DISEÑO DOCUMENTAL DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS QUE PLATINO SISTEMAS PUEDA OFRECER COMO SERVICIO A SUS CLIENTES

JOHN ANDRÉS JIMÉNEZ CANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

DISEÑO DOCUMENTAL DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS QUE PLATINO SISTEMAS PUEDA OFRECER COMO SERVICIO A SUS CLIENTES

JOHN ANDRÉS JIMÉNEZ CANO

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Danny Fernando León
Director de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 11-12-2021

DEDICATORIA

Con todo lo que soy dedico este trabajo a Dios, por su voluntad es que he podido alcanzar estos nuevos logros en mi crecimiento profesional, con amor a mi madre, quien con su temple, paciencia y dedicación ha formado en mi la persona que soy hoy en día. A mi esposa quien me ha acompañado en este nuevo proyecto de vida, a mi padre, quien ha sido mi ejemplo a seguir para tener las convicciones que poseo en mi pensamiento y a mis hermanos que han estado siempre para acompañar mis venturas y desventuras manteniendo fuerte los lazos fraternales para compartir risas, alegrías, llantos y tristezas.

AGRADECIMIENTOS

Agradezco a la Universidad, las directivas y los tutores, quienes encendieron las luminarias que llevaron mi andar por mi carrera profesional y esta especialización, y quienes sin su participación, apoyo y asesoría reconozco que hubiese sido más difícil conseguir este logro.

También doy gracias a los compañeros que se tuvieron en cada una de las materias cursadas, quienes también aportaron de una manera u otra su granito de arena para aprender, debatir, contrastar o apoyar cada uno de los peldaños alcanzados a través de la realización de las guías de cada uno de los trabajos de aprendizaje.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

GLOSARIO

Amenaza: Es la causa que puede ocasionar un incidente a cualquier activo de la empresa y que se puede materializar.

Cibernética: Ciencia que estudia los sistemas de comunicación y de regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos que se parecen a ellos

CSIRT: (*Computer Security Incident Response Team*) Equipo de respuesta a incidentes de seguridad de la información, por sus siglas en inglés es un grupo de personas que buscan las acciones para responder ante la materialización de un riesgo con el impacto mínimo aceptable para las organizaciones

Directrices: Son instrucciones que se dan a cierto grupo de personas a fin de ejecutar procesos y procedimientos en la realización de una actividad, siendo la base fundamental de un desarrollo y/o sistema y están dictadas por la alta gerencia participante en el mismo

Estándares: Son guías documentadas acordadas por diferentes partes en un proceso de estandarización con bastante contenido técnico bajo el amparo de un ente de estandarización. Están hechas para marcar el camino de las actividades de una empresa u organización y otorgar una certificación

IDS: (*Intrusion Detection System*) o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva.

IPS (*Intrusion Prevention System*) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su

actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.[1]

ISAC: (*Information Sharing Analisys Center*) Centro de análisis de información compartida, por sus siglas en inglés es una plataforma de cooperación para equipos de seguridad con un objetivo en común.

ISO27001: Norma estandarizada por la ISO para la gestión de sistemas de seguridad de la información en una organización.

Organización: Estructura ordenada, donde se tienen diferentes personas que desempeñan funciones de roles específicos ejerciendo responsabilidades y cargos para alcanzar una meta en conjunto de un objetivo particular.

Políticas: Es un documento donde se establecen los procesos que se deben llevar a cabo para lograr un determinado resultado en relación a un control establecido en una entidad. Las políticas deben ser creadas, publicadas, comunicadas y educadas a los participantes del proceso de la entidad.

Procedimientos: Son acciones que llevan una secuencia que se debe llevar a cabo a fin de obtener siempre el mismo resultado, los procedimientos son la consecuencia de las directrices a través de un método claro que se definió en un proceso

Procesos: Es un documento donde se establecen los procesos que se deben llevar a cabo para lograr un determinado resultado en relación a un control establecido en una entidad. Las políticas deben ser creadas, publicadas, comunicadas y educadas a los participantes del proceso de la entidad

Riesgo: Posibilidad de que una amenaza se materialice ya sea en un activo o en una empresa.

[1] INCIBE, ¿Qué son y para qué sirven los SIEM, IDS e IPS?, [En línea], Septiembre 2020, [Consultado 08 de octubre de 2022]. Disponible en Internet: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

Seguridad de la Información: disciplina que busca salvaguardar la información de una organización a través de la aplicación de controles y un proceso continuo de mejora por medio de métricas monitoreadas con ejecución de auditorías y resolución de no conformidades.

SGSI: Sistema de gestión de seguridad de la información, es un compendio de estrategias, normas, políticas y controles que permite evaluar todo tipo de riesgos y amenazas de una organización basado en el ciclo de mejora continua PHVA (*Planear, Hacer, Verificar y Actuar)*

SOC: (*Security Operation Center*) Centro de operaciones de seguridad, por sus siglas en inglés, es un servicio que se extiende mucho más allá de solo dar respuesta a incidentes, realizando monitoreo en tiempo real y recopilando métricas para el servicio al cliente como proveedor de servicios de seguridad administrador.

Taxonomía: Ciencia que trata de los principios, métodos y fines de la clasificación, generalmente científica; se aplica, en especial, dentro de la biología para la ordenación jerarquizada y sistemática de un tema apremiante en particular.

Vulnerabilidad: Es una debilidad en el sistema de información el cual puede ser explotada por una amenaza.

RESUMEN

La construcción del diseño documental del CSIRT para la empresa Platino Sistemas se estructuró a partir de los modelos tecnológicos de equipos de respuestas a incidentes tecnológicos, guías y estándares nacionales e internacionales ya constituidos. El procedimiento de manejo en la clasificación de incidentes de seguridad informática y sus publicaciones. Este diseño está basado en la normatividad y legislación actual del país y se lleva a cabo el desarrollo de los objetivos a través de una investigación cualitativa.

Esta investigación permitió conocer los diferentes tipos de CSIRT que existen a nivel mundial y hacía que tipos de empresas en función de su negocio se puede ofrecer, con esto es posible definir el tipo de CSIRT que en su primera etapa ofrecerá la empresa a sus clientes. Este CSIRT se construye para ayudar a los clientes con los ciberataques mayormente presentados en Colombia, y estructurar la clasificación que se le puede dar a estos ataques con el fin de agruparlos y crear diferentes acciones estandarizadas para ayudar a mitigarlos.

Así mismo, con base en los ataques y el campo de acción del CSIRT Platino Sistemas, se definieron los tipos de servicios que la empresa puede brindar, clasificándolos en proactivos, reactivos y complementarios. Esta clasificación es la base para crear los acuerdos de niveles de servicio que se pueden ofrecer. De igual forma, la aplicación del estudio permitió desarrollar las políticas iniciales que harán parte del CSIRT de la empresa Platino Sistemas y que da pasó a la concepción de los procesos y procedimientos que respaldan los sub-servicios del servicio CSIRT que Platino Sistemas ofrecerá a sus clientes.

El diseño documental propuesto quedó en una etapa inicial, con una taxonomía definida con base en el estudio realizado, un campo de acción definido, las políticas, procesos y procedimientos estructurados en su primera publicación y el camino a seguir en la construcción del servicio trazado. Lograr implementar un servicio de esta clase, requiere inversión y dedicación, por lo cual el punto de partida está dado en este proyecto, pero el camino ha de ser recorrido para la maduración propia de un buen servicio a ofrecer a los clientes de Platino Sistemas.

ABSTRACT

The construction of the documentary design of the CSIRT for the Platino Sistemas company was structured based on the technological models of technological incident response teams, guides and national and international standards already established. The handling procedure in the classification of computer security incidents and their publications. This design is based on the current regulations and legislation of the country and the development of the objectives is carried out through qualitative research.

This research allowed us to know the different types of CSIRT that exist worldwide and what types of companies can be offered depending on their business, with this it is possible to define the type of CSIRT that the company will offer to its clients in its first stage. This CSIRT is built to help clients with the most common cyberattacks in Colombia, and structure the classification that can be given to these attacks in order to group them and create different standardized actions to help mitigate them.

Likewise, based on the attacks and the field of action of the CSIRT Platinum Systems, the types of services that the company can provide were defined, classifying them as proactive, reactive and complementary. This classification is the basis for creating the service level agreements that can be offered. In the same way, the application of the study allowed the development of the initial policies that will be part of the CSIRT of the company Platino Sistemas and that gives way to the conception of the processes and procedures that will support the sub-services of the CSIRT service that Platino Sistemas will offer to its customers.

The proposed documentary design remained in an initial stage, with a defined taxonomy based on the study carried out, a defined field of action, the policies, processes and procedures structured in its first publication and the path to follow in the construction of the outlined service. Achieving the implementation of a service of this kind requires investment and dedication, for which the starting point is given in this project, but the path must be traveled for the proper maturation of a good service to offer to Platino Sistemas' clients.

INTRODUCCIÓN

Los ciberataques son parte propia de nuestra realidad, en la década de los noventa, apareció un tipo de guerra que se concentraba en mayor parte en las computadoras y el internet. En 1993 se hablaba de guerra cibernética, donde los piratas militares informáticos no utilizarían solo la red para el reconocimiento y el espionaje de los sistemas enemigos, sino para realizar ataques que interrumpieran los equipos de comunicación que el bando enemigo utilizaba para el mando y control.

Con el pasar del tiempo, estos piratas militares informáticos no solamente estarían atacando a sus enemigos, sino también podrían hacerlo con civiles en un mundo cada vez más dependiente de las computadoras, atacando de esta manera, vías férreas, aeropuertos, bolsas de valores entre otros. Es así como los ataques cibernéticos en sí mismos podrían ser un arma de guerra. Y aunque no existe una guerra, si existen estos ataques que desde aquella época han ido evolucionando haciéndose más complejos y peligrosos. Es por esto que existen los ***Equipos de Respuesta los Ataques Informáticos*** que serían como la policía de la Internet, que nos ayuda a identificar cómo se pueden dar estos ataques, cómo prevenirlos, cómo mitigarlos y cómo hacer investigación forense después de que hayan ocurrido.

En el 2010, un malware denominado *STUXnet* fue encontrado por *VirusBlokAda* una empresa de seguridad de Bielorrusia, encontrando el equipo de seguridad que este era la pieza de código más sofisticada para un ataque cibernético. *STUXnet* es conocido como el primer ataque cibernético jamás diseñado para dañar directamente el equipo físico.

En agosto de 2017 un malware llamado Tritón o Trisis obligó al cierre de una refinería de petróleos de Arabia Saudita el cual no quería provocar este cierre sino deshabilitar los sistemas de seguridad instrumentados de la planta que sirven para evitar situaciones inseguras.

El potencial destructivo de los ataques cibernéticos es para prestarle mucha atención en una época en las que todos dependemos de las computadoras para vivir. “Es sorprendente ver cómo la tecnología de la información se incorpora cada vez más a nuestras vidas, inclusive atravesando la última frontera. Algunas de las prestaciones de dispositivos, aplicaciones y sistemas de mayor desarrollo en la actualidad ingresan al interior de nuestro cuerpo con singular éxito: sondas, marcapasos, microelectrónica aplicada para la asistencia a personas con

discapacidades auditivas o visuales, localización permanente de personas" (Carozo)[2] En las empresas también es igual, la tecnología ha penetrado en cada una de las áreas y cada vez es más indispensable las redes, los computadores, las redes y los servicios que dependen de estos sistemas.

Estos sistemas al igual que todos o muchos de los sistemas en que está conformado el mundo, tiene sus propias fallas, porque fueron creados por humanos y los humanos tenemos fallas, pero, ¿cuánto tiempo puede pasar en que una empresa se dé cuenta de una falla? ¿cuánto puede costar esta falla a la empresa? (De la Torre & Parra, 2018)[3] "Las actividades maliciosas asociadas a la tecnología se han incrementado y son la principal causa de gastos realizados para su contención, resolución y prevención de daños potenciales, sin considerar el lucro cesante al interrumpir los servicios de los clientes".

Colombia no es la excepción, el año pasado los ataques reportados por el grupo de respuestas a incidentes cibernéticos (CSIRTPonal) evidenció un incremento significativo, en la cantidad de incidentes – cincuenta y cuatro por ciento (54%) – en relación al 2018, y en el 2020 dado la situación actual de pandemia esta cifra sigue en aumento.

"Los ciberataques a nuestras empresas pueden generar una serie de efectos colaterales que incluyen reducir su productividad, causar daños reputacionales e incluso pueden llegar a generar demandas y otros retos de carácter legal por fuga de información privilegiada y datos sensibles de clientes y proveedores, entre otros" (Yohai, 2019) es así, ya sea por desconocimiento de los incidentes de seguridad, porque la empresa no tiene los recurso para montar toda la infraestructura que necesita para su seguridad o protección que se ven vulnerables a estos ciberataques.

---

[2] CAROZO B., Eduardo. Implantación del sistema de gestión de seguridad de la información en una empresa compleja. Memoria de Trabajos de Difusión Científica y Técnica. [en línea]. 2007. No. 5, p. 77-87. ISSN 1510-7450. [consultado 20 de octubre 2020]. Disponible en Internet: https://www.researchgate.net/publication/38290247_Implantacion_del_sistema_de_gestion_de_seguridad_de_la_informacion_en_una_empresa_compleja

[3] DE LA TORRE M., Hugo y PARRA R., Mario. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. Tesis de pregrado. Universidad de las Fuerzas Armadas ESPE. 2018. [consultado 19 de octubre 2020]. Disponible en Internet: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/15071/T-ESPE-040447.pdf?sequence=1&isAllowed=y

Es por esto, que ***PLATINO SISTEMAS***, empresa líder en seguridad informática en el país, quiere brindar a sus clientes un equipo de respuesta a incidentes de seguridad informática (CSRIT, por sus siglas en inglés), para ayudar a mitigar y reducir significativamente la cifra de ciber incidentes que se presentan en el país, permitiendo que muchas personas cuenten con sus servicios y conozcan lo que cuesta no tener la información o el servicio noventa y nueve (99%) disponible.

“Si bien, para una persona en particular, es importante la seguridad de su información, para una empresa u organización será de más relevancia, debido a que en ella se maneja información crítica y centralizada, un verdadero botín para las personas malintencionadas. No olvidemos que hoy en día todo nuestro entorno está conectado, que todo nuestro mundo está siendo virtualizado y que la seguridad de los sistemas se ha convertido no tan sólo en una necesidad, sino en una prioridad para todo los que hacemos uso de éstos”. (Mejía, Muñoz &Ramírez), es por esto que la seguridad informática ha pasado de ser una necesidad a una prioridad, es que ***PLATINO SISTEMAS*** entendiendo esto quiere ofrecer una manera de ayudar a las empresas que no tienen o no les alcanza para este servicio, la posibilidad de priorizar la seguridad de su compañía.

Pero más que hacerlo de manera reactiva, también quiere hacerlo de forma proactiva, con un constante monitoreo de su infraestructura – sea grande o pequeña – evitando o reduciendo al máximo los riesgos a los que se pueda ver expuesta la empresa u organización, para que esto no cause ningún impacto, ni de imagen ni económico a su compañía.

Es por esto que, durante este escrito, se encontrarán las pautas que se deben tener en cuenta para la creación de la documentación necesaria de la conformación de un equipo de respuesta a incidentes de seguridad informática como servicio de ***PLATINO SISTEMAS.***

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En el mundo y en Colombia muchas compañías hablan de sistemas de gestión de seguridad tecnológica, de seguridad informática, de seguridad de la información, y todo aquello para que la compañía sea menos vulnerable a los incidentes informáticos y cibernéticos. Sin embargo, la seguridad no es algo 100% resuelto y más aún en este mundo informático en que por cada ataque o incidente que se detiene o frustra, aparecen a diario 10 formas nuevas de realizarlo. Y es que en la actualidad muchos de estos ataques no son ejecutados por personas, son personas que programan cientos o miles de máquinas que pueden lanzar un ataque a gran escala concurrentemente en cuestión de segundos. Y dichos ataques cada vez son más intrincados y más difíciles de detectar para las personas que están tratando de proteger la seguridad en una empresa.

La empresa Platino Sistemas, es una empresa colombiana que se enfoca en los servicios de seguridad para la protección de la información, y que durante los últimos años ha sido consciente de esta problemática en Colombia, ha visto el incremento de diferentes incidentes cibernéticos en el país y en sus clientes en particular, lo que ha dado paso a Platino Sistemas a pensar en cómo ayudar a su clientes y a otras compañías en el país en la mitigación de estos incidentes informáticos y en la reducción de sus brechas de seguridad. Cómo ofrecer un servicio de ayuda proactivo y reactivo que brinde atención y soporte ante estos eventos las empresas del territorio nacional, ya sea bien para dar respuesta a estos incidentes o gestionando las vulnerabilidades en la infraestructura tecnológica que los mismos puedan tener en sus empresas.

Aunque no existe la forma de asegurar todo completamente, Platino Sistemas busca ayudar a todas estas empresas, desde las que se encuentran certificadas en la norma ISO/IEC 27001, hasta las que no han empezado o no conocen la norma. Así como, a las empresas que conocen cómo actuar ante un incidente de ciberseguridad materializado como a las que no tienen idea de por qué les pasó. Platino Sistemas quiere entregar a sus clientes el servicio que ayude a mitigar los incidentes de seguridad que se puedan dar, o simplemente definir algunas políticas de seguridad dependiendo del tamaño de la empresa para que puedan mitigar sus vulnerabilidades y así salvaguardar su información.

Platino Sistemas quiere implementar este servicio, que permitiría a los clientes contar con un Equipo de respuesta ante los incidentes de seguridad informática, que les brinde la oportunidad de tener medios con los cuales sus organizaciones puedan identificar, medir y corregir el impacto de un incidente de seguridad que se

pueda presentar o se haya presentado. Para lograr este CSIRT, Platino Sistemas ha pedido a su equipo de trabajo crear el diseño documental que permita el desarrollo de las actividades propias de este nuevo servicio, por lo cual es necesario conocer todos aquellos apartes que componen el diseño documental para crear el CSIRT dentro de la empresa y preguntarse:

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué se necesita para crear el diseño documental de un equipo de respuesta de incidentes de seguridad informática – CSIRT en la organización Platino Sistemas que cumplan con las normativas vigentes y pueda brindar un servicio de calidad para los clientes de la organización?

2 JUSTIFICACIÓN

Comenzamos cosas sin definir apropiadamente una estructura de las mismas muchas veces y aunque con el tiempo funcionan y salen bien, el camino para llegar a ello es más largo y con los años no se sabe por qué se hacen las cosas. La respuesta más simple es “porque así se han hecho siempre” y esto no permite tener documentado los procesos ni los procedimientos, y la experiencia casi siempre está en la cabeza de quienes han realizado estos pasos y a quienes ellos lo han transmitido. De igual forma, muchas veces el no tener estructurado algo, hace que la mejora, el cambio y la evolución del mismo sea caótico y a veces hasta imposible, dando paso a iniciar de nuevo o dejar de lado, porque no es posible sostenerlo en el tiempo.

La construcción del diseño documental CSIRT para la empresa Platino Sistemas es necesaria e inamovible porque es la base fundamental del nuevo servicio que la empresa quiere brindar a otras compañías en Colombia, con el fin de ayudar a aumentar las soluciones de seguridad informática y de la información en sus infraestructuras tecnológicas. De hecho, identificada la necesidad en los antecedentes mencionados en lo relacionado a la seguridad informática en la infraestructura tecnológica de los clientes de la empresa Platino Sistemas, el servicio de Equipo de Respuesta ante Incidentes Informáticos, es una alternativa viable y de grandes proyecciones para la empresa.

Sin embargo, cabe resaltar que, como líder del equipo de desarrollo, y como especialista en seguridad informática la construcción de este diseño debe ser en una etapa inicial, partiendo del principio de definición del CSIRT de acuerdo a “***Trusted Introducer***”, por lo cual estaría en una etapa de Listado, permitiendo un crecimiento a futuro en las etapas consecuentes de acreditado y certificado.

De igual forma, la construcción de este diseño documental inicial en la etapa Listado, debe crearse bajo un modelo que esté a la altura de los estándares internacionales, por ejemplo, de los estándares de SIM3 el cuál basa en tres (3) parámetros básicos que a la vez pertenecen a cuatro (4) cuadrantes escogidos para ser mutuamente independientes dentro de lo posible y a su vez cada parámetro tiene cinco (5) niveles. Así que se puede verificar el nivel de madurez del CSIRT a través de las evaluaciones en línea.

Como especialista en seguridad informática, se establece el desarrollo de este proyecto a través de una investigación cualitativa, con la cual, a través de diferentes fuentes, documentos, guías y alternativas de estudios y lecturas entregará las herramientas necesarias para la construcción del diseño documental en su etapa inicial, entregando las bases y la estructura apropiada del nuevo servicio a Platino Sistemas como nuevo servicio con la organización de la taxonomía de los eventos de seguridad, clasificación del incidente en relación a su severidad y al cliente al que se le esté brindando el servicio, así como el proceso para la resolución de incidentes y el manejo que se le tiene que dar al mismo durante su ciclo de vida, reporte y definición del incidente. Todo bajo las normas y metodologías de clasificación de riesgos específicas para este nuevo servicio de CSIRT.

3 OBJETIVOS

3.1 OBJETIVOS GENERALES

Construir un diseño documental que permita el desarrollo de las actividades propias del CSIRT para la organización Platino Sistemas.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer el campo de acción del CSIRT dónde se estructure el entorno (clientes) del CSIRT como servicio de la empresa Platino Sistemas con base al panorama actual de la ciberseguridad en Colombia.

- Estructurar la taxonomía de los incidentes de seguridad del CSIRT de acuerdo a los ataques más presentados en el panorama actual de ciberseguridad en Colombia.

- Integrar los servicios de Platino Sistemas en Proactivos, reactivos y complementarios que serán parte del CSIRT, y que la organización Platino Sistemas puede ofertar a sus clientes.

- Construir las políticas, procesos y procedimientos operacionales, manuales e instructivos basados en la norma ISO/IEC 27000 para verificar el estado de obligatorio cumplimiento por parte de los clientes para definir el grado de responsabilidad del CSIRT

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

4.1.1 Propósito del CSIRT

El crecimiento de los dispositivos a través de los cuales se maneja la información y las redes por las cuales lo hacen es desaforado en la actualidad, y junto con ellas la sofisticación, versatilidad y aumento de las amenazas a dicha información que hacen que muchos expertos se planteen que solo es cuestión de tiempo antes de que muchas empresas empiecen a padecer los riesgos de la seguridad informática. Y es que ya pasamos de tener una persona sentada frente a un computador queriendo hacer daño a una compañía, a ataques a gran escala, con miles de bots y máquinas zombis listas para atacar un sector o una nación por completo (y se pudo evidenciar hace unos años con el Ransomware Wannacry). Y es así como más allá de expertos investigadores es necesario contar con equipos dedicados a dar respuesta de manera pronta y oportuna ante los nuevos riesgos de orden cibernético.

> *Dado este escenario de evolución del malware y otras amenazas, cobran relevancia los equipos de respuesta a incidentes de seguridad (CSIRT por las siglas de Computer Security Incident Response Team). Su razón de ser radica en que aunque resulte casi imposible evadir todos los riesgos, en caso de que alguno se materialice, sus consecuencias puedan ser mitigadas y las actividades primordiales restablecidas en el menor tiempo posible, con el impacto mínimo aceptable para las organizaciones*.[4]

Entonces un CSIRT está diseñado para medir, reducir y ayudar a las organizaciones cuando un evento o incidente se seguridad se materializa.

Aparte de su función primordial, también puede aportar si está diseñado para realizar una investigación forense sobre el evento con una correcta preservación de la evidencia, y si llega más allá puede optar por el monitoreo en tiempo real de vulnerabilidades, incidentes y amenazas.

[4] ESET. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [sitio web] 18 de mayo de 2015 welivesecurity. [consulta: 15 de noviembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Pero no es solo un equipo de respuesta inmediata a las amenazas materializadas, porque debe ser proactivo, informando de aquellas amenazas que se han podido presentar en otros lados y que gracias a la comunidad conoce como remediarlas antes de que se presenten a sus usuarios. De igual manera que tiene que aprender de los eventos ocurridos para prevenir la ocurrencia de los mismos en un futuro, radicando de ser posible la causa raíz del incidente.

Por consiguiente contar con CSIRT como parte fundamental de la protección de la seguridad de la información puede proveer los servicios desde una perspectiva proactiva/reactiva, ya que funcionan como educadores de las nuevas amenazas que se presentan en el mundo actual y aquellas derivadas de la experiencia, brindando información para la protección de la infraestructura tecnológica de su empresa, evitando estas amenazas y por otro lado reactiva, ya que apoyan y ejecutan las actividades cuando un evento de seguridad se ha presentado.

4.1.2 Construcción de un CSIRT

La construcción de un CSIRT es una tarea compleja, que debe empezar en un nivel incipiente e ir escalando a medida que se van probando las funciones y ventajas de poseer esta estructura orgánica para dar respuesta a los incidentes de seguridad hasta llegar a poseer un nivel de respuesta a eventos de madurez superior.

Para la construcción de un equipo de respuesta inmediata a incidentes de seguridad de la información, se debe contar con el apoyo necesario para llevarlo a cabo, ya que en principio, este se va a ver como un gasto, ya que no retornará inversión, - es como una especie de servicio de emergencia, no se le ve la utilidad hasta que no tienes la emergencia, o como un seguro, no se le ve la inversión hasta que te toca depender de él – porque mientras la amenaza no se materialice, el CSIRT no presenta una verdadera necesidad.

Cómo la mayoría de las acciones o empresas que iniciamos, el CSIRT debe tener claro un plan estratégico, también se puede ver como un marco de trabajo, determinando o respondiendo preguntas tales como: ¿Qué hará el CSIRT? ¿De dónde vendrán los recursos? ¿De dónde vienen los miembros del equipo? Además de esto, es bueno definir el objetivo del CSIRT, planificar el manejo de un incidente, el equipo y el ambiente de trabajo.

Todo lo anterior, solo hace parte de la etapa de planificación del CSIRT, ya que es

necesario entender que esta es la etapa preliminar donde se realiza el diseño documental del mismo, el segundo aparte es la ejecución del CSIRT y la última la de cierre y retroalimentación, dónde se evaluarán las etapas de planificación y ejecución a través de la realización de las actividades para encontrar puntos de mejora y adaptación del CSIRT a las nuevas amenazas para saber si el equipo es suficiente o debe ser incrementado, o si por el contrario se dimensionó exageradamente y el personal puede ser disminuido.

4.2 ANTECEDENTES O ESTADO ACTUAL

Platino Sistemas, es una organización colombiana que se enfoca en servicios y que presta servicios de seguridad para la protección de la Información. Una de las metas para el año 2022 es crear un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT, el cual tendrá como propósito crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio contratado los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades.

4.3 MARCO LEGAL

Es necesario considerar que un CSIRT debe conocer las normas regulatorias de Colombia para el tratamiento de datos y seguridad de la información, la ley 1581 del 2012 de protección de datos que contempla el derecho al tratamiento de los datos personales, la responsabilidad que tiene cada titular de las empresas y entidades para que dicha información no sea entregada a personas sin el consentimiento del dueño de los datos.

La ley 1273 del 2009 que contempla la confidencialidad, integridad y disponibilidad de la información en sistemas informáticos, así como los delitos informáticos conocidos y los ataques informáticos los cuales tienen una pena legal según se identifique el delito cometido. Los abusos cometidos a la infraestructura por parte de terceros son delitos que son castigables en la ley colombiana

5 DISEÑO METODOLÓGICO

Para el desarrollo de esta investigación se utilizará un método cualitativo, por medio del cual la investigación colectará los datos en los sitios de las comunidades internacionales y nacionales que existen actualmente tales como colCERT, http://www.colcert.gov.co/, o el foro de equipos de seguridad y respuesta a incidentes FIRST http://www.first.org/, ingresar a estos portales nos permitirán tomar notas sobre la manera en que operan los CERT o CSIRT, participar en el foro y hacer parte de estas comunidades nos permitirán orientar el desarrollo de la creación del CSIRT para la empresa Platino Sistemas.

Participar en estas organizaciones será fructuoso en el desarrollo de este proyecto por toda la documentación que se puede obtener, y es que ellos ya han enfrentado diferentes incidentes de seguridad que tal vez se desconozcan por parte de nosotros como pioneros en la creación de un CSIRT. Es por esto que la investigación cualitativa se basará en:

Documentos Cualitativos: Foros, publicaciones en revistas, minutas de reuniones, reportes oficiales, guías de creación, periódicos, investigaciones anteriores, casos de estudio, proyectos de implementación de CSIRT en sector gobierno, educación, empresarial entre muchos otros.

Materiales Digitales y audiovisuales: vídeos, páginas web, correos electrónicos, mensajes de texto, podcast, redes sociales y cualquier formato de sonido que se pueda obtener.

Entrevistas Cualitativas: Involucrarnos en grupos de investigación, entrevistar a personajes que ya hayan desarrollado un CSIRT, vídeo conferencias, seminarios, talleres entre otros.

6 DISEÑO DOCUMENTAL DEL CSIRT DE PLATINO SISTEMAS

6.1 CAMPO DE ACCIÓN CSIRT DE PLATINO SISTEMAS

Primordialmente, es indispensable pensar en la comunidad objetivo a la que se va a ofrecer el CSIRT de ***Platino Sistemas*** como servicio. “La Comunidad objetivo, conocida en inglés como <<*constituency*>> es quiénes reciben los servicios del CSIRT”[5]

El entendimiento de a quienes se quiere ofrecer estos servicios del equipo de respuesta a incidentes de seguridad informática ayuda a determinar al equipo cuales son las necesidades de cada uno de los clientes, los activos que cada cliente tiene y se diferencia de los otros clientes y que necesita ser protegido y de qué manera el cliente va a interactuar con el CSIRT de ***Platino Sistemas***

“Cada equipo debe tener una Comunidad objetivo claramente definida. De existir solapamiento con algún otro equipo esto debe ser dado a conocer a la Comunidad objetivo para que tengan claro qué servicio solicitar a cada equipo”.[6]

En concordancia a esto, ***Platino Sistemas*** define que su comunidad objetivo son todas aquellas empresas que son sus clientes y pueda ofrecerles el servicio de CSIRT, lo cual convierte al CSIRT de ***Platino Sistemas*** en un CSIRT comercial.

*Tabla 1 Definición de CSIRT de **Platino Sistemas***

CSIRT COMERCIAL	
Por diversas razones, incluyendo limitaciones de recursos humanos o muchas otras, algunas empresas optan por externalizar los servicios de CSIRT en lugar de internamente crear y gestionar las funciones de respuesta a incidentes. Esto ha dado lugar a un mercado robusto para CSIRT comerciales, que ofrecen servicios pagos de respuesta a incidentes para clientes. La relación entre un CSIRT comercial y su cliente a menudo se rige por acuerdos de nivel de servicio (SLA por sus siglas en inglés), que son necesarios para establecer lineamientos	

[5] PÉREZ E. Ernesto, y BERNAL B. Paul F. Estableciendo un CSIRT [en línea] 2020 Traducción al español de Van der Heide, Martjin “Establishing a CSIRT” con el apoyo de ThaiCERT y ETDA, p. 45. [consultado 18 de octubre 2020]. Disponible en Internet. https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf

[6] Ibid., p. 13.

de respuesta a incidentes y asegurar que la información se maneja de acuerdo a las necesidades del cliente[7].

Fuente: ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

Sin embargo, aunque el CSIRT de ***Platino Sistemas*** es comercial su comunidad objetivo serán, todas aquellas partes interesadas en la implementación de este CSIRT, entre ellas podemos encontrar a las personas o las organizaciones a las que se les prestará el servicio por la implementación de este CSIRT definiendo el uso o ámbito del servicio, estableciendo a quien va dirigido y de qué modo ayudará a la seguridad informática de su infraestructura.

Este concepto posibilita que la solución de seguridad que brinda el equipo de ***Platino Sistemas*** abarque no solamente dónde brindar el servicio, sino que además a quien se le va a brindar y que clase de cliente se puede proteger.

6.1.1 Ámbito de Aplicación

"En la descripción de los ámbitos se tiene en cuenta las empresas y organizaciones según el tamaño y su repercusión ante cualquier incidente de seguridad, así como su infraestructura"[8]

- Microempresas / Autónomos

Las empresas que figuran en este ámbito de aplicación son aquellas que cuentan con 10 o menos trabajadores, en muchos casos autónomos, manejan un volumen de negocio pequeño, por lo general no tienen personal calificado en lo referente a las soluciones de seguridad informática ni de sus infraestructuras. Es común que los servicios hacia este ámbito se encaminen al cumplimiento normativo y

[7] ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

[8] ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Taxonomía de soluciones de ciberseguridad [en línea] 2015. p. 57 Disponible [consultado 30 de octubre 2020]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

legislativo, implementación de soluciones que mitiguen casi cualquier incidente de seguridad, herramientas de protección y recuperación, aportando seguridad física a local, el hardware y el software de la empresa.

- Pymes (pequeña /mediana empresa)

Las empresas que figuran en este ámbito son aquellas entre 10 y 250 empleados, con un volumen de negocio medio, en muchos casos tienen su propio equipo técnico y entre ellos un responsable de la seguridad de la información, siendo ellos los que se encargan de implementar las soluciones de protección que necesiten conforme vaya avanzando su gestión.

Bajo este ámbito se encuentran las soluciones de seguridad dirigidas a la selección, implementación y operación de las soluciones de seguridad. Se encuentran los servicios que detectan los posibles fallos de seguridad de la infraestructura, y los que proporcionan los recursos necesarios de seguridad y la gestión de los incidentes de seguridad[9]

- Gran empresa

En este ámbito están las empresas con más de 250 empleados, poseen sus propias instalaciones y un volumen de negocio grande, aquí ya existe un departamento de TI especializado y con personal encargado de la seguridad y los incidentes de seguridad que se puedan presentar. La solución de seguridad en este ámbito recoge los valores anteriores y también soportan la aplicación de auditorías, protección, detección y reacción ante incidentes de seguridad. Aplicación de medidas de seguridad organizacionales, y políticas de seguridad definidas e implementadas.

- Infraestructuras Críticas

Dentro de este ámbito se encuentran las infraestructuras críticas que son los activos esenciales para el funcionamiento de la sociedad y la economía. Centrales y redes de energía, servicios de transporte, servicios financieros, entre otros. Estas empresas tienen áreas específicas de ciberseguridad y están protegidas por los organismos públicos.

[9] Ibid., p. 10.

Muchas de las personas y empresas interesadas se encuentran en este ámbito y se pueden clasificar por sus funciones o ejercicio en:

6.1.2 Entorno de Clientes

- **Clientes Académicos:** Todas aquellas instituciones que brindan educación a la comunidad, como colegios, instituciones educativas y universidad

- **Clientes Proveedores de Servicios:** Todas aquellas organizaciones que brinden servicios a la comunidad, dentro de esta categorización de clientes podemos encontrar los prestadores de servicio de internet (ISP, por sus siglas en inglés) los prestadores de servicios públicos y los prestadores de servicios de telecomunicaciones o televisión paga.

- **Clientes Sector Privado:** En este entorno están definidas todas las empresas privadas que por su dimensión necesiten de los servicios de CSIRT, que operen infraestructura de TI, o que se orienten a la fabricación de un producto y necesiten apoyo para la mitigación de un ataque.

- **Clientes Sector Financiero:** En este entorno está definido las empresas bancarias, bancos centrales, casas de bolsa, casas de chance, casas de cambio, cajas de compensación familiar y cooperativas entre todos aquellos que manejen grandes sumas de dinero y necesiten los servicios, o también pueden ser patrocinadores y hacer una alianza para brindar el servicio de CSIRT a cambio de sponsor.

- **Clientes Sociedad Civil:** Aquí podemos ubicar aquellas empresas que prestan servicios a la sociedad en organizaciones profesionales, aquellas que son sin ánimo de lucro como las fundaciones o las ONG, academias deportivas o instituciones del deporte, comunidades de grupos de usuarios que se reúnan para eventos propios entre otros.

- **Clientes Fuerzas del Orden:** Aquí se pueden ubicar las fuerzas militares y de policía o secreta, o de inteligencia de un país, aunque en el país ya existe un equipo de respuesta a incidentes de la policía nacional del país, no es necesariamente descartable este grupo, ya que se podría brindar apoyo a ellos, o tal vez al ejército o algún otro grupo que clasifique dentro de este entorno.

- **Clientes Sector Gobierno:** El sector del gobierno es tal vez uno de los más grandes dentro de la nación colombiana, tiene muchas empresas a las que se le puede brindar este servicio, sin embargo, en muchas ocasiones este servicio deberá ir unido de otros servicios que se le pueda brindar, calculando costos del servicio a precios muy bajos hasta que ellos puedan identificar el valor agregado de este servicio y sea visto como parte esencial de la seguridad informática de su infraestructura.

En esta perspectiva de servicio empresarial, el CSIRT de ***Platino Sistemas*** debe ser multimodal, flexible y polifuncional. Ya que, aunque el equipo se puede ampliar conforme vaya creciendo la demanda, en principio las personas del orden administrativo y gerencial del servicio deberán ser conocedores de diferentes disciplinas a las que les puedan brindar este servicio.

Siendo cierto esto, el CSIRT de la empresa prestará servicios a diferentes comunidades objetivos, ya que todos son posibles clientes, basados en la guía de ENISA[10], los sectores en los que CSIRT brindará sus servicios son:

Tabla 2 Descripción de sectores de ENISA

Sector	Descripción	Grupo de clientes atendidos
Académico	Los CSIRT del sector académico prestan servicios a centros académicos y educativos, como universidades o centros de investigación, y a sus campus virtuales.	El grupo típico de clientes atendido por estos CSIRT está formado por el personal y los estudiantes de las universidades
Comercial	Los CSIRT comerciales prestan servicios comerciales a sus clientes. En el caso de un proveedor de servicios de Internet, el CSIRT presta principalmente servicios relacionados con el abuso a los clientes finales (conexión por marcación telefónica, ADSL) y	Por lo general, los CSIRT comerciales prestan sus servicios a un grupo de clientes que paga por ello

[10] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMCIÓN – ENISA. Cómo crear un CSIRT paso a paso [en línea]. 2006. Consultado 18 de octubre de 2020. Disponible en Internet: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

Sector	Descripción	Grupo de clientes atendidos
	servicios de CSIRT a sus clientes profesionales	
Infraestructura Crítica (CIP)	Los CSIRT de este sector se centran principalmente en la protección de la información vital (CIP) y de la información y las infraestructuras vitales (CIIP). Por lo general, estos CSIRT especializados colaboran estrechamente con un departamento público de protección de la información y las infraestructuras vitales. Estos CSIRT abarcan todos los sectores vitales de las TI del país y protegen a los ciudadanos	Sector público; empresas de TI de importancia fundamental; ciudadanos
Gobierno	Los CSIRT del sector público prestan servicios a agencias públicas y, en algunos países, a los ciudadanos	Agencias gubernamentales
Interno	Los CSIRT internos únicamente prestan servicios a la organización a la que pertenecen, lo que describe más su funcionamiento que su pertenencia a un sector. Numerosas organizaciones de telecomunicaciones y bancos, por ejemplo, cuentan con sus propios CSIRT internos. Por regla general, estos CSIRT no mantienen sitios web públicos	Personal y departamento de TI de la organización a la que pertenece el CSIRT
Militar	Los CSIRT de este sector prestan servicios a organizaciones militares con responsabilidades en infraestructuras de TI necesarias con fines de defensa	Personal de instituciones militares y de entidades estrechamente relacionadas con éstas, como por ejemplo del Ministerio de Defensa.
PYMES	Se trata de un CSIRT organizado por sí mismo que presta servicios a las empresas	El grupo de clientes atendido por estos CSIRT pueden ser las PYME y su personal, o

Sector	Descripción	Grupo de clientes atendidos
	del ramo o a un grupo de usuarios similar	grupos de interés especial como la «Federación de municipios» de un país
SOPORTE	Los CSIRT de soporte se centran en productos específicos. Suelen tener por objetivo desarrollar y facilitar soluciones para eliminar vulnerabilidades y mitigar posibles efectos negativos.	Propietarios de productos

Fuente: Elaboración propia con base en la guía de la AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMCIÓN – ENISA. Cómo crear un CSIRT paso a paso [en línea]. 2006. [consultado 18 de octubre de 2020]. Disponible en Internet: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

En revisión de la guía de ENISA, y los sectores y definidos con anterioridad, vemos que son muy parecidos y algunos nuevos por lo cual se establece que el campo de acción que llevará a cabo la empresa ***Platino Sistemas*** es la siguiente:

Tabla 3 Estructura entorno clientes CSIRT Platino Sistemas

PLATINO SISTEMAS		
No.	**ENTORNO / SECTOR**	**SERVICIO CSIRT OFERTADO**
1	Académico	CSIRT Académico
2	Comercial	CSIRT Comercial – Sector Privado
3	CIP / CIIP	CSIRT CIP – CIIP
4	Financiero	CSIRT Financiero
5	Sociedad Civil	CSIRT S-Civil
6	Interno	CSIRT PS
7	Militar / Fuerzas del Orden	CSIRT Militar
8	Pymes	CSIRT Pymes
9	Gobierno	CSIRT Gobierno
10	Soporte	CSIRT Soporte

Fuente: Elaboración propia

De acuerdo a la anterior tabla, se define que ***Platino Sistemas*** tiene diez posibilidades de clientes en los cuales puede ofrecer el servicio de acuerdo a las comunidades objetivo ("*constituency*") que existen en el país, aunque cada una de estas tienen necesidades de seguridad específicas y requieren de igual manera servicios reactivos, proactivos y complementario diferentes. Es cierto que con base en la norma ISO/IEC 27001, muchas de las empresas toman este estándar como

un modelo de sistema de gestión de seguridad informática a seguir. Por lo cual también presentan en un porcentaje muy alto necesidades y servicios en común.

Teniendo en cuenta esto, se puede estructurar un equipo que multimodal y flexible que pueda hacer parte de los diferentes CSIRT – servicio ofertado – al mismo tiempo y en caso que la demanda sea creciente, se vinculará más personal a la empresa con el fin de mantener la influencia y el interés de los clientes de la empresa ***Platino Sistemas***.

6.2 TAXONOMÍA DE INCIDENTES DE SEGURIDAD CSIRT

Según el estudio Tendencias del Cibercrimen en Colombia 2019-2020, y el programa de seguridad Aplicada para el Fortalecimiento Empresarial (SAFE) en asocio con la Policía Nacional – Centro Cibernético Policial, presenta las cifras y modalidades de los ciberdelitos en 2019 y las tendencias que seguramente enfrentarán las empresas colombianas y los ciudadanos en el 2020[11]. (CCIT, 2019). Este informe es una muestra en conjunto con el CSIRT – Ponal de cómo han ido creciendo los cibercrímenes en el país y cuáles son los principales o más explotados por los ciberdelincuentes en relación a los datos recolectados por las denuncias que los ciudadanos del país han presentado.

En esto se han identificado los 6 tipos de incidentes de seguridad que más afectan a las empresas colombianas y a los ciudadanos, a través de los 30.410 casos que fueron reportados a la Policía Nacional durante el 2019 y que de estos reportes realizados por empresas y ciudadanos al Centro Cibernético Policial CECIP el 57% son de cibercrímenes (17.531)[12]

Figura 1 Cifras denuncias 2015 - 2019

Fuente: CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020 [en línea] 29 de octubre de 2019. Primera Edición. Bogotá D.C. p. 1 - 36. [consultado 13 de noviembre 2020] Disponible en Internet: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Los incidentes reportados se han realizado a en su mayoría a través de la aplicación "*ADenunciar*"[13] que ha estado en línea desde julio del 2017. Donde entre los

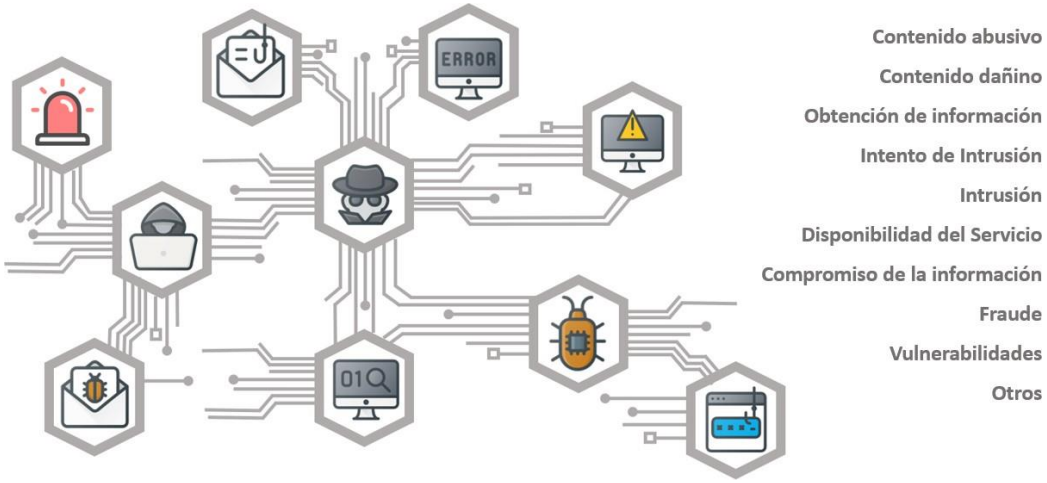
[11] [6] CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020 [en línea] 29 de octubre de 2019. Primera Edición. Bogotá D.C. p. 1 - 36. [consultado 13 de noviembre 2020] Disponible en Internet: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

[12] Ibid., p. 8.

[13] https://adenunciar.policia.gov.co/Adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2f

incidentes más reportados han sido el de *Phishing, la suplantación de identidad, el envío de malware y los fraudes en medios de pago en línea.*
En concordancia a lo anterior, se puede definir que existe diversidad en los incidentes y ataques informáticos que se han reportado en el país y que estos, no poseen las mismas características, ni causan el mismo daño ni tampoco tienen el mismo modo operandi. Sin embargo, los delitos informáticos o ciberdelitos presentados en el país no son muy diferentes de los que se llevan a cabo en otros países y se pueden establecer en la siguiente taxonomía que encierra las categorías de los delitos informáticos a nivel mundial más precisa posible y que serán la aplicada para el CSIRT de la empresa ***Platino Sistemas***

Figura 2 Taxonomía de Incidentes Informáticos



Fuente: Propia

Estas categorías son utilizadas por la mayoría de los CSIRT y CERT a nivel mundial, y serán adoptados también para la empresa ***Platino Sistemas*** y determinar los mecanismos que se deben tener para ofrecer el CSIRT como servicio a las empresas del sector para dar respuesta a estos incidentes informáticos, identificando el ciclo de vida del mismo y las herramientas y medios para atacar e interactuar en cada parte de esos ciclos de vida, validando dichas herramientas por medio de las metodologías, estándares e indicadores.

En el siguiente cuadro se hace una descripción de los tipos de incidentes que se pueden englobar dentro de las categorías descritas[14]:

[14] ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciberincidentes [en línea] 2019. p. 60 [consultado 15 de noviembre 2020]. Disponible en Internet:

Tabla 4 CLASIFICACIÓN / TAXONOMÍA DE CIBERINCIDENTES

CLASIFICACIÓN / TAXONOMÍA DE CIBERINCIDENTES		
TAXONOMÍA	Tipo de Incidente	Descripción y ejemplos Prácticos
Contenido Abusivo	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de Odio	Contenido difamatorio o discriminatorio. Ejemplo: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos
	Pornografía Infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, entre otros.
Contenido dañino	Sistema Infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit
	Servidor C&C (Mando y control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados
	Distribución de Malware	Recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.
	Configuración de Malware	Recurso que aloje ficheros de configuración de malware Ejemplo: ataque de webinjects para troyano.
	Malware dominio DGA	Nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C)
Obtención de Información	Escaneo de Redes (Scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y

http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

CLASIFICACIÓN / TAXONOMÍA DE CIBERINCIDENTES		
TAXONOMÍA	Tipo de Incidente	Descripción y ejemplos Prácticos
		cuentas. Ejemplo: peticiones DNS, ICMP, SMTP, escaneo de puertos
	Análisis de paquetes (Sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería Social	Recopilación de información personal sin el uso de la tecnología. Ejemplo: mentiras, trucos, sobornos, amenazas
Intento de Intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ejemplo: desbordamiento de buffer, puertas traseras, Cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ejemplo: intentos de ruptura de contraseñas, ataque por fuerza bruta
	Ataque desconocido	Ataque empleando exploit desconocido
Intrusión	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegio
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL
	Robo	Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos
Disponibilidad del Servicio	DoS (Denegación de Servicio)	Ataque de denegación de servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio
	DDoS (Denegación Distribuida de Servicio)	Ataque de denegación distribuida de servicio. Ejemplo: inundación de paquetes SYN, ataques de reflexión y

CLASIFICACIÓN / TAXONOMÍA DE CIBERINCIDENTES		
TAXONOMÍA	Tipo de Incidente	Descripción y ejemplos Prácticos
		amplificación utilizando servicios basados en UDP
	Sabotaje	Sabotaje físico. Ejemplo: cortes de cableados de equipos o incendios provocados
	Interrupciones	Interrupciones por causas ajenas. Ejemplo: desastre natural.
Compromiso de la Información	Acceso NO Autorizado a Información	Acceso no autorizado a información. Ejemplo: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación NO Autorizada de información	Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware
	Pérdida de Datos	Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico
Fraude	Uso NO Autorizado de Recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales
	Derechos de Autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplo: Warez.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas
Vulnerabilidades	Criptografía Débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplo:

CLASIFICACIÓN / TAXONOMÍA DE CIBERINCIDENTES		
TAXONOMÍA	Tipo de Incidente	Descripción y ejemplos Prácticos
		DNS open-resolvers o Servidores NTP con monitorización monlist
	Servicios con Acceso Potencial no deseado	Telnet, RDP o VNC
	Revelación de Información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ejemplo: SNMP o Redis
	Sistemas Vulnerables	Sistema vulnerable. Ejemplo: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
	Ciberterrorismo	Uso de redes o sistemas de información con fines de carácter terrorista
	Daños Informáticos PIC	Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Fuente: ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciberincidentes [en línea] 2019. p. 60 [consultado 15 de noviembre 2020]. Disponible en Internet:http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

Cada una de estas categorías definidas en la taxonomía anterior se describen a continuación:

6.2.1 Contenido Abusivo

Los incidentes que están dentro de esta categoría son aquellos donde la imagen corporativa de la empresa se ve comprometida, en la mayoría de las ocasiones se utilizan medios electrónicos de la empresa o el correo electrónico de la misma para ejecutar acciones ofensivas, prohibidas o ilícitas. Dentro de esta categoría está también la desacreditación o discriminación de las personas (racismo, amenazas, sexismo, misoginia, misandria entre otras muchas).

6.2.2 Contenido dañino

Esta categoría hace referencia a aquellos programas, o parte de los mismos disfrazados en archivos que generen impacto a los pilares de la información en el sistema. Es casi siempre necesario la interacción de un humano para activar o ejecutar el código malicioso dentro del sistema. En esta categoría se pueden identificar troyanos, gusanos, malwares, spywares, Adware/Hoax, rogueware, exploits, entre otros.

6.2.3 Obtención de información

En esta categoría se encuentran todas las técnicas que se puedan dar para socavar y recoger la mayor cantidad de información disponible sobre la infraestructura tecnológica de la empresa, esta recolección se realiza para hacerse un perfil objetivo de lo que se quiere atacar, incrementando la probabilidad de éxito de su motivación. Aquí se enuncian ataques como escaneo de puertos, cuentas y servicios (*Scanning*), observación e interceptación del tráfico de red (*Sniffing*) y técnicas de ingeniería social.

6.2.4 Intento de intrusión

En esta taxonomía están contemplados todos aquellos delitos que intentan comprometer el sistema o realizar la interrupción de un servicio pero que no llegan a ser efectivos, sin embargo, su intento de intrusión puede comprometer un sistema o provocar su caída tras consumir bastante de sus recursos. Entre algunos ejemplos tenemos los desbordamientos de buffer, puertas traseras, (XSS), intento de ruptura de contraseña entre otros.

6.2.5 Intrusión

Aquí están contemplados todos aquellos delitos que comprometen los mecanismos de autenticación y acceso del sistema, acceso a recursos con autorización o privilegios o sin ellos, ya sea por conocer, adivinar o violentar las claves del sistema (ataques de fuerza bruta). Ataques como *Pash the Hash*, elevación de privilegios, o mediante la ejecución de exploits, en ataques conocidos como *Poissoning.*

6.2.6 Disponibilidad del Servicio

Como su nombre lo indica, ataca uno de los pilares de la seguridad informática, afectando el acceso, uso y disponibilidad de un sistema, aplicación o servicio. Entre los ataques más comunes se encuentran el de "*denegación de servicio*" "denegación distribuida de servicio". En este apartado, también se encuentran los ataques por sabotaje como daño a cable o sistemas desde el hardware en si o la interrupción por causas como incendios o inundaciones.

6.2.7 Compromiso de la Información

Son todas aquellas acciones que llegan a suponerse como una amenaza contra la información en todos sus aspectos, desde interceptación, alteración directa o indirecta o acceso no autorizado, no importa la categorización de la información desde sensible, privada o de uso exclusivo, perdida o borrado de la misma de forma intencionada o no intencionada, hasta fuga de información sensible a través de la inserción de metadatos en documentos (esteganografía). En esta categoría podemos clasificar el Ransomware.

6.2.8 Fraude

Es el uso de herramientas, técnicas o mecanismos tecnológicos con el fin de lograr que un usuario o victima realice una actividad que provoque la afectación de la seguridad informática, una forma de fraude puede ser la suplantación de un sitio o entidad, el robo de credenciales, la clave de tarjetas de crédito o los números de cuentas bancarias. También se considera como fraude la violación de propiedad intelectual y derechos

de autor. Entre algunos de los incidentes podemos encontrar, el phishing y el Spoofing.

6.2.9 Vulnerabilidades

Todos aquellos incidentes de seguridad que son concebidos al explotar alguna vulnerabilidad del sistema, aquí están los ataques de tipo XSS, XSRF, SQL Injection, ataques SSL, ataques basados en web (Cookie reply, clonación de sesión), vulnerabilidades conocidas, entre otros.

“Adicionalmente, se incluyen dentro de esta categoría las acciones que se realizan mediante la explotación de vulnerabilidades con un identificador estandarizado como el nombre CVE (por ejemplo, desbordamiento de búfer, puerta trasera, secuencias de comandos entre sitios, etc.)”[15]

6.2.10 Otros

Incidentes que no están contemplados en las categorías anteriores, entre estos también se pueden enumerar el daño a datos por cualquier técnica no medible o contemplada anteriormente, uso de la infraestructura de la empresa con fines terroristas entre otros.

6.2.11 Nivel de Peligro del Incidente Informático

La taxonomía anterior necesita de una clasificación de acuerdo al nivel de peligrosidad que este pueda tener, dicho nivel se da sin tener en consideración el nivel de impacto del mismo, haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia. (GUIA NOTIFICACIONES Y GESTION DE CIBERINCIDENTES,2020)[16]

---

[15] BOLSA DE VALORES DE COLOMBIA, BOLETÍN INFORMATIVO No. 218. [en línea]. 07 de julio 2020, BOGOTÁ D.C. p. 1-36. [consultado 16 de noviembre de 2020]. Disponible en Internet: https://www.bvc.com.co/pps/tibco/portalbvc/Home/Mercados/boletines?com.tibco.ps.pagesvc.action=updateRenderState&rp.currentDocumentID=1ebbd6af_1732a600d64_-52bbc0a84ca9&rp.attachmentPropertyName=Attachment&com.tibco.ps.pagesvc.targetPage=1f9a1c33_132040fa022_-78750a0a600b&com.tibco.ps.pagesvc.mode=resource&rp.redirectPage=1f9a1c33_132040fa022_-787e0a0a600b

[16] CCIT, Óp. Cit., p. 8.

Los incidentes de seguridad de CSIRT de ***Platino Sistemas*** se asociarán a alguno de los siguientes niveles de peligrosidad.

Figura 3 Niveles de Peligrosidad de un Incidente CSIRT

Fuente: Propia

Para realizar una clasificación del nivel de peligrosidad de un incidente cibernético dentro del panorama actual de Colombia, se deben conocer cuáles son los ataques más comunes en nuestro país.

El delito informático más denunciado en Colombia es el *Hurto por medios informáticos* con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca

En segundo lugar, se encuentra la *Violación de datos personales* con 8.037 casos. Este dato revela que la segunda amenaza en Colombia para empresas y ciudadanos es el Robo de Identidad

El tercer delito más denunciado es el *Acceso abusivo a sistema informático* con 7.994 casos, y esto se explica en razón a que, en las fases primarias de los Ciberataques, los cibercriminales buscan comprometer los sistemas informáticos logrando ganar el acceso a los mismos.
En cuarto lugar, con 3.425 casos se encuentra la *Transferencia no consentida de activos*, conducta criminal que facilita al atacante sustraer el dinero o transferir valiosos activos financieros de las víctimas.

Finalmente, en quinto lugar, se sitúa el delito de *Uso de Software Malicioso* con 2.387 casos

De acuerdo a este reporte, donde se evidencian que tipos de incidentes informáticos tienes mayor auge en la actualidad colombiana, se definen los criterios de nivel de peligrosidad para la clasificación de los incidentes de seguridad informática evidenciados anteriormente.

Tabla 5 Criterios de Nivel de Peligrosidad de Incidentes Informáticos

CRÍTICO	Otros	• APT • Daños Informáticos
MUY ALTO	Fraude	• Ataque BEC • Suplantación
	Fraude Phishing	• Phishing
	Compromiso de la Información	• Acceso no autorizado a información. • Violación de datos personales. • Modificación no autorizada de información.
	Intento de Intrusión	• Ataque desconocido
	Intrusión	• Acceso abusivo a sistema informático • Robo
	Obtención de Información	• Transferencia no consentida de activos. • Ingeniería social.
ALTO	Código dañino	• Distribución de Malware • Configuración de Malware
	Disponibilidad	• Sabotaje • Interrupciones
	Código dañino	• Sistema infectado • Servidor C&C • Malware Dominio DGA
	Intento de Intrusión	• Compromiso de aplicaciones
	Disponibilidad	• DoS • DDoS
	Compromiso de la Información	• Perdida de datos

MEDIO	Intento de Intrusión	• Explotación de vulnerabilidades conocidas • Intento de acceso con vulneración de credenciales.
	Intrusión	• Compromiso de cuentas con privilegios
	Fraude	• Uso no autorizado de recursos • Derechos de autor
	Vulnerabilidades	• Criptografía débil • Amplificador DDoS • Servicios con acceso potencial no deseado • Revelación de Información • Sistema vulnerable
BAJO	Contenido Abusivo	• Spam
	Obtención de Información	• Escaneo de redes (Scanning) • Análisis de paquetes (Sniffing)
	Intrusión	• Compromiso de cuentas sin privilegios
	Otros	• Otros no críticos

Fuente: Propia, basado en ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD. [diapositivas] La Ciberseguridad como parte del nuevo paradigma de la seguridad. [en línea]. 3 de junio 2020. p. 28. [consultado 28 de noviembre 2020]. Disponible en Internet: https://www.aesseguridad.es/documentacion/GRUPO_TRABAJO_Ciberseguridad_web_v2.pdf

6.3 SERVICIOS DE PLATINO SISTEMAS

En la primera fase, el ofrecimiento de los servicios del CSIRT de Platino Sistemas se prestarán hacía sí mismo, atendiendo el personal propio de la empresa y su departamento de TI, apoyando y coordinando de manera transversal a la empresa en todo lo referente al tratamiento de los incidentes relacionados con la seguridad de las tecnologías de la información.

Bastantes servicios pueden ofrecer un CSIRT, sin embargo, mientras se da su crecimiento y maduración, es fundamental empezar solo con los servicios básicos

e ir creciendo con base en la experiencia, recursos existentes y vinculación de clientes al proyecto.

> "*cabe resaltar que cada CSIRT es distinto y sus servicios están basados en la misión, propósito y el grupo de clientes atendidos, de esta manera, algunos de los servicios que se ofrecen se relacionan con el tratamiento de incidentes, otros servicios como la capacitación en seguridad o las auditorías se relacionan indirectamente con el tratamiento de incidentes*"[17]

Sin embargo, existen algunos servicios básicos, definidos por *West Brown* y que un CSIRT debe prestar a sus clientes desde un principio, los cuales se resumen en emisión de comunicados, alertas y advertencias, y tratamiento de incidentes, los cuales son un valor añadido y siempre serán considerados valiosos.

Tabla 6 Servicios básicos de CSIRT Platino Sistemas

Servicios Proactivos	Servicios Reactivos	Servicios Complementarios
• Comunicados • Observatorio de Tecnología • Evaluaciones o auditorías de la seguridad. • Configuración y mantenimiento de las herramientas de seguridad, aplicaciones e infraestructura. • Desarrollo de herramientas de seguridad.	• Alertas y advertencias • Tratamiento de Incidentes ○ Análisis de Incidentes ○ Respuesta a Incidentes en el sitio. ○ Apoyo en la respuesta a Incidentes. ○ Coordinación de la respuesta de Incidentes • Tratamiento de Vulnerabilidades	• Análisis de riesgos • Continuidad del negocio y recuperación tras un desastre. • Consultoría de Seguridad. • Sensibilización • Educación/Formación • Evaluación o certificación.

[17] MEJÍA M., Jezreel, MUÑOZ, Mirna y URIBE, Edgar. Establecimiento de Servicios en Equipos de Respuesta ante Incidentes de Seguridad Informática: Una Revisión del Estado del Arte. (En español). Conferencia Ibérica de Sistemas y Tecnologías de la Información, CISTI. vol. 1, pp. 1033–1038, 2015. Disponible en Internet: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=114061193&lang=es&site=eds-live&scope=site

Servicios Proactivos	Servicios Reactivos	Servicios Complementarios
• Servicio de detección de intrusos. • Difusión de información relacionada con la seguridad.	○ Análisis de Vulnerabilidades ○ Respuesta a vulnerabilidades ○ Coordinación de la respuesta • Manejo de Instancias.	

Fuente: Propia, basado en ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD. [diapositivas] La Ciberseguridad como parte del nuevo paradigma de la seguridad. [en línea]. 3 de junio 2020. p. 28. [consultado 28 de noviembre 2020]. Disponible en Internet: https://www.aesseguridad.es/documentacion/GRUPO_TRABAJO_Ciberseguridad_web_v2.pdf

6.3.1 Servicios Proactivos del CSIRT de Platino Sistemas

Estos servicios tienen como objetivo mejorar los procesos de infraestructura y de seguridad de la comunidad objetivo para prevenir incidentes de seguridad o reducir su impacto cuando se producen. Los principales tipos de servicios proactivos consisten en la realización del seguimiento, la distribución de alertas y el ofrecimiento de servicios de investigación y desarrollo.[18]

6.3.1.1 Comunicaciones

La generación de comunicaciones sigue el mismo procedimiento para completar las tareas, y es transversal a todos los CSIRT que existan, ya que todos son sensibles a estos comunicados.

- Recopilación de Información
- Evaluación de la información sobre la pertinencia y la fuente
- Evaluación del riesgo de la información obtenida
- Distribución de la información hacía los clientes.

- **Recopilación de información sobre la vulnerabilidad**

La recopilación de información sobre una vulnerabilidad se puede dar de dos formas, la información sobre la propia vulnerabilidad del sistema, experimentada por CSIRT Platino Sistemas en sus propios equipos, en su laboratorio o en algún cliente.

[18] OEA, Óp. Cit., p. 43

O, la recopilación de información por reporte de incidentes de terceros con su solución.

Así mismo, dependiendo del tipo de cliente, existen numerosas fuentes para comunicar la información sobre la vulnerabilidad

- Listas de correo, públicas y cerradas
- Información propia de vulnerabilidades facilitada por los proveedores o fabricante de los productos.
- Sitios de Internet dedicados
- Información pública a través de buscadores
- Aliados, públicos o privados que otorguen información sobre la vulnerabilidad. (FIRST, CSIRTS, CERT, entre otros).

- **Evaluación de la información sobre la pertinencia y la fuente**

Con este proceso, se quiere lograr establecer si el impacto que lleva la explotación de la vulnerabilidad aplica a la infraestructura del cliente(s) atendido(s) por el CSIRT de Platino Sistemas.

La fuente de la información que se quiere entregar a los clientes, siempre debe ser verificada para determinar si la fuente es de confianza, para no generar falsos positivos que pueden provocar molestias en los procesos empresariales y perjudicar la imagen de la empresa.

Existen algunas preguntas que pueden ayudar a esta evaluación de pertinencia

- ***Lista de comprobación general***

    1. ¿La fuente es conocida y está registrada como tal?
    2. ¿La información llega por un canal regular?
    3. ¿El mensaje contiene información «extraña« que «parece» errónea?
    4. Si intuitivamente una información parece dudosa, antes de actuar hay que volver a verificarla.

- ***Correo electrónico – Fuentes***

    1. ¿La dirección de la fuente es conocida por la organización y figura en la lista

fuentes?
2. ¿Es correcta la firma PGP?
3. Si surgen dudas con un mensaje, compruebe la cabecera completa.
4. Si surgen dudas, use «nslookup» o «dig» para comprobar el dominio remitente.

- **WWW – Fuentes**

1. Cuando conecte con un sitio web protegido, compruebe los certificados navegador (https ://).
2. Compruebe el contenido y la validez (técnica) de la fuente.
3. Si duda, no entre en los vínculos ni descargue software.
4. Si duda, haga un «lookup» y un «dig» en el dominio, así como un «traceroute»” (ENISA, 2006)

- **Evaluación del riesgo de la información obtenida**

El riesgo es la oportunidad potencial del aprovechamiento de una vulnerabilidad, para poder evaluar el riesgo de la información obtenida, es necesario validar las siguientes preguntas.

- ¿Es bastante conocida la vulnerabilidad?
- ¿Qué tanto ha llegado a expandirse la vulnerabilidad (nivel mundial, continental o nacional)?
- ¿Es bastante fácil explotar la vulnerabilidad?

Después de esta evaluación se puede añadir un aviso a la comunicación, identificando el riesgo de la vulnerabilidad y los potenciales daños. Esta clasificación puede ser ALTO, MEDIO, BAJO.

- **Distribución de la información hacía los clientes**

Cómo último paso del servicio proactivo de la comunicación, podemos definir el método por el cual vamos a entregar la información al cliente final y como parte de su propia estrategia de comunicación.

Entre estos podemos encontrar diferentes métodos de envío tales como:

- Sitio web del CSIRT de Platino Sistemas.

- Correo electrónico
- Informe
- Archivo de investigación (Foro, Folleto, Infografía, entre otros)

6.3.1.2 Observatorio de Tecnología

Este servicio comprende la constante búsqueda de información en relación a los referentes de seguridad, noticias y artículos de índole científica, tecnológica, político y público para conseguir toda la información sobre seguridad informática, seguridad de la información, redes y sistemas de nuestros clientes.

De esta manera, CSIRT de Platino Sistemas supervisa los nuevos desarrollos tecnológicos, las actividades de intrusión e identifica las tendencias de futuras amenazas de los ciberdelincuentes.

De igual manera este servicio de investigación, puede estar apoyado por autoridades propias de la materia de ciberseguridad para aseverar así que la información y la interpretación que se obtiene es más precisa.

En concreto, se les permitirá estar al día sobre las alertas, las amenazas en evolución, los vectores de ataque que emergen, las mejores prácticas y nuevas normas en los servicios, así como sobre el mantenimiento y la operación de dispositivos, las estrategias de defensa y varios otros temas. (OEA, 2016)[19]

6.3.1.3 Evaluaciones de seguridad

Este servicio de Platino Sistemas, consiste en evaluar de manera apropiada y práctica la infraestructura del cliente con base en las buenas prácticas de la seguridad informática, teniendo en cuenta las normas de la industria que se puedan aplicar, existen muchos tipos de evaluaciones y/o auditorias que se puedan aplicar a los clientes,

- **Revisión de la infraestructura**: Revisión manual de las configuraciones del Hardware y Software del cliente, buscando que cumplan con las buenas prácticas de seguridad informáticas o normas de la industria, así como una buena configuración.

[19] OEA, Óp. Cit., p. 43.

- **Revisión de políticas y documentación**: Entrevista con el personal de la organización (cliente) para determinar si se están cumpliendo con las políticas, manuales o instructivos definidos para las mejores prácticas y que tan alineados están estos con sus comportamientos en pro de la seguridad.
- **Escaneo**: Uso de herramientas que permitan identificar, virus, malwares y malas configuraciones de seguridad a nivel informático y de red dentro de la organización.
- **Pentesting**: Comprobación de los niveles de seguridad de los sistemas con técnicas de penetración o intrusión en sistemas a fin de evidenciar las vulnerabilidades.

6.3.1.4 Configuración y mantenimiento de las herramientas de seguridad

Este servicio permitirá a Platino Sistemas identificar y dar orientación tanto a sus clientes como así mismo de la correcta configuración y mantenimiento de seguridad de las diferentes herramientas de seguridad de la infraestructura que estos posean o quieran adquirir. Aparte de la orientación para su correcta configuración, permite notificar al cliente de las actualizaciones o mejoras que se desarrollen sobre sus herramientas como, Sandbox, IDS, IPS, CASB, Firewall, FNG, entre otros. El CSIRT de Platino Sistemas, puede ir más allá.

6.3.1.5 Desarrollo de las herramientas de seguridad

Este servicio permitirá a Platino Sistemas entregar un valor agregado a la empresa propiamente y al cliente final, cuando un cliente quiera el desarrollo para sacarle el mayor provecho a una de sus herramientas de seguridad, Platino Sistemas se asegurará de contar con el personal o con el contacto de casa matriz que le permita cumplir con apartes como:

- Desarrollo de actualizaciones de seguridad a medida para el software propio del cliente.
- Recuperación de datos de computadores comprometidos.
- Creación de nuevos pluggins para una vulnerabilidad.
- Secuencia de comandos para actualizaciones automáticas

6.3.1.6 Sistema de Detección de Intrusos

Este servicio que prestará CSIRT de Platino Sistemas, permitirá realizar una revisión de los registros de diferentes IDS / IPS que tenga el cliente, iniciando una respuesta en caso de detectar un evento que tenga un comportamiento anormal o que supere un umbral definido, enviando la alerta y entregando la estrategia de mitigación. Aunque el análisis de los registros pueda ser una tarea tediosa, ya que muchas veces no es fácil identificar la intrusión, es bueno contar con el personal especializado o con las herramientas indicadas para el análisis del gran volumen de datos. Es bueno este análisis, ya que permite identificar alarmas falsas, o ataques falsos.

En principio, la Detección de Intrusos se realizará, si es posible con las herramientas IDS / IPS que el cliente tenga en su infraestructura. Sin embargo, si el cliente no posee es bueno brindar estas herramientas desde el mismo CSIRT de Platino Sistemas, algunas de estas herramientas pueden ser:

a. NIDS: Sistemas de detección de Intrusos Basados en Red, colocados en puntos estratégicos de la red del cliente para monitorear el tráfico entrante y saliente de todos los dispositivos de la organización.

   Un viejo conocido de la industria es **SNORT**, el cual, está en uso desde 1998, y ha evolucionado bastante bien, llegando a ser un gran IPS (*Intrusion Prevention System*), de fácil implementación es una excelente herramienta para el análisis de paquetes. Aunque no posee una interfaz de usuario y su administración necesita de conocimiento para no hacer tan difícil su curva de aprendizaje. Cuenta con aliados como **SNORBY** o **SQUIL**, que compensan esta falencia.

   SURICATA es otra herramienta muy aclamada de open source para la detección de comportamientos en red. Esta herramienta posee las mismas firmas que SNORT y es rápido y muy robusto. A diferencia de SNORT, SURICATA utiliza la tecnología multihilo, lo que le permite separar los flujos en los hilos de los procesadores y contar con diferentes módulos como son los de captura, recopilación, decodificación, detección y salida.

b. HIDS: Sistemas de detección de Intrusos Basados en Hosting, A diferencia de los anteriores, estos se ejecutan en los equipos EndPoint para detectar comportamiento sobre archivos, evidenciando comportamientos como la

modificación no autorizada, la eliminación o la agregación en amenazas desde el exterior.

Una de las herramientas que se pueden categorizar en este tipo de IDS es **OSSEC**, el cual realiza tareas como análisis de registro, comprobación de integridad, detección de rootkits y alertas basadas en el tiempo de respuesta activa. Se ejecuta sin problemas en cualquier sistema operativo y utiliza una arquitectura de cliente – servidor. Esto permite un control centralizado, que evita en buena parte ser atacado directamente sobre la máquina cliente. Además de permitir controlar los agentes desplegados desde un único punto y tener control de los mismos en bloque.

TRIPWIRE, es un software de open source que también posee una versión empresarial (de paga). Siendo también uno de los veteranos de la industria, lanzándose en el año de 1992, ha ayudado a convertir muchas de sus características en estándares para la industria. Su versión gratuita está dirigida solo a sistemas operativos Linux, sin embargo, su versión empresarial si soporta correr en Windows.

TRIPWIRE, monitoriza los sistemas para detectar y reportar cambios no autorizados en directorios y archivos, estas acciones las realiza a través de la creación de una imagen del sistema actual y posterior a esto realizará un seguimiento para evitar cambios de archivos, entre otros sin permiso.

Una de las desventajas de esta herramienta, es que no detectará amenazas previamente existentes en el sistema, por lo cual se recomienda instalar la solución tan pronto se termine de instalar el sistema operativo.

6.3.1.7 Difusión de información relacionada con la seguridad

Este servicio proporciona al grupo de clientes una colección completa y de búsqueda fácil de información útil para mejorar la seguridad. Dicha información puede incluir:

- *Directrices de comunicación e información de contacto del CSIRT de Platino Sistemas.*
- *Alertas, advertencias y otros comunicados,*
- *Documentación acerca de las mejores prácticas actuales,*
- *Asesoramiento general sobre seguridad informática,*

- *Políticas, procedimientos y listas de comprobación,*
- *Desarrollo de actualizaciones correctivas y difusión de información,*
- *Enlaces con proveedores,*
- *Estadísticas y tendencias actuales de la comunicación de incidentes,*
- *Otras informaciones que puedan mejorar las prácticas generales de seguridad.*

Esta información la puede desarrollar y publicar el CSIRT u otra parte de la organización, (TI, recursos humanos o relaciones con los medios) y puede incluir informaciones procedentes de fuentes externas tales como otros CSIRT, proveedores, y expertos en seguridad (Enisa, 2016)[20]

6.3.2 Servicios Reactivos del CSIRT de Platino Sistemas

Estos servicios se activan por un evento o una solicitud, como un informe de un host comprometido, un código malicioso generalizado, una vulnerabilidad de software o algo que haya sido identificado por un sistema de registro o detección de intrusos. Los servicios reactivos son el componente central de Trabajo CSIRT.[21]

Se diseñan con el propósito de ofrecer asistencia por los incidentes que se presentan cuándo son notificados (herramienta o personal), o cuándo se evidencian en el monitoreo, entre otros. De esta manera, el propósito de estos incidentes es dar respuesta oportunamente para considerar un tratamiento que luego genera un base de conocimiento para cuándo se vuelvan a presentar.

6.3.2.1 Alertas y advertencias

A diferencia del servicio de comunicaciones, este servicio incluye la difusión del mensaje cuándo un ataque ha o una vulnerabilidad ha sido transgredida, por un intruso, un virus o cualquier otra amenaza, la alerta no debe ser un mensaje de semáforo en rojo, debe ir acompañada de una vía de acción a corto plazo recomendada para enfrentar la trasgresión recibida. La alerta, solo debe ser la primera reacción al incidente acontecido, y entre más rápido mejor. Esto con el fin de que el cliente pueda reaccionar y orientarlos para que protejan los sistemas que no han sido afectados.

[20] ENISA, Óp. Cit., p. 75.

[21] UNIVERSIDAD CARNEGIE MELLON. CSIRT SERVICES [en línea] 2002. Instituto de Ingeniería de Software. p. 12. [consultado 21 de agosto 2021]. Disponible en internet: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

6.3.2.2 Tratamiento de incidentes

El tratamiento de incidentes consiste en la recepción, clasificación de acuerdo al triage del incidente, respuesta a solicitud y/o reporte, análisis del incidente, acción a realizar para mitigarlo, cierre del incidente, clasificación del mismo, archivado y actualización de la base de conocimiento, acciones aprendidas y propuestas de mejoras.

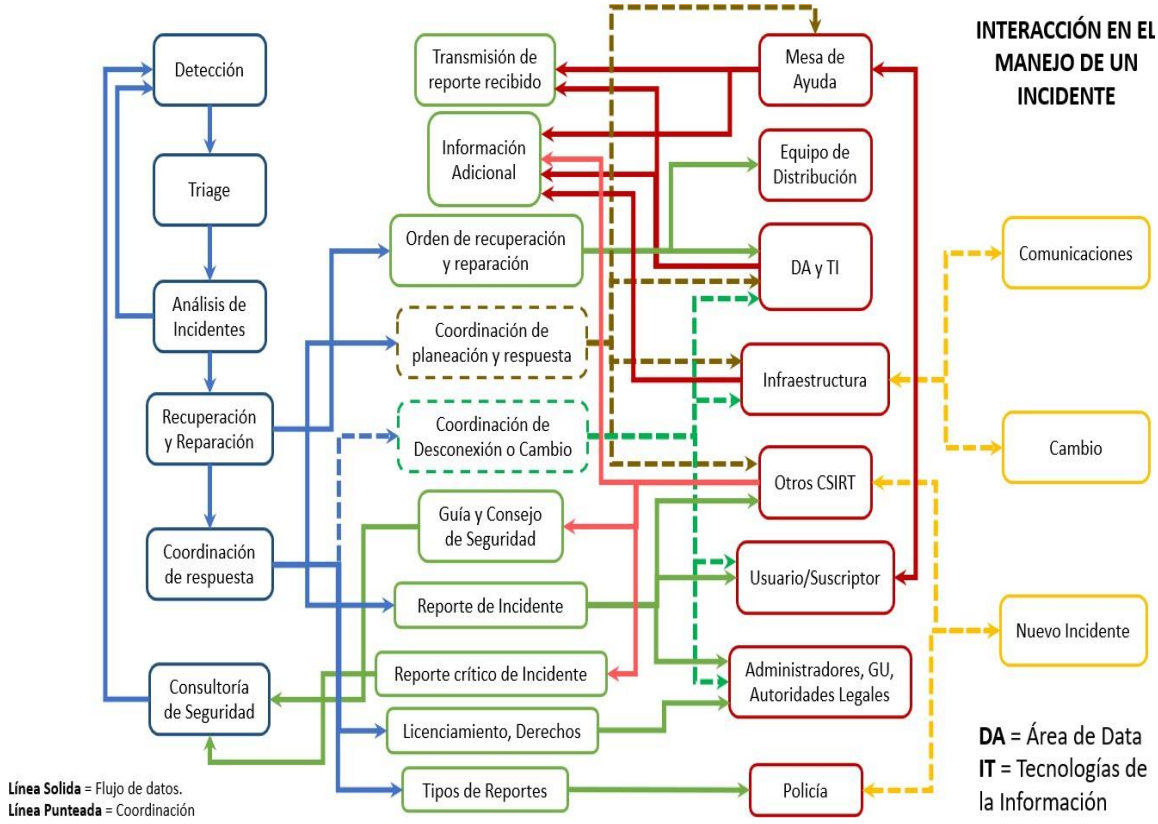
CSIRT de Platino Sistemas en su proceso de recepción y clasificación debe determinar el tipo de incidente, el impacto potencial y la gravedad, así como designar el equipo de respuesta que diseñara las acciones (plan de acción) para restaurar los servicios o los sistemas del cliente mitigando así el impacto del evento de ciberseguridad presentado. En ocasiones, el personal del CSIRT de Platino Sistemas deberá visitar las instalaciones del cliente.

De ser necesario, CSIRT de Platino Sistemas puede contar con la participación de diferentes actores que le ayuden a solucionar el incidente, incluyendo pero no limitando a CSIRT de orden nacional o mundial, comunidades propias del activo comprometido, ISP, proveedores de tecnología, equipos legales, prensa y todas las áreas que CSIRT Platino Sistemas considere necesarias para dar respuesta y comunicar a los interesados sobre el incidente y reducir los tiempos de solución, comunicación y propagación de la información.

Entre algunas de las actividades que se pueden llevar a cabo son:

- Proteger los sistemas y redes amenazadas por el evento a fin de reducir su propagación. Se puede aislar el/los componente(s) afectados.
- Establecer las soluciones o estrategias de mitigación ante alertas o avisos de relevancia de eventos ocurridos en otras partes antes de que los clientes propios se encuentren afectados.
- Hacer un escaneo de toda la infraestructura del cliente para buscar intrusos o daños en otras partes del cliente.
- Aplicar reglas de seguridad mayores en el tráfico de red mientras pasa el evento o de forma permanente.
- Limpiar o reconstruir el sistema afectado. Parchar la vulnerabilidad para que no se vuelva a presentar el incidente.
- Desarrollar las estrategias que den el resultado de la mitigación de la intrusión.

Figura 4 Interacción en el Manejo de un Incidente



Fuente: Propia, traducido de la imagen de [25] NASERI, Ali y AZMOON, Omid. Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran. International Journal of Computer Science Issues. [en línea] 2012, Vol. 9 p. 1 – 5. [consultado 15 de septiembre 2021]. ISSN: 1694–8114. Disponible en Internet: https://www.researchgate.net/publication/268347788_Proposition_of_Model_for_CSIRT_Case_Study_of_Telecommunication_Company_in_a_Province_of_Iran/download

- Análisis de Incidentes

El análisis de incidentes es una parte fundamental del tratamiento de incidentes, se debe examinar toda la información y la evidencia que exista, además de examinar todos los artefactos relacionados con el mismo. De esta manera se buscará identificar, el alcance, el impacto y la gravedad del daño causado. De igual forma confirmar la naturaleza del incidente, y de esta manera entregar un reporte actualizado y completo del análisis, más allá de la reacción primaria de contención del mismo.

CSIRT Platino Sistemas debe correlacionar cualquier actividad entre los sistemas, los comportamientos para determinar tendencias, patrones o características propias y ver si existe un antecedente.

- Respuesta a Incidentes en el sitio.

Este servicio es un plus que puede ofrecer CSIRT de Platino Sistemas a los clientes que así lo requieran, y trata de ofrecer apoyo directo en las instalaciones del cliente para ayudar a la recuperación del mismo, prestando los servicios de tratamiento y análisis del incidente, con sus posteriores actividades de mitigación y recuperación de sistema desde las instalaciones del cliente, y no solamente el apoyo de comunicación por vía teléfono o correo electrónico. El equipo de CSIRT Platino Sistemas se desplazará hasta las instalaciones del cliente o apoyar un equipo satélite que se haya colocado en el cliente, si las condiciones iniciales de la vinculación laboral así lo hayan predispuesto. De esta manera, se enviará un equipo especializado que logre apoyar al primero.

- Apoyo en la respuesta a Incidentes.

La finalidad de este servicio es guiar y estar con las víctimas que hayan sufrido el incidente, también puede incluir el apoyo a otros CSIRT o a las autoridades, en brindar información importante que se tenga sobre los eventos del incidente. La idea es que CSIRT Platino Sistemas brinde guía, apoyo remoto o en situ de tal forma que las actividades propias del cliente evoluciones hacía una normalidad con las mejoras que se puedan implementar y que el incidente sea solo un escalón de aprendizaje hacía la mejora continua de la ciberseguridad.

- Coordinación de la respuesta de Incidentes

De igual forma como CSIRT Platino Sistemas puede dar apoyo en la respuesta de incidentes, también puede realizar las labores de coordinación de los diferentes equipos que se tengan que involucrar en las actividades de solución del incidente, estos comúnmente son la víctima del incidente, los equipos internos, otros CSIRT, autoridades, o ISP. La coordinación más allá del solo apoyo, involucra actividades como la recolección de información, la elaboración de estadísticas, el análisis de los eventos, la divulgación y comunicación de la información que apoye a otros a lograr superar los eventos del incidente y seguir con normalidad sus actividades.

6.3.2.3 Tratamiento de vulnerabilidades

De la misma forma en que CSIRT Platino Sistemas reaccionará ante un incidente, un servicio previo debe ser el del tratamiento de vulnerabilidades, recibir la

información y los reportes sobre las posibles vulnerabilidades que se presenten en Software y/o Hardware, permitirá al laboratorio de tecnologías del CSIRT analizar su naturaleza, la mecánica utilizada y los efectos de las mismas. De esta manera puede descubrir cosas que en la información recibida no se haya tenido en cuenta y retroalimentar los nuevos hallazgos. Las actividades de manejo de vulnerabilidades, a diferencia del tratamiento de incidentes, debe ser particular para cada cliente de CSIRT, dado que no todos pueden tener la misma infraestructura y no a todos les debe llegar la información, ya que eso terminará aburriendo a los clientes a quienes las vulnerabilidades no les interese por información innecesaria.

- Análisis de Vulnerabilidades

CSIRT Platino Sistemas, debe realizar un análisis técnico de las vulnerabilidades de Hardware y Software, estas se pueden realizar en el laboratorio de tecnologías. La vulnerabilidad sospechosa debe ser confirmado, y entregar un reporte del análisis sobre la misma, determinar de dónde puede provenir y como puede ser explotada. Este análisis puede recurrir de ser necesario a la revisión del código fuente y de ser posible crear un escenario de prueba para reproducir el problema de la vulnerabilidad.

- Respuesta a Vulnerabilidades

Este servicio consiste en dar las respuestas adecuadas a las pruebas de las vulnerabilidades, informar a los clientes y a los proveedores de tecnología, así como compartir la información de los resultados obtenidos con otros CSIRT. La comunicación a los clientes servirá de alerta sobre la vulnerabilidad que tienen en sus sistemas, la comunicación con los proveedores con el fin de desarrollar parches, actualizaciones o soluciones alternativas a la vulnerabilidad. Y la comunicación con otros CSIRT o autoridades tiene como finalidad la de propagar la información para corroborar los hallazgos y que ellos con un laboratorio más grande brinden alternativas de solución.

- Coordinación de la respuesta de Vulnerabilidades

CSIRT Platino Sistemas debe notificar a los diferentes grupos y clientes sobre la vulnerabilidad y compartir la información sobre cómo arreglarla o mitigarla. Debe implementar una estrategia de que las respuestas a las vulnerabilidades han sido aplicadas con éxito en los clientes que la posean. De igual forma, debe consignar

toda esta información en una base de conocimientos sobre la vulnerabilidad y las respuestas correspondientes.

6.3.3 Servicios Complementarios del CSIRT de Platino Sistemas

Estos servicios complementas los servicios anteriores de proactividad y reactividad del CSIRT de Platino Sistemas, consisten en mayor grado en eventos y cursos de formación de seguridad, campañas de sensibilización, BCP (*Planes de continuidad de negocio,* por sus siglas en inglés) y DRP (*Pan de recuperación de desastres,* por sus siglas en inglés), estos servicios generan confianza en el cliente y dentro de la comunidad, así como crear la conciencia de la función y el propósito del CSIRT de Platino Sistemas, permitiéndole operar con mayor eficacia al identificar las carencias y necesidades tanto de los clientes como del CSIRT propiamente.

6.3.3.1 Análisis de riesgos

CSIRT Platino Sistemas debe estar en la capacidad de dar valor agregado al análisis de riesgos proporcionando evaluaciones cualitativas y cuantitativas de los riesgos a los que son expuestos los activos de información, así como la evaluación de las estrategias de protección y respuesta. De esta manera las evaluaciones no solo serían proactivas, sino que podrían ayudar en el análisis de los procesos del cliente y evaluar su evolución en sus sistemas y políticas con mediciones reales.

6.3.3.2 BCP y DRP

Los diferentes eventos de incidentes informáticos que han sufrido las empresas, han demostrado que uno de los mayores impactos que puede sufrir un cliente o empresa es la degradación comercial de la mismas. Algunas veces esta lucha por mantenerse en un mercado tan competitivo se ve de mucha mayor preocupación a la hora de frenar operaciones por culpa de un incidente que la misma pérdida económica. Es que el dinero se recupera, pero cuándo una empresa empieza a perder confianza y credibilidad, es muy complicada recuperarla en el medio en el que se desenvuelva.

Por eso como servicio complementario basado en las experiencias y las recomendaciones de CSIRT de carácter nacional e internacional, es indispensable que CSIRT Platino Sistemas ofrezca soluciones que permitan cumplir a sus clientes

con la continuidad de sus operaciones comerciales a través del Plan de continuidad del negocio (BCP) y del plan de recuperación de desastres (DRP). Por esto la participación propia de CSIRT Platino Sistemas es la de ayudar en ambos planes para los eventos relacionados con amenazas y ataques a la seguridad informática.

6.3.3.3 Consultoría de seguridad

CSIRT Platino Sistemas puede brindar asesoramiento o consultoría en seguridad para aquellas empresas que no son clientes, o potencialmente como servicio agregado a sus clientes en relación a las mejores prácticas de seguridad a implementar en cada uno de los tipos de clientes que vaya a asesorar. De esta manera CSIRT Platino Sistemas puede participar en la identificación de requisitos para comprar, instalar o asegurar nuevos sistemas, procesos en la empresa, aplicaciones entre otros. De igual manera se puede brindar asesoramiento en el desarrollo de políticas de seguridad de circunscripción u organizativas.

6.3.3.4 Sensibilización

CSIRT Platino Sistemas puede identificar en que parte sus clientes requieren mayor información y orientación para ajustarse mejor a las prácticas de seguridad aceptadas y las políticas de seguridad de la organización. Aumentar la conciencia de seguridad general de los clientes o de las áreas dónde los clientes lo necesiten no solamente mejorará su comprensión de los problemas de seguridad, sino también ayuda a que sus operaciones diarias sean más seguras. Esto facilita considerablemente la reducción de que los ciberataques sean exitosos y aumenta la probabilidad de que el recurso humano del cliente detecte e informen de los ataques, mitigando la ocurrencia de estos eventos.

De esta manera, se crea la oportunidad para construir conciencia sobre la seguridad de la organización (cliente) mediante el desarrollo de artículos, carteles, boletines, o cualquier recurso informático que expliquen y aconsejen sobre las mejores prácticas de seguridad que se deben tomar. Este servicio también puede incluir realizar charlas, reuniones, seminarios, transferencias de conocimiento para exponer los nuevos riesgos que se pueden presentar y mantener al día a la comunidad del cliente sobre la seguridad en curso y las potenciales nuevas amenazas a los sistemas de la organización.

Figura 5 Ficha técnica transferencia de conocimiento

LOGO PLATINO SISTEMAS	CONTROL DE ASISTENCIA TRANSFERENCIA DE CONOCIMIENTO	LOGO DEL CLIENTE

LUGAR: [describir dirección del cliente y/o virtual]	**Fecha:**	
ORGANIZADOR: [describir el nombre de la persona que dictará la transferencia de conocimiento]	**Hora Inicio:**	
TEMAS A TRATAR: [describir el tema que tratará la transferencia]	**Hora Fin:**	

Mediante el registro en el presente formato, usted autoriza a la **PLATINO SISTEMAS** para la recolección, almacenamiento y uso de audio, video, fotografía y demás datos personales, con la finalidad de "registrar la evidencia de asistencia a la transferencia de conocmiento, evento de formación y/o participación en una video conferencia". Como Titular de la información usted tiene derecho a conocer, actualizar y rectificar sus datos personales, ser informado sobre el uso que se ha dado a los mismos, revocar la autorización y/o solicitar la supresión de sus datos en los casos en que sea procedente. Para consultas y reclamos comuníquese al correo electrónico: conocimiento@platinosistemas.co y demás canales habilitados para tal fin, en virtud de los dispuesto en la Ley 1581 de 2012. Mayor información consúltela en nuestro Manual de Políticas de Tratamiento de datos personales, disponible en https://www.platinosistemas.co/politica-tratamiento-datos.

ASISTENTES

NOMBRE(S) Y APELLIDOS	CARGO	TELÉFONO	DEPENDENCIA/ENTIDAD	CORREO ELECTRÓNICO	FIRMA

Fuente: Propia

6.3.3.5 Educación / Formación

Este servicio implica proporcionar información a los clientes sobre temas de seguridad informática a través de seminarios, talleres, cursos y tutoriales. Los temas pueden incluir pautas de notificación de incidentes, métodos de respuesta apropiados, herramientas de respuesta a incidentes, métodos de prevención de incidentes y otra información necesaria para proteger, detectar, informar y responder a incidentes de seguridad informática.[22]

6.3.3.6 Evaluación / Certificación

CSIRT Platino Sistemas, puede ofrecer un servicio de evaluación y certificación para sus diferentes clientes o para un grupo no cliente en una herramienta en especial, más allá de certificar directamente, se pueden impartir los cursos y los váuchers que permitan al personal que así lo requiera conseguir la certificación que quiera, dar el mapa de ruta a seguir en su estudio, evaluación y aprendizaje a fin de que puedan lograr la certificación de una mejor manera en todo lo referente a la seguridad informática.

[22] Ibid., p. traducido.

6.4 REQUISITOS Y PERFILES DEL EQUIPO DE TRABAJO PARA LA CONFORMACIÓN DE CSIRT PLATINO SISTEMAS

6.4.1 Requisitos para el equipo del CSIRT

6.4.1.1 Dirección

Es importante que un director tenga experiencia en liderazgo como que posea conocimiento técnico. Es importante que el candidato escogido para este puesto satisfaga varios requerimientos para su perfil, aunque es claro, que tal vez no los pueda tener todos, pero entre más mucho mejor.

Tabla 7 Requisitos para el puesto de Dirección

FORMACIÓN	Requerido	• **Pregrado**: título profesional en Ingeniería de: Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática, Electrónica, Sistema y Computación o afines entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional. • **Posgrado**: Postgrado en Gerencia (MBA, MMoT o similar).
	A Considerar	• **Certificación Obligatoria**: Seguridad Cibernética (CISSP, CISM, CISA o similar) • Certificación adicional en una de las siguientes disciplinas: o PMP o COBIT o TOGAF o SCRUM MASTER
EXPERIENCIA	Requerido	**General**: Con experiencia profesional mínima de diez (10) años en proyectos relacionados con técnicas en TI o Seguridad Cibernética, a partir de la terminación y aprobación del pénsum académico de la respectiva formación profesional, en el ejercicio de las actividades propias de la profesión o disciplina académica exigida.

		Específico: tres (3) años en posiciones de gerencia de TI.
	A Considerar	Experiencia en Respuesta en incidentes de seguridad cibernética y/o posiciones similares

6.4.1.2 Operaciones

A diferencia del director, las personas de operación no requieren un postgrado como parte de su formación, sin embargo, es igual que también tengan conocimientos en seguridad cibernética y una experiencia bastante amplia, más allá de un junior para el puesto, ya que resolverán aquellos incidentes que los agentes les escalen.

Tabla 8 Requisitos para el puesto de operaciones

FORMACIÓN	Requerido	• **Pregrado**: título profesional en Ingeniería de: Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática, Electrónica, Sistema y Computación o afines entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.
	A Considerar	• **Certificación Obligatoria**: Seguridad Cibernética (CISSP, CISM, CISA o similar) • Certificación adicional en una de las siguientes disciplinas: Curso de especialización en informática forense, curso de especialización en áreas de la seguridad informática, seguridad cibernética y/o aseguramiento de la información.
EXPERIENCIA	Requerido	**General**: Con experiencia profesional mínima de cinco (5) años en proyectos relacionados con técnicas en TI o Seguridad Cibernética, a partir de la terminación y aprobación del pénsum académico de la respectiva formación profesional, en el ejercicio de las actividades propias de la profesión o disciplina académica exigida.
	A Considerar	Experiencia en Operaciones y Respuesta en incidentes de seguridad cibernética y/o posiciones similares, así como también experiencia en metodologías de gestión agiles. En administración de sistemas, en soporte a

		infraestructura tecnológica y desarrollo de actividades utilizando ITIL.

6.4.1.3 Investigación y Desarrollo

Las personas que apliquen para este perfil, más allá de conocer sobre la seguridad cibernética, deben tener alguna especialidad en el manejo de herramientas y/o lenguajes de programación, con el fin de que puedan explorar diferentes softwares, así como también mostrar experiencia en investigación y desarrollo.

Tabla 9 Requisitos para el puesto de investigación y desarrollo

FORMACIÓN	Requerido	• **Pregrado**: título profesional en Ingeniería de: Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática, Electrónica, Sistema y Computación o afines entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional. • Posgrado: Especialización en desarrollo de Software
	A Considerar	• **Certificación Obligatoria**: Seguridad Cibernética (CISSP, CISM, CISA o similar). • **Certificación Obligatoria**: Certificación en lenguajes de programación (C++, PHP, Java, BasShell, Phyton, entre otros). • Certificación adicional en una de las siguientes disciplinas: Curso de especialización en informática forense, curso de especialización en áreas de la seguridad informática, seguridad cibernética y/o aseguramiento de la información.
EXPERIENCIA	Requerido	**General**: Con experiencia profesional mínima de cinco (5) años en proyectos relacionados con técnicas en TI o Seguridad Cibernética, a partir de la terminación y aprobación del pénsum académico de la respectiva formación profesional, en el ejercicio de las actividades propias de la profesión o disciplina académica exigida.

	A Considerar	Experiencia en I+D y/o posiciones similares, así como también experiencia en metodologías de gestión agiles. Experiencia en trabajos con infraestructura de llave pública y sistemas criptográficos.

6.4.1.4 Tecnologías de Información

Las personas en este nivel, son aquellas que prestarán el servicio como agentes de seguridad cibernética, siendo este el nivel que realizará el primer filtro de aquellos eventos totales, hasta llevarlos a un número total de alertas principales, que serán analizados por ellos o pasarán a segundo nivel, al personal de operaciones. Para ellos también obligatoria una formación en seguridad cibernética.

Tabla 10 Requisito para puesto tecnologías de información

FORMACIÓN	Requerido	• Cumplir con los requisitos de Pregrado como se indican a continuación: • Tecnólogos o estudiantes universitarios con mínimo sexto semestre de carreras profesionales de ingeniería de Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática o afines entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.
	A Considerar	• **Certificación Obligatoria**: Curso de ITIL v. 3 o superior. • **Certificación Obligatoria**: Seguridad Cibernética (CISSP, CISM, CISA o similar).
EXPERIENCIA	Requerido	**General**: Con experiencia profesional mínima de tres (3) años en proyectos relacionados con técnicas en TI o Seguridad Cibernética, a partir de la terminación y aprobación del pénsum académico de la respectiva formación profesional, en el ejercicio de las actividades propias de la profesión o disciplina académica exigida.
	A Considerar	Experiencia en Administración de sistemas usando ITIL, así como también experiencia en

		metodologías de gestión agiles. Experiencia en trabajos con infraestructura de llave pública.

6.4.2 Funciones y responsabilidades

En cada uno de los equipos deben existir ciertos perfiles que cumplan las funciones de coordinación o administración de los equipos entre ellos podemos encontrar los siguientes:

Tabla 11 Requisitos por perfil

DISTINTIVO	PERFIL	EQUIPOS
	Gerencia • Dirección estratégica del CSIRT • Supervisa a todos los equipos. • Recibe reportes del Jefe Oficial Ejecutivo del CSIRT • Asiste a las sesiones del consejo asesor de seguridad, si es requerido.	Gerente de Platino Sistemas, no está en ningún equipo sino por encima de ellos
	Jefe Principal CRIST • Dirección estratégica de los equipos. • Supervisión de todos los equipos. • Entrevista Final a los nuevos miembros de los equipos. • Asiste a las sesiones del consejo asesor de seguridad.	Es el jefe de todos los equipos, todos los equipos están estratégicamente bajo su mando.
	Director (Mandos Medios) • Da soporte y reportes al jefe principal. • Lidera el equipo en las actividades diarias. • Asigna deberes y tareas. • Conduce la gestión de claves. • Autoriza los permisos de accesos a la información.	Existe un director para cada uno de los equipos. • Soporte y Seguridad. • Análisis y Evaluación Técnica. • Coordinación y respuesta a Incidentes. • Producción de Contenido y Formación. • Apoyo.

	Clasificador de Eventos • Provee asistencia inicial de respuesta a incidentes. • eres y tareas. • Clasifica y prioriza la información recibida de un caso.	• Coordinación y respuesta a Incidentes.
	Líder TRIAGE • Clasifica y prioriza los eventos. • Asigna casos a personal técnico. • Lidera el equipo en las actividades diarias. • Asigna deberes y tareas. • Conduce la gestión de claves. Autoriza los permisos de accesos a la información.	• Coordinación y respuesta a Incidentes.
	Gestor de Incidentes • Analiza incidentes, monitoreo, registro y respuesta. • Coordina respuesta a incidentes. • Colabora con otros grupos, equipos o técnicos para resolver un incidente.	• Coordinación y respuesta a Incidentes.
	Analista / Investigador • Realiza investigaciones específicas. • Desarrolla material técnico para el uso interno o de formación. • Realiza tareas de monitoreo de vulnerabilidades. • Desarrolla herramientas.	• Análisis y Evaluación Técnica.
	Líder de Comunicaciones • Desarrolla y publica documentos CSIRT. • Mantiene el sitio web del CSIRT. • Mantiene el perfil de las redes sociales.	• Producción de Contenido y Formación.

	Administrador de Red • Gestiona y mantiene la infraestructura de Red del CSIRT. • Ayuda en la respuesta a incidentes en casos relacionados a redes.	• Soporte y Seguridad
	Administrador de Sistemas • Administra y mantiene los sistemas del CSIRT. • Gestiona el acceso a la información. • Asiste en la respuesta a incidentes cuando se necesita experticia en sistemas.	• Soporte y Seguridad
	Representante • Representa al CSIRT en eventos. • Encargado del marketing de la empresa. • Si se le indica, puede dar capacitación a otros representantes.	• Apoyo
	Vocero • Encargado del canal de comunicaciones con la prensa	• Apoyo
	Custodio de Registro • Acceso a repositorios seguros de información.	• Apoyo
	Asistente • Asiste al personal en las tareas que se le indiquen, encargado de cumplir dichas tareas según el equipo para el que sea contratado.	• Soporte y Seguridad. • Análisis y Evaluación Técnica. • Coordinación y respuesta a Incidentes. • Producción de Contenido y Formación. • Apoyo.

6.5 POLÍTICAS, PROCESOS, PROCEDIMIENTOS, MANUALES E INSTRUCTIVOS BASADOS EN LA NORMA ISO/IEC 27000

6.5.1 POLÍTICAS DE CSIRT PLATINO SISTEMAS

6.5.1.1 Política de Clasificación de Información

i. Actividades Previas

Siendo la información, uno de los principales activos de cualquier empresa es necesario crear una política de protección adecuada. La información de la empresa se puede encontrar en medios digítales (archivos ofimáticos, imágenes, archivos multimedia, bases de datos, entre otros), que son leíbles por nosotros a través de los programas y sistemas que los soportan. O físicos (papel, película, fotográfica, entre otros).

Es por esto que, para poder realizar una correcta clasificación de la información, y aplicar las medidas de seguridad apropiadas para cada activo, se hace necesario realizar un inventario y tener una clasificación en concordancia al impacto que ocasiona para la empresa su perdida, difusión, acceso sin autorización, alteración o destrucción. Aplicando en ellos las dimensiones de la seguridad informática CID (Confidencialidad, Integridad y disponibilidad). De esta forma es más práctico clasificar la información a cifrar, el quien puede acceder a ella en diferentes niveles, quien responde por ella y cada cuánto se debe realizar una copia de respaldo, entre otras actividades.

Algunos ejemplos de las actividades de acuerdo a la clasificación:

- Determinar permisos al personal del equipo de talento humano para el manejo del aplicativo de nómina por su confidencialidad.
- Determinar permisos al personal del equipo de marketing para el acceso al gestor de la página web institucional.
- Cifrar los documentos enviados por correo electrónico, así como su clasificación propia para que, en caso de caer en manos diferentes a las enviadas, no puedan ser visualizados si son clasificados.
- Realizar una copia de respaldo periódica del Plan de Recursos Empresariales (ERP, por sus siglas en inglés).

Además de la clasificación y las medidas de seguridad aplicadas, es igual de necesario establecer el ***ciclo de vida***, que dependerá de conocer el contenido de la información, así como la vida útil y el fin del soporte (físico o lógico). Si el soporte caduca previo al contenido, es necesario regenerarlo en otro soporte. El ciclo de vida ayuda a determinar en qué momento la información ya no es útil y de esta forma cuándo se debe eliminar de forma adecuada.

ii. Objetivo de la clasificación

Clasificar los activos de información garantiza un manejo eficaz y eficiente de la información con base en una gestión de seguridad con los criterios de CID (Confidencialidad, Integridad y disponibilidad).

iii. Lista de verificación

Aplicar controles que permitan la revisión oportuna del cumplimiento de seguridad en lo concerniente a la **clasificación de la información**

Los controles pueden definirse de acuerdo a niveles de complejidad:

- Primarios (P): Los esfuerzos y los recursos que se necesitan para instaurarlos son asumibles. Pueden aplicarse por medio del uso de funcionalidades sencillas que ya procedan de aplicaciones comunes. A través de la instalación de herramientas sencillas se pueden prevenir ataques.
- Avanzados (A): Los esfuerzos y los recursos que se necesitan para instaurarlos deben ser puestos en consideración. Requieren de configuraciones complejas en programas más especializados. Es posible precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance (INCIBE, S.F)[23]

- Procesos (**PRO**): Aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): Aplica al personal técnico especializado.

[23] ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Clasificación de la Información, Política de Seguridad para la pyme [en línea] 2018. p. 7. [consultado 10 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

- Personas (**PER**): Aplica a todo el personal.

Tabla 12 Política clasificación de información

NIVEL	ALCANCE	CONTROL	CHECK
P	PRO	**Inventario de Información** Se elaboró un inventario detallado de los activos de información de la empresa	☐
P	PRO	**Criterios de Clasificación de la información** Se determina claramente los criterios de seguridad con los que se clasificarán los activos de información de la empresa.	☐
P	PRO	**Clasificación de la información** Se etiquetan los activos de información según los criterio de seguridad establecidos.	☐
P	PRO	**Tratamientos de seguridad disponibles** Se establece una lista con todos los tratamientos de seguridad de la información disponibles en la empresa	☐
A	TEC	**Establecer y aplicar los tratamientos que corresponden a cada tipo de información** Se aplican correctamente los tratamientos de seguridad que corresponden a cada activo de información.	☐
A	TEC	**Auditorías** Se realizan auditorias de comprobación (definir tiempo)	☐

Revisado Por:_____ Fecha: _____

Fuente: ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Clasificación de la Información, Política de Seguridad para la pyme [en línea] 2018. p. 7. [consultado 10 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

iv. Puntos clave

Para esta política se pueden mencionar los siguientes puntos clave.

- **Inventario de Información:** El establecimiento del inventario de los activos de información de la empresa debe registrar características como, tamaño, servicios, ubicación, a quienes está dirigido, responsables y tiempo de vida.
- **Criterios de clasificación de la información:** El establecimiento de los criterios de clasificación deben estar relacionados a las medidas de seguridad, algunos de estos son:

    - Por nivel de accesibilidad o confidencialidad:
        - Información Confidencial: Accesible solo por personal en concreto o por la alta gerencia.
        - Información Interna: Accesible solo por el personal de la empresa.
        - Información Pública: Información para todas las personas que la quieran consultar.

    - Por su utilidad o funcionalidad:
        - Información de clientes y proveedores
        - Información de compras y ventas
        - Información del personal y la gestión interna.
        - Información sobre pedidos y almacén.

    - Por el impacto, pérdida, borrado o robo:
        - Daño a la imagen empresarial
        - Consecuencias legales.
        - Consecuencias económicas
        - Paralización de las actividades de la empresa.

- **Clasificación de la información:** Es necesario etiquetar cada tipo de información, de acuerdo a los criterios establecidos.
- **Tratamientos de seguridad disponibles:** Se debe tener enlistados todos los tratamientos de seguridad que posea la empresa, herramientas de cifrado, sistema de copias de seguridad, sistemas de control de accesos entre otros.
- **Establecer y aplicar los tratamientos correspondientes a cada tipo de información:** Posterior a la clasificación de la información y tener el listado de

los tratamientos de seguridad para cada uno de ellos se deben asignar y aplicar estos últimos a los primeros. Se pueden considerar los siguientes:

- Limitar el acceso a personal o grupos de personal.
- Aplicar cifrado a la información.
- Realizar copias de seguridad de la información.
- Aplicar medidas específicas de las normas vigentes
- Realizar acuerdos de confidencialidad para cierta información.
- Tener controles de acceso a la información, así como a la modificación de la misma.

- **Auditoría:** Realizar periódicamente auditorías de seguridad para certificar la aplicación de los tratamientos que se tienen con el fin de salvaguardar nuestra información.

6.5.1.2 Política de Protección de datos

Los datos personales es toda aquella información en lo referente a una persona, los cuales son parte de su identificación y muchas veces permite conocer diferentes aspectos de su situación, social, financiera, política entre otros aspectos. También de carácter sensible como su estado de salud su vida sexual y hasta su aspecto físico.

Los tipos de datos tienen una clasificación sencilla en **públicos** (dato permitido por la constitución política de Colombia como tal), **semiprivado** (es un dato de naturaleza íntima, cuyo contenido puede ser compartido con ciertos grupos, pero no es lo suficientemente abierto para ser público.), **privado** (es un dato que solo es relevante para el titular de la información) y **sensible** (este dato puede ocasionar afectación a la intimidad del titular o su uso indebido generar discriminación).

Se tendrá en cuenta la ley colombiana 1581 de 2012 que define la protección de datos que contempla el derecho al tratamiento de los datos personales, la responsabilidad que tiene cada titular de las empresas y entidades para que dicha información no sea entregada a personas sin el consentimiento del dueño de los datos.

Considerando las siguientes definiciones a los diferentes datos (artículo 3 de la ley 1581 de 2012):

- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Transferencia:** La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del Tratamiento y se encuentra dentro o fuera del país.

- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Y que en su capítulo III habla de las políticas de tratamiento

- **Aviso de privacidad:** En los casos en los que no sea posible poner a disposición del titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un “Aviso de Privacidad” al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.

- **Contenido mínimo del aviso de privacidad:** El aviso de privacidad, como mínimo, deberá contener la siguiente información: 1. Nombre o razón social

y datos de contacto del responsable del tratamiento. 2. El tratamiento al cual serán sometidos los datos y la finalidad del mismo. 3. Los derechos que le asisten al titular. 4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el aviso de privacidad correspondiente. En todos los casos, debe informar al titular cómo acceder o consultar la política de tratamiento de información. No obstante, lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos. En todo caso, la divulgación del aviso de privacidad no eximirá al responsable de la obligación de dar a conocer a los Titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.

Deber de acreditar puesta a disposición del aviso de privacidad y las políticas de tratamiento de la información: Los responsables deberán conservar el modelo del aviso de privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999.

- **Medios de difusión:** del aviso de privacidad y de las políticas de tratamiento de la información. para la difusión del aviso de privacidad y de la política de tratamiento de la información, el responsable podrá valerse de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

  Procedimientos para el adecuado tratamiento de los datos personales: Los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los titulares de la información e incluirse en la política de tratamiento de la información.

- **Medidas de seguridad:** La Superintendencia de Industria y Comercio impartirá las instrucciones relacionadas con las medidas de seguridad en el tratamiento de datos personales.[24]

6.5.1.3 Política de Retención de Información

El apropiado manejo de la información es indispensable para Platino Sistemas. De cierto modo, algunos documentos e información deben retenerse de acuerdo a las leyes colombianas que le apliquen. Por otra parte, los documentos e información que prescriba o sea obsoleta o irrelevante, debe ser eliminada de acuerdo a un periodo de retención establecido, dado que su retención acarrea costos, es una carga, reduce la productividad y eficiencia, así como incrementa riesgos para la empresa en los ámbitos legales y operativos de la misma.

Es por esto que es apropiado identificar los plazos en los que se debe retener los diferentes tipos de información, al tiempo que se define la eliminación periódica de la información no relevante.

La información se divide en cuatro grupos generales:

(1) Información que legalmente debe ser conservada por periodos de tiempos prescritos.

(2) Información necesaria para la operación del CSIRT, negocios y proyectos

(3) Información incidental y de algún otro tipo generada durante los diferentes proyectos y en el curso propio del CSIRT de Platino Sistemas.

(4) Información personal, que no tiene relación con el CSIRT propia de la ley de protección de datos.

i. Alcance

[24] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial Bogotá D.C., 2012 No. 48.587. p 1 – 301. Recuperado de: wsp.presidencia.gov.co

Esta política es completamente aplicable a todos los usuarios, internos y externos que tengan relación con el CSIRT de Platino Sistemas y que no tengan definida su propia política de retención de información, así mismo como en cualquier región del país dónde Platino Sistemas tenga operación.

Esta política no se aplica a aquella información de carácter personal o no relacionada con el negocio. Este grupo de información no puede ser almacenado sin previo consentimiento de las personas en los medios propios de resguardo de la empresa para la información institucional de CSIRT Platino Sistemas.

ii. Objetivo

Crear las directrices de conservación y retención de la información propia de CSIRT Platino Sistemas de forma consistente y efectiva.

iii. Roles y responsabilidades

- **Administradores de la política**

Esta política será administrada por el *Jefe Principal CSIRT* y un representante del *Equipo de Apoyo* de orden jurídico. Los cuáles serán responsables de:

- Actualizar la política si requiere de lo mismo.
- Comunicar a todo el CSIRT de los cambios, excepciones y otros asuntos que modifiquen esta política.
- Coordinar las campañas de comunicación y entrenamiento a los usuarios de CSIRT propios de esta política.
- Resolver las dudas y comentarios que se generen propios y referentes a estas políticas.
- Coordinar las auditorías y otras actividades que permitan verificar el efectivo cumplimiento de la política.
- Realizar y presentar los informes estadísticos y cualquier otra información relevante al gerente del CSIRT de Platino Sistemas.

- **Líder de Equipo**

Los líderes de cada equipo, serán responsables de informar al Jefe de CSIRT el nivel de cumplimiento de la política por cada uno de sus equipos.

- **Delegado por Equipo**

Los encargados de cada equipo designaran a una persona (“delegado”) para que vigile el cumplimiento oportuno de esa política dentro de los siguientes 30 días posterior a la entrada en vigor de la misma o cuándo haya una vacante, según el caso. El delegado será responsable de:

- Capacitación a su equipo acerca de esta política.
- Resolver dudas e inquietudes acerca del cumplimiento de esta política
- Coordinación con el equipo de apoyo (jurídico) en lo relacionado a la retención de información y los cambios que pueda presentar.
- Promover y monitorear el cumplimiento de la misma
- Informar al jefe de equipo y al jefe del CSIRT de Platino Sistemas sobre el cumplimiento de la misma.

- **Grupo de apoyo – Jurídico**

La parte jurídica del grupo de apoyo debe revisar de manera continua cualquier aspecto de las leyes nacionales o locales que puedan afectar la política e informar al jefe de CSIRT, así como a los jefes de equipo para que la política sea actualizada. Así como debe apoyar en la comunicación, difusión y transferencia de conocimiento de los empleados y usuarios del CSIRT Platino Sistemas con relación a esta política.

iv. Cumplimiento

- **Obligatoriedad**

Esta política es de estricto cumplimiento obligatorio. Toda persona relacionada de alguna forma con CSIRT Platino Sistemas deberá conocer esta política, entender su rol y responsabilidad en el correcto cumplimiento de la misma.

- **Incumplimiento**

El incumplimiento de esta política puede dar como resultado acciones disciplinarias y/o el ejercicio de acciones legales, dependiendo de la falta, la naturaleza, su magnitud e incumplimiento o violación.

Cualquier incumplimiento que se presente debe ser reportado de inmediato al jefe correspondiente.

Es competencia de los delegados evaluar de forma inmediata el incumplimiento reportados – y de ser necesario – comunicarlos de forma inmediata a sus superiores.

- **Salvedades**

En caso de que CSIRT Platino Sistemas reciba un aviso de una demanda potencial o real, o algún otro procedimiento o investigación oficial, o algún requerimiento que le obligue a proporcionar documentos o información, el jurídico del equipo de apoyo, deben identificar los documentos e información que deben conservarse, así como salvaguardar la información de las personas afectadas. De igual forma deben comunicar cualquier excepción a esta política las personas afectadas sobre la petición en curso desde el ente oficial. Un procedimiento oficial incluye, entre otros, cualquier procedimiento ante un juez, tribunal o dependencia de gobierno. **ESTA EXCEPCIÓN DEJARÁ SIN EFECTO CUALQUIER OTRA DISPOSICIÓN DE ESTA POLÍTICA.**

v. Retención

- **Información a conservar por un plazo de tiempo determinado**

- Documentos e información legal según los requisitos propios de las leyes colombianas.
- Estos documentos conservados de acuerdo a los términos legales, deberán ser eliminados una vez vencidos los periodos de retención aplicables a los mismos.
- Bajo ninguna circunstancia los tiempos pueden ser menores a los establecidos.

- **Información requerida para la operación y los negocios**

- los documentos e información propia de los proyectos, debe conservarse según los requerimientos propios de cada proyecto o si se necesitan para continuar con actividades operativas relevantes. Los documentos a retener deben ser necesariamente para completar el proyecto o realizar actividades de operación del mismo posterior a su finalización.
- La operación del CSIRT y los requisitos propios de cada proyecto deben tener un tiempo estipulado en el mismo de conservación, autorizado por el delegado correspondiente del proyecto. Los periodos de conservación del proyecto no

podrán ser superiores a diez (10) años. Excepción de aquellos que, autorizados por el delegado, previamente escrito en un documento autorizando conservar por un tiempo mayor con justificación propia de su determinación.

- **Información, asesoría u otra información generada en el CSIRT durante los proyectos**

  - Toda la información que se genere durante los proyectos y que no estén en la política de conservación del ítem anterior deben eliminarse de manera segura a la menor brevedad de tiempo, de cualquier forma, no en un plazo mayor a 60 días.

- **Correo electrónico**

  - Los usuarios deben conservar los correos electrónicos relevantes en sus bandejas de entrada. En caso de verse lleno el espacio de la bandeja de correo electrónico, los usuarios son los encargados de hacer la depuración de aquellos correos no relevantes.
  - El equipo y los procedimientos empresariales de conservación de correo electrónico conservarán información por año del correo electrónico, eliminando la copia de respaldo del año anterior.

- **Documentos en Proceso**

Las versiones preliminares y los borradores de los documentos, así como, la información electrónica, documentos y papeles obsoletos y demás información transitoria, deben conservarse o eliminarse de la misma forma que se ha tratado los documentos anteriormente descritos en esta política. El jurídico del equipo de apoyo puede establecer requisitos y lineamientos adicionales para el tratamiento de este tipo de documentos e información.

vi. Almacenaje adecuado de la información

- **Documentos**

Cada equipo es responsable de definir y adoptar los procedimientos necesarios para el manejo y la conservación de la información y los documentos, con el fin de asegurar su debida retención.

- **Información electrónica**

El comité de seguridad de la información del CSIRT dictará los lineamientos y directrices sobre el manejo y los medios aceptables de conservación de la información electrónica que puede estar en diversas ubicaciones, tales como servidores, discos duros, computadores, discos externos, archivos, correos electrónicos entre otros.

El CPD (Centro de Procesamiento de Datos) del CSIRT de Platino Sistemas es autoridad para almacenar la información electrónica fuera de las oficinas de Platino Sistemas y de su recuperación en caso de un desastre.

Los empleados del CPD son los responsables en adoptar las diferentes medidas y procedimientos propios del manejo adecuado de documentos electrónicos e información digital que deban conservarse, incluyendo los correos electrónicos, con el fin de que se resguarden de manera apropiada en el cumplimiento de esta política.

Mientras no se estipule de forma contraria en las leyes propias del país o de otra política de CSIRT Platino Sistemas que pueda modificar esta, los usuarios finales serán los responsables de adoptar los procedimientos adecuados para el manejo y conservación de documentos electrónicos propios y que se encuentren en sus equipos, incluyendo correos electrónicos con las medidas propias de salvaguarda.

Cualquier medio usado para el almacenamiento de los documentos electrónicos o de información, debe ser conservado dentro de las instalaciones de CSIRT Platino Sistemas y estar protegido bajo las medidas razonables de seguridad.
Antes de realizar alguna copia de seguridad de LTR (larga retención, por sus siglas en inglés), los usuarios deben realizar una depuración de los documentos electrónicos y la información no relevante o no necesaria, incluyendo los correos electrónicos.

6.5.1.4 Política de Destrucción de Información

Toda empresa en la actualidad basa su información en diferentes repositorios: bases de datos, archivos de texto, hojas de cálculo, imágenes entre otros. Toda

información debe cumplir con un ciclo de vida en la forma más elemental posible de generación, transformación y destrucción.

Figura 6 Ciclo de vida de la Información

Fuente: Propia, tomado de ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Guía de borrado seguro de la información, una aproximación para el empresario [en línea] 2016. p. 12. [consultado 12 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

De igual forma, entre la información que maneja la empresa, existe aquella que no se debe borrar porque puede comprometer el normal funcionamiento de la empresa, eliminar este tipo de información pondría en aprietos la compañía, algunos ejemplos de este tipo de información son la información confidencial y los datos de carácter personal.

Con la destrucción de la información (discos duros, memorias USB, papel, vídeos, entre otros) se busca proteger a la organización de la difusión de material confidencial y de los datos personales que pudiese haber en estos medios.

i. Destrucción certificada

La norma ISO 15713: 2010 Destrucción segura del material confidencial, código de buenas prácticas da las pautas para la eliminación de la información que contengan datos personales en cualquier tipo de soporte. Así mismo es funcional para la destrucción de datos de índole confidencial, en el caso que una ley u empresa nos obligue a ello.

La norma define los requisitos para la gestión y control de recogida, transporte y destrucción del material confidencial. Indica los niveles de destrucción (nivel de triturado) según el tipo de información a eliminar y el soporte (papel, tarjetas SIM y negativos, cintas de audio y video, ordenadores, CD, DVD, microfichas…). Los niveles más altos hacen que la recuperación de la información sea más difícil. Hay empresas (como comentaremos en el apartado de Soluciones del Catálogo [3]) que real[25]

[25] ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Guía de borrado seguro de la información, una aproximación para el empresario [en línea] 2016. p. 12. [consultado 12 de noviembre 2021]. Disponible en Internet:

ii. Métodos de destrucción de la información

Existen diferentes métodos para la destrucción segura de la información, de tal forma que no sea posible la recuperación de los datos contenidos en los dispositivos de almacenamiento.

- **Desmagnetización**: Este método es la exposición de los medios de almacenamiento a un imán de grandes proporciones, de esta forma se realiza un borrado al cambiar la distribución de las partículas del dispositivo. Es un método muy usado para la eliminación de datos de dispositivos como diskettes, discos duros, cintas magnéticas para backup, entre otros.

  Cada dispositivo dependiendo de sus características de forma, tipo y tamaño requiere una potencia específica del imán para que las partículas se polaricen y reacomoden.

- **Destrucción física**: Este método busca la destrucción física del medio que contiene la información.

  existen diferentes medios para realizar este proceso de destrucción tales como la desintegración, pulverización, incineración y fusión. Es común que este método se practique por medio del fuego o en una planta de metal, se busca dejar ningún rastro o el mínimo rastreable del medio que contenía la información, estas actividades es mejor que se realicen por un experto para que se lleven a cabo de manera eficaz, segura y sin peligro.

  Otro medio para realizar la destrucción es la trituración, para esto existen máquinas denominadas “destructoras de papel” las cuales fragmentan el medio que contiene la información, es mejor cuándo el fragmento es lo suficientemente pequeño lo cual brinda una seguridad considerable a la confidencialidad de la información. Algunos medios de almacenamiento (CD, magneto-ópticos) deben ser destruidos por la pulverización, o trituración de corte transversal. Cuando el medio se desintegra, los residuos deben reducirse a fragmentos de cinco milímetros (5 mm).

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

Dado que la destrucción es física, no es posible realizar la recuperación posterior por ningún método, medio o procesos conocido. Para la destrucción de los discos duros, debe asegurarse que tanto los discos como las celdas (SDD) queden completamente inservibles, no solamente su cubierta exterior.

- **Sobreescritura:** Este método busca la destrucción de la información escribiendo un patrón definido sobre los datos de los dispositivos que contiene la información. Para que los datos queden por completo destruidos debe ser sobre escrito en su totalidad. Este método se realiza al acceder al dispositivo y modificando los datos almacenados. Este método no se puede utilizar en dispositivos dañados o en aquellos que no son re-escribibles

En la siguiente tabla podemos evidenciar las características que cumplen cada uno de los tipos de borrado de información.

Tabla 13 Comparativa de los métodos de borrado seguro

DESTRUCCIÓN FÍSICA		DESMAGNETIZACIÓN		SOBREESCRITURA	
✓	Eliminación de forma segura de la información	✓	Eliminación de forma segura de la información	✓	Eliminación de forma segura de la información
✗	Un sistema de destrucción para cada soporte	✗	Una configuración del sistema para cada soporte	✓	Una única solución para todos los dispositivos
✗	Dificultad de certificación del proceso	✗	Dificultad de certificación del proceso	✓	Garantía documental de la operación
✗	Necesidad de transportar los dispositivos a una ubicación externa	✗	Necesidad de transportar los dispositivos a una ubicación externa	✓	Posibilidad de eliminación en las propias oficinas de la compañía
✗	Medidas extraordinarias para garantizar la cadena de custodia	✗	Medidas extraordinarias para garantizar la cadena de custodia	✓	Garantía de la cadena de custodia
✓	Destrucción de dispositivos, no recargables, ópticos	✗	Solo valido para dispositivos de almacenamiento magnético	✗	No válido para dispositivos no regrabables, ni ópticos
✗	Destrucción definitiva y dificultad	✗	Tras el proceso el dispositivo deja de	✓	Reutilización de los dispositivos con

de reciclaje de materiales	funcionar correctamente.	garantías de funcionamiento.	

Fuente: Propia, tomado de ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Guía de borrado seguro de la información, una aproximación para el empresario [en línea] 2016. p. 12. [consultado 12 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

De igual forma, podemos evidenciar en la siguiente tabla a qué tipo de dispositivo de almacenamiento podemos aplicar cada uno de los métodos de borrado seguro con el fin de conseguir el mejor tipo de eliminación de información. Indicando cuál es el más efectivo.

Tabla 14 Método de borrado adecuado en función del dispositivo

DISPOSITIVO	TIPO	DESTRUCCIÓN FÍSICA	DESMANEGTIZACIÓN	SOBRE ESCRITURA
Discos Duros	Magnético	✓	✓	✓
Discos Flexibles	Magnético	✓	✓	✓
Cintas de Backup	Magnético	✓	✓	✓
CD	Óptico	✓	✗	✗
DVD	Óptico	✓	✗	✗
Blue-ray Disc	Óptico	✓	✗	✗
Pen Drive	Electrónico	✓	✗	✓
Discos Duros SSD	Electrónico	✓	✗	✓

Fuente: Propia, tomado de ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Guía de borrado seguro de la información, una aproximación para el empresario [en línea] 2016. p. 12. [consultado 12 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

6.5.1.5 Política de Divulgación De Información

i. Objetivo

Definir la información que puede ser revelada, a quien, cómo y en qué circunstancias se puede dar esta divulgación, incluyendo las partes interesadas, socios, organismos de gobierno, y en sí mismo los miembros del CSIRT de Platino Sistemas. De acuerdo al nivel de clasificación de la información y la protección de datos se debe establecer como se comparte esta información.

ii. Alcance

Toda la información generada o en poder de CSIRT Platino Sistemas

iii. Declaración de la política

- **Información Pública**

Toda información que esté clasificada como pública, es libre de ser divulgada, sin embargo, su divulgación debe ser por canales establecidos y gestionada por el equipo de producción, contenido y formación, este equipo tratará todos los asuntos públicos del CSIRT Platino Sistemas y lo llevara a cabo de acuerdo con los procedimientos propios establecidos por este equipo.

- **Información Clasificada**

Esta información solo se puede divulgar cuando haya una autorización propia por parte del Jefe Principal del CSIRT o del Gerente de Platino Sistemas en su defecto. En cualquier caso, se firmará un acuerdo propio de no divulgación con las personas o destinatarios con quienes sea compartida esta información, en la cual se establece que cualquiera a quien se le comunique esta información clasificada será debidamente notificado de la categorización de la información que está reviviendo.

- **Información clasificada de uso comunitario**

Toda información que es clasificada pero que ha sido autorizada para ser difundida dentro de la comunidad se convierte en un tipo especial de información. Todas las consideraciones anteriormente mencionadas son válidas, excepto que la divulgación que realizan algunos o todos los miembros del CSIRT Platino Sistemas sean autorizadas por el Gerente.

- **Información Confidencial**

Excepto autorización expresa de las leyes propias de Colombia, o una autorización de un requerimiento legal, CSIRT Platino Sistemas ni su personal podrá divulgar información confidencial. Si, por razones operativas o legales, se hace necesario compartir esta información, se debe informar al propietario de la información para un consentimiento. Si el propietario de la información está de acuerdo con la divulgación de la información, es necesario exigir al receptor de la misma firmar un

acuerdo de no divulgación, este acuerdo puede ser redactado y establecido por el dueño de la información o por el CSIRT.

- **Información Secreta**

Bajo ninguna circunstancia CSIRT Platino Sistemas revelará o divulgará información secreta por la ley.

- **Información Incompleta/No terminada**

La información que aún se encuentre sin terminar o en borrador y que llegue a tener información de carácter confidencial, puede ser divulgada de forma individual siguiendo las directrices propiamente definidas para este fin.

iv. Aspectos Legales

CSIRT Platino Sistemas acatará todas las leyes nacionales o políticas organizacionales para responder a todas las peticiones de información por parte de terceros. Dichas solicitudes de información deben hacerse por medio del departamento jurídico o el asesor del CSIRT Platino Sistemas.

v. Información de pedidos

- **Grupo de Respuesta a Incidentes**

Cooperar e intercambiar información con otros CSIRT es vital para el respectivo funcionamiento y supervivencia de CSIRT Platino Sistemas y las diferentes comunidades de orden nacional e internacional. Mucha de la información generada por el CSIRT platino Sistemas será compartida con otros grupos de respuesta a incidentes, así como el CSIRT Platino Sistemas se alimentará de mucha información propia de ellos para tener mejor forma de reaccionar ante incidentes. De acuerdo a esta política, mediante la evaluación de cada caso de forma individual y con el permiso del gerente o su designado esta información será comunicada y enviada a diferentes grupos.

- **Prensa**

La comunicación y el enlace con la prensa en todas sus formas, (radial, televisión, periódico escrito o Internet) serán realizados por el equipo de producción de contenido o formación o a quien estos designen exclusivamente para la comunicación de la información, previa aprobación del Jefe de CSIRT Platino Sistemas. En caso de que algún miembro del CSIRT sea contactado por un representante de prensa, estas solicitudes deben ser trasladadas al portavoz, ya que estos no están autorizados a divulgar ninguna información o revelar información bajo ninguna circunstancia, independientemente de la clasificación de la información.

6.5.1.6 Comunicado de Prensa de Información Sensible

Siempre que sea necesario, la información confidencial puede ser divulgada de tal manera que evite tener acceso a la misma por un tercero no autorizado.

6.5.1.7 Política de Acceso a la Información

i. Objetivo

La presente política busca facilitar de forma más amplia el acceso a la información en poder de CSIRT Platino Sistemas, reafirmando así el compromiso con respecto a la transparencia de sus actividades, pero en el mismo orden sentando un precedente, que permita mantener el equilibrio con la obligación de respetar la privacidad en las relaciones con sus clientes, usuarios y contratistas entre otros.

ii. Definiciones

- **Información:** Es cualquier archivo (físico, electrónico, multimedia y/o digital) independiente de su forma, origen, fecha de creación o medio de comunicación que se encuentre en poder de CSIRT Platino Sistemas.

- **Solicitante:** Persona natural o jurídica que solicite información a CSIRT Platino Sistemas.

- **Oficial de Información:** Contacto único y principal de CSIRT Platino Sistemas para la recepción y decisión en primera mediad de las solicitudes de información, brinda asistencia a los solicitantes y recepción de las apelaciones

ante la negativa del acceso a la información. Promueve las mejores prácticas en relación con el mantenimiento, archivado y destrucción de la información.

- **COACCI:** (*Comité de Acceso a la Información*), formado por el Gerente de CSIRT, el Jefe Oficial del CSIRT, el Oficial de la Información y un representante designado por cada equipo. El comité interpreta la política, hace revisión periódica de la misma con base en la evolución propia de la información, confirma o revoca en forma definitiva la decisión previa del Oficial de Información de negar acceso a la información cuándo este pida consejo o cuándo se haya presentado una apelación. Imparte y orienta a los clientes, usuarios y contratistas de CSIRT Platino Sistemas sobre la política.

- **Socio cooperativo**: Es un CSIRT al que se le puede compartir información y que hace parte del grupo de cooperación del CSIRT Platino Sistemas.

- **Usuario**: Miembro de CSIRT Platino Sistemas, que puede ser empleado, cliente o socio cooperativo.

- **Contratista Independiente:** Es una persona natural o jurídica por CSIRT Platino Sistemas para suministrar productos y/o servicios.

iii. Divulgación activa

CSIRT Platino Sistemas activamente divulga y actualiza la información por diferentes medios, en especial su página web. Esta información incluye su estructura orgánica, normas, procedimientos, funciones y actividades, copias permitidas, acuerdos bilaterales, entre otros. De igual forma, CSIRT Platino Sistemas mediante un sistema de reuniones virtuales facilitará el acceso a las reuniones de los diferentes miembros y asociados, internos y externos de la empresa, en conformidad de las normas pertinentes y las decisiones de dichos miembros al respecto.

iv. Excepciones

Aunque la política tiene como finalidad ofrecer al público el mayor acceso posible a la información que se encuentra en poder de CSIRT Platino Sistemas, es indispensable de la misma manera proteger la confidencialidad de cierta información propia del CSIRT, de sus miembros, usuarios, contratistas y de todo el

personal involucrado con el CSIRT. Es por esto que el CSIRT Platino Sistemas no proporciona acceso a:

a. Información Personal. Excepción de aquella que las normas, procedimientos, leyes o prácticas pertinentes lo permitan, CSIRT Platino Sistemas no brinda acceso a:

   (1) Información médica y comunicaciones personales.
   (2) Información que pueda ser considerada una invasión a la privacidad si se llegase a divulgar.

b. Informes de auditoría o de investigaciones por el equipo de apoyo o legal de CSIRT, salvo que sean solicitados por un organismo propio de la legislación colombiana.

c. Información que pueda colocar en riesgo la seguridad de los miembros, usuarios o contratistas de CSIRT o de sus familias.

d. Información sobre los procesos de licitación.

e. Información de secreto profesional, incluidas las comunicaciones efectuadas por los abogados del equipo legal y/o asesores jurídicos de CSIRT Platino Sistemas.

f. Información protegida por acuerdos de confidencialidad.

g. Información financiera o comercial que pudiera perjudicar los intereses comerciales o financieros del CSIRT Platino Sistemas si se llega a divulgar, o perjudique a otras partes involucradas, salvo cuando la misma sea solicitada por un miembro del CSIRT o por una autoridad del país.

h. Información de carácter interno, deliberativa o que se haya intercambiado entre diferentes usuarios del CSIRT Platino Sistemas o con terceros, incluyendo correos electrónicos, correspondencia, informes, memorando entre otros.

i. Información proporcionada por un usuario, cliente o tercero en calidad de confidencial de la misma, salvo cuando este usuario, cliente o tercero otorgue un consentimiento previo expreso para su divulgación.

j. Información protegida por el derecho de propiedad intelectual.

k. Cualquier información que en la opinión del Oficial de Información o del COACCI sea considerada en un nivel de sensibilidad protegida por los párrafos anteriores de este numeral.

v. Procedimiento para solicitud de información

A. Solicitud

1. El solicitante debe usar un canal de comunicación escrito – correo electrónico, correspondencia entre otro – hacía el Oficial de la Información.

2. La solicitud debe contener:

a. Información de contacto del solicitante.
b. Descripción detallada de la información solicitada (se puede incluir, título, palabras claves y fecha)
c. Medio o forma en que quiere que la información sea entregada.

B. Respuesta

1. El oficial de la Información registra la solicitud y asigna un número de seguimiento. Dentro de un plazo de diez (10) días calendario posterior a la recepción de la solicitud, se debe dar un acuse de recibido al solicitante informando del número de seguimiento asignado. De igual forma, el Oficial de la Información dentro del mismo plazo podrá solicitar mayor claridad o precisión sobre la información solicitada.

2. Si la información solicitada se encuentra pública, el Oficial de la Información puede dar la solicitud como resuelta indicando al solicitante donde puede encontrar la información.

3. Si la información solicitada no se encuentra pública, el Oficial de la Información debe dar respuesta al solicitante dentro de los veinte (20) días calendario posterior a la recepción de la solicitud. Este tiempo es prorrogable en solicitudes de carácter complejo o de cantidad considerable, notificando la prórroga de tiempo al solicitante hasta por

veinte (20) días más máximo. La falta de respuesta dentro de los tiempos establecidos debe entenderse como una solución denegatoria a la solicitud. La respuesta puede ser:

a. La información se encuentra dentro de las excepciones descritas en esta política.
b. CSIRT Platino Sistemas no cuenta con la información solicitada o los datos proporcionados por el solicitante no permiten localizar la información de forma oportuna.
c. CSIRT Platino Sistemas cuenta con la información, sin embargo, su reproducción y envío acarrea un costo que no es cubierto por CSIRT Platino Sistemas, por lo cual debe comunicarse de este costo al solicitante y se tiene diez (10) días hábiles posterior a la confirmación de la recepción del pago de este rubro para que el CSIRT Platino Sistemas proceda al envío de la información solicitada.

vi. Apelación

1. El solicitante quien haya recibido por respuesta una denegatoria puede presentar el recurso de apelación, si considera que la denegatoria es injustificada.

2. Las apelaciones a la denegatoria deben usar un canal de comunicación escrito – correo electrónico, correspondencia entre otro – y deberán dirigirse al COACCI dentro de los treinta (30) días calendario siguientes a la expiración de los términos de tiempos anteriores. Las apelaciones recibidas después de este plazo se considerarán extemporáneas y serán desestimadas.

3. Las apelaciones deben contener la siguiente información:

a. Número de solicitud consignado en el acuse de recepción de la solicitud en primera instancia.
b. Información de contacto del solicitante.
c. Descripción de la información solicitada originalmente, entre más específico es mucho mejor.
d. Exposición de los hechos y los fundamentos que sustentan la apelación.

4. COACCI podrá contactar al solicitante para pedir mayor información sobre su apelación.

5. Dentro de los treinta (30) días calendario posterior a la recepción de la apelación, COACCI dará una respuesta con una sentencia definitiva, revocando o confirmando la decisión del Oficial de la Información en primera instancia. Este plazo se puede ampliar por veinte (20) días más calendario en casos excepcionales.

6. COACCI notificará la decisión por escrito. Si es el caso, y la decisión revoca la decisión del Oficial de la Información, el solicitante recibirá la información, pero en ningún caso tendrá derecho al pago de una indemnización.

vii. Propiedad intelectual

La información en poder del CSIRT Platino Sistemas que se encuentre sujeta a los derechos de propiedad intelectual puede ser puesta a disposición del público con propósitos informativos, pero la copia, reproducción o distribución dependerá de los derechos intelectuales pertinentes.

viii. Exoneración de responsabilidad

CSIRT Platino Sistemas no garantiza la integridad y veracidad de la información provista, así como no será responsable de ningún daño y/o perjuicio ocasionados por la manipulación de la información provista.

Cada una de estas políticas está respaldada por una cláusula de confidencialidad entre las partes PLATINO SISTEMAS y el cliente, la cual se firmará al inicio de la relación comercial con el cliente que adquiera el servicio de CSIRT

6.5.1.8 Política de Uso apropiado de los Sistemas del CSIRT

i. Objetivo

Establecer usos aceptables e inaceptables de cada uno de los dispositivos electrónicos y recursos que pertenecen a CSIRT Platino Sistemas. Estableciendo el cumplimiento de las normas éticas y legales establecidas, basada en la confianza, la integridad y las transparencias de las actividades propias del CSIRT.

CSIRT Platino Sistemas gestiona los diferentes dispositivos de computación, redes y consecuentes sistemas de información con el fin de llevar a cabo sus directrices,

objetivos e iniciativas. Gestionando todos y cada uno de ellos de manera idónea y responsable para mantener la CID (Confidencialidad, Integridad y Disponibilidad) de los activos de información que CSIRT Platino Sistemas tiene en su poder o utiliza para trabajar.

Esta política requiere que todos los usuarios de los diferentes dispositivos y recursos de red acepten y cumplan con cada uno de los parágrafos definidos, a fin de proteger el CSIRT Platino Sistemas, su personal, sus operaciones, sus socios de daños y demandas.

ii. Alcance

Todo el personal, incluyendo contratistas, terceros, consultores, pasantes, empleados y cualquier otro que labore de forma directa o indirecta con CSIRT Platino Sistemas deben cumplir con esta política. La misma se aplica a todos los activos de información que son propiedad o arrendados por CSIRT Platino Sistemas, o a aquellos dispositivos que se conectan a la red de CSIRT Platino Sistemas o que están alojados en alguna de las instalaciones del CSIRT.

En circunstancias especiales, la administración del CSIRT Platino Sistemas pueden aprobar excepciones contrarías a esta política. Cualquier excepción debe ser aprobada por el Jefe de CSIRT formalmente y por escrito, e incluir una justificación y evaluación de los riesgos a la excepción.

iii. Declaración de la Política

- **Requerimientos Generales**

Todo empleado de CSIRT Platino Sistemas es responsable de ejercer buen juicio con respecto al uso apropiado de los recursos y activos de información de conformidad con las políticas y los procedimientos propios y establecidos por el CSIRT Platino Sistemas. Los recursos del CSIRT Platino Sistemas no pueden ser utilizados con fines ilícitos o que estén en violación de otra política de CSIRT Platino Sistemas.

- **Cuentas del Sistema**

Todo empleado de CSIRT Platino Sistemas es responsable de la seguridad de los datos, las cuentas y los sistemas bajo su control. Debe mantener contraseñas seguras de acuerdo a la política de gestión de usuarios y contraseñas. No debe compartir la información de la cuenta ni la contraseña con ninguna otra persona, incluyendo otros empleados, familiares o amigos. Es una violación a esta política facilitar a otra persona, de manera intencional o por falta de garantía de acceso, el manejo de sus contraseñas o accesos.

Todo empleado de CSIRT Platino Sistemas debe estar seguro, por medio legales o tecnológicos, que la información con la que opera en la empresa está bajo su control y la gestión del CSIRT en todo momento. El almacenamiento, así como el acceso a la información confidencial en aplicaciones o ambientes gestionados por un tercero o no directamente operados o controlados por CSIRT Platino Sistemas está totalmente prohibido. Esto incluye aquellos dispositivos que son mantenidos u operados por terceros con los que no haya un acuerdo contractual. Además, esto prohíbe rotundamente el acceso y uso de una cuenta de correo electrónico que no haya sido proporcionada por el CSIRT Platino Sistemas para intercambiar información propia o a nombre del CSIRT Platino Sistemas.

- **Activos Informáticos**

Todo empleado es responsable de garantizar la protección de los activos informáticos que le fueron asignados por CSIRT Platino Sistemas. Esto incluye cualquier dispositivo de seguridad. Computadores portátiles entre otros. Cualquier pérdida o robo de alguno de estos activos o computadores debe ser reportado inmediatamente a la administración del CSIRT Platino Sistemas.

Todas las estaciones de trabajo y dispositivos deben estar protegidos por contraseña, y se debe bloquear o cerrar la sesión cuándo se retira del puesto de trabajo. De igual forma la opción de bloqueo automático por tiempo se debe activar como establece el procedimiento de configuración de puesto de trabajo. Cualquier dispositivo que se conecte a la red debe cumplir con la política de acceso mínimo.

- **Uso de comunicaciones electrónicas e Internet**

Todo empleado es responsable de la seguridad y el uso adecuado de los recursos de red y de las herramientas bajo su control. Está prohibido de manera especial, los recursos que puedan llegar a ocasionar:

- Un fallo de seguridad o violación a uno o más recursos de red de CSIRT Platino Sistemas.
- Una interrupción del servicio a uno o más recursos de red de CSIRT Platino Sistemas.
- Violen la disposición y las leyes de derecho de autor.
- Violen las políticas de seguridad establecidas por las leyes colombianas.
- Apoyen cualquier actividad ilegal incluyendo la transmisión o ayuda en la transmisión de información confidencial o propiedad de CSIRT Platino Sistemas.

iv. Implementación

Un usuario de CSIRT Platino Sistemas que viole esta política o cualquier otra política, estará sujeto a medidas disciplinarias, que pueden ir desde el despido o implicaciones legales. Una violación a esta política por parte de personal temporal, contratista o proveedor puede resultar en la terminación unilateral del contrato o cesión con CSIRT Platino Sistemas.

6.5.2 PROCESOS DE CSIRT PLATINO SISTEMAS

6.5.2.1 Proceso de Gestión de Incidentes

La gestión de incidentes es la actividad principal de todo CRIST, y en el caso de Platino Sistemas es su prioridad, de esta forma, el proceso de gestión de incidentes del CSIRT Platino Sistemas se desarrolla en los siguientes pasos:

1. Detección de eventos: Determinar comportamientos sospechosos de acuerdo a los niveles de prioridad y criterios de detección. Estos criterios deben ser establecidos previamente por los responsables del equipo de Análisis y evaluación técnica. Estos comportamientos pueden ser el resultado de una investigación inicial (monitorización de redes) o de las notificaciones recibidas de otras fuentes (colaboración con CSIRT).

2. Clasificación de eventos: Discernir entre los diferentes eventos detectados con el fin de poder catalogar entre eventos de interés, eventos medios, irrelevantes y falsos positivos.

3. Registro de eventos: En una herramienta de gestión de incidentes, se debe realizar la inscripción de los eventos clasificados como “de interés y medios” con un mínimo de información

4. Posterior al registro del evento, en un segundo nivel se debe comenzar con el TRIAGE del evento.

5. Con el evento identificado como incidente, clasificado y priorizado (triage) de forma correcta se debe identificar y registrar las partes afectadas (clientes y/o comunidades).

   En una última fase se realiza un seguimiento, se puede de ser necesario colocar al equipo de I+D a buscar una solución, se colabora con la reducción de los daños, erradicación de causas, implantación de mejoras y controles de seguridad para evitar el incidente en el futuro.

6.5.2.2 Proceso de Definición de Incidentes de Seguridad

1. Clasificación del incidente: Aunque al principio no haya demasiada información para una clasificación clara, esto puede ser recategorizado más adelante, la clasificación ayuda a determinar la gravedad del incidente, la prioridad de atención y el personal o recursos con el fin de dar solución.

Tabla 15 Clasificación de incidentes según su gravedad

Grupo	Severidad	Ejemplos
Rojo	Muy Alta	Phishing, Ataque desconocido, APT, Acceso abusivo
Naranja	Alta	Malware, sabotaje, DDoS, DoS, Perdida de datos
Ámbar	Normal	Compromiso de cuentas con privilegios, Sistema vulnerable, Uso no autorizado de recursos.
Amarillo	Baja	Spam, Compromiso de cuentas sin privilegios, otros no críticos.

Fuente: Propia

2. Gravedad y Prioridad: La categorización del incidente está dado con base a la taxonomía de los incidentes de seguridad.

De esta manera, se pueden identificar de acuerdo cada grupo, que prioridad debería tener los diferentes clientes que maneje CSIRT Platino Sistemas identificados con número de prioridad del uno al cinco (1= altamente prioritario, 5= prioridad baja) la atención que podría dar.

Tabla 16 Clasificación de incidentes según su prioridad

Prioridad	Gobierno	Financiero	Militar	Académico	CIP / CIIP	Otros
Rojo	1	1	1	1	2	2
Naranja	1	1	1	2	2	3
Ámbar	1	2	1	3	3	4
Amarillo	2	2	2	4	4	5

Fuente: Propia

3. Asignación de responsables: El incidente debe ser asignado al área del equipo de *coordinación de y respuesta a incidentes* que sea apropiado para dar respuesta pronto a este incidente.

4. Error conocido: Definir si el incidente tiene un antecedente conocido del mismo tipo de ataque ayudará a probar más rápido soluciones anteriores, si estas no son efectivas deben involucrarse al personal de I+D para que pueda probar nuevas soluciones.

6.5.2.3 Proceso de Cooperación

Es importante que CSIRT Platino Sistemas haga parte de los grupos de CSIRT a nivel nacional e internacional con el fin de fomentar la unión para la resolución de incidentes de seguridad a través de los boletines, información y canales de comunicación que se puedan establecer con estos grupos y con los clientes.

1. Contar con listado actualizado de los canales de comunicación de los diferentes CSIRT. El primero en la lista debería ser el ser miembro de FIRST (Foro de equipos de respuesta a incidentes y seguridad, por sus siglas en inglés). La suscripción está alrededor de los US $ 2000 por año y su suscripción se puede realizar en la siguiente página https://www.first.org/members/

2. Establecer contacto con los principales CSIRT del país, se puede realizar mediante una visita entre el Jefe Principal y un representante de estos. En

Colombia existen tres (3) CSIRT principales bastante reconocidos: Grupo de respuesta a emergencias cibernéticas de Colombia – colCERT (https://www.colcert.gov.co/), el CSIRT del Gobierno de Colombia (https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/) y el CSIRT de la Policía nacional (https://cc-csirt.policia.gov.co/). La reunión es de utilidad para recoger ejemplos de las metodologías de trabajo y conseguir la conformación de una red de trabajo o el apoyo de parte de ellos.

3. Conocer los canales de comunicación propios que se tiene para informar de los incidentes de seguridad que se puedan presentar y los mismos que se puedan documentar apoyados en la información aportada por otros CSIRT o equipos de apoyo que tengamos.
   Entre estos los más efectivos pueden ser:

   a. Sitio web público, para publicar boletines, información relevante e importante en relación a los incidentes de seguridad entre otros.
   b. Zonas reservadas a los miembros en el sitio web, para que realicen sus publicaciones y hasta un enlace a la Herramienta ITSM (gestión de los sistemas de tecnologías de información, por sus siglas en inglés) que permita el registro de incidentes de seguridad por parte de los clientes.
   c. Formularios web para comunicar incidentes.
   d. Listas de correo
   e. Correo electrónico con el dominio propio de la empresa, para ser cuenta oficial.
   f. Teléfono o número de celular.
   g. Mensajería de texto.
   h. Informes mensuales en medio físico.

4. El tratamiento de los incidentes de seguridad es más fácil a través de la cooperación con clientes y equipos de apoyo a los que estemos vinculados. El tratamiento de estos incidentes se puede realizar a través de correo electrónico, los formularios web o el teléfono (recibir los informes de incidentes de los clientes para darles solución, coordinación con otros equipos realizando comentarios, prestando ayuda y apoyo a las víctimas del incidente).

De ser posible, la información a difundir de un modo seguro. Los datos del incidente que sean delicados como la información de un cliente siempre deben evitarse en su mayoría o por el contrario ser encriptados y no revelados.

5. Se debe analizar la posibilidad para futuras cooperaciones la de establecer vínculos internacionales en la funcionalidad de <<*siguiendo el sol*>>, con el fin de brindar servicios a partes donde es de noche, pero tal vez por alguna razón necesiten reportar o conocer cómo resolver un incidente en un horario no regular de trabajo.

6.5.3 PROCEDIMIENTOS DE CSIRT PLATINO SISTEMAS

6.5.3.1 Procedimiento de clasificación, priorización y asignación de incidentes

La clasificación del Incidente es la manera primaria de abordar todos aquellos eventos que se pueden presentar y que deben tener una clasificación en orden de gravedad y prioridad dependiendo el cliente. En la siguiente tabla se muestra el paso a paso del procedimiento para la clasificación de un incidente.

Tabla 17 Actividades del procedimiento de clasificación de incidentes

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	PCC	SALIDAS
1.Recepción del incidente.	Seguimiento y monitoreo	El equipo de seguimiento y monitoreo obtiene un informe de un nuevo incidente, por observación propia o por otra fuente.		Registro del incidente en la herramienta de gestión
2.Clasificación del Incidente	Mesa de ayuda	El equipo de mesa de servicio del CSIRT realizará una clasificación del incidente en orden de gravedad y prioridad.	X	Priorización del nivel de atención del incidente en virtud de su prioridad y gravedad.
3. Priorización del Incidente	Mesa de ayuda	De acuerdo al tipo de cliente al que el incidente puede impactar, se debe proceder a realizar las tareas posteriores con la menor pérdida de tiempo. Para frenar el impacto de la materialización del riesgo.		Activar los equipos de respuesta a incidentes.
4.Asignación del Incidente	Control de procesos de trabajo	El equipo de control de procesos de trabajo activará los equipos necesarios de acuerdo al incidente. De esta manera se pueden activar solo el equipo de TRIAGE para tratar el incidente, o el equipo de contención de código malicioso. Así mismo, se activarán los equipos de estadística y reporte para realizar el		Informe del incidente por cada equipo de trabajo activado.

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	PCC	SALIDAS
		seguimiento de los números del incidente. Se activará el equipo de documentación, para dejar toda evidencia propia de solución del incidente.		
5.Seguimiento a la resolución	Control de Procesos de trabajo	Se debe seguir a cada uno de los equipos activados hasta el cierre del incidente, que contempla su divulgación.	X	Cierre del incidente.

6.5.3.2 Procedimiento de atención de incidentes

Se le denomina grupo TRIAGE a aquellos que determinan como proceder ante la clasificación dada a un incidente, ellos serán los encargados de analizar la clasificación dada por el grupo de mesa de trabajo, y dar solución desde sus especialidades a cada incidente en particular.

Tabla 18 Actividades del procedimiento de atención de incidentes

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	PCC	SALIDAS
1.Analizar los datos.	TRIAGE	Se debe buscar la mayor cantidad de información posible, la que haya proporcionado el equipo de seguimiento y monitoreo, como el de la experiencia del equipo o de otros equipos. Se debe recolectar toda la información propia del incidente. Logs, lugares, dispositivos afectados, configuración de los sistemas. Se debe ser pragmático, para no gastar tiempo de más en la recolección de la información ya que el incidente puede estar en curso y la demora puede perjudicar el ejercicio de solución.		Conocimiento necesario para encontrar una solución. De forma general, el 20% de los datos, pueden darnos el 80% del conocimiento necesario para encontrar una solución.[26]
2.Investigar formas de solución	TRIAGE	Con base en soluciones anteriores y la información recopilada, se debe proponer la mejor solución para este incidente. Se puede consultar y hablar sobre las observaciones y conclusiones, o equiparando máquinas de características similares.	X	Plan de trabajo.

[26] PÉREZ E. Ernesto, y BERNAL B. Paul F Op. Cit., p. 32

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	PCC	SALIDAS
		También se puede realizar una lluvia de ideas para probar la solución más óptima.		
3. Propuesta de acción	TRIAGE	Pueden ser propuestas una o más acciones según la complejidad del incidente. De igual forma se pueden activar otros equipos como mitigación de código malicioso, comunicaciones o financiera si la solución requiere la compra de algún software o dispositivo de seguridad.		Activar los equipos de respuesta a incidentes diferente al TRIAGE
4.Acción realizada	Equipos.	Cada equipo que haya sido activado en el paso anterior debe verificar la acción realizada y si la misma ha resuelto el problema. Si los clientes o dispositivos de los clientes que se veían al principio vulnerables han superado esta vulnerabilidad. Si se tiene monitoreo de todo el tráfico de red y el incidente puede ser visualizado y corregido.	X	Informe del incidente por cada equipo de trabajo activado.
5.Erradicación y recuperación	TRIAGE	Posterior a la resolución del incidente, el equipo de TRIAGE debe regresar el dispositivo o software a producción, con las subsanaciones pertinentes o las mejoras realizadas. Si el equipo de investigación ha sido convocado, el tiempo de investigación supone no cerrar el incidente. Si alguna autoridad ha sido involucrada, toca esperar su solución o investigación (puede incurrir una investigación penal). Si el área de documentación ha sido involucrada se debe asegurar que sus comunicados han sido actualizados.	X	Cierre del incidente.

6.5.3.3 Procedimiento de cierre de incidentes y lecciones aprendidas

Una parte importante de solución de un incidente es la documentación del mismo con el fin que esto quede como una lección aprendida o un problema con solución, ya sea que el incidente sea materializado o se pueda materializar, lo importante es conocer y documentar para futuras ocasiones su solución. Esto hará que se pueda proceder de forma más efectiva y oportuna ante la posible amenaza convertida en incidente.

Tabla 19 Actividades del procedimiento de cierre de incidentes

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	PCC	SALIDAS
1. Verificar la información final	Documentación de Incidentes	Es necesario asegurar que toda la información que soporta el registro del incidente está en el mismo. Así mismo informar a las clientes y partes interesadas sobre el cierre del incidente por su solución. Resumen de lo acontecido durante el incidente. Resultado del trabajo de remediación y mitigación. Hallazgos y recomendaciones.	X	Registro de incidente correctamente documentado y gestionado.
2.Clasificación final	Documentación de Incidentes	Una vez reunida toda la información del incidente. Se debe reevaluar si se hace necesario una reclasificación del incidente. O si la que se tiene cumple con lo necesario. Si debe existir una reclasificación, es posible que el TRIAGE pueda verse beneficiado con la información adicional para una mejor clasificación.	X	Mejor clasificación o reafirmación de la clasificación primariamente establecida.
3. Crear archivo del incidente	TRIAGE	Si el incidente puede ser cerrado, dado que no se presenta ninguna actividad faltante y está correctamente clasificado. Se debe proceder a crear un archivo del incidente. El archivo del incidente debe quedar disponible para todo el equipo, preferiblemente en un sistema que permita su búsqueda de forma rápida y por diferentes parámetros. Esto permitirá solucionar en el futuro incidentes similares. Ahorrando considerable cantidad de tiempo y haciendo más eficiente y proactivo al CSIRT.	X	Activar los equipos de respuesta a incidentes diferente al TRIAGE
4.Analizar la estadística del incidente.	Equipos.	Realizar un análisis detallado de la afectación real del incidente		Informe del incidente por cada equipo de trabajo activado.
5. Lecciones Aprendidas	Todos los equipos	Adición o esclarecimiento de políticas, procesos y procedimientos. Mejoras en la arquitectura de infraestructura de red, hardware y/o software del CSIRT y de los clientes. Realizar mejoras en los mecanismos de detección y/o compra de herramientas de seguridad (hardware o software) que pudieron mejorar el análisis. Identificar nuevos tipos de ataques y compartir esta documentación con la comunidad de CSIRT a los que se		Revisión de la documentación del CSIRT

		encuentre agregado el CSIRT de Platino Sistemas.		

6.5.3.4 Procedimiento de divulgación de incidentes

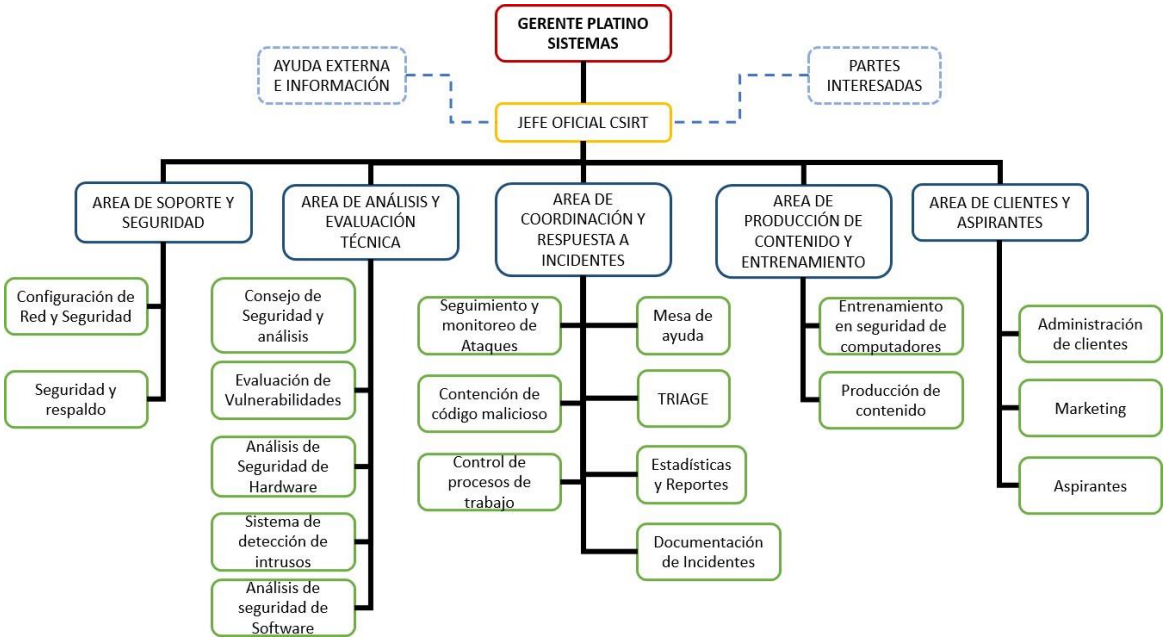
La comunicación siempre debe ser efectiva y CSIRT Platino Sistemas no puede ser contrario a esta premisa, de esta manera CSIRT Platino Sistemas debe contar con un canal de comunicaciones de los incidentes hacía los interesados, ya sean los clientes, los CSIRT a los cuales está asociado y/o a las autoridades del país.

Tabla 20 Actividades del procedimiento de divulgación de incidentes

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	PCC	SALIDAS
1.Verificación del comunicado	Documentación de Incidentes	El grupo debe determinar qué información no es privada ni pertenece a un cliente y puede ser puesta en el comunicado del incidente para no comprometer la integridad de información privada o clasificada.	X	Borrador de comunicado.
2.Escoger canal de comunicación	Documentación de Incidentes	El equipo debe seleccionar si el incidentes y su resolución será transmitido por todos los canales o solo por algunos, si será compartido solo con sus clientes, con sus clientes y la comunidad CSIRT, o al público en general.	X	Incidente comunicado por el/los canal(es) seleccionados.
3. Informar a las autoridades	TRIAGE	Se debe determinar si el incidente requiere de una investigación de las autoridades del país. De ser así se les debe informar de manera oportuna. Y recordar que el incidente no se puede dar por cerrado mientras exista la investigación.	X	Informe a las autoridades.

6.6 ESTRUCTURA ORGÁNICA DEL CSIRT

Figura 7 Organigrama de la estructura de CSIRT Platino Sistemas



Fuente: Propia

El CSIRT en su etapa inicial estará conformada por 5 grandes equipos, que darán inicio a las actividades de la organización. Entre ellos tenemos

Equipo de Soporte y Seguridad

Este equipo es el menos especializado en la solución de incidentes, es un equipo básico de ingenieros que resolverán de manera reactiva los eventos de seguridad que se presenten en CSIRT Platino Sistemas y que puedan dar apoyo a los clientes gracias a sus conocimientos. Este equipo no es necesariamente especialista en seguridad informática o de la información, en la mayoría serán administradores de sistemas, especialistas en firewalls, especialistas en red, especialistas en almacenamiento, entre otros.

Este equipo es en la mayoría reactivo, en un término coloquial "*los apaga incendios*", pero no tendrá los conocimientos necesarios ni la experiencia para llevar a cabo operaciones de seguridad informática sólidas. En pocas palabras, son capaces de resolver los incidentes, pero no en determinar sus

causas, en algunos casos, determinan sus causas, pero no una solución efectiva, por lo cual dejan nuevamente expuesta la organización a que se presente el evento.

La naturaleza del área de soporte y seguridad en la mayoría de las ocasiones impide la aplicación de mejores prácticas, investigación y desarrollo y monitoreo de alertas de seguridad.

Equipo de Análisis y Evaluación Técnica

Este equipo es más especializado que el anterior, no tiene cómo el anterior una especialidad para la solución de incidentes, sin embargo, este equipo será el encargado de buscar vulnerabilidades o confirmar las entregadas por otros CSIRT con el fin de determinar el potencial riesgo que puede existir y que son de vital importancia comunicar a los clientes. Estos personajes pueden tener una especialidad propia en un sistema, en un hardware y/o en un software.

Este equipo debe ser coordinado por un consejo de seguridad y análisis el cual determinará en sus proyectos, a quien contratar, sea de planta a freelance para que haga la investigación pertinente, el tiempo que durará la investigación, y la forma como debe entregar los resultados de su investigación, ya sea sobre software, hardware o una vulnerabilidad en particular.

Las investigaciones de este equipo permitirán al CSIRT Platino Sistemas mantener actualizados a sus clientes y a su personal propiamente. Esta área es necesaria dentro del CSIRT, sin embargo, contando con los recursos iniciales, puede ser un área para una segunda fase de operación, más allá de la de implementación.

Equipo de Coordinación y respuesta a Incidentes

Este equipo es el CORE del CSIRT, ellos son los encargados directamente de dar solución a los incidentes, apoyados en muchas ocasiones en el **Equipo se Soporte y Seguridad**, a diferencia de este último, este equipo si es especialista en la ejecución de actividades de seguridad informática, no solamente dará solución al incidente sino que permitirá realizar una investigación forense para determinar las causas propias del incidente, allí se puede apoyar en el **Equipo de Análisis y Evaluación Técnica**, así mismo como activará todos los componentes propios del CSIRT que necesite

para llevar a cabo todo el tratamiento de incidentes que tiene como servicio el CSIRT de Platino Sistemas.

Este equipo se compone de diferentes partes de su núcleo para dar una respuesta integral a los incidentes, de esta manera brinda procedimientos de respuesta efectivos y estandarizados, mantiene las estadísticas de los incidentes, aumenta la sinergia entre los diferentes equipos de la organización y promueve el trabajo colaborativo a través del intercambio de buenas prácticas, lecciones aprendidas y asignación adecuada de los recursos de seguridad con los diferentes CSIRTS asociados y las partes interesadas.

De igual manera este equipo, determina la comunicación y nuevas pautas de formación hacia el **Equipo de Producción de Contenido y Formación**, para que se establezca como realizar los comunicados sobre los incidentes que se presentaron en algún cliente, sobre como informar al cliente para que estos incidentes no se presenten en su infraestructura, y si debe o no tener una formación adicional para evitarlos en un futuro. De igual forma el entrenamiento propio del personal para evitar o saber reaccionar si el incidente llega a materializarse en un futuro en alguno de los clientes o en la organización propiamente.

Equipo de Producción de Contenido y Formación

Este equipo es el encargado de publicar, informar, notificar, comunicar y mantener la página web del CSIRT actualizada. Como parte de compartir toda la información relevante para los clientes de la empresa. Este equipo tiene la función principal de traducir toda la información técnica que se produzca al interior del CSIRT Platino Sistemas y que llegue de los diferentes CSIRT a un lenguaje claro que pueda ser entendido de forma amena por los clientes de la empresa como valor agregado.

De igual forma también es la encargada de cumplir con muchos de los servicios complementarios que tiene el CSIRT como son los de evaluación, formación, y transferencia de conocimiento o capacitación.

Equipo de Apoyo

Aunque no lo parezca, este es el equipo más importante que puede tener CSIRT Platino sistemas, es la base de toda la organización del CSIRT, su principal función es la de mantener todo funcionando, desde la relación con los clientes, así como el marketing, los asistentes, los aspirantes, la parte legal de la empresa y la parte financiera. Es el encargado de la contratación del personal, el pago de sueldo, la verificación de que todo lo que se está haciendo está en regla y es la parte vital de la empresa, así como el **Equipo de Coordinación y respuesta a Incidentes** es el corazón del CSIRT, esta parte es el cerebro de la organización.

7 CONCLUSIONES

- Las políticas, procesos y procedimientos del CSIRT Platino Sistemas, se construyeron en su fase inicial. Estas políticas se hicieron bajo la normativa ISO/IEC 27001 para dar gestión de forma eficiente y oportuna a los incidentes de los clientes del CSIRT y aportan como el punto de partida de la construcción de una base de conocimiento en las acciones pre, durante y post incidente. Estas políticas están complementadas por los procesos y procedimientos que se establecieron de forma general para las infraestructuras de hardware y software que puedan tener los clientes a través de un enfoque administrativo empresarial.

- CSIRT Platino Sistemas puede ofrecer estos servicios a empresas grandes, medianas o pequeñas que deleguen la tercerización de su seguridad informática. De esta forma el campo inicial de acción de CSIRT Platino Sistemas ha de ser comercial. Brindando así el acompañamiento en la prevención, detección y gestión de incidentes a sus clientes. Empezando por un enfoque amplio, y acotando su campo de acción en concordancia con aquellos que estén brindando rentabilidad. Reduciendo sectores o manteniendo los clientes que brinden ganancias a la empresa.

- La taxonomía que emplea CSIRT Platino Sistemas está definida con base en los ataques reconocidos a nivel mundial por los diferentes equipos de respuesta a ataques cibernéticos. Interiorizar esta taxonomía permite que se hable el mismo idioma a la hora de exponer, divulgar y retroalimentar los ataques que se puedan presentar. De esta forma, al ser parte de la red de CSIRT de los cuales Platino Sistemas hace parte le permite realizar el análisis de los incidentes sin empezar desde el principio, sino contando con una jerga y un conocimiento amplio que le puede ser compartido desde el exterior.

- Como resultado del proyecto, se establece que CSIRT Platino Sistemas debe empezar por ofrecer los servicios básicos, propios de todo CSIRT y recurrentes en los mismos grupos a nivel internacional. Estos servicios son siete (7) servicios proactivos, cuatro (4) servicios reactivos y seis (6) servicios complementarios. Sin embargo, el nivel inicial de maduración de CSIRT

permitirá que estos servicios evolucionen con el tiempo, dando pasos a diferentes y nuevos servicios que dejen su propia huella en los clientes y ayuden a acrecentar su portafolio de servicios hacía nuevos clientes en la solución integral de incidentes.

- El cumplimiento de estos objetivos, permite que se elabore un diseño documental adecuado para el desarrollo de las actividades propias de un CSIRT para la empresa Platino Sistemas, este diseño solo comprende la etapa de planificación del CSIRT, estableciendo los cimientos del nuevo servicio de la compañía, cabe aclarar que para llegar a la construcción completa del CSIRT se ha de pasar por las etapas de Ejecución y producción.

- La realización de este diseño documental, identificó que un CSIRT es una parte fundamental de la seguridad informática, y que toda empresa debe contar con uno como parte de sus buenas prácticas hacía un SGSI (Sistema de gestión de seguridad de la información). Ya sea propio o tercerizado, este servicio permite contar con aliados estratégicos que nos mantienen informados sobre los incidentes de seguridad de la información en el planeta de las tecnologías.

- Platino Sistemas puede contar con este servicio como parte de su portafolio de servicios de seguridad de la información que brinda a sus clientes y como uso propio interno. Ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio contratado los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades.

8 RECOMENDACIONES

Ampliar el personal de la empresa una vez haya pasado su etapa inicial de la fase de implementación del CSIRT de Platino Sistemas. Esto permitirá tener mayor disponibilidad de personal para atender a un número mayor de clientes. Además de dividir el trabajo en más integrantes podrá reducir esfuerzos y dar una mayor efectividad y mayor eficiencia. La producción es una variable que depende del número de clientes, pero a mayor cantidad de personal el trabajo puede ser más prolífico. El CSIRT de Platino Sistemas tiene grandes ventajas en su implementación en nuestro país, ya que muchas empresas pequeñas no cuentan con equipos de respuesta ante un incidente computacional en sus empresas, dado que sus departamentos de TI son bastante pequeños. Por lo cual esto podría ser una gran oportunidad de negocio.

Por consiguiente, el CSIRT podría evolucionar de la siguiente forma:

Tabla 21 Evolución del personal CSIRT Platino Sistemas

Equipos CSIRT	**PERSONAL**	
	1. Fase Implementación Etapa Inicial	2. Fase Operación Etapa Posterior
Principal 	1 jefe / Coordinador	1 jefe principal 1 coordinador
Apoyo de TI 	1 Líder por equipo 2 Especialistas técnicos	1 líder por equipo 2 especialistas técnicos en administración de redes 2 especialistas técnicos en administración de sistemas
Investigación y Desarrollo 	1 líder en el equipo 1 especialista técnico	1 líder en el equipo 1especialistas en seguridad 1 especialista analista de seguridad 1 especialista investigador de seguridad 1 Custodio de registros.
Operaciones 	1 líder de equipo 1 especialista técnico	1 líder de equipo 1 especialista en clasificación de incidentes. 1 especialista en triage

Equipos CSIRT	PERSONAL 1. Fase Implementación Etapa Inicial	 2. Fase Operación Etapa Posterior
		2 especialistas en manejo de incidentes.
Servicios de apoyo 	1 abogado (apoyo legal) 1 reportero (comunicaciones) 1 analista financiero	2 abogados (apoyo legal) 2 reporteros (comunicaciones) 1 analista financiero 1 personal de marketing

Fuente: ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

Implementar la etapa de ejecución del CSIRT es el siguiente paso una vez aprobado por la junta de Platino Sistemas el modelo administrativo. Este modelo se convierte en un pilar más en conjunto con el legal y el financiero, convirtiéndose junto a estos dos últimos en los cimientos en los que se desarrollaría el servicio de la organización. Es así, que aquí se deja un boceto con las actividades y el tiempo que tomaría el desarrollo de la siguiente etapa posterior al desarrollo de este modelo administrativo.

Tabla 22 Etapas de implementación del CSIRT Platino Sistemas

	NOMBRE	DURACIÓN	PREDECESORES
01	Obtener las aprobaciones necesarias	60 días	
02	Conseguir las instalaciones	20 días	01
03	Contratar los recursos humanos	40 días	02
04	Capacitar los recursos humanos	60 días	03
05	Adquirir la infraestructura tecnológica	40 días	04
06	Implementar infraestructura tecnológica	20 días	05

07	Definir plan de comunicación y dispersión	40 días	04
08	Ejecutar plan de comunicación y Dispersión	20 días	01
09	Definir políticas, procesos y procedimientos	20 días	03
10	Comienzo de la operación	0 días	06 – 07 - 09

Fuente: ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

Adquirir la infraestructura tecnológica debe ser una parte fundamental del mismo proyecto, ya que estos van a ser los dispositivos y sistemas de información con los que el equipo de respuesta a incidentes de seguridad computacional de Platino Sistemas va a responder por el desarrollo de sus actividades. Por lo cual una infraestructura recomendada para el inicio del proyecto podría ser.

- **Servidor Web:** Aquí estará almacenada el portal institucional del CSIRT Platino Sistemas, en esta página se puede encontrar la información no sensible de la entidad.

- **Servidor de Correo:** Este servidor se encargará de uno de los medios de comunicación del CSIRT Platino Sistemas, y almacenará los buzones de correos electrónico propios del CSIRT.

- **Servidor Intranet:** Este servidor tendrá información relevante para todo el equipo, sin que la misma sea pública, puede almacenar las técnicas de respuesta a incidentes, así como las mejores prácticas, manuales de operación, documentación de interés y la trazabilidad de los incidentes.

- **Servidor de archivos:** Este servidor puede ser utilizado para almacenar los archivos importantes de la compañía a los que se debería tener una copia de respaldo de la información.

- **Copias de seguridad de los servidores:** este servidor o sistema de copias de respaldo de la información, tiene como función crear un backup de respaldo de la información propia del CSIRT Platino Sistemas y de las estaciones de

trabajo si así se considera necesario. De igual forma cumplir con la política de mantener una copia de respaldo extra fuera del mismo servidor.

- **Servidor DNS:** Este servidor es el encargado de la resolución de nombres y el enrutamiento del CSIRT Platino Sistemas.

- **Servidor de Monitoreo:** Este servidor es el encargado de realizar el monitoreo activo de los sistemas, así como el monitoreo de la infraestructura de los clientes que tengan este servicio con nosotros. Así mismo este servidor entregará la información para los tableros de control visibles para el personal del CSIRT.

- **Servidor de recolección y correlación de eventos:** Este servidor permite realizar la correlación de eventos y los registros de las transacciones propias de los diferentes sistemas del CSIRT Platino Sistemas desplegados en la red propia interna o red de los clientes, con el fin de encontrar patrones de comportamientos similares.

- **Registro de seguimientos e incidentes:** Este servidor es el corazón de toda la infraestructura tecnológica, aquí se tendrá el registro y seguimiento de los incidentes propios del CSIRT Platino Sistemas, así como los otros que se den en diferentes CSIRT y sean comunicados. También funciona como una KDB (Base de datos de conocimiento, por sus siglas en inglés). Así como cada respuesta dada a los incidentes.

- **Estaciones de trabajo:** El personal de CSIRT debe contar con estaciones de trabajo (Desktop, portátiles o Workstation) que utilicen exclusivamente para las funciones de trabajo y que cumplan con GPO propias y que cuenten con DLP (prevención de pérdida de información, por sus siglas en inglés).

- **Teléfonos:** CSIRT Platino Sistemas, debe contar servicios de telefonía fija, telefonía IP, telefonía celular, que permita la comunicación oportuna y efectiva entre los miembros del CSIRT Platino Sistemas a través de llamadas locales, nacionales e internacionales según la dimensión de la operación.

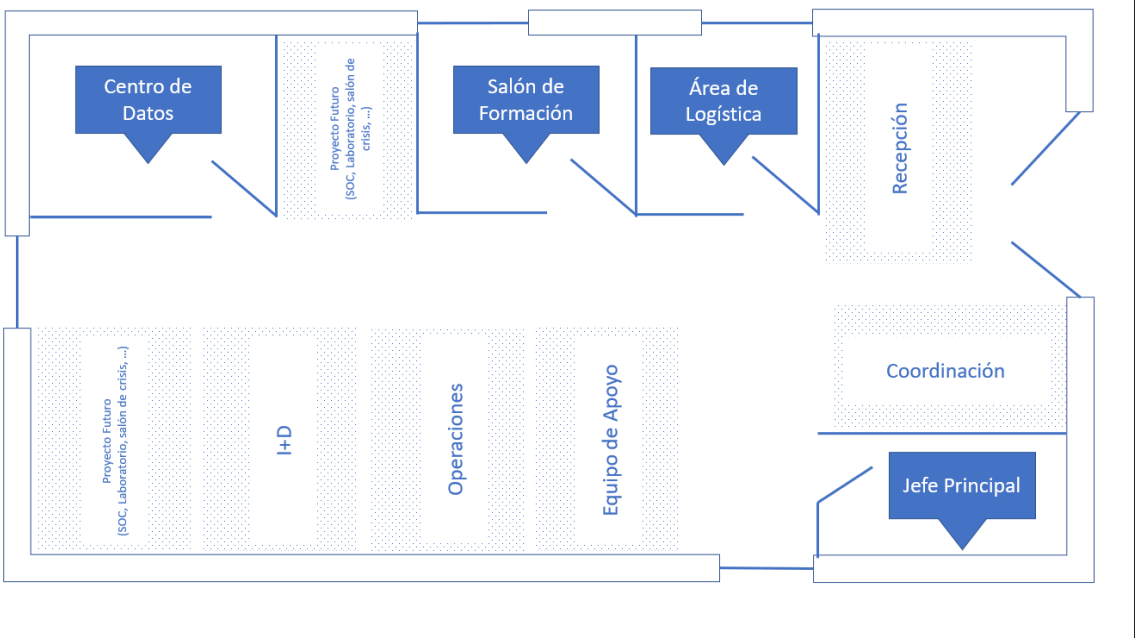
- **Trituradoras de papel:** CSIRT Platino Sistemas debe contar con trituradoras de papel que le permitan eliminar información sensible impresa o en CD (Discos compactos, por sus siglas en inglés). La destrucción de esta

información debe ser realizada por el personal de CSIRT Platino Sistemas, de acuerdo a la política de destrucción de información.

Considerar las instalaciones, las cuales deben permitir tener espacios para la ampliación de equipos o partes de los mismos en proyección de hacer al CSIRT Platino Sistemas mucho más grande y robusto, con el fin que tenga su propio equipo de investigación y desarrollo (I+D) como equipo independiente, así como poder llegar a tener un SOC (Centro de operaciones de seguridad, por sus siglas en inglés).

A continuación, se propone una división de las instalaciones del CSIRT Platino Sistemas:

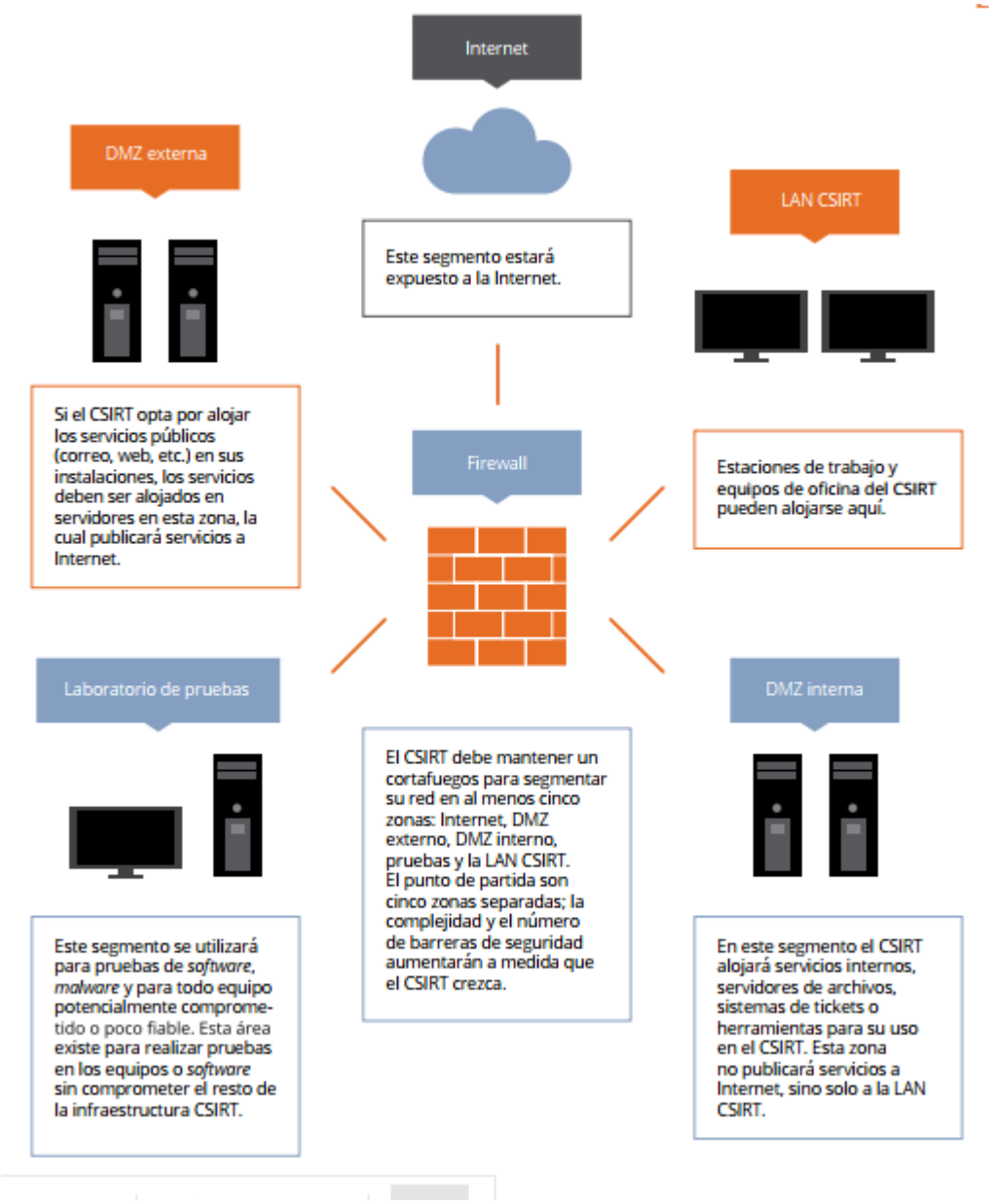
Figura 8 Plano de distribución de planta física CSIRT Platino Sistemas



Fuente: Propia, basado en imagen de ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

Establecer un diseño de la red que debería tener CSIRT Platino Sistemas de manera general, a fin de que pueda mantener diferenciado lo que expone en internet y es público de sus dispositivos de configuración propios que no deben ser expuestos.

Figura 9 Configuración de red de CSIRT Platino Sistemas



Fuente: ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

BIBLIOGRAFÍA

[1] ABRIL, Ana., PULIDO, Jarol A. y BOHADA John A. Análisis de riesgo en seguridad de la información. *Ciencia, innovación y tecnología (RCIYT)* [en línea]. 2013, enero – diciembre. vol. 1, p. 39 -53. [consultado 14 de diciembre 2020] ISSN: 2422-0264. Disponible en Internet: https://revista.jdc.edu.co/index.php/rciyt/article/view/121

[2] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMCIÓN – ENISA. Cómo crear un CSIRT paso a paso [en línea]. 2006. Consultado 18 de octubre de 2020. Disponible en Internet: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

[3] ANDRADE P., Roberto. Diseño y dimensionamiento de un equipo de respuesta ante Incidentes de Seguridad Informática (CSIRT) para la Escuela Superior Politécnica del Ejército. [en línea] Tesis de Maestría. Escuela Politécnica del Ejercito. 2013. [consultado 19 de octubre 2019] Disponible en Internet: http://repositorio.espe.edu.ec/handle/21000/6953

[4] ARMAS M., Hernán. Gestión de seguridad en la red de datos de la Corte Constitucional mediante el diseño de un CSIRT (Equipo de respuesta a incidentes de seguridad). Tesis de pregrado. Universidad Politécnica Salesiana 2020. [consultado 20 de octubre 2019] Disponible en Internet: http://dspace.ups.edu.ec/handle/123456789/3776

[5] ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD. [diapositivas] La Ciberseguridad como parte del nuevo paradigma de la seguridad. [en línea]. 3 de junio 2020. p. 28. [consultado 28 de noviembre 2020]. Disponible en Internet: https://www.aesseguridad.es/documentacion/GRUPO_TRABAJO_Ciberseguridad_web_v2.pdf

[6] BOLSA DE VALORES DE COLOMBIA, BOLETÍN INFORMATIVO No. 218. [en línea]. 07 de julio 2020, BOGOTÁ D.C. p. 1-36. [consultado 16 de noviembre de 2020]. Disponible en Internet: https://www.bvc.com.co/pps/tibco/portalbvc/Home/Mercados/boletines?com.tibco.ps.pagesvc.action=updateRenderState&rp.currentDocumentID=1ebbd6af_1732a600d64_-52bbc0a84ca9&rp.attachmentPropertyName=Attachment&com.tibco.ps.pagesvc.targetPage=1f9a1c33_132040fa022_-78750a0a600b&com.tibco.ps.pagesvc.mode=resource&rp.redirectPage=1f9a1c33_132040fa022_-787e0a0a600b

[7] CAROZO B., Eduardo. Implantación del sistema de gestión de seguridad de la información en una empresa compleja. *Memoria de Trabajos de Difusión Científica y Técnica*. [en línea]. 2007. No. 5, p. 77-87. ISSN 1510-7450. [consultado 20 de octubre 2020]. Disponible en Internet: https://www.researchgate.net/publication/38290247_Implantacion_del_sistema_de_gestion_de_seguridad_de_la_informacion_en_una_empresa_compleja

[8] CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020 [en línea] 29 de octubre de 2019. Primera Edición. Bogotá D.C. p. 1 - 36. Disponible en Internet: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

[9] CHOI, Kyung y TORO A., Marlon. Cibercriminología, Guía para la investigación del Cibercrimen y mejores prácticas en seguridad digital. Bogotá D.C.: Universidad Antonio Nariño. 2017, 604 p. ISBN 978-958-8687-71-1.

[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”-… Diario Oficial Bogotá D.C., 2009 No. 47.223. p 1 – 4. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[11] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial Bogotá D.C., 2012 No. 48.587. p 1 – 301. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

[12] DE LA TORRE M., Hugo y PARRA R., Mario. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. Tesis de pregrado. Universidad de las Fuerzas Armadas ESPE. 2018. [consultado 19 de octubre 2020]. Disponible en Internet: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/15071/T-ESPE-040447.pdf?sequence=1&isAllowed=y

[13] ESET. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [sitio web] 18 de mayo de 2015 welivesecurity. [consulta: 15 de noviembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

[14] ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de

Notificación y Gestión de Ciberincidentes [en línea] 2019. p. 60 [consultado 15 de noviembre 2020]. Disponible en Internet: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

[15] ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Taxonomía de soluciones de ciberseguridad [en línea] 2015. p. 57 [consultado 30 de octubre 2020]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

[16] ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Clasificación de la Información, Política de Seguridad para la pyme [en línea] 2018. p. 7. [consultado 10 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

[17] ESPAÑA. MINISTERIO DE DFENSA. SECRETARÍA GENERAL TÉCNICA. Centro Criptológico Nacional. (septiembre 2011). Guía de Creación de un CERT/CSIRT, p. 60. NIPO: 075-11-053-3. Disponible en Internet: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

[18] ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Guía de borrado seguro de la información, una aproximación para el empresario [en línea] 2016. p. 12. [consultado 12 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

[19] FUERTES, Walter. *et al.* An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. *Systems.* [en línea] 2017. Vol. 5, Artículo 52. ISSN. 2079-8954 Disponible en Internet https://doi.org/10.3390/systems5040052

[20] GÓMEZ H., Marcos. Ciberseguridad y protección en la red: los CERTs/CSIRTs. *Dialnet.* [en línea]. 2014. p. 81 – 106. [consultado 14 de diciembre 2020]. ISBN 978-84-290-1776-2. Disponible en Internet: http://dialnet.unirioja.es/servlet/articulo?codigo=4969962

[21] GROBLER, Marthie y BRYK, Harri. "Common challenges faced during the establishment of a CSIRT," *Conference: Information Security for South Africa, Sandton, Johannesburg*, [en línea]. 2010. p. 1-6. Disponible en Internet: http://dx.doi.org/10.1109/ISSA.2010.5588307.

[22] INCIBE, ¿Qué son y para qué sirven los SIEM, IDS e IPS?, [En línea], septiembre 2020, [Consultado 08 de octubre de 2022]. Disponible en Internet: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

[23] ISOTOOLS EXCELLENCE. ISO 27001: Aspectos claves de su diseño e implementación, [En línea], www.isotools.org s.f. 23 p. [Citado 15 de abril 2019] Disponible en Internet: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

[24] MALAGÓN, Chelo. Organización y operación de un CSIRT, [Diapositivas] [En Línea]. Galicia – España. Universidad de Santiago de Compostela. II Foro de Seguridad de Red IRIS. 25 y 26 de marzo de 2004. p. 81. Disponible en Internet: https://www.rediris.es/cert/doc/reuniones/fs2004/archivo/csirt.pdf

[25] MUÑOZ, Mirna y RIVAS, Lizbeth. Estado actual de equipos de respuesta a incidentes de seguridad informática. *Revista Ibérica de Sistemas y Tecnologías de la Información RISTI*. [en línea] 2015, No. Especial 3. p.1-15. [consultado 10 de septiembre 2021.] ISSN 1646–9895. Disponible en Internet: http://dx.doi.org/10.17013/risti.e3.1-15.

[26] NASERI, Ali y AZMOON, Omid. Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran. *International Journal of Computer Science Issues*. [en línea] 2012, Vol. 9 p. 1 – 5. [consultado 15 de septiembre 2021]. ISSN: 1694–8114. Disponible en Internet: https://www.researchgate.net/publication/268347788_Proposition_of_Model_for_CSIRT_Case_Study_of_Telecommunication_Company_in_a_Province_of_Iran/download

[27] NEIRA, Francisco. Creación de un equipo de respuesta a incidentes de seguridad Informática: Un proceso para empezarlo. (s.f.p) traducción no oficial con el permiso especial del instituto de Ingeniería de Software de la Universidad Carnegie Mellon, EE.UU. p. 10 [consultado 19 de octubre 2020]. Disponible en Internet: https://csirtpe.files.wordpress.com/2013/06/crearuncsirt-final.pdf

[28] ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

[29] Olivares O., Jorge. Estableciendo un ecosistema de CSIRT sectoriales para la Industria 4.0, *Revista electroindustria* [en línea]. Universidad Nacional

Autónoma de México. 05 de marzo de 2013. Nro. 16. [consultado 14 de diciembre 2020] Disponible en Internet: https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-inform%C3%A1ticos-para-qu%C3%A9

[30] PÉREZ E. Ernesto, y BERNAL B. Paul F. Estableciendo un CSIRT [en línea] 2020 Traducción al español de Van der Heide, Martjin "*Establishing a CSIRT*" con el apoyo de ThaiCERT y ETDA, p. 45. [consultado 18 de octubre 2020]. Disponible en Internet. https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf

[31] RAMÍREZ L., Heltton y MEJÍA M., Jezreel. Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). *ReCIBE Revista de computación, informática, biomédica y electrónica* [en línea] 2015. Año 4 No. 1. p. 1–17. [consultado 19 de octubre 2020]. E-ISSN: 2007-5448 Disponible en Internet: https://www.redalyc.org/articulo.oa?id=512251501006

[32] REYES-MENA, Francisco. X. *et al*. Aplicación de Inteligencia de Negocios para el análisis de vulnerabilidades en pro de incrementar el nivel de seguridad en un CSIRT académico. *Revista Facultad de Ingeniería* [en línea]. 2018. Tunja – Boyacá, Colombia. Vol. 27 No. 47. p. 21–29. [consultado 17 de octubre 2019] ISSN Online 2357-5328 [versión en inglés]. DOI: http://doi.org/10.19053/01211129.v27.n47.2018.7747

[33] WEST-BROWN, Moira J. *et al.* Handbook for Computer Security Incident Response Teams (CSIRTs). EE.UU. Universidad Carnegie Mellon. Instituto de Ingeniería de Software. 1998. 223 p. Consultado el 18 de octubre de 2021. Disponible en Internet: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

[34] URIBE R. Edgar F. Proceso para la definición de servicios iniciales en un Equipo de Respuesta ante incidencias de seguridad Informática. Tesis de maestría. Centro de Investigación en Matemáticas A. C. - CIMAT 2016. [consultado 14 de diciembre 2020] Disponible en Internet: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/442/1/ZACTE47.pdf

[35] UNIVERSIDAD CARNEGIE MELLON. CSIRT SERVICES [en línea] 2002. Instituto de Ingeniería de Software. p. 12. [consultado 21 de agosto 2021]. Disponible en internet: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

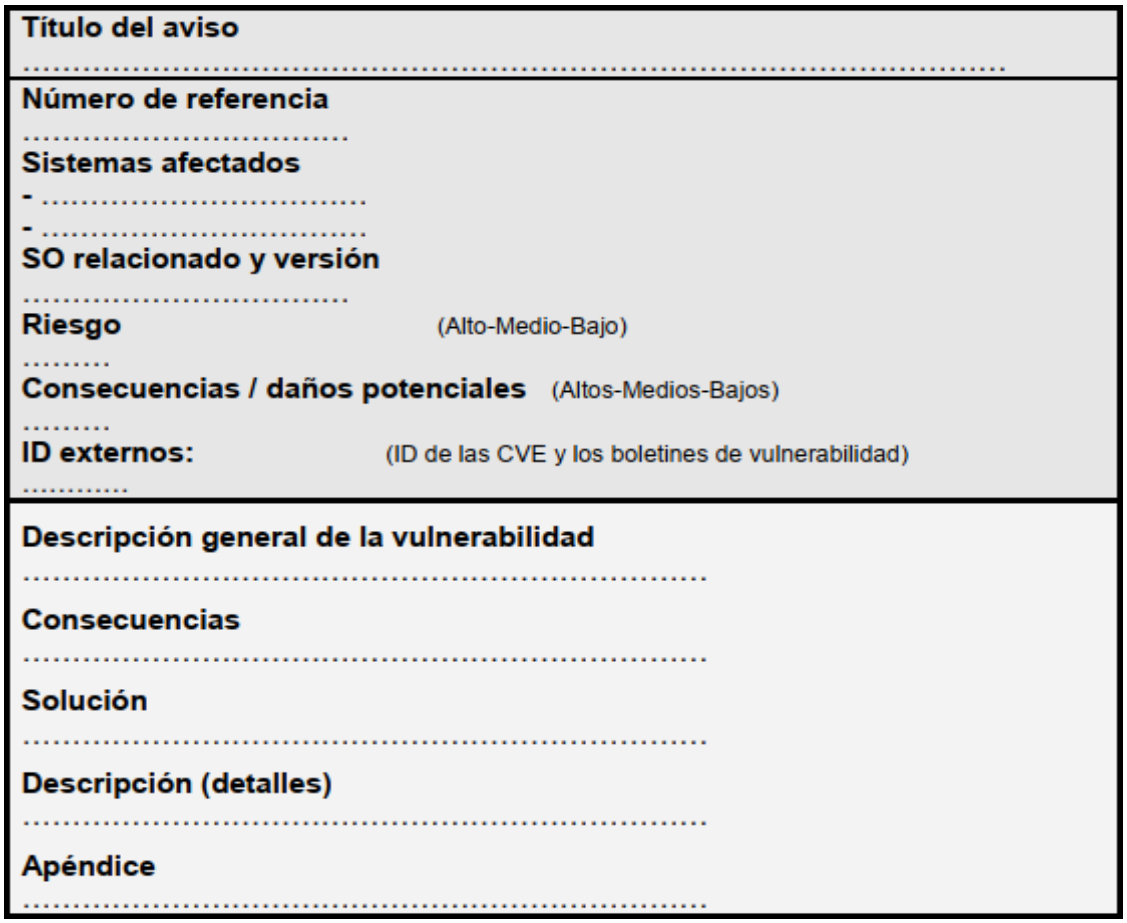
ANEXOS

INFORMACIÓN DE UN AVISO DE UN CSIRT

Los avisos de seguridad distribuidos por un CSIRT deberían seguir siempre la misma estructura, para mejorar la legibilidad y permitir que el lector encuentre rápidamente la información pertinente.

Un aviso debe contener, como mínimo, la información siguiente:[27]

Figura 10 Ejemplo de proyecto de un Aviso



Fuente: Elaboración propia con base en la guía de la AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMCIÓN – ENISA. Cómo crear un CSIRT paso a paso [en línea]. 2006. [consultado 18 de octubre de 2020]. Disponible en Internet: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

[27] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMCIÓN, Op. Cit., p. 48

ACTA DE CLAUSULA DE CONFIDENCIALIDAD

Figura 11 Acta de Confidencialidad CSIRT Platino Sistemas

LOGO DE PLATINO SISTEMAS	ACTA DE CONFIDENCIALIDAD PARA EL CIRST DE PLATINO SISTEMAS

IDENTIFICACIÓN DEL CLIENTE
NOMBRE DE LA SOCIEDAD: XXXXXXXXXXXXX
NIT.: XXXXXXXXXXXXX
REPRESENTANTE LEGAL: XXXXXXXXXXXXX
NÚMERODE IDENTIFICACIÓN: XXXXXXXXXXXXX
CONTRATO DE FIDUCIA MERCANTIL No: XX de XX

CLAÚSULAS
PRIMERA. PLATINO SISTEMAS se obliga a no divulgar a terceras partes, la "**Información confidencial**", que reciba por parte del CLIENTE_____ , y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad. Para efectos de la presente acta, "Información Confidencial" comprende toda la información divulgada por _____ ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora.
SEGUNDA. PLATINO SISTEMAS se obliga a mantener de manera confidencial la "**Información confidencial**" que reciba de _____ y a no darla a una tercera parte diferente de su equipo de trabajo y asesores que tengan la necesidad de conocer dicha información para los propósitos autorizados, y quienes deberán estar de acuerdo en mantener de manera confidencial dicha información.
TERCERA. Es obligación de PLATINO SISTEMAS no divulgar la "**Información confidencial**", incluyendo, mas no limitando, el informar a sus empleados que la manejen, que dicha información es confidencial y que no deberá ser divulgada a terceras partes.
CUARTA. PLATINO SISTEMAS se obliga a utilizar la "**Información confidencial**" recibida, únicamente para el desarrollo el objeto del contrato de fiducia mercantil suscrito con el cliente _____.
QUINTA. PLATINO SISTEMAS se compromete a efectuar una adecuada custodia y reserva de la información y gestión -es decir tratamiento- de los datos suministrados por el cliente _____ al interior de las redes y basesde datos (físicas y/o electrónicas) en donde se realice su recepción y tratamiento en general.
SEXTA. Para el caso del manejo de información que incluya datos personales, el PLATINO SISTEMAS dará estricto cumplimiento a las disposiciones constitucionales y legales sobre la protección del derecho fundamental de habeas data, en particular lo dispuesto en el artículo 15 de la Constitución Política y la ley 1581 de 2012.
SÉPTIMA. En caso de que el PLATINO SISTEMAS incumpla parcial o totalmente con las obligaciones establecidas en la presente acta éste será responsable de los daños y perjuicios que dicho incumplimiento llegase a ocasionar a al cliente _____.
OCTAVA. La vigencia de la presente acta será indefinida y permanecerá vigente mientras exista relación receptora, se hará acreedora a la Pena Convencional establecida en la Cláusula Séptima del presente Contrato.

Suscrita a los XXX días del mes de XXXX de 2022, en Bogotá D.C.

Firma:

XXXXXXXXXXXXXCSIRT PLATINO SISTEMAS

Fuente: Propia

RESUMEN ANALÍTICO ESPECIALIZADO – RAE

Tema:	Seguridad Informática - CSIRT
Título:	Diseño documental de un centro de respuesta a incidentes cibernéticos que ***Platino Sistemas*** pueda ofrecer como servicio a sus clientes
Autor(es):	Jiménez Cano John Andrés
Año:	2022
Resumen:	
Palabras Claves:	CSIRT, Magerit, ISO 27001, Incidentes Informáticos, taxonomía
Contenidos:	**DISEÑO DOCUMENTAL DEL CSIRT DE PLATINO SISTEMAS** • Campo de Acción CSIRT de Platino Sistemas • Taxonomía de Incidentes de Seguridad CSIRT • Servicios de Platino Sistemas • Requisitos y Perfiles del Equipo de Trabajo para la Conformación de CSIRT Platino Sistemas • Políticas, Procesos, Procedimientos, Manuales e Instructivos basados en la norma ISO/IEC 27000
Descripción del Problema:	En el mundo y en Colombia muchas compañías hablan de sistemas de gestión de seguridad tecnológica, de seguridad informática, de seguridad de la información, y todo aquello para que la compañía sea menos vulnerable a los incidentes informáticos y cibernéticos. Sin embargo, la seguridad no es algo 100% resuelto y más aún en este mundo informático en que por cada ataque o incidente que se detiene o frustra, aparecen a diario 10 formas nuevas de realizarlo. Y es que en la actualidad muchos de estos ataques no son ejecutados por personas, son personas que programan cientos o miles de máquinas que pueden lanzar un ataque a gran escala concurrentemente en cuestión de segundos. Y dichos ataques cada vez son más intrincados y más difíciles de detectar para las personas que están tratando de proteger la seguridad en una empresa. La empresa Platino Sistemas, es una empresa colombiana que se enfoca en los servicios de seguridad para la protección de la información, y que durante los últimos años ha sido consciente de esta problemática en Colombia, ha visto el incremento de diferentes incidentes cibernéticos en el país y en sus clientes en particular, lo que ha dado paso a Platino Sistemas a pensar en cómo ayudar a su clientes y a otras compañías en el país en la mitigación de estos incidentes informáticos y en la reducción de sus brechas de seguridad. Cómo ofrecer un servicio de ayuda proactivo y reactivo que brinde atención y soporte ante estos eventos las empresas del territorio nacional, ya sea bien para dar respuesta a estos incidentes o gestionando las vulnerabilidades en la infraestructura tecnológica que los mismos puedan tener en sus empresas. Aunque no existe la forma de asegurar todo completamente, Platino Sistemas busca ayudar a todas estas empresas, desde las que se encuentran certificadas en la norma ISO/IEC 27001, hasta las que no han empezado o no conocen la norma. Así como, a las empresas que conocen cómo actuar ante un incidente de ciberseguridad materializado como a las que no tienen idea de por qué les pasó. Platino Sistemas quiere entregar a sus clientes el servicio que ayude a mitigar los incidentes de seguridad que se puedan dar, o simplemente definir algunas políticas de seguridad

	dependiendo del tamaño de la empresa para que puedan mitigar sus vulnerabilidades y así salvaguardar su información. Platino Sistemas quiere implementar este servicio, que permitiría a los clientes contar con un Equipo de respuesta ante los incidentes de seguridad informática, que les brinde la oportunidad de tener medios con los cuales sus organizaciones puedan identificar, medir y corregir el impacto de un incidente de seguridad que se pueda presentar o se haya presentado. Para lograr este CSIRT, Platino Sistemas ha pedido a su equipo de trabajo crear el diseño documental que permita el desarrollo de las actividades propias de este nuevo servicio, por lo cual es necesario conocer todos aquellos apartes que componen el diseño documental para crear el CSIRT dentro de la empresa y preguntarse: ***¿Qué se necesita para crear el diseño documental de un equipo de respuesta de incidentes de seguridad informática – CSIRT en la organización Platino Sistemas que cumplan con las normativas vigentes y pueda brindar un servicio de calidad para los clientes de la organización?***
Objetivos:	**OBJETIVOS GENERALES** Construir un diseño documental que permita el desarrollo de las actividades propias del CSIRT para la organización Platino Sistemas. **OBJETIVOS ESPECÍFICOS** • Establecer el campo de acción del CSIRT dónde se estructure el entorno (clientes) del CSIRT como servicio de la empresa Platino Sistemas con base al panorama actual de la ciberseguridad en Colombia. • Estructurar la taxonomía de los incidentes de seguridad del CSIRT de acuerdo a los ataques más presentados en el panorama actual de ciberseguridad en Colombia. • Integrar los servicios de Platino Sistemas en Proactivos, reactivos y complementarios que serán parte del CSIRT, y que la organización Platino Sistemas puede ofertar a sus clientes. • Construir las políticas, procesos y procedimientos operacionales, manuales e instructivos basados en la norma ISO/IEC 27000 para verificar el estado de obligatorio cumplimiento por parte de los clientes para definir el grado de responsabilidad del CSIRT
Metodología:	Investigación cualitativa, por medio de la cual se colectaron los datos en los sitios de las comunidades internacionales y nacionales que existen actualmente tales como colCERT, http://www.colcert.gov.co/, o el foro de equipos de seguridad y respuesta a incidentes FIRST http://www.first.org/
Conclusiones:	Las políticas, procesos y procedimientos del CSIRT Platino Sistemas, se construyeron en su fase inicial. Estas políticas se hicieron bajo la normativa ISO/IEC 27001 para dar gestión de forma eficiente y oportuna a los incidentes de los clientes del CSIRT y aportan como el punto de partida de la construcción de una base de conocimiento en las acciones pre, durante

	y post incidente. Estas políticas están complementadas por los procesos y procedimientos que se establecieron de forma general para las infraestructuras de hardware y software que puedan tener los clientes a través de un enfoque administrativo empresarial. CSIRT Platino Sistemas puede ofrecer estos servicios a empresas grandes, medianas o pequeñas que deleguen la tercerización de su seguridad informática. De esta forma el campo inicial de acción de CSIRT Platino Sistemas ha de ser comercial. Brindando así el acompañamiento en la prevención, detección y gestión de incidentes a sus clientes. Empezando por un enfoque amplio, y acotando su campo de acción en concordancia con aquellos que estén brindando rentabilidad. Reduciendo sectores o manteniendo los clientes que brinden ganancias a la empresa. La taxonomía que emplea CSIRT Platino Sistemas está definida con base en los ataques reconocidos a nivel mundial por los diferentes equipos de respuesta a ataques cibernéticos. Interiorizar esta taxonomía permite que se hable el mismo idioma a la hora de exponer, divulgar y retroalimentar los ataques que se puedan presentar. De esta forma, al ser parte de la red de CSIRT de los cuales Platino Sistemas hace parte le permite realizar el análisis de los incidentes sin empezar desde el principio, sino contando con una jerga y un conocimiento amplio que le puede ser compartido desde el exterior. Como resultado del proyecto, se establece que CSIRT Platino Sistemas debe empezar por ofrecer los servicios básicos, propios de todo CSIRT y recurrentes en los mismos grupos a nivel internacional. Estos servicios son siete (7) servicios proactivos, cuatro (4) servicios reactivos y seis (6) servicios complementarios. Sin embargo, el nivel inicial de maduración de CSIRT permitirá que estos servicios evolucionen con el tiempo, dando pasos a diferentes y nuevos servicios que dejen su propia huella en los clientes y ayuden a acrecentar su portafolio de servicios hacía nuevos clientes en la solución integral de incidentes. El cumplimiento de estos objetivos, permite que se elabore un diseño documental adecuado para el desarrollo de las actividades propias de un CSIRT para la empresa Platino Sistemas, este diseño solo comprende la etapa de planificación del CSIRT, estableciendo los cimientos del nuevo servicio de la compañía, cabe aclarar que para llegar a la construcción completa del CSIRT se ha de pasar por las etapas de Ejecución y producción. La realización de este diseño documental, identificó que un CSIRT es una parte fundamental de la seguridad informática, y que toda empresa debe contar con uno como parte de sus buenas prácticas hacía un SGSI (Sistema de gestión de seguridad de la información). Ya sea propio o tercerizado, este servicio permite contar con aliados estratégicos que nos mantienen informados sobre los incidentes de seguridad de la información en el planeta de las tecnologías. Platino Sistemas puede contar con este servicio como parte de su portafolio de servicios de seguridad de la información que brinda a sus clientes y como uso propio interno. Ofreciendo servicios que permitan dar soporte a

	sus clientes teniendo presente el nivel de servicio contratado los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades

Fuentes bibliográficas destacadas:

ABRIL, Ana., PULIDO, Jarol A. y BOHADA John A. Análisis de riesgo en seguridad de la información. *Ciencia, innovación y tecnología (RCIYT)* [en línea]. 2013, enero – diciembre. vol. 1, p. 39 -53. [consultado 14 de diciembre 2020] ISSN: 2422-0264. Disponible en Internet: https://revista.jdc.edu.co/index.php/rciyt/article/view/121

AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMCIÓN – ENISA. Cómo crear un CSIRT paso a paso [en línea]. 2006. Consultado 18 de octubre de 2020. Disponible en Internet: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

BOLSA DE VALORES DE COLOMBIA, BOLETÍN INFORMATIVO No. 218. [en línea]. 07 de julio 2020, BOGOTÁ D.C. p. 1-36. [consultado 16 de noviembre de 2020]. Disponible en Internet: https://www.bvc.com.co/pps/tibco/portalbvc/Home/Mercados/boletines?com.tibco.ps.pagesvc.action=updateRenderState&rp.currentDocumentID=1ebbd6af_1732a600d64_-52bbc0a84ca9&rp.attachmentPropertyName=Attachment&com.tibco.ps.pagesvc.targetPage=1f9a1c33_132040fa022_-78750a0a600b&com.tibco.ps.pagesvc.mode=resource&rp.redirectPage=1f9a1c33_132040fa022_-787e0a0a600b

CCIT. Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020 [en línea] 29 de octubre de 2019. Primera Edición. Bogotá D.C. p. 1 - 36. Disponible en Internet: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

CHOI, Kyung y TORO A., Marlon. Cibercriminología, Guía para la investigación del Cibercrimen y mejores prácticas en seguridad digital. Bogotá D.C.: Universidad Antonio Nariño. 2017, 604 p. ISBN 978-958-8687-71-1.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial Bogotá D.C., 2012 No. 48.587. p 1 – 301. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

ESET. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [sitio web] 18 de mayo de 2015 welivesecurity. [consulta: 15 de noviembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciberincidentes [en línea] 2019. p. 60 [consultado 15 de noviembre 2020]. Disponible en Internet: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Taxonomía de soluciones de ciberseguridad [en línea] 2015. p. 57 [consultado 30 de octubre 2020]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Clasificación de la Información, Política de Seguridad para la pyme [en línea] 2018. p. 7. [consultado 10 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

ESPAÑA. INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Guía de borrado seguro de la información, una aproximación para el empresario [en línea] 2016. p. 12. [consultado 12 de noviembre 2021]. Disponible en Internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

MEJÍA M., Jezreel, MUÑOZ, Mirna y URIBE, Edgar. Establecimiento de Servicios en Equipos de Respuesta ante Incidentes de Seguridad Informática: Una Revisión del Estado del Arte. (En español). Conferencia Ibérica de Sistemas y Tecnologías de la Información, CISTI. vol. 1, pp. 1033–1038, 2015. Disponible en Internet: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=aci&AN=114061193&lang=es&site=eds-live&scope=site

NASERI, Ali y AZMOON, Omid. Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran. *International Journal of Computer Science Issues*. [en línea] 2012, Vol. 9 p. 1 – 5. [consultado 15 de septiembre 2021]. ISSN: 1694–8114. Disponible en Internet: https://www.researchgate.net/publication/268347788_Proposition_of_Model_for_CSIRT_Case_Study_of_Telecommunication_Company_in_a_Province_of_Iran/download

ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). Buenas Prácticas para establecer un CSIRT nacional. [en línea]. Washington D. C. abril de 2016, EE.UU. p 1-55, [consultado 10 de noviembre 2020] Disponible en Internet:

https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

PÉREZ E. Ernesto, y BERNAL B. Paul F. Estableciendo un CSIRT [en línea] 2020 Traducción al español de Van der Heide, Martjin "*Establishing a CSIRT*" con el apoyo de ThaiCERT y ETDA, p. 45. [consultado 18 de octubre 2020]. Disponible en Internet. https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf

UNIVERSIDAD CARNEGIE MELLON. CSIRT SERVICES [en línea] 2002. Instituto de Ingeniería de Software. p. 12. [consultado 21 de agosto 2021]. Disponible en internet: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf