la ciberseguridad se refieren a la elaboración de soluciones de hardware o software que incluyen, entre otras cosas, cortafuegos, sistemas anti-intrusión, sistemas de señuelos y módulos de seguridad del hardware. La existencia de un órgano nacional supervisor mejorará la coordinación entre las instituciones y la distribución de recursos.

a) En el sector público
b) En el sector privado
c) En instituciones educativas superiores (sector académico) Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad
d) Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética
e) Otros

Comentario: Si mediante evaluaciones de nuevas plataformas

6. ¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro?

a) No es importante
b) Es relativamente importante
c) Es importante
d) Es muy importante

Comentario: La tecnología no es perfecta siempre hay una brecha, sensación de manejo de riesgo.

7. ¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en Ecuador?

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

Comentario: No existe, solo en el sector privado bajo sus propios intereses

8. ¿Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas)

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

Comentario: Recomienda cambiar a Seguridad personal.

9. ¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden.

a) Seguridad en Internet

b) Privacidad 2
c) Fraude 3
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores 1
g) Otros

Comentario: Seguridad en Internet, seria seguridad personal.

10. ¿Conoce usted sobre algún Observatorio en Seguridad de la Información?

a) ¿Qué hace?
Colecta información de ciberseguridad de amenazas y seguridad
b) ¿Quiénes conforman el Equipo?
Ingenieros en ciberseguridad capacitados y certificados en el exterior.
c) ¿Qué objetivos se plantea?
Mejorar el ecosistema a los prestadores de servicios en ciberseguridad
d) ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en Ecuador? - ¿Comprende la función que aspira desempeñar?
Si

Comentario: Si totalmente.

11. ¿Considera usted que la propuesta del Observatorio en Seguridad de la Información, permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas?

Si, Bajo la estructura. Si no hay ejecución y regulación

12. ¿La arquitectura planteada se relaciona a sus Actividades?

Si se relaciona

13. ¿Cuál es la utilidad, facilidad de uso y satisfacción de los expertos en seguridad de la información con la propuesta?

- Llegar donde no se ha llegado a la comunidad, escuelas y compañías.
- Como ejemplos con se realiza para un simulacro

14. ¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en las Instituciones, Organizaciones y Empresas?

Si es un proceso continuo. Está totalmente de acuerdo

15. ¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información de las Organizaciones?

- SI. Mediante competencias, aptitudes, quien como y cuando.
- Mesa de crisis, con diferentes habilidades.
- Similar al ecosistema de crisis.

16. ¿Considera que la seguridad de la información debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?

- Si. Tomar como el marco de referencia. SI no establece como hacerlo buscar otros actores.
- Aplicar la legislación y objetivos claros

- Los ISP trabajan con los usuarios
- Observar donde no llega la seguridad informática.

ENTREVISTA 2

Entrevistado 2: Ing. Raúl González **Empresa:** Deloitte

Cargo: Gerente de Riesgo.

1. **¿Cree usted que deberíamos desarrollar y aplicar un marco de referencia de mejores prácticas de ciberseguridad en Ecuador como otros países o simplemente aplicar los disponibles?**

Enuncie tres razones a favor de su recomendación.

Ideas relevantes:

a) Se requiere adoptar las prácticas internacionales que ya existen, como las que hay en España, por ejemplo.
b) Se requiere adecuar las prácticas internacionales a nuestras necesidades y utilizar el marco global que ya existe como IS027001 e IS022301.
c) Deberíamos desarrollar los propios con base a la situación de la empresa Ecuatoriana y considerando el marco legal que prevalece en el país.
d) Sí se debe desarrollar, hay talento en el país para hacerlo.

Comentario: Se debería desarrollar

2. **¿Cuáles son nuestras oportunidades para desarrollar talento especializado y proyectos de I + D + I en ciberseguridad?**

Enuncie tres oportunidades y como cultivarlas

Ideas relevantes:

a) Existe potencial en Ecuador
b) Se requiere crear áreas especializadas
c) Se debe invertir para desarrollar al personal interno
d) Que la asignatura de ciberseguridad sea obligatoria desde la primaria
e) Intensificar la oferta de carreras en ciberseguridad.

3. **¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?**

a) Identificación riesgos
b) Análisis riesgos
c) Evaluación de riesgos

Comentario: Deloitte realiza proyectos reactivos

4. **¿Se realizan con frecuencia auditorías de ciberseguridad?**

a) Evaluaciones sistemáticas de la seguridad de un sistema de información
b) Evaluar la seguridad de la configuración y el entorno físico del sistema
c) Procesos de gestión de la información y las prácticas de los usuarios

5. **¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad?**

Explicación: Estos incluyen, entre otros, análisis de programas informáticos dañinos o investigaciones sobre criptografía, vulnerabilidades de los sistemas y modelos y conceptos de seguridad. Los programas de

desarrollo de la ciberseguridad se refieren a la elaboración de soluciones de hardware o software que incluyen, entre otras cosas, cortafuegos, sistemas anti-intrusión, sistemas de señuelos y módulos de seguridad del hardware. La existencia de un órgano nacional supervisor mejorará la coordinación entre las instituciones y la distribución de recursos.

a) En el sector público
b) En el sector privado
c) En instituciones educativas superiores (sector académico) Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad
d) Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética
e) Otros

Comentario: No solo reactivo

6. ¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro?

a) No es importante
b) Es relativamente importante
c) Es importante
d) Es muy importante

7. ¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en Ecuador?

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

8. ¿Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas)

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

Comentario: Si

9. ¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden.

a) Seguridad en Internet 2
b) Privacidad
c) Fraude 1
d) Suplantación de identidad 3
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

10. ¿Conoce usted sobre algún Observatorio en Seguridad de la Información?

a) ¿Qué hace?
b) ¿Quiénes conforman el Equipo?
c) ¿Qué objetivos se plantea?
d) ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en Ecuador? - ¿Comprende la función que aspira desempeñar?

Comentario: No conoce

11. ¿Considera usted que la propuesta del Observatorio en Seguridad de la Información, permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas?

Si permitiría

12. ¿La arquitectura planteada se relaciona a sus Actividades?

Si está de acuerdo, pero no está en sus actividades

13. ¿Cuál es la utilidad, facilidad de uso y satisfacción de los expertos en seguridad de la información con la propuesta?

Prevenir, detectar y enfrentar casos de riesgo y ciber-riesgos

14. ¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en las Instituciones, Organizaciones y Empresas?

Si considera que cubre parte de la ISO 27001

15. ¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información de las Organizaciones?

Si inciden. No se puede prevenir los eventos, se debe tener una base de incidentes

16. ¿Considera que la seguridad de la información debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?

Si debería ser preventivo.

ENTREVISTA 3

Entrevistado 3: TNFG–Ingeniero Eddy Espinosa Daquilema **Empresa:** Armada del Ecuador (DIRTIC)

Cargo: Jefe del departamento de seguridad informática.

1. **¿Cree usted que deberíamos desarrollar y aplicar un marco de referencia de mejores prácticas de ciberseguridad en Ecuador como otros países o simplemente aplicar los disponibles?**

Enuncie tres razones a favor de su recomendación.

Ideas relevantes:

a) Se requiere adoptar las prácticas internacionales que ya existen, como las que hay en España, por ejemplo.
b) Se requiere adecuar las prácticas internacionales a nuestras necesidades y utilizar el marco global que ya existe como IS027001 e IS022301.
c) Deberíamos desarrollar los propios con base a la situación de la empresa Ecuatoriana y considerando el marco legal que prevalece en el país.
d) Sí se debe desarrollar, hay talento en el país para hacerlo.

Comentario:

Las normas internacionales como las ISO, tienen un alcance global, sin embargo cada país tiene normativas legales distintas, en este sentido es importante que las reglas y políticas informáticas de cada país vayan alineadas con las normas jurídicas vigentes. La obligatoriedad de implementar estas normas permitirá madurar la cultura organizacional con respecto a la seguridad de la información.

2. **¿Cuáles son nuestras oportunidades para desarrollar talento especializado y proyectos de I + D + I en ciberseguridad?**

Enuncie tres oportunidades y como cultivarlas

Ideas relevantes:

a) Existe potencial en Ecuador
b) Se requiere crear áreas especializadas
c) Se debe invertir para desarrollar al personal interno
d) Que la asignatura de ciberseguridad sea obligatoria desde la primaria
e) Intensificar la oferta de carreras en ciberseguridad.

Comentario:

Semilleros de investigación desde la escuela

Mejorar infraestructura tecnológica en las entidades educativas, de tal forma que estén disponibles al estudiante.

Obligar a las pymes y grandes empresas el establecimiento de ISO 27001 como mínimo para poder ejercer en el país.

3. **¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?**

a) Identificación riesgos
b) Análisis riesgos
c) Evaluación de riesgos

Comentario:

No, lastimosamente nuestro medio no entiende la importancia que incurre el descuido de la seguridad de la información.

4. ¿Se realizan con frecuencia auditorías de ciberseguridad?

a) Evaluaciones sistemáticas de la seguridad de un sistema de información
b) Evaluar la seguridad de la configuración y el entorno físico del sistema
c) Procesos de gestión de la información y las prácticas de los usuarios

Comentario:

No, las auditorías deberían ser un mecanismo de prevención sin embargo en el medio se usan para responder a un evento de afectación.

5. ¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad?

Explicación: Estos incluyen, entre otros, análisis de programas informáticos dañinos o investigaciones sobre criptografía, vulnerabilidades de los sistemas y modelos y conceptos de seguridad. Los programas de desarrollo de la ciberseguridad se refieren a la elaboración de soluciones de hardware o software que incluyen, entre otras cosas, cortafuegos, sistemas anti-intrusión, sistemas de señuelos y módulos de seguridad del hardware. La existencia de un órgano nacional supervisor mejorará la coordinación entre las instituciones y la distribución de recursos.

a) En el sector público
b) En el sector privado
c) En instituciones educativas superiores (sector académico) Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad
d) Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética
e) Otros

Comentario:

Considero que falta concientización de las autoridades para fortalecer esta rama de la informática que tiene connotación transversal porque la información es el principal activo de toda empresa.

6. ¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro?

a) No es importante
b) Es relativamente importante
c) Es importante
d) Es muy importante

Comentario:

Definitivamente, hay que empezar con la concientización, ya que el desconocimiento crea focos de vulnerabilidad en la sociedad.

7. ¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en Ecuador?

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

Comentario:

Gubernamentales, sin embargo no se exige la implementación.

8. ¿Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas)

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

Comentario:

Programas informáticos dañinos (Virus), fraude, suplantación de identidad.

9. ¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden.

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

Comentario:

e), c), d), b), a), f), g)

10. ¿Conoce usted sobre algún Observatorio en Seguridad de la Información?

e) ¿Qué hace?
f) ¿Quiénes conforman el Equipo?

g) ¿Qué objetivos se plantea?
h) ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en Ecuador? - ¿Comprende la función que aspira desempeñar?

Comentario:

NO

11. ¿Considera usted que la propuesta del Observatorio en Seguridad de la Información, permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas?

Comentario:

Totalmente de acuerdo

12. ¿La arquitectura planteada se relaciona a sus Actividades?

SI

13. ¿Cuál es la utilidad, facilidad de uso y satisfacción de los expertos en seguridad de la información con la propuesta?

Fortalecer los mecanismos de aseguramiento de la información.

14. ¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en las Instituciones, Organizaciones y Empresas?

Por supuesto, debería abarcar todas las áreas. Sin embargo no sirve una propuesta si no se ejecuta, no debemos dejar plasmadas las grandes ideas en papeles.

15. ¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información de las Organizaciones?

Definitivamente.

16. ¿Considera que la seguridad de la información debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?

SI

ENTREVISTA 4

Entrevistado 4: Ing. Carlos Montesinos **Empresa:** APPLE

Senior Product Manager

1. **¿Cree usted que deberíamos desarrollar y aplicar un marco de referencia de mejores prácticas de ciberseguridad en Ecuador como otros países o simplemente aplicar los disponibles?**

Enuncie tres razones a favor de su recomendación.

Ideas relevantes:

a) **Se requiere adoptar las prácticas internacionales que ya existen, como las que hay en España, por ejemplo.**
b) **Se requiere adecuar las prácticas internacionales a nuestras necesidades y utilizar el marco global que ya existe como IS027001 e IS022301.**
c) **Deberíamos desarrollar los propios con base a la situación de la empresa Ecuatoriana y considerando el marco legal que prevalece en el país**.
d) Sí se debe desarrollar, hay talento en el país para hacerlo.

Comentarios:

De acuerdo al objetivo de la propuesta. Ademas empezar desde empresas grandes. Si se debería aplicar estandares internacionales y crear estándares

2. **¿Cuáles son nuestras oportunidades para desarrollar talento especializado y proyectos de I + D + I en ciberseguridad?.**

Enuncie tres oportunidades y como cultivarlas

Ideas relevantes:

a) **Existe potencial en Ecuador**
b) **Se requiere crear áreas especializadas**
c) **Se debe invertir para desarrollar al personal interno**
d) Que la asignatura de ciberseguridad sea obligatoria desde la primaria
e) Intensificar la oferta de carreras en ciberseguridad.

Comentarios:

En un escenario es muy probable que se tenga q contratar a personal internacional y si es que hay problema del talento en ecuador. Además si el problema es concentrarlo en un grupo que está enfocado a la industria

3. **¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?**
   a) **Identificación riesgos**
   b) **Análisis riesgos**
   c) **Evaluación de riesgos**

4. **¿Se realizan con frecuencia auditorías de ciberseguridad?**

a) Evaluaciones sistemáticas de la seguridad de un sistema de información
b) Evaluar la seguridad de la configuración y el entorno físico del sistema
c) Procesos de gestión de la información y las prácticas de los usuarios

Comentario: Desconoce la frecuencias de auditorías en Ecuador

5. ¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad?

Explicación: Estos incluyen, entre otros, análisis de programas informáticos dañinos o investigaciones sobre criptografía, vulnerabilidades de los sistemas y modelos y conceptos de seguridad. Los programas de desarrollo de la ciberseguridad se refieren a la elaboración de soluciones de hardware o software que incluyen, entre otras cosas, cortafuegos, sistemas anti-intrusión, sistemas de señuelos y módulos de seguridad del hardware. La existencia de un órgano nacional supervisor mejorará la coordinación entre las instituciones y la distribución de recursos.

a) En el sector público
b) En el sector privado
c) En instituciones educativas superiores (sector académico) Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad
d) Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética
e) Otros

Comentario: Desconoce el financiamiento en Ecuador

6. ¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro?

a) No es importante
b) Es relativamente importante
c) Es importante
d) Es muy importante

7. ¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en Ecuador?

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

8. ¿Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas)

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

Comentario: Desconoce las compañías de Ecuador

9. ¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden.

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

Comentario: Es muy importante a todo nivel depende del grupo y del problema de seguridad de la creación de cuentas falsas

10. ¿Conoce usted sobre algún Observatorio en Seguridad de la Información?

a) ¿Qué hace?
b) ¿Quiénes conforman el Equipo?
c) ¿Qué objetivos se plantea?
d) ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en Ecuador? - ¿Comprende la función que aspira desempeñar

Comentario: No.

11. ¿Considera usted que la propuesta del Observatorio en Seguridad de la Información, permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas?

Comentario: Si

12. ¿La arquitectura planteada se relaciona a sus Actividades?

Comentario: No

13. ¿Cuál es la utilidad, facilidad de uso y satisfacción de los expertos en seguridad de la información con la propuesta?

Comentario: Si se ultilizaria los boletines, haciendo conferencias compartiendo experiencia y como experto pedir los servicios de una institución

14. ¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en las Instituciones, Organizaciones y Empresas?

Comentario: Desconoce las instituciones en Ecuador

15. ¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información de las Organizaciones?

Comentario: No está convencidos pero si añadiría un observatorio a la gestión de una empresa

16. ¿Considera que la seguridad de la información debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?

Comentario: Claro por supuesto es importante la seguridad informática. Ahora es importante, no puede ser secundario es principal para la continuidad del negocio

ENTREVISTA 5

Entrevistado 5: Ing. Pablo Paredes **Empresa:** Stanford University

Puesto: Docente

1. **¿Cree usted que deberíamos desarrollar y aplicar un marco de referencia de mejores prácticas de ciberseguridad en Ecuador como otros países o simplemente aplicar los disponibles?**

Enuncie tres razones a favor de su recomendación.

Ideas relevantes:

a) **Se requiere adoptar las prácticas internacionales que ya existen, como las que hay en España, por ejemplo.**
b) **Se requiere adecuar las prácticas internacionales a nuestras necesidades y utilizar el marco global que ya existe como IS027001 e IS022301.**
c) Deberíamos desarrollar los propios con base a la situación de la empresa Ecuatoriana y considerando el marco legal que prevalece en el país.
d) Sí se debe desarrollar, hay talento en el país para hacerlo.

2. **¿Cuáles son nuestras oportunidades para desarrollar talento especializado y proyectos de I + D + I en ciberseguridad?.**

Enuncie tres oportunidades y como cultivarlas

Ideas relevantes:

a) Existe potencial en Ecuador
b) Se requiere crear áreas especializadas
c) Se debe invertir para desarrollar al personal interno
d) Que la asignatura de ciberseguridad sea obligatoria desde la primaria
e) Intensificar la oferta de carreras en ciberseguridad.

3. **¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?**

a) Identificación riesgos
b) Análisis riesgos
c) Evaluación de riesgos

4. **¿Se realizan con frecuencia auditorías de ciberseguridad?**

a) Evaluaciones sistemáticas de la seguridad de un sistema de información
b) Evaluar la seguridad de la configuración y el entorno físico del sistema
c) Procesos de gestión de la información y las prácticas de los usuarios

Comentario: Desconoce la frecuencia en Ecuador

5. **¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad?**

Explicación: Estos incluyen, entre otros, análisis de programas informáticos dañinos o investigaciones sobre criptografía, vulnerabilidades de los sistemas y modelos y conceptos de

seguridad. Los programas de desarrollo de la ciberseguridad se refieren a la elaboración de soluciones de hardware o software que incluyen, entre otras cosas, cortafuegos, sistemas anti-intrusión, sistemas de señuelos y módulos de seguridad del hardware. La existencia de un órgano nacional supervisor mejorará la coordinación entre las instituciones y la distribución de recursos.

a) En el sector público
b) En el sector privado
c) En instituciones educativas superiores (sector académico) Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad
d) Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética
e) Otros

Comentario: Si

6. ¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro?

a) No es importante
b) Es relativamente importante
c) Es importante
d) Es muy importante

7. ¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en Ecuador?

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

8. ¿Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas)

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

9. ¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden.

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad

e) Programas informáticos dañinos
f) Protección de menores
g) Otros

10. ¿Conoce usted sobre algún Observatorio en Seguridad de la Información?

a) ¿Qué hace?

Respuesta: Observar el ecosistema, colecta gran cantidad de información

b) ¿Quiénes conforman el Equipo?

Respuesta: Ingenieros en sistemas, especialistas en seguridad informática e investigadores

c) ¿Qué objetivos se plantea?

Respuesta: La misión es informar y monitorear.

d) ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en Ecuador? - ¿Comprende la función que aspira desempeñar

Respuesta: Si, mediante la publicación de la investigación

Comentario: Si. El observatorio aporta conocimiento radactando informe y presentando parte importante.

11. ¿Considera usted que la propuesta del Observatorio en Seguridad de la Información, permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas?

Comentario: Si

12. ¿La arquitectura planteada se relaciona a sus Actividades?

Comentario: No se desempeña a otras actividades actualmente

13. ¿Cuál es la utilidad, facilidad de uso y satisfacción de los expertos en seguridad de la información con la propuesta?

Comentario: Actualmente se desempeña a otras áreas, pero si está de acuerdo con la propuesta

14. ¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en las Instituciones, Organizaciones y Empresas?

Comentario: Actualmente se desempeña a otras áreas, pero si está de acuerdo con la propuesta por la experiencia.

15. ¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información de las Organizaciones?

Comentario: Si lo realizan las empresas

16. ¿Considera que la seguridad de la información debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?

Comentario: Si

VALIDACIÓN DEL CUESTIONARIO

PREGUNTAS	TITULO	AÑO	AUTORES
¿Cree usted que deberíamos desarrollar y aplicar un marco de referencia de mejores prácticas de ciberseguridad en Ecuador como otros países o simplemente aplicar los disponibles? e) Se requiere adoptar las prácticas internacionales que ya existen, como las que hay en España, por ejemplo. f) Se requiere adecuar las prácticas internacionales a nuestras necesidades y utilizar el marco global que ya existe como IS027001 e IS022301. g) Deberíamos desarrollar los propios con base a la situación de la empresa Ecuatoriana y considerando el marco legal que prevalece en el país. h) Sí se debe desarrollar, hay talento en el país para hacerlo.	Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i.	2017	Víctor E. Vera Pinto
¿Cuáles son nuestras oportunidades para desarrollar talento especializado y proyectos de I + D + I en ciberseguridad? f) Existe potencial en Ecuador g) Se requiere crear áreas especializadas h) Se debe invertir para desarrollar al personal interno i) Que la asignatura de ciberseguridad sea obligatoria desde la primaria j) Intensificar la oferta de carreras en ciberseguridad.	Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i.	2017	Víctor E. Vera Pinto
¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad? d) Identificación riesgos e) Análisis riesgos f) Evaluación de riesgos	Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i.	2017	Víctor E. Vera Pinto

¿Se realizan con frecuencia auditorías de ciberseguridad? d) Evaluaciones sistemáticas de la seguridad de un sistema de información e) Evaluar la seguridad de la configuración y el entorno físico del sistema f) Procesos de gestión de la información y las prácticas de los usuarios	Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i.	2017	Víctor E. Vera Pinto
¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad? a) En el sector público b) En el sector privado c) En instituciones educativas superiores (sector académico) Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad d) Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética e) Otros	Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad	2017	International Telecomunications Union (ITU)
¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro? e) No es importante f) Es relativamente importante g) Es importante h) Es muy importante	Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad	2017	International Telecomunications Union (ITU)
¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en Ecuador? i) Niños j) Jóvenes k) Estudiantes l) Personas mayores m) Personas con discapacidad n) Instituciones privadas o) Agencias gubernamentales p) Otros	Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad	2017	International Telecomunications Union (ITU)

Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas). h) Seguridad en Internet i) Privacidad j) Fraude k) Suplantación de identidad l) Programas informáticos dañinos m) Protección de menores n) Otros	Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad	2017	International Telecomunications Union (ITU)
¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden. h) Seguridad en Internet i) Privacidad j) Fraude k) Suplantación de identidad l) Programas informáticos dañinos m) Protección de menores n) Otros	Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad	2017	International Telecomunications Union (ITU)
¿Conoce usted sobre algún Observatorio en Seguridad de la Información? a) ¿Qué hace? b) ¿Quiénes conforman el Equipo? c) ¿Qué objetivos se plantea? d) ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en Ecuador?	Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i.	2017	Víctor E. Vera Pinto
¿Considera usted que la propuesta del Observatorio en Seguridad de la Información, permite el monitoreo, tratamiento, además de mejorar y gestionar la seguridad respecto a los activos de información de la Ciudadanía, Instituciones, Organizaciones y Empresas?	La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior	2018	Natalia Judith Crespo Chávez
¿La arquitectura planteada se relaciona a sus Actividades?	La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior	2018	Natalia Judith Crespo Chávez
¿Cuál es la utilidad, facilidad de uso y satisfacción de los expertos en seguridad de la información con la propuesta?	La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior	2018	Natalia Judith Crespo Chávez

¿Considera usted que la propuesta respecto al marco regulatorio para la seguridad de la información que abarque no solo el cumplimiento de la norma vigente, sino que establezca políticas respecto a la organización interna, recursos humanos, activos de información, gestión de proyectos y manejo de incidentes, contribuye a una adecuada gestión de la seguridad de la información en las Instituciones, Organizaciones y Empresas?	La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior	2018	Natalia Judith Crespo Chávez
¿Considera usted que la propuesta respecto a la necesidad de contar un plan de gestión de incidentes que asegure los responsables, acciones y respuestas ante tales eventos; incide en la seguridad de la información de las Organizaciones?	La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior	2018	Natalia Judith Crespo Chávez
¿Considera que la seguridad de la información debe ser apoyada mediante un plan de monitoreo y continuidad, que considere las responsabilidades del personal, planes de mantenimiento, capacitación, actualización de controles de seguridad y revisión de políticas de seguridad, conforme la propuesta?	La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior	2018	Natalia Judith Crespo Chávez

ANEXO B

A continuación se presentará el presupuesto del personal requerido con el equipamiento para la implantación del Observatorio de Seguridad de la Información.

Costos de Personal OTSI

Concepto	Cantidad	Sueldo	Valor Parcial	Tiempo (Meses)	Valor Total
Líder del OTSI	1	$2.500	$2.500	12	$30.000
Agentes de Información	4	$1.200	$4.800	12	$57.600
Investigadores - Expertos	4	$2.000	$8.000	12	$96.000
Total					$183.600

Costos de Equipamiento OTSI

Concepto	Cantidad	Costo	Valor Total
Servicio de Internet con un ancho de banda de 8 MB por 12 meses	1	$6.700	$6.700
Firewall capa 3	1	$2.000	$2.000
Router capa 3	1	$4.000	$4.000
IPS	1	$1.200	$1.200
Laptops core i7 1 TB 8GB memoria	6	$1.200	$7.200
Servidor Web	1	$3.500	$3.500
Página Web del OTSI	1	$1.000	$1.000
Servidor proxy	1	$3.500	$3.500
Servidor para recopilación y análisis de datos	2	$3.500	$7.000
Servidor de respaldo	2	$3.500	$7.000
Unidad de almacenamiento de 24 TB raid 5	1	$50.000	$50.000
Total			$93.100

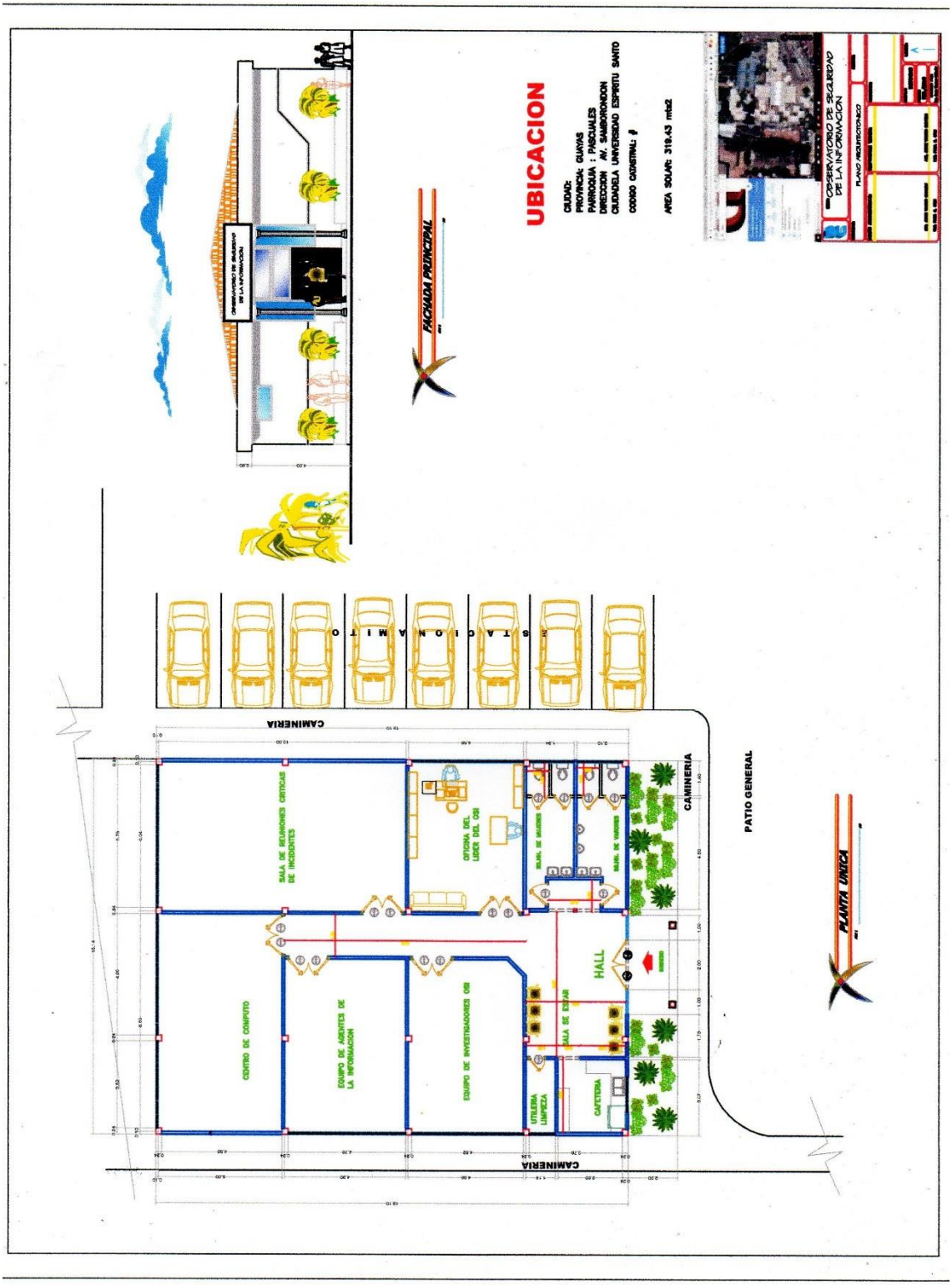
Costos de Obra áreas OTSI

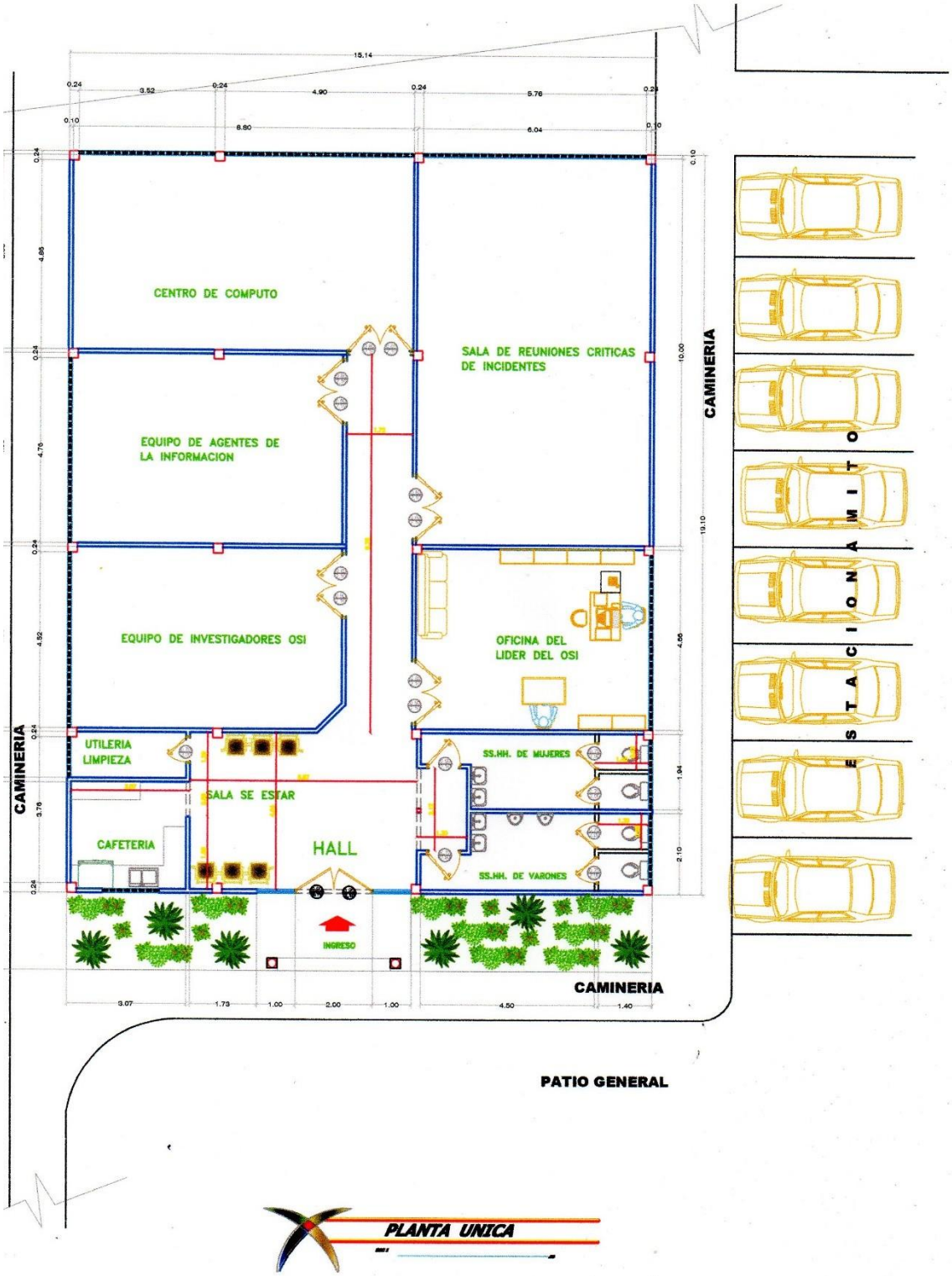
Características del Rubro	Valor Total
Obra arquitectónica	$74.776,52
Total	$74.776,52

COSTO TOTAL PARA CREACIÓN DE PROPUESTA

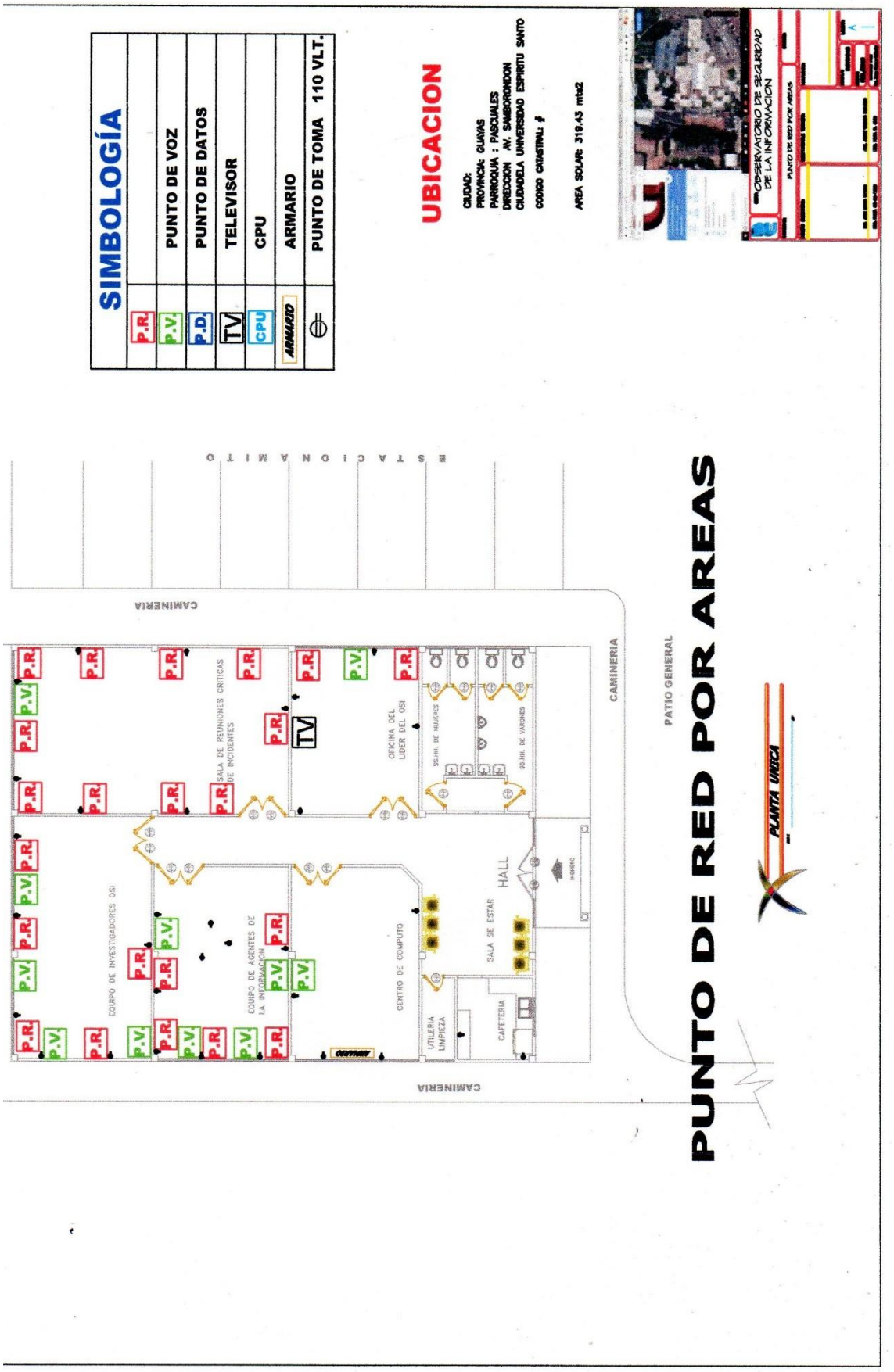
Total de Costo de Personal	$183.600
Total de Costo de Equipamiento	$93.100
Total de Costo de Obra áreas OTSI	$74.776,52
Costo Total	**$351.476,52**

ANEXO C
PLANO ARQUITECTONICO




CENTRO DE COMPUTO
SALA DE REUNIONES CRITICAS DE INCIDENTES
EQUIPO DE AGENTES DE LA INFORMACION
EQUIPO DE INVESTIGADORES OSI
OFICINA DEL LIDER DEL OSI
UTILERIA LIMPIEZA
SALA SE ESTAR
SS.HH. DE MUJERES
CAFETERIA
HALL
SS.HH. DE VARONES
INGRESO
CAMINERIA
CAMINERIA
CAMINERIA
ESTACIONAMIENTO
PATIO GENERAL
PLANTA UNICA


OBSERVATORIO DE SEGURIDAD
DE LA INFORMACION
0.60
4.00
FACHADA PRINCIPAL


SIMBOLOGÍA
P.R
PUNTO DE VOZ
P.V
PUNTO DE DATOS
P.D
TELEVISOR
TV
CPU
CPU
ARMARIO
ARMARIO
PUNTO DE TOMA 110 VLT.
UBICACION
CIUDAD:
PROVINCIA: GUAYAS
PARROQUIA : PASCUALES
DIRECCION AV. SAMBORONDON
CIUDADELA UNIVERSIDAD ESPIRITU SANTO
CODIGO CATASTRAL: #
AREA SOLAR: 319.43 mts2
OBSERVATORIO DE SEGURIDAD DE LA INFORMACION
PUNTO DE RED POR AREAS
PUNTO DE RED POR AREAS
PLANTA UNICA
PATIO GENERAL
CAMINERIA
CAMINERIA
CAMINERIA
ESTACIONAMIENTO
EQUIPO DE INVESTIGADORES OSI
EQUIPO DE AGENTES DE LA INFORMACION
CENTRO DE COMPUTO
SALA DE REUNIONES CRITICAS DE INCIDENTES
OFICINA DEL LIDER DEL OSI
SS.HH. DE HOMBRES
SS.HH. DE VARONES
SALA SE ESTAR
HALL
UTILERIA LIMPIEZA
CAFETERIA
INGRESO
P.R
P.V
TV

PRESUPUESTO REFERENCIAL DE OBRA **hoja n° 1**

EDIFICACION DE UNA PLANTA

Ubicación: AVENIDA SAMBORONDON **FECHA: 13-02-2019** **Area de Const.** **289,17 m2**

PRESUPUESTO: Arq. JORGE VIVANCO SUIKOSKY **Area de Terreno** **319,43 m2**

OBRA : OBSERVATORIO DE SEGURIDAD DE LA INFORMACION

COD.	RUBRO	UNID.	CANTIDAD	PRECIO UNIT.	PARCIAL	GASTADO
0100.-	**PRELIMINARES E INSTALACION DE OBRAS**					
00111	Trazado, replanteo y limpieza	m2	319,43	3,73	1.191,47	
00112	instalacion provicional de agua y luz	gbl	319,43	0,70	223,60	
00113	escavacion, desalojo y compactacion	m3	13,82	45,00	621,90	
00114	muro de piedra base	ml	135,00	10,60	1.431,00	**3.467,97**
0200.-	**CIMENTACION**					
00211	Replantillo	m3	11,80	28,00	330,40	
00212	Plintos	m3	5,76	310,00	1.785,60	
00213	Riostra	m3	5,94	350,00	2.079,00	**4.195,00**
0300.-	**ESTRUCTURAS**					
00311	Columnas planta baja 0,22X0,20	m3	4,60	691,87	3.182,60	
00312	Vigas de cubierta 15X20	ml	135,00	12,50	1.687,50	
00313	pilaretes de puertas y ventanas 0,10x0,20	ml	52,00	18,00	936,00	
00314	Hormigón de Elementos de Fachadas	m3	0,61	120,00	73,20	
00315	2 columnas redondas	ml	13,00	22,30	289,90	**6.169,20**
0400.-	**ALBAÑILERIA**					
00401	Emblocado y rebocado de Paredes e = 9cms exterior	m2	119,00	25,20	2.998,80	
00402	Emblocado y rebocado de Paredes e = 7cms interior	m2	350,00	16,67	5.834,50	
00403	Enlucido de Pared en fachada	m2	245,00	16,67	4.084,15	
00504	Enlucido de Pared interior	m2	250,00	16,50	4.125,00	
00405	Filos, cuadrada de boquetes en puertas	ml	65,00	5,61	364,65	
00406	Filos, cuadrada de boquetes en ventanas	ml	45,00	4,51	202,95	
00407	Enlucido de alero y taco de cubierta en fachada	ml	19,00	12,98	246,62	
00408	contra piso de hormigon	m2	289,00	5,98	1.728,22	
00409	Nivelacion de pisos	m2	289,00	1,50	433,50	**20.018,39**
0500.-	**PISOS Y SOBREPISOS**					
00510	piso ceramica anti deslizante	m2	289,00	17,00	4.913,00	**4.913,00**
0600.-	**ALUMINIO Y VIDRIO**					
00610	ventanas de aluminio y vidrio (de celocias)	m2	21,00	75,00	1.575,00	
00611	ventanas de aluminio y vidrio (de 1.00x2.45 m.)	m2	1,90	75,00	142,50	**1.717,50**

PRESUPUESTO REFERENCIAL DE OBRA **hoja n° 2**

EDIFICACION DE UNA PLANTA

Ubicación: AVENIDA SAMBORONDON **FECHA: 13-02-2019** **Area de Const.** **289,17 m2**

PRESUPUESTO: Arq. JORGE VIVANCO SUIKOSKY **Area de Terreno** **319,43 m2**

OBRA : OBSERVATORIO DE SEGURIDAD DE LA INFORMACION

COD.	RUBRO	UNID.	CANTIDAD	PRECIO UNIT.	PARCIAL	GASTADO
0700.-	**PUERTAS inlcuye cerradura**					
00702	Puertas principal metalica pintadas	u	2,00	280,00	560,00	
00703	Puertas de Madera de 0,80	u	12,00	120,00	1.440,00	
00704	Puertas de Madera de 0,60	u	5,00	90,00	450,00	**2.450,00**
0800.-	**REVESTIMIENTO**					
00801	Ceramica en paredes (baño y cafeteria)	m2	39,40	23,00	906,20	**906,20**
0900.-	**INSTALACIONES ELECTRICAS**					
00010	punto de luz	punt.	34,00	28,00	952,00	
00902	tomacorriente de 110v	punt.	20,00	28,00	560,00	
00903	panel de distribucion planta alta	punt.	1,00	250,00	250,00	
00904	Punto de Red	punt.	22,00	60,00	1.320,00	
00905	Punto de Voz	punt.	11,00	40,00	440,00	
00905	Armario principal	unidad	1,00	1.500,00	1.500,00	**5.022,00**
100.-	**INSTALACIONES SANITARIAS**					
00101	Tuberia deaguas servidas PVC2"	ml	16,00	7,10	113,60	
00102	Tuberia deaguas servidas PVC4"	ml	12,00	35,00	420,00	
00103	Punto de Agua Fria	punto	13,00	45,00	585,00	
00104	Inodoro Blanco	u	4,00	120,00	480,00	
00105	Lavatorio Blanco edesa	u	4,00	120,00	480,00	
00106	urinario Blanco edesa	u	2,00	80,00	160,00	
00107	lavaplato galvanizado	u	1,00	120,00	120,00	**2.358,60**
00108	lavaplato galvanizado	u	1,00	120,00	120,00	
00109	lavaplato galvanizado	u	1,00	120,00	120,00	
1100.-	**CUBIERTA**					
01101	Cubierta de estructura metalica conPlancha de Supertecho	m2	304,00	22,00	6.688,00	**6.688,00**
1200.-	**Pintura Exterior e Interior**					
01201	Pintura Exterior	u	245,00	16,00	3.920,00	
01202	Pintura Interior	u	416,00	14,00	5.824,00	**9.744,00**
1300.-	**LIMPIEZA**					
01301	Limpieza y Desalojos de desechos	viaje	12,00	70,00	840,00	**840,00**

	TOTAL DE COSTOS DIRECTOS					**68.489,87**
					-	
	IMPREVISTOS		**B**	**2,73%**	**355,00**	**656,99**
	DIRECCION TECNICA		**C**	**10,00%**	**1.300,00**	**2.395,60**
	FISCALIZACION		**D**	**1,50%**	**195,00**	**359,34**
	IVA DE COSTOS INDIRECTOS		**E**	**12,00%**	**1.560,00**	**2.874,72**
	COSTO TOTAL =(B+C+D+E)				**$**	**74.776,52**

Nota:

Presupuesto referencial para una construccion de 289.17 m2 ,es de 258.59 dolares por cada m2

ARQ. JORGE VIVANCO SUIKOSKY
GERENTE GENERAL
C.I. 090600746-3