SATHIRÍ Sembrador

EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS PARA LA SEGURIDAD DE LA INFORMACIÓN (CSIRT-UPEC)

COMPUTER INCIDENT RESPONSE TEAM FOR INFORMATION SECURITY (CSIRT UPEC)

Recibido: 01/10/2021 - Aceptado: 11/01/2023

Anderson Daniel Chamorro Pantoja

Ingeniero en Computación - Universidad Politécnica Estatal del Carchi

anderson.chamorro@upec.edu.ec
https://orcid.org/0000-0001-5702-6410

Silvia Verónica Pupiales Chacón

Ingeniero en Computación - Universidad Politécnica Estatal del Carchi

silvia.pupiales@upec.edu.ec
https://orcid.org/0000-0002-1420-1482

Jairo Vladimir Hidalgo Guijarro

Msc. Redes de Comunicaciones - Pontificia Universidad Católica del Ecuador

Docente de la Universidad Politécnica Estatal del Carchi

jairo.hidalgo@upec.edu.ec
https://orcid.org/0000-0001-8165-0192

Cómo citar este artículo:

Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229. https://doi.org/10.32645/13906925.1200

Resumen

Toda la información digital se encuentra expuesta constantemente a incidentes o vulnerabilidades. La presente investigación establece los recursos necesarios para la conformación de un equipo de respuesta ante incidentes informáticos (CSIRT) en la Universidad Politécnica Estatal del Carchi (Ecuador). El CISRT-UPEC está integrado por expertos profesionales en el área redes de computadoras y seguridad informática y también por equipos tecnológicos con la finalidad de brindar apoyo y soporte en temas de seguridad de la información, especialmente en las unidades educativas y gobiernos seccionales de la provincia del Carchi; el trabajo contiene una investigación documental y de campo para el análisis e interpretación de los datos, y un enfoque cualitativo para obtener realidades investigativas de otros CSIRT a nivel del Ecuador , además se generó un muestreo por conveniencia para establecer los servicios, políticas y procesos operacionales para el CSIRT-UPEC. Como resultado de la investigación, se conforma el CSIRT-UPEC, con el establecimiento de la misión, visión y valores como identidad institucional, además de cuatro servicios, ocho políticas, cinco procesos operacionales y un acuerdo de nivel de servicios SLA para el inicio de sus actividades. Actualmente se está gestionando la habilitación, operación y el funcionamiento de CSIRT-UPEC en la institución, con la asociación al Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones - EcuCERT de Arcotel y del grupo de centros de respuesta a incidentes informáticos CSIRT del Ecuador.

Palabras claves: incidentes informáticos, incidentes informáticos, seguridad de la información

Abstract

All digital information is constantly exposed to incidents or vulnerabilities. The present investigation establishes the necessary resources for the conformation of a computer incident response team (CSIRT) at the State Polytechnic University of Carchi, (Ecuador), the CISRT-UPEC, is integrated by professional experts in the area of computer networks and computer security and also by technological teams with the purpose of providing support and assistance in information security issues especially in the educational units and sectional governments of the province of Carchi; the work contains documentary and field research for the analysis and interpretation of the data, and a qualitative approach to obtain research realities from other CSIRT in Ecuador, in addition, a convenience sample was generated to establish the services, policies and operational processes for the CSIRT-UPEC. As a result of the research, the CSIRT-UPEC is formed, with the establishment of the mission, vision and values as institutional identity, in addition to four services, eight policies, five operational processes and a service level agreement (SLA) for the start of its activities. At the moment, the enabling, operation and functioning of CSIRT-UPEC in the institution is being managed, with the association to the Computer Incident Response Center of the Telecommunications Regulation and Control Agency - EcuCERT of Arcotel and the group of computer incident response centers CSIRT of Ecuador.

Keywords: computer incidents, computer incidents, information security

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

Introducción

Conforme se incrementa el uso de las tecnologías, también surgen nuevos incidentes provocados por terceras personas para obtener beneficios con los datos de sus víctimas, al igual que las vulnerabilidades como la causa del incorrecto uso de medidas preventivas y reactivas para la protección de los sistemas. La ciberseguridad se ha visto afectada más de lo habitual desde el año 2020 por el incremento de ataques que se han vuelto más sofisticados, junto con esto se ha presentado grandes fugas de información, estafas, fraudes y desinformación (Ranchal, 2020).

La seguridad de la información es un tema que no debe ser ignorado. Hoy en día, la información se intercambia a través de la red, los pagos en línea son cada vez más comunes y el teletrabajo y la educación en línea debido al COVID-19 han aumentado considerablemente, esto trae consigo el peligro constante de que nuestra información se encuentre expuesta a cualquier persona por no conocer de procesos o medidas necesarias para evitar, detectar o detener incidentes.

Un reporte de seguridad de ESET de 2021 menciona que los códigos maliciosos más usados en Latinoamérica son: virus, troyanos, spyware, ransomware y gusanos, y reciben alrededor de 450 mil muestras de malware nuevas para todas las plataformas. ESET afirma que, en el año 2020, en Ecuador hubo más de 51 mil registros de malware utilizados para minería de criptomonedas, cerca de 140 mil detecciones de código malicioso para vulnerabilidades en software y es el sexto país con más detecciones de malware, esto se debe a la falta de personal capacitado en temas de seguridad y tecnologías de protección, por lo que varias empresas se vieron afectadas por ataques informáticos y no actuaron debidamente a ello (Abril, 2021).

Según un reporte de la *Revista Vistazo* (2020), los ciberdelincuentes han cambiado su objetivo, pues preparan sus ataques con el fin de aumentar los daños en los sistemas y de forma económica en las organizaciones, pero Ecuador aún no se encuentra preparado para este tipo de amenazas cibernéticas; por otra parte BBC News Mundo (2019) , menciona que la fuga de datos personales de millones de ecuatorianos, no estaban resguardados con los protocolos adecuados para su protección, por lo que se le considera una falla informática muy grave.

El Comercio (2021) afirma que el virus RansomEXX afectó los sistemas de CNT y provocó graves alteraciones de recargas, activaciones y facturación, pero su proceso de recuperación tardó más de una semana ya que no contaban con las respectivas medidas o procesos para hacerlo.

La conformación de un CSIRT tiene el objetivo de aumentar la capacidad de mitigación y eliminación de eventos indeseados o inesperados como los mencionados anteriormente, que atentan contra las actividades de las organizaciones, seguridad de la información digital y sus equipos. Además, brinda servicios proactivos tales como el manejo de alertas y advertencias, mejoras de la calidad en concientización y educación sobre las mejores prácticas de políticas y normas, permitiendo anticiparse ante ciertas amenazas; y reactivos mediante reporte, análisis y manejo de incidentes proporcionando una actuación inmediata y así evitar que terceras personas logren su objetivo.

Hidalgo (2017) menciona que, el uso de las tecnologías en el ámbito educativo , ayudan a forjar unidades educativas inclusivas y que transforman las necesidades en oportunidades para adquirir nuevos conocimientos, pero esto también requiere de capacitaciones a todo el personal educativo con el fin de hacer el uso correcto de las tecnologías de la información y evitar incidentes, por otra parte, Medina & Meza (2019) explica que los sistemas de municipalidades, gestionan información de los ecuatorianos, por lo tanto, siempre son el foco de incidentes potenciales y aún más porque las autoridades no aplican los procesos o políticas correctas para evitar o mitigar ciertas amenazas.

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

Materiales y métodos

El tipo de investigación es documental por el análisis e interpretación de información en libros, artículos, videos y documentos físicos o digitales para recolectar la información relacionada con el caso de estudio, se logró una mayor organización, un análisis propio y conllevó a formular preguntas sobre el tema, generando fases de implementación requeridas para llegar al resultado esperado.

Se aplicó un muestreo por conveniencia en unidades educativas y gobiernos seccionales de la provincia del Carchi como población, para la toma de decisiones de acuerdo a los resultados encontrados. La aplicación del método analítico permitió la obtención de similitudes o conceptos que se complementan con los de otras fuentes, el método inductivo – deductivo por el análisis y adquisición de más conocimientos referentes a la seguridad informática y todo lo referente con la conformación de un equipo de respuesta, y, además, el uso de una entrevista semiestructurada como instrumento de recolección de información.

Los requerimientos para la conformación de CSIRT UPEC son: autorización para conformar el equipo y obtener un espacio en el disco del servidor del Laboratorio de Ciberseguridad, correo institucional y nombre de dominio con upec.edu.ec, certificados SSL, sistemas operativos Kali Linux 2021.2 y CentOS 7.0, acceso al sistema de tickets Centro de Respuesta y Soporte a Incidentes de Seguridad y recursos humanos.

Resultados y discusión

La recolección de información de acuerdo a las variables reporte y seguimiento a incidentes informáticos y seguridad de la información, arroja que un CSIRT opera de diferentes maneras, de acuerdo con el aporte de Ramírez y Mejía (2017), la forma de actuar de un CSIRT depende de la institución a la que se oriente y el tipo de vulnerabilidades o incidentes que presenta. CSIRT UPEC brinda sus servicios a unidades educativas y gobiernos seccionales de la provincia del Carchi.

Mediante el análisis de la investigación de Chacha (2019), se tiene que todos los equipos de respuesta a incidentes se forjan dentro o fuera de otras instituciones, por lo que CSIRT UPEC es un modelo incrustado que consta con misión, visión y valores de identidad operacional, se encuentra dentro de las instalaciones de la Universidad Politécnica Estatal del Carchi, y los recursos tecnológicos y humanos los provee la institución.

Tabla 1.
Entidad operacional de CSIRT UPEC

Misión	Ser un elemento de apoyo para unidades educativas y gobiernos seccionales de la provincia del Carchi en la gestión de incidentes y fomentar una cultura de buenas prácticas en seguridad informática.
Visión	Ser un equipo reconocido a nivel nacional e internacional por su dedicación y aporte a la seguridad de la información.
Valores	• Trabajo en equipo • Impacto social • Compromiso • Empatía • Mejora • Integridad • Respeto

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

De acuerdo con la OEA (2016), la designación del personal es esencial para que el CSIRT gestione sus servicios de manera correcta, por lo que se constituye un líder para cada departamento como recursos humanos en el inicio de las actividades. Se tiene un responsable en el departamento de dirección para realizar la gestión estratégica, control de actividades, cooperación externa y ser el portavoz del equipo, un responsable para el departamento de tecnología para administrar la infraestructura tecnológica y colaborar con el departamento de operaciones, mismo que se encarga de la gestión y monitoreo de incidentes.

Por otra parte, menciona que el catálogo de servicios debe colaborar en la gestión de incidentes o vulnerabilidades de los sistemas; y Sánchez y Parra (2019) mencionan que los procesos operacionales de un CSIRT deben optimizar tiempo y recursos, aportar en la priorización de los servicios y colaborar en la calidad de los mismos. Con la recolección de información en los gobiernos seccionales y unidades educativas vigentes en los distritos de la provincia, CSIRT UPEC maneja cinco procesos operacionales para brindar los siguientes servicios:

Manejo de incidentes: en el proceso de gestión de incidentes intervienen cuatro fases: gestiona el proceso de reportes y solicitudes, realiza el triage en donde lleva a cabo un análisis inicial para determinar su nivel de criticidad, orienta recursos al caso, analiza el evento o incidente y genera recomendaciones de solución.

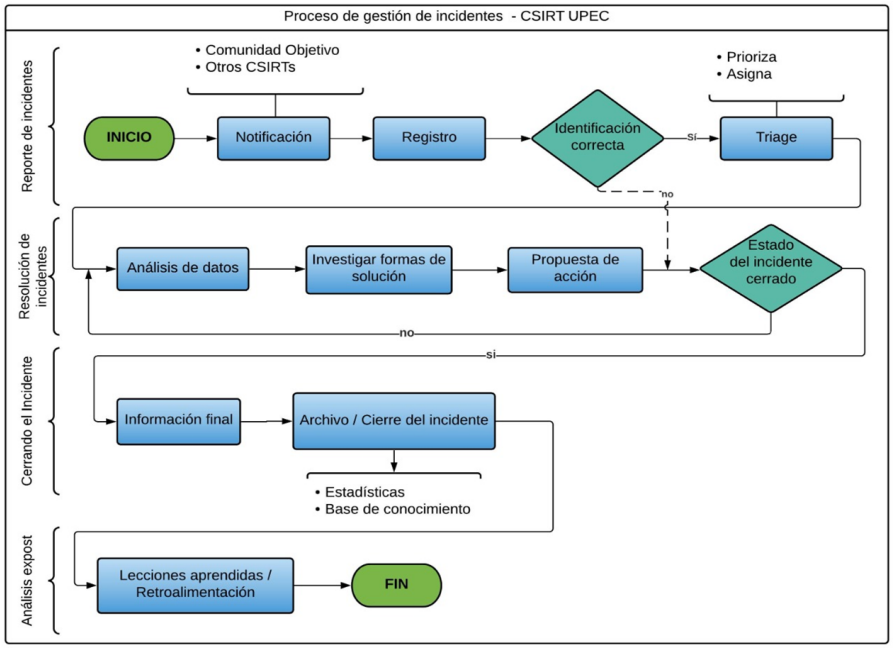

Figura 1. Diagrama de procesos para el servicio de gestión de incidentes

Alertas y avisos: El equipo se encuentra a la vanguardia de nuevos ataques, realiza la recopilación de información de distintas fuentes, se efectúa un análisis de veracidad de la fuente, se evalúan los riesgos y vulnerabilidades que presenta el caso y se distribuye la información para conocimiento de la comunidad objetivo.

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

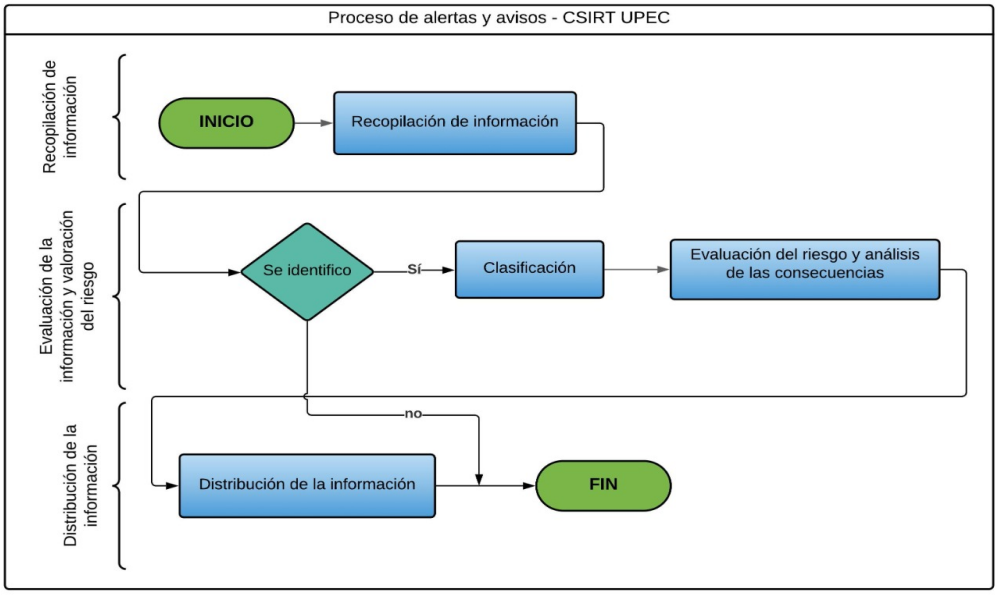

Figura2. Diagrama de procesos para el servicio de alertas y avisos

Publicación de anuncios: emite anuncios a sus miembros, para que les permita estar a la vanguardia en temáticas de seguridad informática e información de interés relacionadas con sus operaciones diarias; sus categorías son: tendencias tecnológicas, seguridad informática, tips de productividad, recomendaciones de mejores prácticas y concientización tecnológica como los principales.

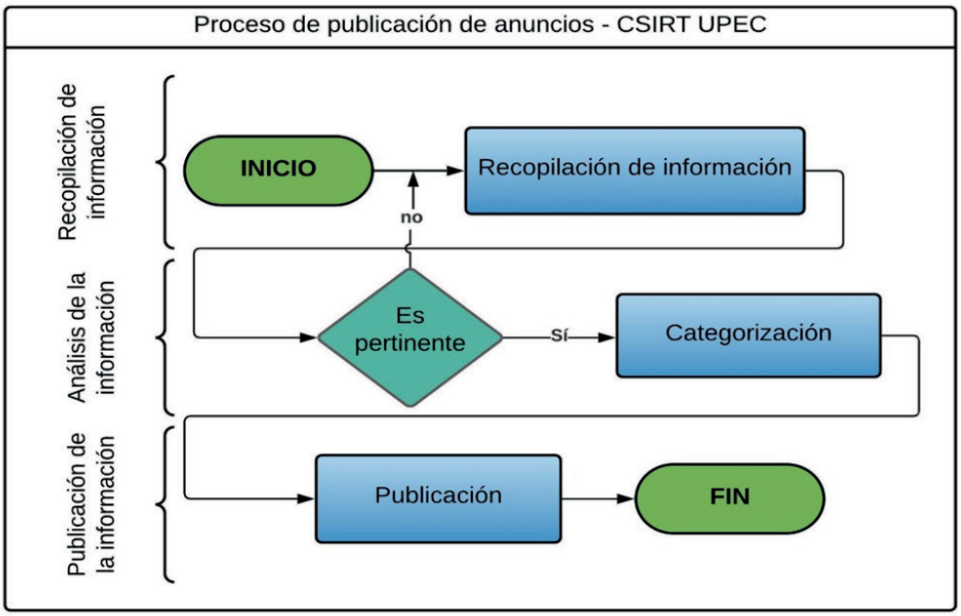

Figura 3. Diagrama de procesos para el servicio de anuncios

Concientización tecnológica: CSIRT-UPEC está comprometido en la concientización de seguridad informática con la comunidad objetivo, se pretende reducir significativamente los incidentes y aumentar la capacidad de detectar vulnerabilidades para que los sistemas sean protegidos o recuperados en menor tiempo.

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

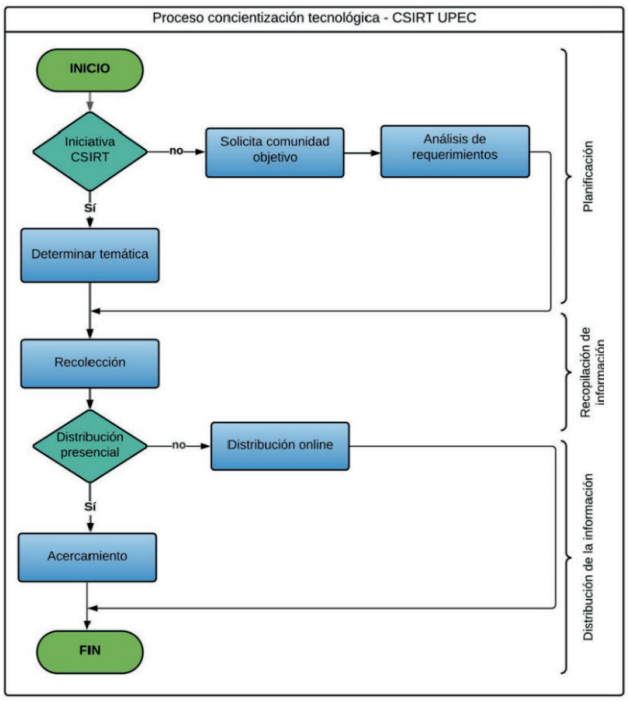

Figura 4. Diagrama de procesos para el servicio de concientización tecnológica

Gestión de riesgos: permite priorizar el riesgo y definir los tiempos de respuesta que serán establecidos en el acuerdo de nivel de servicios (SLA) de CSIRT-UPEC.

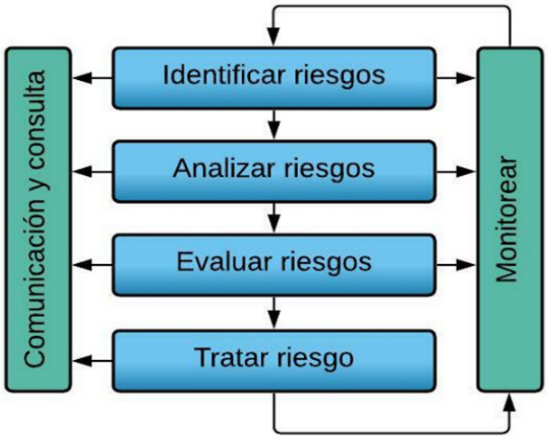

Figura 5. Diagrama de procesos para la gestión de riesgos de los servicios

Fuente: ISOTools (2017) , 10 pasos para implementar un plan de Gestión de Riesgos de acuerdo a ISO 31000. Página web oficial de normativas ISO.

Chacha (2019) menciona que las políticas de seguridad van de la mano con los servicios y sus procesos. Se constituyen políticas para la seguridad de la información y recursos que maneja CSIRT UPEC, además de aportar al correcto funcionamiento del equipo.

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

Tabla 2.
Políticas de CSIRT-UPEC

Política	Objetivo
Clasificación de la información	Definir como clasificar la información en términos de confidencialidad (confidencial, restringido, interno y público).
Protección de datos	Establecer procedimientos que aseguren la confidencialidad e integridad de los datos al ser almacenados o compartidos.
Destrucción de la información	Garantizar que la información de CSIRT-UPEC sea eliminada de manera correcta y segura
Divulgación de información	Establecer la información que puede ser divulgada de acuerdo a quien la requiera, cómo debería ser revelada y las circunstancias para hacerlo. Teniendo en cuenta su nivel de clasificación y protección de la información.
Acceso a la información	Garantizar medidas adecuadas para el acceso a la información tomando en consideración la seguridad y difusión de la información.
Uso apropiado de los sistemas de CSIRT-UPEC	Establecer el uso adecuado de los sistemas de CSIRT UPEC para cumplir con la integridad, confidencialidad y transparencia en todas las actividades.
Cooperación	Determinar las organizaciones con las que puede cooperar CSIRT-UPEC y de qué forma.
Privacidad	Demostrar transparencia acerca del uso de la información.

Al igual que otros equipos, se maneja un sitio web https://csirt.upec.edu.ec como un medio para brindar los servicios de manejo de incidentes, alertas y avisos, anuncios y concientización tecnológica como actividades iniciales y principales del CSIRT, además de mostrar información de contacto y razón de ser como equipo. Por otra parte, está el sistema de tickets donde se realizó la configuración de los servicios de reporte de incidentes y concientización tecnológica, el sistema de monitoreo configurado sobre el sistema operativo kali linux 2021.2, con las herramientas nmap, wireshark, whatweb, dmitry, dnsenum, dnstracer, dnswalk, dotdotpwn y nesuss que permiten obtener más información sobre los incidentes reportados, y se creó redes sociales, correo electrónico csirt.computacion@upec.edu.ec como medios adicionales de comunicación con la comunidad objetivo.

Conclusiones

Con la investigación realizada se afirma que las variables equipo de respuesta ante incidentes informáticos y seguridad de la información se relacionan entre sí, pues la seguridad de la información en la comunidad objetivo depende de los servicios, recursos operacionales y seguimiento a incidentes informáticos del CSIRT.

Los elementos de constitución de un CSIRT son diferentes a cualquier otro equipo, ya que esto se establece de acuerdo a la comunidad objetivo a la que se oriente y el servicio que esta requiera.

Los procesos operacionales colaboran en la eficiencia del servicio y los recursos humanos gestionan los procesos y la información que se involucra, con la finalidad de aportar en la seguridad de la información y disminuir los incidentes o vulnerabilidades en una organización.

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200

Para establecer el catálogo de servicios, los procesos operacionales y las políticas correctas para la protección de la información de la comunidad objetivo, se requiere de una investigación de campo que permita determinar sus requerimientos.

Referencias

Abril, L. (29 de Julio de 2021). Ecuador está entre los países con más ciberataques en América Latina. Obtenido de El Comercio: https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html

BBC News Mundo. (19 de Septiembre de 2019). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. Obtenido de BBC News Mundo: https://www.bbc.com/mundo/noticias-america-latina-49721456

Cano, J. (2020). Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD, Cundinamarca, Bogotá DC, Colombia. Obtenido de https://repository.unad.edu.co/handle/10596/36488

Chacha, M. (2019). Análisis de las metodologías enisa y apcert para la creación del centro de respuesta a incidentes informáticos (csirt). caso práctico: prototipo de un CSIRT en la Universidad Nacional de Chimborazo [Tesis de pregrado]. Universidad Nacional de Chimborazo, Riobamba, Ecuador. Obtenido de http://dspace.unach.edu.ec/handle/51000/6284

De la Torre, H., & Parra, M. (2018). Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. Univeridad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador. Obtenido de http://repositorio.espe.edu.ec/handle/21000/15071

El Comercio. (23 de Julio de 2021). Virus RansomEXX es el responsable del ciberataque a CNT. Obtenido de El Comercio: https://www.elcomercio.com/actualidad/negocios/virus-ransomeware-cnt-ministerio-telecomunicaciones.html

Hidalgo, J. (2017). Importancia de las tic en la enseñanza aprendizaje de los estudiantes de la unidades educativas de la ciudad de Tulcán [Artículo científico]. SATHIRI, Tulcán, Ecuador. Obtenido de https://scholar.google.com/citations?view_op=view_citation&hl=es&user=cKYw7NAAAAAJ&citation_for_view=cKYw7NAAAAAJ:d1gkVwhDpl0C

ISOTools. (2017). 10 Pasos para implementar un plan de Gestión de Riesgos de acuerdo a ISO 31000. Obtenido de ISOTools: https://www.isotools.org/2017/05/14/10-pasos-para-implementar-un-plan-de-gestion-de-riesgos-de-acuerdo-a-iso-31000/

Medina, J., & Meza, A. (2019). Diseño de un marco de referencia para el análisis de vulnerabilidades a un segmento de la red corporativa de una empresa de telecomunicaciones en Quito basado en las principales metodologías de pruebas de seguridad informática [Tesis de postgrado]. Uiversidad Internacional SEK Ecuador, Quito, Ecuador. Obtenido de http://repositorio.uisek.edu.ec/handle/123456789/3348

OEA. (2016). Buenas Prácticas para establecer un CSIRT. Obtenido de Bibliotecadeseguranca: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229. https://doi.org/10.32645/13906925.1200

PROYECTO AMPARO. (2012). Manual básico de:GESTIÓN DE INCIDENTES DE SEGURIDAD. Obtenido de CSIRTLACNIC: https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

Quiroz, B. (2017). Análisis y gestión de la seguridad en la red del GAD Municipio de Rioverde, mediante el diseño del equipo de respuesta a incidentes de seguridad informática, CSIRT. Universidad Politécnica Salesiana, Quito, Ecuador. Obtenido de http://dspace.ups.edu.ec/handle/123456789/14466

Ramírez, H., & Mejía, J. (2017). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante [Artículo científico]. Universidad de Guadalajara, Guadalajara, México. Obtenido de https://www.redalyc.org/pdf/5122/512251501006.pdf

Ranchal, J. (30 de Diciembre de 2020). Los 10 peores incidentes de ciberseguridad en 2020. Obtenido de MC (My Computer): https://www.muycomputer.com/2020/12/30/ciberseguridad-en-2020/

Revista Vistazo. (23 de Diciembre de 2020). Ciberataques: Un riesgo latente y en aumento en el Ecuador. Obtenido de Vistazo: https://www.vistazo.com/enfoque/ciberataques-un-riesgo-latente-y-en-aumento-en-el-ecuador-GDVI215276

Sánchez, H., & Parra, A. (2019). Constitución de un CSIRT para una Entidad Financiera en Colombia. Universidad de los Andes, Bogotá, Colombia. Obtenido de https://proyectosmaestrias.virtual.uniandes.edu.co/images/TNQzugjz0p1d26AM6aQVaAs8MbHg9RzfnHBnKmhf.pdf

Cómo citar este artículo:
Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229.
https://doi.org/10.32645/13906925.1200