METODOLOGÍA PARA LA IDENTIFICACIÓN DE INDICADORES DE COMPROMISO PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Trabajo Fin de Máster

Autores: Miguel Andrés Ávila y María Liliana Granada

Tutor: Manuel Sánchez Rubio

Máster en Ciberdefensa

MCD

Universidad de Alcalá

fundación IN-NOVA Centro de Innovación

Trabajo Fin de Máster
Metodología para la identificación de indicadores de compromiso para la protección de infraestructuras críticas

Autores: Miguel Andrés Ávila y María Liliana Granada
Tutor: Manuel Sánchez Rubio

Fecha de Presentación: Abril 2018
Máster en Ciberdefensa
Universidad de Alcalá

CONTENIDO

1. RESUMEN

Cada día las naciones y sus infraestructuras críticas son más dependientes de las Tecnologías de Información y Comunicaciones, las cuales a su vez son más complejas de implementar y mantener y esta complejidad lleva a que se presenten fallos de configuración y vulnerabilidades de seguridad que podrían ser potencialmente explotados por hackers, organizaciones cibercriminales, países enemigos, etc. para generar caos, desestabilización y problemas económicos y de seguridad nacional. Existen varias metodologías desarrolladas por fabricantes de tecnologías de seguridad, para la identificación y establecimiento de indicadores de compromiso – IoC en infraestructuras de TIC sin embargo, la definición por si sola de IoC desde el punto de vista técnico no es suficiente para garantizar una reducción del riesgo de ataque e incrementar la protección de infraestructuras críticas. Este trabajo de grado tiene como objetivo proponer una metodología para la identificación de IoC para la protección de infraestructuras críticas no con el enfoque técnico que proponen los fabricantes de tecnologías de seguridad, sino con un énfasis más estratégico orientado a proteger los procesos de negocio que soportan las infraestructuras críticas.

Palabras Claves: Metodologia IoC, Indicadores de Compromiso, Ciberseguridad.

ABSTRACT

Every day, nations and their critical infrastructures are more dependent on Information and Communication Technologies, which in turn are more complex to implement and maintain, and this complexity leads to configuration failures and security vulnerabilities that could potentially arise. exploited by hackers, cybercriminal organizations, enemy countries, etc. to generate chaos, destabilization and economic problems and national security. There are several methodologies developed by security technology manufacturers for the identification and establishment of IoC commitment indicators in ICT infrastructures; however, the technical definition of IoC alone is not enough to guarantee a reduction of the IoC. attack risk and increase the protection of critical infrastructure. The purpose of this degree project is to propose a methodology for the identification of IoC for the protection of critical infrastructures, not with the technical approach proposed by the manufacturers of security technologies, but with a more strategic emphasis aimed at protecting the business processes that support the critical infrastructures.

Key Words: IoC Methodology, Indicators of Commitment, Cybersecurity.

2. INTRODUCCIÓN

Actualmente vivimos una era en la cual la información va de la mano de la tecnología, por ello, la población en general puede acceder a una gran cantidad de información en tan solo unos pocos segundos, sin importar la distancia que separe a un país de otro. Así mismo, no solo el flujo de información ejerce el control en una sociedad cada vez más globalizada, también es importante tener en cuenta la tecnificación de bienes y servicios que ahora funcionan por medio de computadoras a través del "ciberespacio" término acuñado por William Gibson en su novela Neuromante 1984, dando a entender este, como "Espacio virtual creado con medios cibernéticos".

Todo este proceso evolutivo de ideas en el área de la Computación ha servido para facilitar las tareas cotidianas del ser humano, llegando al punto de observar la virtualidad convertida en una "realidad", escenario que en la actualidad se ha transformado en el quinto dominio de la guerra "El Ciberespacio", por medio del cual a través del desarrollo de software[1] se logra contemplar un conjunto de órdenes, programas o instrucciones informáticas, las cuales sirven para ejecutar ciertas tareas en una computadora, con el fin de aprovechar brechas de seguridad, que permitan tomar el control de la misma y de esta forma obtener ventaja de los sistemas comprometidos.

Esto se apoya en lo que hoy conocemos como la "cibernética", definida según Norbert Wiener 1948, como "el control y comunicación en el animal y en la maquina", dando paso a un nuevo campo de acción para los delincuentes en el que se pueden efectuar robos, ataques e incluso "ciberguerras" descritas según Richard Clarke, como "conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar prejuicio o alteración".

Lo anterior nos hace pensar en que a nivel Estado es importante proteger las Infraestructuras Estratégicas soportadas por las tecnologías de información y comunicaciones o tecnologías operacionales, cuyo funcionamiento es indispensable para las personas, por lo que su destrucción o sabotaje tendría un grave impacto sobre los servicios esenciales, con los que cuenta un País.

En el comienzo de este avance tecnológico no se visualizaba que el malware pudiera efectuar daños a equipos físicos, debido a que el nacimiento de virus, gusanos, troyanos, entre otros, estaba enfocado a la modificación o destrucción de datos, aplicaciones, imágenes, etc… pero a medida que se expandió el auge de nuevas tecnologías y la facilidad que brindan en los procesos industriales, este paradigma se destruyó, haciendo posible que en la actualidad se conozcan algunos casos de ataques a sistemas físicos, ejemplos que se escuchan como una lección aprendida en la protección de las Infraestructuras Criticas Cibernéticas (ICC), dando inicio a lo que hoy se conocen como ciberataques, los cuales utilizan un gran número de

[1] Real Academia Española. «Significado de la palabra Software». Diccionario de la Lengua Española, XXIIº Edición. Consultado el 15 de marzo de 2018.

recursos humanos, tecnológicos y económicos, para afectar la provisión de bienes y servicios públicos esenciales de un País (hospitales, aeropuertos, transporte, industrias químicas y nucleares, sistemas financieros, entre otros), comprometiendo la Seguridad Nacional y causando pérdidas económicas, físicas e incluso de vidas humanas.

Entre los varios ejemplos que se pueden mencionar, se encuentra el popular ataque del gusano informático Stuxnet, el cual en el 2010 rompió las centrifugas y las turbinas en las instalaciones de enriquecimiento nuclear de Irán, al tomar control de los controladores lógicos programables (PLC); lo preocupante de esto, es que en la actualidad existen miles de variaciones de diferentes tipos de malware, tales como: Duqu, Flame y Gauss, al igual que diferentes amenazas sofisticadas llamadas Armas Cibernéticas, las cuales podrían afectar las ICC de un País y generar caos interno entre sus habitantes, ocasionando mucho más daño que una bomba nuclear.

De acuerdo con el estudio de la empresa McAfee (McAfee Labs 2018 Threats Predictions Report)[2], se predice un crecimiento en el uso del Machine Learning para hacer que los ataques tengan un aprendizaje automático de los entornos y los objetivos para los que fueron creados, por tal razón, para defenderse de esto es importante crecer en los modelos de detección y corrección de errores, al igual que avanzar en la generación de capacidades defensivas más rápido de lo que un adversario puede intensificar un ataque, en este punto es vital conocer lo que está sucediendo en las redes y en los equipos a nivel organización, con el fin de detectar situaciones anómalas o inusuales que puedan alertar de una posible amenaza o actividad sospechosa dentro de las Infraestructuras Criticas.

Por lo anterior nace el término Indicadores de Compromiso (IOC), con el fin de describir un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones para ser identificado en una red o endpoint pudiendo mejorar así las capacidades ante la gestión de incidentes[3]; teniendo en cuenta que es importante cerrar la ventana de tiempo en la detección y respuesta ante un incidente, es necesario contar con una metodología que permita obtener una reacción efectiva, facilitando la contención, corrección y recuperación, ante un incidente cibernético.

[2] 'McAfee Labs 2018 Threats Predictions Report' Previews Five Cybersecurity Trends. Noviembre 29 del 2017. https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/

[3] IOCs, una palabra de moda, un tema caliente. Pero, ¿realmente conocemos sus capacidades? Marzo 25 de 2016. https://www.pandasecurity.com/spain/mediacenter/seguridad/iocs-y-sus-capacidades/

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Proponer una metodología para la identificación de IoC para la protección de infraestructuras críticas no con el enfoque técnico que proponen los fabricantes de tecnologías de seguridad, sino con un énfasis más estratégico orientado a proteger los procesos de negocio que soportan las infraestructuras críticas que ayuden a garantizar de manera proactiva la prevención, detección temprana y gestión de incidentes de seguridad a los activos críticos de información.

3.2. OBJETIVOS ESPECÍFICOS

Lograr a través del modelo propuesto, dar una orientación más estratégica a la definición de los Indicadores de Comrpomiso – IoC y no centrarse solamente en la descripción de las características técnicas de las evidencias de afectación de compromiso que deja una amenaza en un equipo o sistema de información comprometido; para esto se trabajará en la definición de los IoC, aspectos como:

1. Entender los flujos de información de las infraestructuras críticas.

2. Identificación de activos de información críticos según el flujo de información.

3. Clasificación de los tipos de ataque que afecten Integridad, Confidencialidad, Disponibilidad.

4. Definir casos de uso para la protección de los activos críticos.

4. FUNDAMENTACIÓN TEÓRICA. ESTADO DEL ARTE

Vivimos un nuevo escenario mundial, con una sociedad adicta y altamente dependiente de las tecnologías de la información y comunicaciones, las personas y las "cosas" está cada vez más conectadas al ciberespacio. Esta misma situación la viven las organizaciones públicas o privadas, locales, regionales o globales, donde la información corporativa es un habilitador fundamental a nivel estratégico para la priorización y la toma de decisiones, el desarrollo de las operaciones del negocio, la evaluación del rendimiento y el cumplimiento de las metas propuestas. Al mismo tiempo, el panorama actual del entorno de negocios, apalancado por el acelerado proceso de digitalización, el surgimiento de nuevas tendencias tecnológicas como la nube y el Internet de las cosas – IoT, la fuerte dependencia de las Organizaciones a las tecnologías TIC y las amenazas que surgen asociadas a las vulnerabilidades presentes intrínsecamente en estas tecnologías, generan un mayor riesgo de interrupción económica, social y física y aumenta la probabilidad de perdida de información crítica en todo su ciclo de vida útil, desde su creación hasta su archivo y/o destrucción,

Las organizaciones criminales con motivaciones económicas, grupos de terrorismo organizado con motivación política, ciudadanos malintencionados con intereses particulares, entendieron rápidamente la importancia del ciberespacio, el uso de las TICs, los grandes beneficios que les aporta en el desarrollo de sus actividades criminales y su expansión a nivel global y la posibilidad que tienen de someter a ciudades e incluso países explotando las vulnerabilidades tecnológicas de sus infraestructuras críticas.

Esta evolución constante de las amenazas cibernéticas ha hecho que en la actualidad la protección y defensa de las Infraestructuras Criticas Cibernéticas, se convierta en un tema neurálgico para las organizaciones, por el impacto económico generado, tanto en la contención debido a los recursos que se tienen que disponer para lograr detener el ataque, como en la remediación, en el caso que el ataque sea exitoso,.

Durante el año 2017 parte de los ataques más populares fueron los ransomware, de los cuales se han conocido diferentes variantes, culpables de la pérdida de miles de datos con información sensible y la afectación a muchas empresas a nivel mundial, un informe de la Empresa Kasperky brinda un porcentaje de las computadoras en infraestructura industrial atacadas por un este tipo de amenazas. (Securelist, 2017)

Dentro de este informe presentado por Kaspersky Lab, se observa la publicación de los resultados en Junio de 2017, de la investigación sobre el malware CrashOverride/Industroyer, en el cual expertos de ESET y Dragos Inc., así como una serie de investigadores independientes, llegaron a la conclusión de que el malware estaba diseñado para interrumpir el funcionamiento de los sistemas de control industrial (ICS), en particular

las subestaciones eléctricas. Se logró examinar que es capaz de controlar directamente interruptores automáticos en circuitos de subestaciones eléctricas.

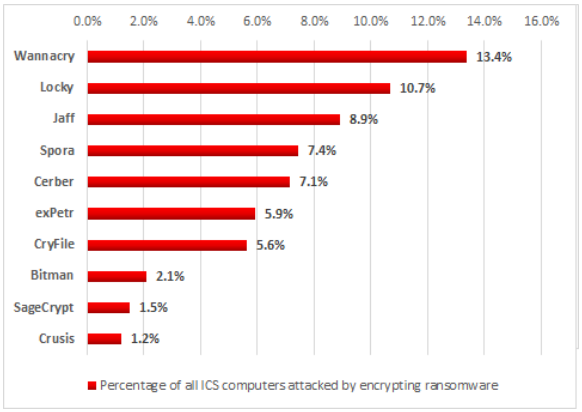


Figura 1. Familias de ransomware más extendidas 2017.

Por otra parte es importante resaltar que en los sistemas de automatización industrial de la Península Ibérica fueron detectadas más de 1100 diferentes modificaciones de malware pertenecientes a 474 familias y en Latinoamérica más de 3000 alteraciones pertenecientes a 800 familias. Las mismas categorías de software que atacan los equipos corporativos, son relevantes para los equipos de sistemas de control industrial. Entre ellos se encuentran los troyanos espías (Trojan-Spy y Trojan-PSW), las "puertas traseras" (Backdoor), los programas extorsionistas (Trojan-Ransom) y los programas de tipo Wiper (KillDisk), que dejan los equipos fuera de servicio y borran los datos del disco duro. Estos programas son particularmente peligrosos para los equipos de la red industrial y una infección puede conducir a la pérdida de control o la interrupción de procesos industriales. (Securelist, 2017)

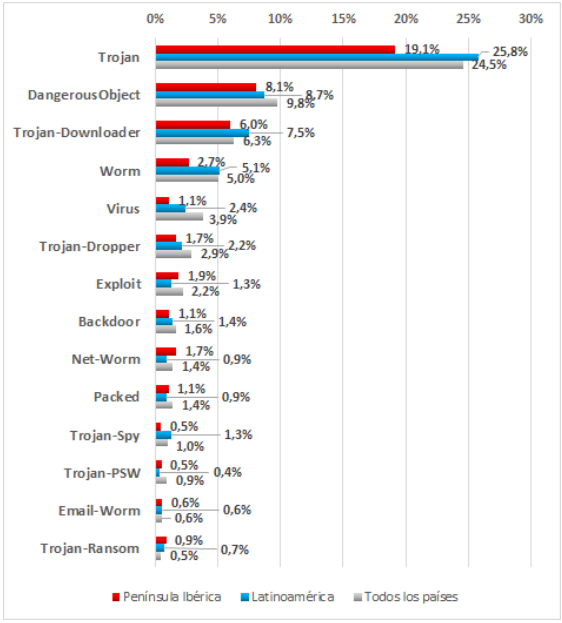


Figura 2. Sistemas de control industrial atacados por malware 2017.

De acuerdo con un informe publicado por la empresa Aranda Software, "Las 15 principales estadísticas de 2017 para TI", se prevé que los daños causados por los delitos cibernéticos lleguen a 6 billones de dólares en el mundo en 2021, frente a los 3 billones de dólares en 2015. Esto incluye daños y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, Fraude, interrupción post-ataque en el curso normal de los negocios, investigación forense, restauración y eliminación de datos y sistemas hackeados y daño a la reputación. Se pronostica que los ataques de Ransomware a las organizaciones sanitarias se cuadruplicarán en 2020. James Comey, director del FBI, pronunció recientemente el discurso principal en la Conferencia de Boston sobre Ciberseguridad (BCCS 2017). Cuando se le preguntó sobre la amenaza cibernética más grande que enfrentan los proveedores de atención médica, Comey respondió "ransomware". (Aranda Software, 2017).

Para el 2018 el panorama no es mejor, para este año se prevé que los ataques se van a intensificar y diversificar, los principales blancos de ataques serán las infraestructuras críticas, teléfonos celulares y dispositivos conectados a Internet (Infobae, 2017).

De acuerdo con el informe anual de riesgos publicado a finales del 2017 por la compañía de seguridad McAfee, el 2018 será un año marcado por ataques informáticos a gran escala, se desarrollarán herramientas aún más destructivas; el impacto generado por los ataques con Bad Rabbit, NotPetya y Wannacry paralizando cientos de miles de computadoras en todo el mundo y llenado los bolsillos de los hackers, será una minucia comparado con los nuevos "modelos económicos" y las nuevas estrategias que desarrollarán los ciberdelincuentes para mantenerse un paso por delante de las herramientas de defensa. (crhoy.com, 2017)

Para enfrentar las amenazas tradicionales y las nuevas amenazas las empresas hacen fuertes inversiones en tecnologías de seguridad para reducir el riesgo de ser atacados exitosamente, y desarrollan estrategias Ciberseguridad con el propósito de permitir que la información pueda ser compartida y utilizada por los interesados, asegurando su protección y la de todos los activos relacionados con ella mediante la adopción de procesos sistemáticos que permitan definir e implementar estrategias de tratamiento de los riesgos, para lograr los niveles de seguridad deseados. Así mismo, las estrategias de ciberseguridad se están convirtiendo también en un generador de valor al negocio de las organizaciones, incrementando y fortaleciendo sus capacidades a nivel del gobierno y gestión de la seguridad de la información corporativa y de negocios y siendo un apalancador en las estrategias de crecimiento de las compañías a nivel nacional, regional y global.

En la estructuración de las estrategias de Ciberseguridad un aspecto muy importante que se debe considerar es la alineación de los requerimientos del negocio vs los requerimientos de seguridad; este es un aspecto fundamental en el modelamiento de la estrategia, ya que es en este punto donde se identifican cuáles son los procesos críticos del negocio de las organizaciones, que infraestructura tecnológica y de seguridad soporta estos procesos y como están siendo gestionados, teniendo claro que cada actividad realizada a nivel de operación, administración y gestión de seguridad tiene una incidencia directa en el cumplimiento o no

de un objetivo de negocio, en una perspectiva de tipo financiero, cliente, imagen, operación, cumplimiento regulatorio o cualquier otra que sea de relevancia para la Organización.

Dentro de esta tarea de alienación de requerimientos, aparece el concepto de: Indicadores de Compromiso – IoC.

Los Indicadores de Compromiso – IoC permiten definir las características técnicas de una amenaza a partir de las evidencias identificadas en los equipos comprometidos, para luego parametrizar la amenaza a través de casos de uso que permitan en el futuro identificar proactivamente y prevenir incidentes de seguridad generados por esta misma amenaza; entendiéndose incidente de seguridad como un "evento adverso que compromete o intenta comprometer la confidencialidad, integridad o disponibilidad de la información"

Los IoC permiten perfilar un incidente, crear una línea base para la identificación de diferentes variables asociadas a ese incidente en particular y comparar un dispositivo potencialmente afectado contra dichos parámetros para dar una respuesta rápida y efectiva.

Si el administrador de seguridad tiene claro cuál es la infraestructura crítica que soporta los procesos del negocio, la definición de IoC se realizará para esta infraestructura crítica evitando desgastes en tiempo y recurso en la protección de otras infraestructuras que no son las críticas para la Organización.

5. METODOLOGÍA PARA DEFINIR INDICADORES DE COMPROMISO – IoC

A continuación, se describe la metodología propuesta para la definición de Indicadores de Compromiso – IoC desde un enfoque estratégico

5.1. ENTENDER LOS FLUJOS DE INFORMACIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

El primer paso para la identificación de los Indicadores de Compromiso – IoC que puedan afectar las infraestructuras críticas de una Organización, es el entendimiento de los flujos de información de dichas infraestructuras críticas.

Los flujos de información se definen como el recorrido que sigue la información desde su origen hasta su destino y se representan mediante diagramas de flujo.

En el mundo empresarial la información fluye de unos empleados a otros, entre estos y la empresa o entre la empresa y sus clientes, proveedores y socios de negocios. Algunas veces se trata de flujos de información informales, no estructurados. Otras veces, estos flujos son formales y están estructurados, soportando procesos críticos en la empresa, o permitiendo la interacción con terceros. Una gestión adecuada de estos flujos de información permite obtener a la empresa una ventaja competitiva, mejorando su eficiencia, la calidad del producto y el servicio ofrecido al cliente. (Mora, 2002)

En las Organizaciones existen diferentes tipos de información, por ejemplo:

- Estratégica
- Financiera
- Recursos humanos
- Jurídica
- Procedimientos
- Comercial
- Mercadeo
- Comunicaciones internas

En el diseño de una estrategia de Ciberseguridad, es importante identificar el tipo de información que fluye dentro de la Organización y su nivel de importancia dentro de los procesos críticos del negocio, ya que esta información es la base para la posterior

definición de las políticas de seguridad y los controles tecnológicos y procedimentales requeridos para la protección de dicha información.

5.1.1. DIAGRAMAS DE FLUJO DE INFORMACIÓN

Los diagramas de flujo de datos permiten visualmente la comprensión del flujo de la información y la identificación de los componentes tecnológicos y de información del proceso crítico de negocio que se quiere proteger.

Los diagramas de flujo de datos los podemos dividir en 5 capas, cada una de las cuales permiten la organización y contextualización de los elementos que intervienen en el flujo de la información identificada como objeto de protección dentro de los procesos críticos de negocios para los cuales se pretende identificar los Indicadores de Compromiso – IoC, que permitan una mejor y más proactiva predicción de los posibles ciberataques.

Figura 3. Capas diagrama flujo de datos

En cada capa se ubican los elementos identificados en la caracterización de activos, es decir, las aplicaciones, los usuarios, los equipos, etc.

- **Capa Red:** En esta capa se identifican las redes y segmentos de red donde la información es procesada. Por ejemplo, si el desarrollo del proceso involucra actividades en oficinas remotas, redes locales y segmentos de red protegidos por Firewalls. Es aquí en esta capa donde deben visualizarse las formas con estos elementos. La identificación de las redes permite visualizar si el diseño de arquitectura de seguridad puede proteger los activos que se requieren dentro del proceso crítico de negocio.

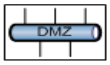
Formas Capa Red		
Forma	**Nombre**	**Descripción**
	Ethernet	Identifica los segmentos de Redes LAN.
	Nube	Identifica Redes especiales por fuera de la organización, ejemplo Internet, redes Wan, proveedores de servicio.

Figura 4. Formas de Red Plantilla Diagrama de Flujo de datos

- **Tecnología:** Aquí se identifican los componentes tecnológicos que soportan las plataformas usadas en el proceso, es decir, el hardware como equipos de escritorio, repositorios de archivos, servidores, impresoras, entre otras.

Formas Capa Tecnología		
Forma	**Nombre**	**Descripción**
	Servidores	Identifica servidores y la prestación de servicios, ejemplo Bases de datos, Ftp, Correo electrónico, Repositorios.
	Unidad de Medios Externa	Representa los medios de almacenamiento externo, como Dispositivos Usb, Unidades de disco extraíbles, Cintas.
	PC	Puede representar un equipo específico por usuario, o un grupo de equipos asociados a un grupo de usuarios.
	Impresora	Impresora, Local o de Red.

Figura 5. Formas Tecnología Plantilla Diagrama de Flujo de datos

- **Usuarios:** En esta capa se organizan los usuarios de los activos identificados en el proceso. Tanto el usuario titular como su respectivo backup deben ser identificados con los cargos según el organigrama y estar relacionados con la información que usan.

Formas Capa Usuarios		
Forma	**Nombre**	**Descripción**
	Usuario	Usuario o perfil de usuario que participa en el proceso, debe ser identificado con el cargo.
	Proveedor	Identifica los funcionarios externos del proceso que proveen información al mismo.
	Departa-mento	Representa un grupo de personas que comparten una característica común, ejemplo un área o departamento.

Figura 6. Formas Usuarios Plantilla Diagrama de Flujo de datos

- **Aplicaciones:** Se identifican las aplicaciones o sistemas de información que son usados para el procesamiento o manejo de la información. Por ejemplo: software

ofimático, aplicaciones de sistemas de información, aplicaciones para la generación de reportes, etc.

Formas Capa Aplicación		
Forma	**Nombre**	**Descripción**
	Aplicación	Forma que ayuda a identificar las aplicaciones en las que se procesa la información.

Figura 7. Formas Aplicación Plantilla Diagrama de Flujo de datos

- **Información:** En esta capa se identifica la información del proceso, como reportes, archivos, bases de datos, etc. Esta es la información que se espera proteger.

Formas Capa Información		
Forma	**Nombre**	**Descripción**
	Documento	Representa uno o un grupo de documentos en Word, Excel, Pdf o Archivos de texto.
	Base de Datos	Identifica las instancias de las bases de datos donde se almacena la información.
	Archivo Presentación	Reportes, Informes, Presentaciones entre otros.
	Correo	Representa notificaciones o el envío de correo con archivos adjuntos a uno o multiples destinatarios.

Figura 8. Formas Información Plantilla Diagrama de Flujo de datos

- **Adicionales:** Existen otros símbolos que ayudan a contextualizar el diagrama de flujo de datos.

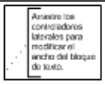
Formas Adicionales		
Forma	**Nombre**	**Descripción**
	Anotación	Pueden estar ubicados en todas las capas, y en ellos de forma breve debe existir información que aporte a la contextualización de la forma.
	Linea Punteada	Lineas de separación vertical, que ayudan a separar los limites entre componentes.
	Flechas	Indican el Flujo de la información entre los usuarios y elementos que intervienen en el proceso.

Figura 9. Formas Adicionales Plantilla Diagrama de Flujo de datos

5.1.2. PASOS PARA LA ELABORACIÓN DE UN DIAGRAMA DE FLUJO DE DATOS

La elaboración de un diagrama de flujo conlleva la distribución de muchos elementos en la plantilla, a continuación se enumeran los pasos recomendados para la elaboración del diagrama de flujo de datos del proceso de negocio.

- **Paso 1. Agregar elementos:** Coloque los activos identificados en la plantilla de caracterización, en la capa correspondiente. Verifique que el nombre utilizado en el diagrama de flujo de datos sea el mismo identificado en la caracterización de activos.

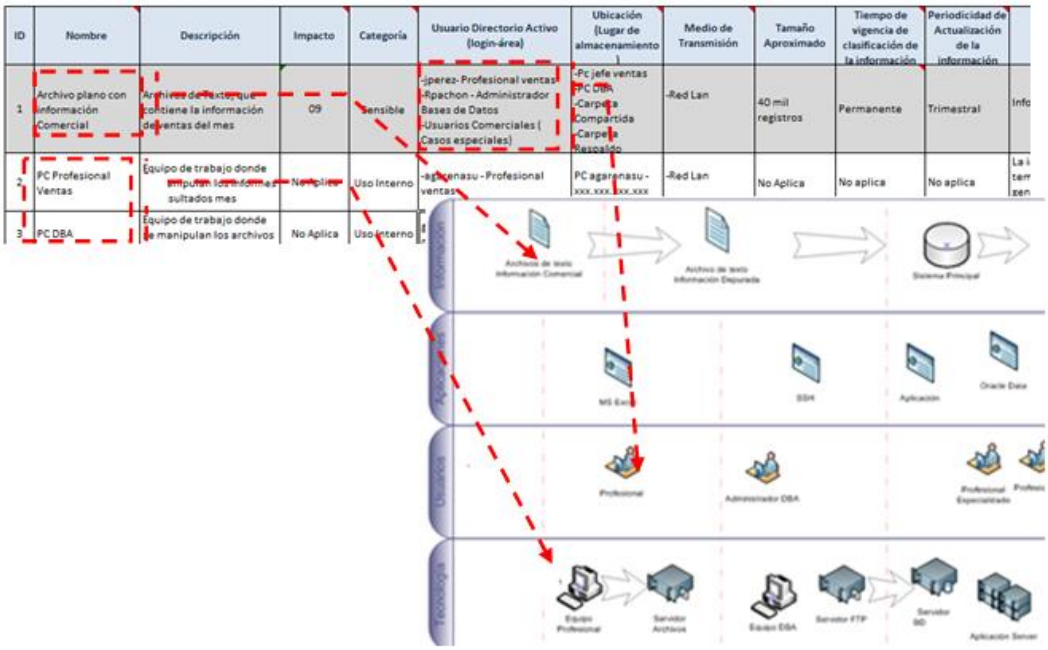


Figura 10. Paso 1 Elaboración de diagrama de Flujo de datos

- **Paso 2. Distribución de elementos:** Organice las formas teniendo en cuenta distribuir los elementos de izquierda a derecha; donde a la izquierda se esperaría encontrar la información de entrada del proceso y hacia la derecha la información resultante del proceso. Posteriormente ubique los activos de la capa superior (información), continúe con la siguiente capa (aplicación) y así por todas las capas hasta llegar a la capa de Red, teniendo en cuenta que las formas puedan asociarse visualmente de forma vertical sobre las capas, cómo lo muestra la siguiente figura de ejemplo:

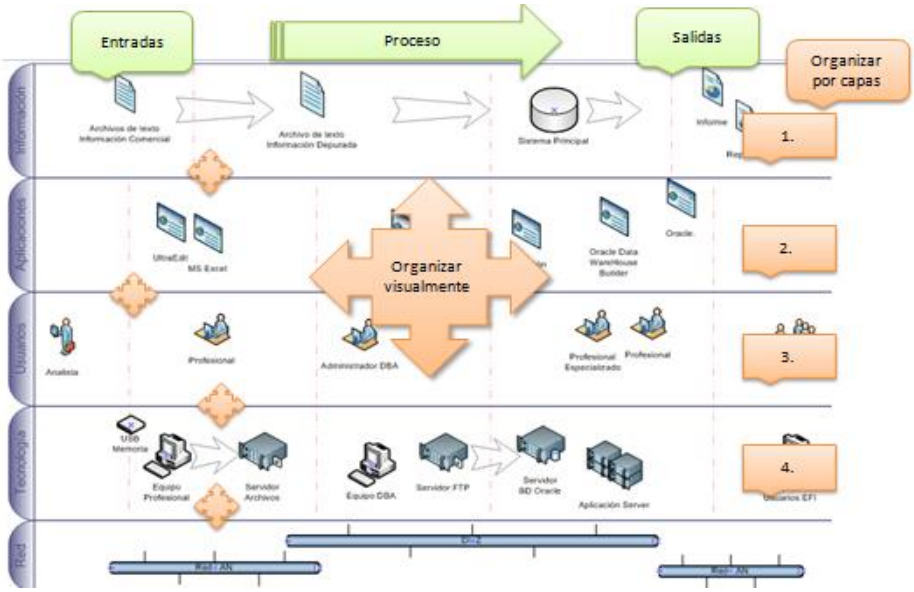


Figura 11. Paso 2 Elaboración de diagrama de Flujo de datos

- **Paso 3. Comentarios:** Si es necesario incluir comentarios cuando se haga la representación de los activos con el fin de contextualizarlos dentro del flujo de datos, disponga de estos al lado de las formas, como se muestra en la siguiente figura:

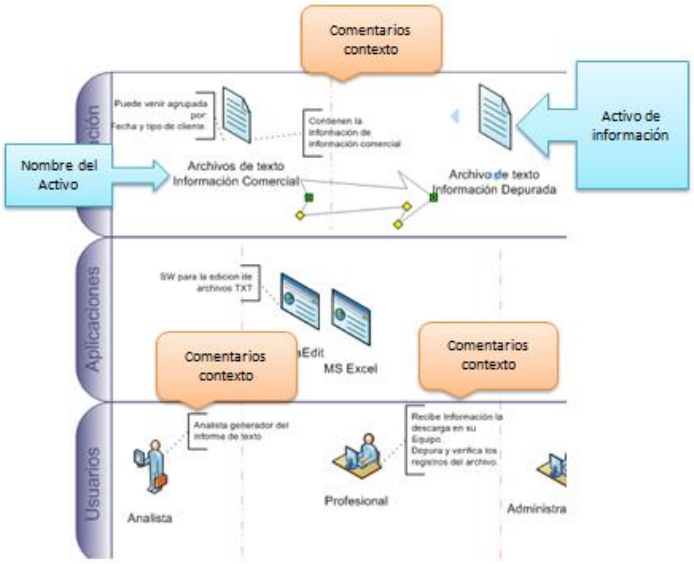


Figura 12. Paso 3 Elaboración de diagrama de Flujo de datos

- **Paso 4. Flujo de Datos:** Coloque las flechas indicando el flujo de información preferiblemente indicando que el flujo de datos va de izquierda a derecha.

Figura 13. Paso 4 Elaboración de diagrama de Flujo de datos

5.2. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN CRÍTICOS A PROTEGER SEGÚN EL FLUJO DE INFORMACIÓN

Una vez finalizada la caracterización de activos y la construcción del diagrama de flujo de datos, se hace el respectivo análisis para establecer en definitiva la información a proteger.

Definimos activo de información como cualquier objeto de información que tiene valor para la organización. Esto incluye información en formato electrónico o impreso y los medios o equipos que almacenan o procesan la información.

El análisis se hace teniendo en cuenta los siguientes aspectos:

a) Valoración en impacto y clasificación de los activos
b) Alcances de la solución
c) Requerimientos de negocio

a) Valoración en impacto y clasificación de los activos

Son los criterios de seguridad establecidos por las políticas de análisis de riesgos y de clasificación de activos de la organización, definidos en la fase de levantamiento de información que pueden ser identificados en el documento de caracterización de activos en las columnas Impacto y Clasificación respectivamente.

El objetivo del análisis de riesgos es identificar y tasar los riesgos a los cuales están expuestos los activos de información, para identificar y seleccionar los controles apropiados de seguridad. La evaluación está basada en los valores de los activos y los requerimientos de los niveles de seguridad, tomando en cuenta los controles existentes.

El proceso de análisis de riesgos está compuesto por una serie de etapas que cumplen los requerimientos del estándar ISO/IEC 27001:2005 y están alineadas con el estándar ISO/IEC 27005:2008. Las etapas se muestran en la Ilustración 1 y se describen a continuación.

Figura 14. Metodología de análisis de riesgos

1. Inventario de activos de información:

El primer paso de esta actividad consiste en la identificación de los activos de información de los procesos objeto de análisis y sus propietarios, seguido por la valoración del impacto de pérdida de las propiedades definidas para cada activo, en este caso, confidencialidad, integridad y disponibilidad.

1.1 Identificación de los principales activos de cada proceso

Esta actividad es desarrollada con los líderes de cada área o proceso mediante entrevistas de entendimiento cuyo objetivo principal es la identificación de los activos de información.

Los posibles tipos de activos de información considerados como parte del análisis son:

- **Información física**: Información que ha sido impresa o se encuentra consignada en medios físicos como papel.
- **Hardware**: Dispositivos de la infraestructura tecnológica que soportas los sistemas de información de la organización. Incluye el dispositivo y el sistema operativo nativo del mismo.
- **Información electrónica**: Información que se encuentra en medio magnético, por ejemplo bases de datos y archivos en Microsoft Office.
- **Medios externos de almacenamiento**: Dispositivos utilizados para almacenar de manera temporal información electrónica como USBs, DVDs, CDs, cintas magnéticas, discos duros, etcétera.
- **Recursos Humanos**: Personal que trabaja en la Organización y tiene acceso a la información y/o la infraestructura para su procesamiento.
- **Enlaces de comunicaciones**: Canales y demás infraestructura asociada a las redes da datos.
- **Servicios de terceros**: Servicios de diferente propósito prestados por empresas o particulares externos a la Organización, tales como tecnología, mensajería y custodia de información.
- **Aplicaciones**: Sistemas de información, bien sean propietarios o comprados.
- **Infraestructura:** Sitios (lugares) de almacenamiento de información o de equipos que soportan la operación de los sistemas de información.

1.2 Valoración de activos

Por cada una de las propiedades de la información contempladas en el análisis, esto es, Confidencialidad, Integridad y Disponibilidad, el propietario del activo asigna una calificación del impacto utilizando la siguiente escala que se muestra en la Figura 15.

Cada uno de los cuatro criterios (estabilidad, financiero, humano y de imagen) se evalúa frente a cada una de las tres propiedades de la información (confidencialidad, integridad y disponibilidad), si aplica.

A partir de esta calificación, se seleccionan los activos de información sobre los cuales se lleva a cabo la etapa de identificación del riesgo.

		ÁREA DE IMPACTO			
		Estabilidad	**Financiero**	**Humano**	**Imagen**
VALOR	**Catastrófico**	Se afectan las relaciones internacionales	La disminución en la asignación presupuestal es muy elevada	Pérdida de varias vidas humanas	Se pierde la confianza en el Ministerio a nivel internacional
	Mayor	Se afecta la estabilidad nacional	La asignación presupuestal disminuye significativamente	Pérdida de vida humana	Se pierde la imagen y la confianza en el Ministerio a nivel nacional
	Moderado	Se afecta la estabilidad de la Institución	Se disminuye la asignación presupuestal de forma moderada	Lesiones de importancia	Se amenaza la imagen del Ministerio
	Menor	Se afecta la operación de una Unidad	Se disminuye levemente la asignación presupuestal	Perjuicios leves a un grupo	Se afecta la imagen del Grupo de Sistemas
	Insignificante	Se afecta la operación de un proceso (o de ninguno)	No afecta la asignación presupuestal	Perjuicios nulos o leves a nivel individual	No hay repercusiones en la imagen

Figura 15. Escala de valoración de impacto

2. Identificación del riesgo

Para la identificación del riesgo se realizan las siguientes cuatro (4) actividades:

- Identificación de las amenazas y vulnerabilidades pertinentes a la Organización y a los activos de información seleccionados;
- Cálculo del nivel de riesgo inherente;
- Identificación y valoración de controles existentes;
- Cálculo del riesgo residual.

Se realiza la identificación y selección de amenazas y vulnerabilidades para los procesos objeto del análisis. A partir de los elementos seleccionados se construyen escenarios de riesgo que ilustran la materialización de una amenaza por el aprovechamiento de una vulnerabilidad.

La determinación del nivel de riesgo inherente se realiza a partir de la probabilidad de ocurrencia del escenario de riesgo y el impacto de la materialización del mismo, suponiendo que no existen controles que lo mitiguen.

La valoración de la probabilidad de ocurrencia se realiza de acuerdo con una escala que contempla dos aspectos (Figura 16):

- **Histórico:** hace referencia a las estadísticas y datos históricos con que cuenta la Organización sobre la materialización de los escenarios de riesgo evaluados. En caso de que la Organización no cuente con esta información, sólo se empleará el aspecto de probabilidad potencial.

- **Potencial:** hace referencia a la probabilidad potencial que existe de que se presente un escenario de riesgo.

	Histórico	Potencial
Muy alta	El evento se presentó más de 3 veces en el último año	Se espera que ocurra en la mayoría de las circunstancias
Alta	El evento se presentó 3 veces en el último año	Probablemente ocurrirá varias veces
Moderada	El evento se presentó 2 veces en el último año	Podría ocurrir en algún momento; sin embargo, se pueden detectar y controlar
Baja	El evento se presentó 1 vez en el último año	Es difícil que ocurra pero en caso que ocurra en caso de ocurrencia son fácilmente detectables y controlables
Muy baja	El evento no se ha presentado en el último año pero si se ha presentado históricamente	Puede ocurrir solo en circunstancias excepcionales y es totalmente controlable

Figura 16. Escala de valoración de ocurrencia

En caso de que se evalúen los dos aspectos, se emplea la matriz de probabilidad (Figura 16), para determinar la probabilidad de ocurrencia total.

Por otra parte, el impacto de cada activo corresponde al valor asignado en la propiedad más relevante en el contexto del escenario de riesgo para dicho activo; por ejemplo, si el escenario afecta principalmente la confidencialidad del activo, el valor a tomar para el impacto será el correspondiente a dicha propiedad.

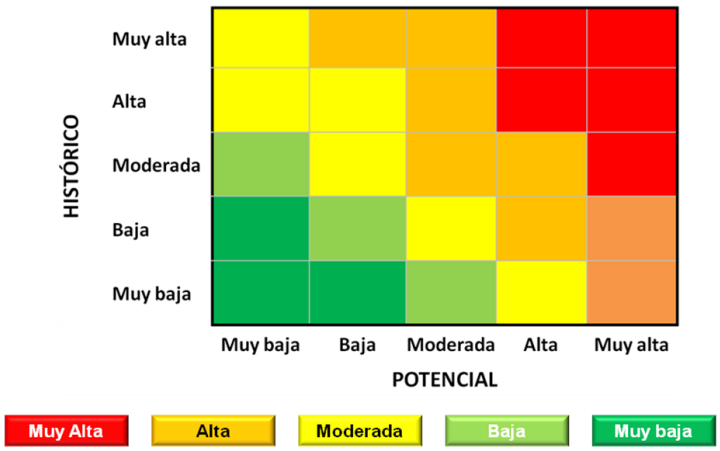


Figura 17. Matriz de probabilidad de ocurrencia

Para evaluar el nivel de riesgo inherente se utiliza la misma escala empleada durante la Fase I, es decir:

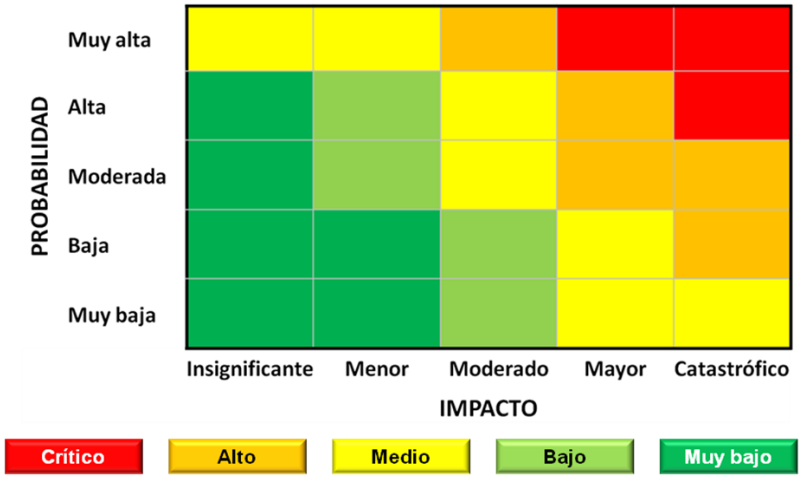


Figura 18. Matriz del nivel de riesgo inherente

Como paso siguiente, se identifican los controles existentes para un escenario de riesgo, para evaluar su eficacia. La escala utilizada para esta valoración es:

	Nivel	Criterio
4	**Excelente**	El control existe, es eficaz y siempre se aplica
3	**Bueno**	El control existe, es eficaz, pero no se aplica siempre
2	**Aceptable**	El control existe, se aplica, pero no siempre es eficaz
1	**Deficiente**	El control existe, no siempre es eficaz y no siempre se aplica
0	**Sin control**	El control no existe

Figura 19. Escala valoración de eficacia de los controles

Finalmente, para determinar el nivel de riesgo residual, es decir, después de la valoración de controles, se emplea una matriz similar a la empleada durante la evaluación de riesgos realizada:

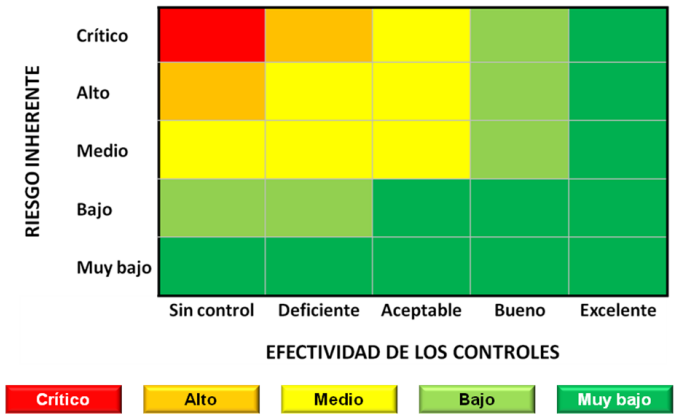


Figura 20. Tabla de nivel de riesgo residual

Cada uno de los niveles de riesgo deberá ser tratado de la siguiente manera:

Nivel de riesgo	Descripción
Crítico	Riesgo extremo que requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a los altos mandos.
Alto	Riesgo alto. Se requiere atención de la Alta Dirección. Planes de tratamiento requeridos, implementados y reportados a los líderes funcionales.
Medio	Riesgo moderado. Se requiere atención del área involucrada, definición de procedimientos y controles de mitigación.
Bajo	Riesgo aceptable. Se administra con procedimientos normales de control.
Muy bajo	Riesgo bajo. Se administra con procedimientos rutinarios.

Figura 21. Descripción de los niveles de riesgo

3. Plan de Tratamiento de Riesgos

Una vez identificados los principales escenarios de riesgo a los cuales están expuestos los activos de información seleccionados, debe definirse cuál se considera el nivel de riesgo aceptable para la Entidad; así, para aquellos activos que se encuentren por encima del nivel de riesgo aceptable, debe definirse un plan de tratamiento que incluya las acciones a tomar para mitigar los niveles de riesgo encontrados.

Para esto se seleccionan del del estándar ISO/IEC 27001:2013 (International Standard Organization) los objetivos de control y controles que cumplen con los requerimientos de seguridad de los activos y permiten reducir los niveles de riesgo a los cuales se encuentran expuestos.

Con respecto a los Indicadores de Compromiso – IoC, su importancia radica en la posibilidad de predecir los ataques a partir de la detección de las mismas vulnerabilidades en equipos diferentes a los que fueron atacados por el malware. Además

de poder predecir los ataques, los IoC permiten también identificar redes o computadoras infectadas cuyos ataques no fueron detectados por los administradores de seguridad de la Organización.

b) Alcances de la solución

Los controles tecnológicos de seguridad son medidas preventivas para brindar seguridad a la información, esto significa que la tecnología no es infalible ante ataques directos o escenarios de riesgo de fuga de información particulares, por tal motivo es importante saber cuáles son las capacidades de las tecnologías de seguridad que se tienen implementadas, es decir que licencias, agentes, componentes de red, canales de protección, características propias de las herramientas y limitaciones entre otras podría llegar a tener.

Los Indicadores de Compromiso - IoC permiten elaborar planes de prevención de incidentes informáticos y fortalecer los sistemas de seguridad en los soportes de infraestructura de las TI. Estos planes de prevención incluyen la implementación de controles de seguridad como:

1. Sistemas de detección de intrusos (IDS)
2. Sistemas de prevención de intrusos (IPS)
3. Sistema de detección de intrusiones en un host (HIDS)
4. Sistema de prevención de intrusiones en un host (HIPS)
5. Firewalls
6. Control de fuga de información confidencial (DLP)
7. User and Entity Behavior Analytics (UEBA)
8. Threat Intelligence Platform (TIP)
9. End Point Detecction and Response (EDR)
10. Security Information and Event Management (SIEM)
11. Vulnerability Management (VM)
12. Soluciones de sandboxing para protección de ataques de día cero
13. Soluciones de seguridad para bases de datos

La posibilidad de contar con los Indicadores de Compromiso – IoC, permite proteger toda la red de un sistema informático a través de la prevención.

c) Requerimientos del Negocio

Estos requerimientos son señalados por el líder del proceso y tiene relación con la identificación de posibles escenarios de riesgo de incidentes de seguridad, cumplimiento a normativas de entes reguladores, o requerimientos de confidencialidad adicionales a los ya establecidos en las políticas de la organización. También pueden existir restricciones propias sobre el manejo de la información, como desclasificación, tamaños o volúmenes, restricciones a sistemas de información donde se procesa la información a proteger o restricciones propias de la operación y del proceso que deben ser evaluadas y consideradas por líder del proceso.

5.3. CLASIFICACIÓN DE LOS TIPOS DE ATAQUE QUE AFECTEN INTEGRIDAD, CONDIDENCIALIDAD y DISPONIBILIDAD

En esta fase se pretende dar una mirada a algunos de los tipos de ataques más relevantes contra los principios de la Seguridad de la Información, con el fin de observar algunos métodos y técnicas que utilizan los atacantes y de esta forma generar conciencia acerca de la necesidad de contar con medidas al igual que métodos, lo cuales que garanticen la seguridad en todo momento, comenzando con principios que den garantía de que la información solo va a ser accedida por las personas correctas y no por otras fuentes ilegales que puedan beneficiarse de ella, es decir que haya *Confidencialidad*, de igual forma es de carácter obligatorio poder contar con la información tal cual es generada sin que hayan variaciones o modificaciones no autorizadas que puedan vulnerar la *Integridad* de los archivos, así mismo se hace necesario garantizar que la información se va a encontrar *Disponible* cuando se requiera; por otra parte se debe proteger la *Autenticidad* de cada documento indicando que es el original y está siendo enviado por la persona correcta y no por un tercero desconocido, todo esto debe tener una constante *Auditoria* acerca del acceso y las evidencias sobre el uso del recurso, y por último el *No Repudio* de la información para comprobar la verdadera identidad de la persona que lo elaboro o lo modifico en el origen y en el destino. En la Figura No.1 se puede apreciar lo descrito anteriormente.

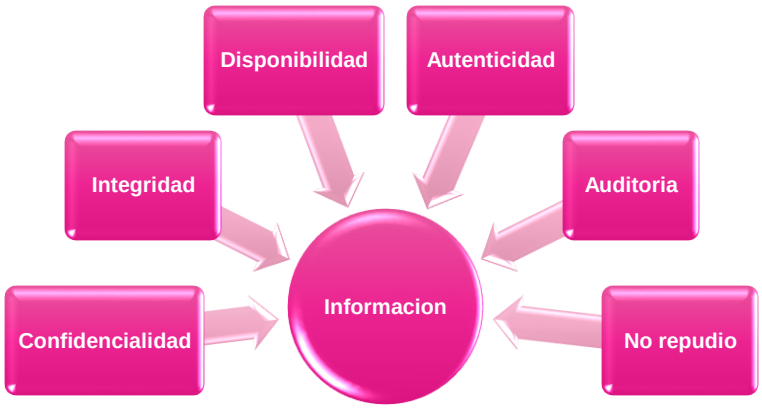


Figura 22. Principios de la Seguridad de la Información.

DISPONIBILIDAD

- **DENEGACIÓN DE SERVICIO DoS.** (Ramiro R. , 2018)

Este tipo de ataque afecta la disponibilidad de los sistemas, impidiendo que los usuarios puedan acceder a la información o los servicios, por lo general el atacante inunda la red con peticiones o información basura, manteniendo ocupado el servidor, hasta tal punto que colapsa y no permite que usuarios legítimos acedan al mismo.

Algunos Indicios:

- ✓ Rendimiento bajo en el procesamiento de peticiones.
- ✓ Indisponibilidad o incapacidad de acceder a un sitio web.

Metodologías más usadas:

- ✓ ICMP Flood Attack
- ✓ Tear Drop Attack
- ✓ Smurf Attack
- ✓ Syn flood
- ✓ Land Attack
- ✓ Jolt Dos Attack
- ✓ Fraggle Dos Attack

Métodos de prevención:

- ✓ Aplicación de filtrado de paquetes
- ✓ Bloquear direcciones IP sin uso y reportadas en listas negras
- ✓ Deshabilitar servicios de red innecesarios
- ✓ Limitar la cantidad de ancho de banda

INTEGRIDAD

- **ARP SPOOFING.** (G. Soto, 2016)

Esta técnica podría afectar la integridad e incluso la confidencialidad de la información, teniendo en cuenta tiene por objetivo interceptar el tráfico en una red local, permitiendo a los atacantes maliciosos interceptar, modificar o incluso retener datos que están en tránsito. Los ataques de suplantación ARP ocurren en redes de área local que utilizan protocolo de resolución de direcciones (ARP)

Algunos tipos son:

- ✓ Ataque de inundación MAC.
- ✓ Envenenamiento de caché DNS.
- ✓ IP Spoofing.

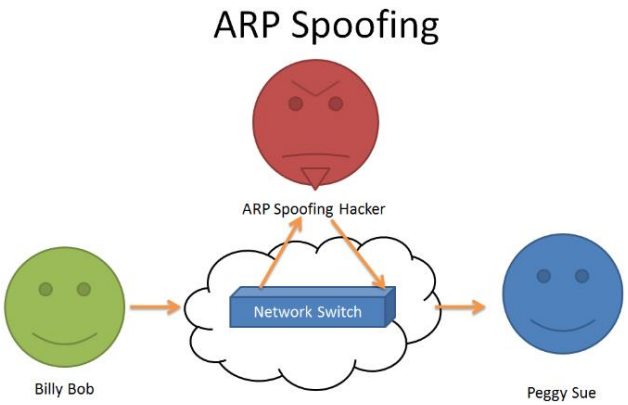


Figura 23. Ejemplo de ilustración ARP Spoofing

- **ATAQUES A APLICACIONES WEB.** (Ramiro R. , 2018)

Este tipo de ataque puede afectar la integridad y la confidencialidad de la información, de diferentes formas:

✓ Inyección SQL: Permite al atacante ejecutar código arbitrario en la base de datos, con el fin de obtener información confidencial, o incluso dañar el uso de la aplicación.

✓ Cross-Site Request: Método para transmitir comandos no autorizados de un usuario en el que el sitio web confía, por ejemplo los scripts de sitios cruzados (XSS) explotan la confianza que un usuario tiene para un sitio en particular y CSRF explota la confianza que un sitio tiene en el navegador de un usuario.

✓ Ataque de envenenamiento de cookies: En este tipo se modifican los contenidos de una cookie para evadir los mecanismos de seguridad que se tienen, esto puede llevar a la obtención no autorizada sobre un usuario o robar su identidad.

✓ Robo de cookies: Se aprovechan del uso de scripts, para hacer que cuando el usuario acceda a un enlace se envié la cookie almacena en la memoria del equipo al atacante.

✓ Ataques de phishing: Este tipo de ataque utiliza información falsa que parece ser confiable para lograr la adquisición de datos sensibles.

✓ Web Defacement: Mediante este tipo de ataque se puede lograr la modificación de la apariencia visual de un sitio Web, afectando su reputación.

CONFIDENCIALIDAD

- **INGENIERÍA SOCIAL.** (Ramiro R. , 2018)

Una de las técnicas más utilizadas que podría afectar la confidencialidad de la información, la cual se basa en lograr manipular a las personas para que renuncien a la reserva de los datos y lograr diferentes objetivos, por ejemplo: el robo de contraseñas, documentos, permitir acceso a zonas no autorizadas, instalación de software o hardware que afecta la seguridad de las redes, entre otros.

Métodos de prevención:

- ✓ Observe más despacio la información que solicitan y analice los riesgos.
- ✓ Investigue si los datos de identificación son legítimos
- ✓ Eliminar cualquier solicitud de información financiera o contraseñas
- ✓ Rechace las solicitudes de ayuda sospechosa.

- **DNS SPOOFING.** (Albors J. , 2017)

Es un método para alterar las direcciones de los servidores DNS que utiliza la potencial víctima y de esta forma poder tener control sobre las consultas que se realizan, con el fin de alterar las direcciones IP para que las peticiones de la víctima apunten a servidores maliciosos.

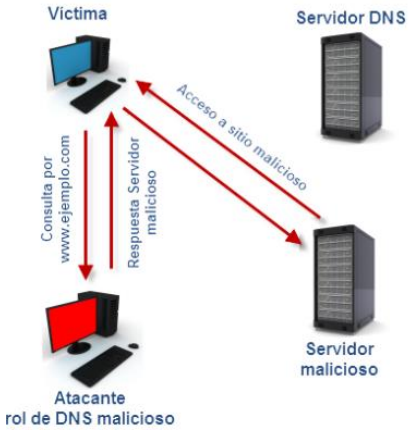


Figura 24. Ejemplo de ilustración DNS Spoofing

- **MALWARE.** (Albors J. , 2015) (Ramiro R. , 2018) (Optical News, 2018)

Debido a la avalancha tecnológica de la actualidad y a la tendencia de converger toda la información a los sistemas de TI, es importante observar que a medida que nace un nuevo Software o Hardware, se crean también métodos, programas y códigos maliciosos que buscan sabotear las estructuras con diferentes fines, dentro de estos encontramos los denominados Malware, los cual abarcan una gran cantidad de software con códigos

maliciosos para efectuar algún tipo de daño en los sistemas o aprovechar las vulnerabilidades que puedan existir, algunos de ellos son:

- ✓ Spyware: Este tipo de software con código malicioso permite realizar una recolección de los datos como un espía (usuarios, organizaciones, programas, tipo de sistema, hardware instalado, acciones realizadas, entre otros), sin que el usuario se percate de lo que es sucediendo.

- ✓ Troyano: Este tipo de malware se hizo muy popular por el relato del Caballo de Troya en donde una figura dada como un obsequio tenia por dentro infiltrados que se aprovecharon para ingresar a las instalaciones de un bando enemigo y lograr vencerlos, su funcionamiento en el área informática es muy parecido, un programa que parece ser confiable contiene una serie de instrucciones o códigos ocultos que se esparcen por todo el sistema para recolectar, alterar, dañar, modificar cualquier tipo de datos, sin que el usuario lo autorice enviando la información al creador e incluso generando conexiones ilegitimas ocultándose en procesos del sistema válidos.

  Un ejemplo son los Backdoors, los cuales tienen la habilidad de permitir el acceso a los sistemas instalando puertas traseras para tener el control del equipo y sus servicios, los más famosos fueron iniciados en los años de 1997 a 1999 bajo el nombre de NetBus, Back Orifice y Sub7. Estos logran conectarse al equipo de forma remota sin que el usuario tenga conocimiento o haya autorizado la conexión, brindando la posibilidad de utilizar el ordenador y sus herramientas para diferentes fines.

- ✓ Gusano: El nombre que lleva este tipo de malware nos puede dar un bosquejo de su finalidad, que no es otra más que ingresar en un sistema y esparcirse a través de toda la red por diferentes medios (correos, mensajes, transferencias, etc…) salta de un sistema a otro recolectando información, desplegando el código malicioso y enviando todo a la fuente, su característica especial radica el esparcimiento rápidamente de un lugar a otro.

- ✓ Ransomware: Estos ataques afectan la disponibilidad y consisten en un tipo de software malicioso diseñado para bloquear el acceso a la información o a un sistema informático, a través de métodos de cifrado, hasta que se pague una cantidad de dinero por recuperarlo.

- **AMENAZA PERSISTENTE AVANZADA (APT).** (Ramiro R. , 2018)

  Estos consisten en el que una persona no autorizada obtiene acceso a una red y permanece allí sin ser detectado durante un período prolongado de tiempo. Normalmente el objetivo de estos es mantener el acceso encubierto y continúo a una red, permitiendo recopilar información, tomar control de dispositivos, acceder a sistemas seguros, entre otros, requiriendo la reescritura continúa de códigos y sofisticadas técnicas de evasión.

5.4. DEFINICIÓN DE INDICADORES DE COMPROMISO - IOC

Utilizando metodologías de análisis de riesgos, como la descrita anteriormente, se busca entender cuál es el flujo de información de los procesos críticos del negocio de la Organización, se identifica que usuarios interactúan con el proceso, cuales es la plataforma tecnológica asociada a los procesos críticos y con qué infraestructura de seguridad cuentan los procesos para protegerlos. Todo esto se identifica, se documenta y se almacena en una base de datos para poder tener un entendimiento completo del proceso.

Los Indicadores de Compromiso – IoC, permiten perfilar un incidente, crear una línea base para la identificación de diferentes variables asociadas a ese incidente en particular y comparar un dispositivo potencialmente afectado contra dichos parámetros para dar una respuesta rápida y efectiva; por lo tanto los Indicadores de Compromiso – IoC sirven para identificar si un sistema ha sido comprometido (a modo de herramienta forense), o si se está intentando comprometerlo". (Andrés Mendez Barco y Centro Criptológico Nacional, 2015, pág. 7)

A partir del entendimiento de los flujos de información de los procesos críticos de la Organización y apoyados en arquitecturas de inteligencia de seguridad (propias o de terceros que ofrezcan el servicio), se toman los eventos de seguridad que se están presentando en la plataforma tecnológica que soporta los procesos críticos y se analizan dichos eventos para poder definir las líneas base de comportamiento y los umbrales de variación de dicho comportamiento, para poder determinar en un momento dado si un repentino cambio de comportamiento corresponde a un intento de ataque, un incidente de seguridad que se esté presentando o se trata de un falso positivo, generado por alteraciones asociadas a cambios del negocio.

Con toda la información de líneas base de comportamiento y sus umbrales de variación, se inicia la construcción de los casos de uso asociados a los Indicadores de Compromiso – IoC que permitan identificar proactivamente posibles incidentes de seguridad y prevenir que estos incidentes se materialicen.

La importancia que tienen los IOC es la posibilidad de predecir los ataques a partir de la detección de las mismas vulnerabilidades en equipos diferentes a los que fueron atacados por el malware sobre el que se define el Indicador de Compromiso - IoC. Además de poder predecir los ataques, los Indicadores de Compromiso – IOC permiten también identificar redes o computadoras infectadas cuyos ataques no fueron detectados por los departamentos de sistemas de las empresas afectadas.

Los Indicadores de Compromiso – IOCS permiten elaborar planes de prevención y atención de incidentes informáticos y fortalecer los sistemas de ciberseguridad de las infraestructuras de TI críticas. Estos planes de prevención incluyen la implementación

de diferentes controles de ciberseguridad para reducir el riesgo de materialización de un ataque, algunos ejemplos de los controles que se pueden implementar son:

- Sistemas de detección de intrusos (IDS)
- Sistemas de prevención de intrusos (IPS)
- Sistema de detección de intrusiones en un host (HIDS)
- Sistema de prevención de intrusiones en un host (HIPS)
- Firewalls
- Sistemas de control de fuga de información confidencial (DLP)
- Sistemas de monitoreo de bases de datos
- Sistemas de protección del end point (EDR)

Así mismo existe una gran cantidad de Indicadores de Compromiso - IoC que describen actividades inusuales en la red o en los sistemas, a partir de los cuales se pueden construir más casos de uso son: (Ciberseguridad al día, 2013)

1. **Trafico inusual de salida de red (Inusual Network Outbound Traffic):** Es importante monitorear y analizar no solo el tráfico interno de la red, sino el saliente, ya que puede tratarse de peticiones fraudulentas o no autorizadas que pueden comprometer la seguridad de la red al generarse puertas traseras a través de las cuales se esté enviando sacando información confidencial, se reciba tráfico malicioso del tipo APT para realizar posteriormente ataques, se realicen mapeos de la red local, acceso a dispositivos, etc.

2. **Anomalías en la actividad de la cuenta de usuario con privilegios:** uno de los mayores factores de riesgo potencial de seguridad en las Organizaciones son los usuarios con privilegios, ya que tienen acceso autorizado a las infraestructuras más críticas, a las bases de datos, a información confidencial y todas las actividades que estos realicen no serán consideradas como maliciosas, por el perfil de usuario que tienen, por lo tanto es importante poder monitorear este tipo de usuarios y definir sus líneas base de comportamiento, para poder identificar cambios de comportamiento inusuales e implementar políticas fuertes para la gestión de roles y credenciales privilegiadas.

3. **Irregularidades geográficas:** intentos o conexiones exitosas desde diferentes partes del mundo, o con cambios de IP repentinos en las peticiones, deben ser considerados como comportamientos anómalos ya que estas conexiones podrían estar dirigidas por un atacante, el cual mediante diferentes herramientas y técnicas estará tratando de eludir la seguridad implantada en los sistemas.

4. **Banderas rojas:** Son comportamientos o circunstancias poco comunes o extrañas, que pudiesen haber generado actos fraudulentos; como resultado se generan una gran cantidad de alertas que se pueden usar para para prevenir ataques a los sistemas, redes o la información.

5. **Incremento en las lecturas de la base de datos:** los cambios de comportamiento en las bases de datos como incremento de consultas, modificación de registros, accesos en horarios poco comunes, son un indicador de compromiso que permite evidenciar si un atacante ha logrado acceder a la base de datos para intentar exfiltrar información; esta situación se puede evidenciar generando alertas que indiquen que se está materializando un ataque y se puede neutralizar o detener mediante la generación de reglas de seguridad bien parametrizadas que restrinja los tiempos de acceso, cambios de registros, número de conexiones, horarios de conexión, etc.

6. **Tamaño del HTML de respuesta:** una forma de ataque muy común orientada a la extracción de información reservada de usuarios, documentos, tablas etc, es mediante la inyección de código malicioso a la página web que le permita al atacante extraer la información confidencial. Es importante monitorear las consultas a las bases de datos a través de las páginas web, ya que en un comportamiento normal, cuando un usuario legítimo hace una consulta a la base de datos, los paquetes de respuesta a estas consultas son pequeños, pero si estos paquetes cambian de tamaño y se dan respuestas con paquetes grandes, podemos decir que se trata de un indicador de compromiso porque se está materializando un ataque.

7. **Un gran número de solicitudes para el mismo archivo:** Este es otro indicador de compromiso donde un atacante intenta acceder a un archivo o a un sistema de forma insistente; en condiciones normales, un usuario legítimo, realiza una petición para acceder a los mismos, pero en cambio, un atacante que no tiene las credenciales de acceso, realizará varias peticiones al mismo archivo o intentará ganar acceso usando herramientas de explotación, por lo cual se deben generar alertas que evidencien esta situación, ya que se puede tratar de un ataque.

8. **Tráfico irregular en los puertos de aplicaciones específicas:** usualmente los ataques se realizan utilizando puertos conocidos, sin embargo, existen técnicas de ataque que utilizan puertos no tan comunes, para reducir el riesgo de ser detectados por los controles de seguridad implementados. Un atacante puede aprovechar un programa legítimo que hace peticiones a un puerto determinado y hacer que este envié paquetes a través de un puerto poco usual para tener mando y control del sistema, evadiendo los controles de seguridad, por lo tanto, es importante monitorear el tráfico que se envían por los diferentes puertos y su aplicación específica.

9. **Cambios sospechosos del sistema de archivos y registros.:** Los atacantes realizan cambios en los archivos del sistema y en los registros, o se aloja en los servicios

legítimos utilizados por el sistema operativo para lograr mantener persistencia en un sistema o equipo, abrir puertas traseras y no ser detectados por los controles de seguridad o los sistemas de monitoreo; por esto es importante tener sistemas de monitoreo y control de cambios de los archivos críticos del sistema y los registros que permitan evidenciar y alertar rápidamente cuando se esté presentando este tipo de ataque y restaure los parámetros originales para evitar que se materialice el ataque**.**

10. **Consultas anómalas de DNS.** Este es un indicador de compromiso donde se efectúan ataques a los sistemas para tomar mando y control de los mismos a través de peticiones reversas y solicitud de conexiones a servidores o IPs desconocidas, ya que esto permite mantener comunicación con la víctima y brinda acceso a sus archivos y al sistema. Este tipo de indicador se enfoca en los patrones que dejan las consultas DNS maliciosas o extrañas a una IP o host específico y sus constantes llamados con tráfico irregular a los mismos servidores para la resolución de nombres de dominio, generando una alerta en comparación de las peticiones legitimas efectuadas a los DNS establecidos.

11. **Autenticaciones fallidas sobre los firewall;** Este tipo de situaciones se da cuando se está intentando hacer un ataque de fuerza bruta sobre el protocolo SSH, es importante monitorear los intentos de conexión al firewall y parametrizar el número máximo de intentos de conexión fallidos, de tal forma que se genere una alerta cuando se supera el número de intentos fallidos.

12. **Acceso remoto de usuarios con VPN:** Este indicador de compromiso busca detectar suplantación de usuarios corporativos. El atacante usa identificación de Usuarios Corporativos que tienen acceso a través de VPN para lograr acceso a la red corporativa y robar o alterar información sensible. Para identificar este intento de ataque, se requiere implementar esquemas de detección de accesos simultáneos del mismo usuario desde ubicaciones geográficas distintas.

13. **Transacciones no permitidas en SAP:** Consiste en el inicio de Transacción de usuarios no autorizados por medio de Listas Blancas en los diferentes ambientes de SAP. Se deben implementar mecanismos de monitoreo que permita la detección de transacciones críticas de usuarios no autorizados.

6. DESARROLLO DEL PROYECTO

Lograr una estrategia de Ciberseguridad y Ciberdefensa más efectiva en la protección de Infraestructuras Críticas, requiere que el proceso de identificación de Indicadores de Compromiso – IoC, esté complementado por un adecuado entendimiento de necesidades, un detallado levantamiento de información, completo inventario y clasificación de activos críticos, arquitectura de seguridad robusta y procesos bien definidos de gestión del riesgo y gestión de incidentes.

Adicionalmente, la constante evolución de las amenazas cibernéticas actuales y la aparición de nuevas cada vez más sofisticadas y complejas, hacen que la identificación de Indicadores de Compromiso – IoC sea un proceso dinámico que debe estar actualizándose para ir a la par con la aparición de nuevas ciberamenazas.

A continuación, se describen el conjunto de actividades a desarrollar en el proceso de identificación de los Indicadores de Compromiso – IoC, la definición de los casos de uso a implementar para la prevención proactiva de posibles incidentes de ciberseguridad y la arquitectura recomendada para lograr un modelo de seguridad más eficiente y efectivo en la protección de las infraestructuras críticas de las Organizaciones.

6.1. IDENTIFICACIÓN DE LA SITUACIÓN ACTUAL

Comprende las actividades de conocimiento de la Organización y levantamiento detallado de información, que permita identificar los controles tecnológicos y administrativos, servicios, iniciativas, planes, proyectos, estrategias, procesos, posturas de seguridad entre otros, existentes en la Organización que se relacionen, dependan, interactúen o alimenten las plataformas y soluciones tecnológicas que soportan los procesos críticos del negocio, para garantizar su integración, así como su adecuado funcionamiento dentro del nivel aceptable de riesgo definido por la Organización.

6.1.1. CONOCIMIENTO DE LA ORGANIZACIÓN

Esta fase contempla el entendimiento de los procesos críticos de la Organización, de tal manera que se pueda identificar:

- Misión y visión de la Organización
- Lineamientos estratégicos de negocio
- Requerimientos legales y regulatorios
- Identificación objetivos de Seguridad de la Información
- Cadena de valor de la Organización - Productos y servicios ofrecidos

- Identificación de información crítica de los procesos de negocio a proteger
- Actores relevantes en el flujo de la información
- Entendimiento del modelo de operación de TI
- Análisis de riesgos realizados previamente
- Otros

Esta actividad se realizará en conjunto con los responsables de los procesos críticos a proteger.

6.1.2. IDENTIFICACIÓN DE NECESIDADES DE CIBERSEGURIDAD

En esta fase se realizar la identificación de las necesidades de ciberseguridad para la protección de las infraestructuras críticas de la Organización, para esto es necesario realizar un levantamiento detallado de la información relacionada con los controles tecnológicos y procedimentales con los que cuenta la Organización para la protección de sus infraestructuras críticas.

Para realizar un óptimo y completo levantamiento de información de las necesidades de seguridad, que permita a la Organización realizar posteriormente la gestión de los controles de seguridad de manera óptima, escalable e integrable, aplicando las mejores prácticas y metodologías de la industria y específicamente lograr una adecuada identificación de los Indicadores de Compromiso – IoC a los que está expuesta la Organización, se recomienda utilizar como marco de referencia el "Marco de Ciberseguridad de NIST".

¿Por qué el Marco de Ciberseguridad de NIST?

A partir de la Orden Ejecutiva 13636 emitida por el presidente Barak Obama en febrero de 2013, se establecieron las bases que debería desarrollar el Marco de Ciberseguridad de NIST para mejorar la seguridad de las infraestructuras críticas (OBAMA, 2013).

Entre los objetivos de ciberseguridad establecidos en el Marco de NIST está el de "Ayudar a los responsables de la administración y operación de las infraestructuras críticas a gestionar los riesgos relacionados con la ciberseguridad." y aunque fue desarrollado inicialmente para la protección de las infraestructuras críticas de Estados Unidos, en la actualidad tiene aplicabilidad a cualquier Organización de cualquier tamaño en cualquier parte del mundo. (NIST, 2018)

El Marco de Ciberseguridad de NIST está dividido en 3 componentes principales: (NIST, 2017, págs. 7 - 12)

Figura 25. Componentes marco de referencia NIST

1. **Marco Central (Core Framework):** Comprende el conjunto de actividades y resultados de Ciberseguridad deseados, organizados en categorías y alineados con referencias informativas. Su organización permite de manera intuitiva y sencilla la comunicación de las actividades de ciberseguridad entre los diferentes niveles de la organización.

   El marco central está compuesto por las siguientes 5 Funciones:

   - **Identificar:** Permite la identificación de los sistemas, activos, datos y capacidades de la organización, su contexto de negocio, los recursos que soportan los procesos críticos y los riesgos de ciberseguridad que afectan el entorno empresarial, permitiéndole a la Organización enfocarse y priorizar sus esfuerzos, alineada con su estrategia de gestión de riesgos y necesidades del negocio.

   - **Proteger:** Permite desarrollar e implementar los controles de seguridad apropiados para garantizar la operación de las infraestructuras críticas, brindando la capacidad de limitar o contener el impacto de un evento potencial de ciberseguridad.

   - **Detectar:** Consiste en el desarrollo e implementación de las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad mediante el descubrimiento oportuno de dichos eventos.

   - **Responder:** Consiste en el desarrollo e implementación de las actividades apropiadas para reaccionar y tomar medidas frente a un evento de ciberseguridad detectado y contener o mitigar el impacto de un potencial evento de ciberseguridad.

   - **Recuperar:** Permite el desarrollo e implementación de actividades para la gestionar planes de resiliencia y retornar a la operación normal las

capacidades o servicios que hayan sido afectados por un evento de ciberseguridad.

Cada una de estas funciones se divide a su vez en categorías, subcategorías y referencias informativas relacionadas (guías, estándares, buenas prácticas de mercado)

2. **Niveles de implementación del marco (Implementation Tiers):** proporciona contexto sobre cómo una organización considera el riesgo de ciberseguridad y los procesos establecidos para gestionar ese riesgo. Se han definido 4 niveles y cada uno describe el incremento del grado de rigor y sofisticación en las actividades de gestión del riesgo de ciberseguridad. La definición del nivel de implementación tiene en cuenta las prácticas actuales de gestión de riesgos, el entorno de amenazas, requisitos legales y normativos, las prácticas de intercambio de información, objetivos corporativos y/o misionales, necesidades de gestión de riesgos de los procesos críticos del negocio y las limitaciones organizacionales. Las organizaciones deben determinar su nivel deseado, asegurando que el nivel seleccionado cumpla con los objetivos de la organización, sea factible de implementar y reduzca el riesgo de ciberseguridad a los activos y recursos críticos a niveles aceptables para la organización.

   Nivel 1 – Parcial:

   - **Procesos de gestión de riesgo:** No están formalizados, el riesgo es gestionado de manera informal (ad-hoc) y en algunos casos reactivamente. La priorización de las actividades de ciberseguridad no necesariamente está alineada con los objetivos de riesgo de la organización, el entorno de amenaza o los requisitos de negocios, corporativos o misiónales.

   - **Programas integrados de gestión de riesgos:** hay una limitada conciencia de riesgo de ciberseguridad en el nivel organizacional. La organización implementa la gestión del riesgo de ciberseguridad en forma irregular caso por caso debido a la experiencia variada o la información obtenida de fuentes externas. Es posible que la organización no tenga procesos que le permitan compartir información de ciberseguridad dentro de la organización.

   - **Participación externa:** La organización conoce su rol en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.

   - **Gestión de riesgos de la cadena de suministros cibernética:** La organización puede no comprender las implicaciones completas de los riesgos de la cadena de suministro cibernética o tener los procesos

establecidos para identificar, evaluar y mitigar los riesgos de su cadena de suministro cibernética.

Nivel 2 - Riesgos informados

- **Procesos de gestión de riesgo:** Las actividades de gestión de riesgos son aprobadas por la administración, pero no pueden establecerse como una política para toda la organización. La priorización de las actividades de ciberseguridad está directamente relacionada con los objetivos de riesgo de la organización, el entorno de amenazas o los requisitos de negocios o corporativos.

- **Programas integrados de gestión de riesgos:** Existe una conciencia de riesgo de ciberseguridad a nivel organizacional, pero no se ha establecido un enfoque en toda la organización para gestionar el riesgo de ciberseguridad. La información de ciberseguridad se comparte dentro de la organización de manera informal. La consideración de la ciberseguridad en los objetivos corporativos o de negocio puede ocurrir en algunos niveles de la organización, pero no en todos los niveles. La evaluación del riesgo cibernético de los activos de la organización no suele ser repetible ni recurrente.

- **Participación externa:** La organización conoce su rol en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.

- **Gestión de riesgos de la cadena de suministros cibernética:** La organización comprende los riesgos de la cadena de suministro cibernético asociados con los productos y servicios que respaldan la estrategia comercial de la organización o que se utilizan en los productos o servicios de la organización. La organización no ha formalizado sus capacidades para gestionar los riesgos de la cadena de suministro cibernética internamente o con sus proveedores y socios y realiza estas actividades de manera inconsistente.

Nivel 3 - Repetible

- **Procesos de gestión de riesgo:** Las prácticas de gestión de riesgos de la organización están formalmente aprobadas y expresadas como política. Las prácticas de ciberseguridad organizacional se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos corporativos y/o misionales y un panorama cambiante de amenazas y tecnología.

- **Programas integrados de gestión de riesgos:** Existe un enfoque en toda la organización para gestionar el riesgo de ciberseguridad. Las políticas, procesos y procedimientos informados sobre riesgos se definen, se implementan según lo planeado y se revisan. Se han implementado métodos consistentes para responder de manera efectiva a los cambios en el riesgo. El personal posee el conocimiento y las habilidades para cumplir con sus roles y responsabilidades asignados. La organización monitorea de manera consistente y precisa el riesgo de ciberseguridad de los activos de la organización. Los altos ejecutivos de ciberseguridad y demás áreas se comunican regularmente sobre el riesgo de ciberseguridad. Los altos ejecutivos aseguran la consideración de la ciberseguridad a través de todas las líneas de operación en la organización.

- **Participación externa:** La organización entiende sus dependencias y socios y recibe información de estos socios, lo que permite la toma de decisiones de gestión basadas en el riesgo dentro de la organización en respuesta a los eventos.

- **Gestión** de **riesgos de la cadena de suministros cibernética:** Un enfoque de toda la organización para gestionar los riesgos de la cadena de suministro cibernética se promulga a través de políticas, procesos y procedimientos de gestión de riesgos corporativo. Es probable que esto incluya una estructura de gobierno (por ejemplo, el Consejo de riesgos) que gestione los riesgos de la cadena de suministro cibernético en equilibrio con otros riesgos corporativos. Las políticas, los procesos y los procedimientos se implementan de forma coherente, según lo previsto y se supervisan y revisan continuamente. El personal posee el conocimiento y las habilidades para realizar las responsabilidades de gestión de riesgos de la cadena de suministro cibernética. La organización tiene acuerdos formales establecidos para comunicar los requisitos de referencia a sus proveedores y socios.

Nivel 4 - Adaptativo

- **Procesos de gestión de riesgo:** La organización adapta sus prácticas de ciberseguridad en base a las lecciones aprendidas y los indicadores predictivos derivados de las actividades de ciberseguridad anteriores y actuales. A través de un proceso de mejora continua que incorpora prácticas y tecnologías avanzadas de ciberseguridad cibernética, la organización se adapta activamente a un entorno cambiante de ciberseguridad y responde a las amenazas cambiantes y sofisticadas de manera oportuna.

- **Programas integrados de gestión de riesgos:** Existe un enfoque de toda la organización para gestionar el riesgo de seguridad cibernética que utiliza políticas, procesos y procedimientos informados sobre riesgos para abordar posibles eventos de ciberseguridad. La relación entre el riesgo de ciberseguridad y los objetivos corporativos y/o de negocio se entiende y se tiene en cuenta claramente al tomar decisiones. Los ejecutivos superiores monitorean el riesgo de ciberseguridad en el mismo contexto que el riesgo financiero y otros riesgos organizacionales. El presupuesto de la organización se basa en la comprensión del entorno de riesgo actual y previsto y los futuros apetitos de riesgo. Las unidades de negocios implementan la visión ejecutiva y analizan los riesgos a nivel del sistema en el contexto del apetito y las tolerancias del riesgo organizacional. La gestión del riesgo de ciberseguridad forma parte de la cultura organizacional y evoluciona a partir de la conciencia de las actividades previas, la información compartida por otras fuentes y el conocimiento continuo de las actividades en sus sistemas y redes. El riesgo de ciberseguridad está claramente articulado y entendido en todos los estratos de la empresa. La organización puede dar cuenta de forma rápida y eficiente de los cambios en los objetivos corporativos y/o misionales y los entornos de amenazas y tecnología en la forma en que se comunica y aborda el riesgo.

- **Participación externa:** La organización gestiona los riesgos y comparte activamente la información con los socios para garantizar que se distribuya y consuma información precisa y actualizada para mejorar la ciberseguridad antes de que ocurra un incidente de ciberseguridad.

- **Gestión** de **riesgos de la cadena de suministros cibernética:** La organización puede dar cuenta rápida y eficientemente de los riesgos emergentes de la cadena de suministro cibernética utilizando información en tiempo real o casi real y aprovechando un conocimiento institucionalizado de la gestión del riesgo de la cadena de suministro cibernético con sus proveedores externos y socios, así como internamente, en áreas funcionales relacionadas y en todos los niveles de la organización. La organización se comunica de manera proactiva y utiliza mecanismos formales (por ejemplo, acuerdos) e informales para desarrollar y mantener relaciones sólidas con sus proveedores, socios y compradores individuales y de la organización.

3. **Perfiles del marco (Framework Profiles):** Es la alineación de las funciones, categorías y subcategorías con los requisitos comerciales, la tolerancia al riesgo y los recursos de la organización. Un perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de seguridad cibernética que está bien alineada con los objetivos organizacionales y sectoriales, considera los requisitos legales/reglamentarios y las mejores prácticas de la industria y refleja las prioridades de gestión de riesgos.

Los perfiles se pueden usar para describir el estado actual o el estado objetivo deseado de actividades específicas de ciberseguridad. El perfil actual indica los resultados de ciberseguridad que se están logrando actualmente. El Perfil objetivo indica los resultados necesarios para alcanzar los objetivos de gestión de riesgos de ciberseguridad deseados. Los perfiles son compatibles con los requisitos de corporativos y de negocios y ayudan en la comunicación del riesgo dentro y entre las organizaciones.

La comparación de perfiles (por ejemplo, el perfil actual y el perfil objetivo) puede revelar brechas que deben abordarse para cumplir con los objetivos de gestión del riesgo de ciberseguridad. Un plan de acción para abordar estas brechas puede contribuir a la hoja de ruta descrita anteriormente. La priorización de la mitigación de brechas es impulsada por las necesidades de negocios de la organización y los procesos de gestión de riesgos. Este enfoque basado en el riesgo permite que una organización calcule las estimaciones de los recursos (por ejemplo, dotación de personal, financiación) para alcanzar los objetivos de seguridad cibernética de una manera rentable y priorizada.

¿Como usar el Framework de Ciberseguridad de NIST para la identificación de necesidades?

Lo primero que debe hacer la Organización es definir el alcance del proyecto, es decir determinar el o los procesos para los cuales va a hacer la identificación de los Indicadores de Compromiso – IoC.

Una vez establecidos los procesos sobre los que se va a hacer la identificación de los Indicadores de Compromiso – IoC, se procede a hacer el levantamiento de información y documentación de la identificación de necesidades; esta labor se puede realizar manualmente, descargando de la página del NIST el siguiente archivo en Excel: draft-2_framework-v1-1_core-excel.xls (Cybersecurity Framework - Draft Version 1.1 , 2017)

https://www.nist.gov/file/412481

Otra opción es descargar la herramienta Cyber Security Evaluating Tool – CSET®, desarrollada por el Industrial Control System Cyber Emergency Response Team – ICS – CERT del Departamento de Seguridad Nacional de Estados Unidos y la cual proporciona un enfoque sistemático, disciplinado y repetible para evaluar la postura de seguridad de una Organización.

Figura 26. Cyber Security Evaluating Tool – CSET®

Para descargar la última versión de la herramienta, se puede entrar al siguiente enlace: (CSET Download, 2017)

https://www.us-cert.gov/forms/csetiso

Figura 27. Página de inicio – CSET®

Al ingresar a la herramienta, en la pestaña **"Preparation"** esta solicita la información de la Organización.

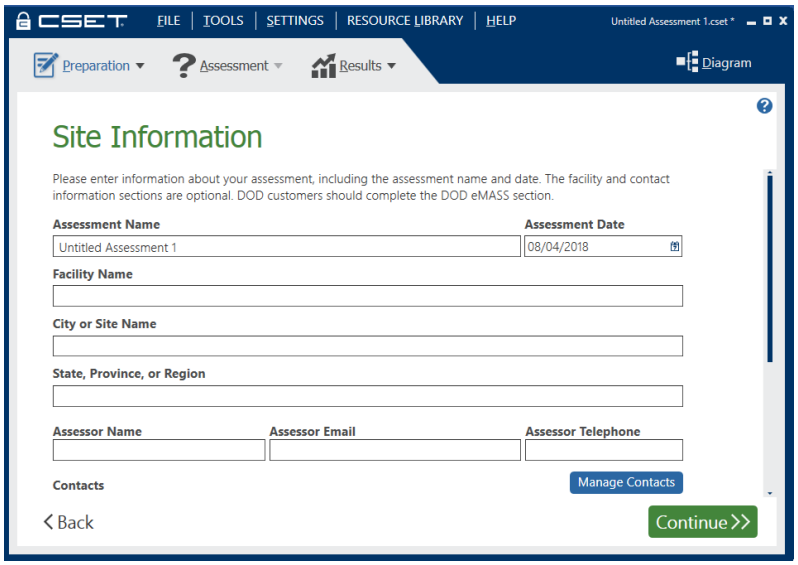


Figura 28. Sección de Preparación – CSET®

Esta misma sección ofrece la posibilidad de seleccionar el marco de referencia o estándar de ciberseguridad a utilizar para realizar la evaluación de la situación actual de la Organización; debemos escoger la opción: "Cybersecurity Framework based Approach" , el cual usa el marco de referencia de NIST.

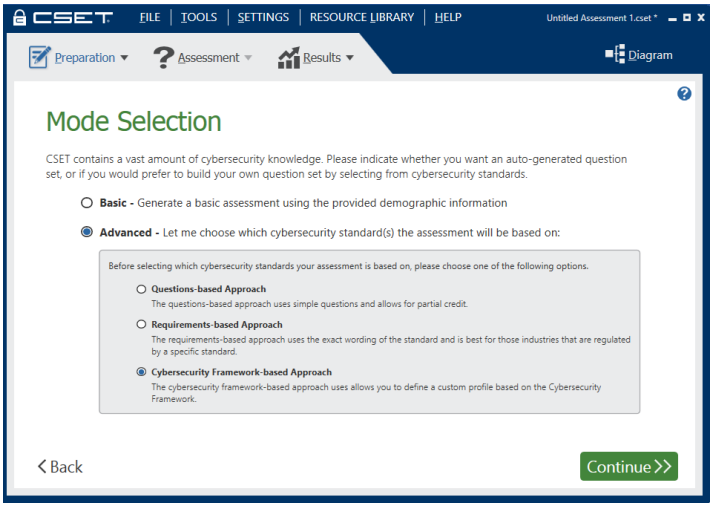


Figura 29. Sección de Preparación – CSET®

El último paso de la fase de preparación en la herramienta CSET® es la creación o del perfil del marco de Ciberseguridad, también se puede usar el perfil que viene precargado en la herramienta.

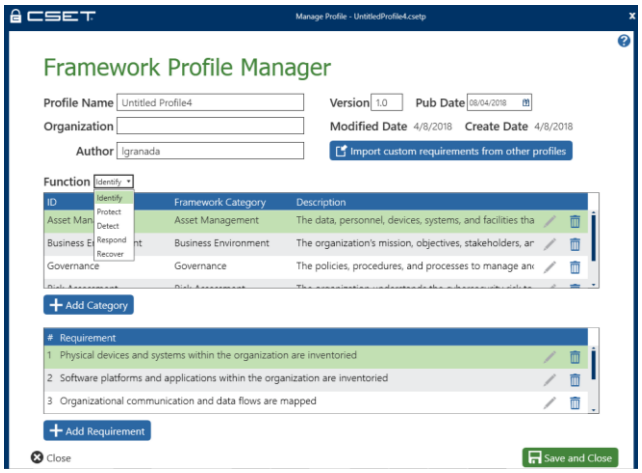


Figura 30. Configuración perfil – CSET®

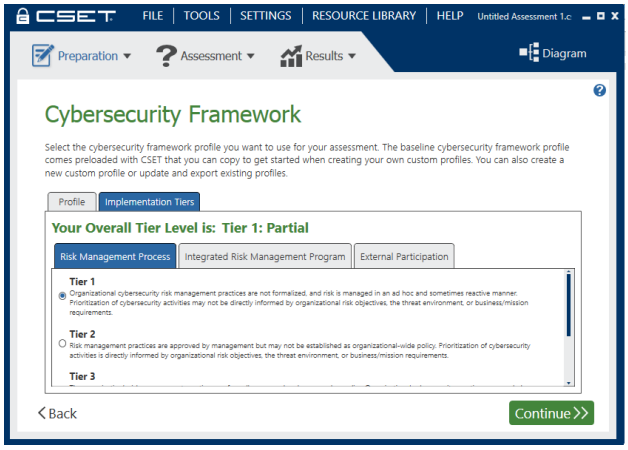


Figura 31. Marco implementación – CSET®

Una vez preparada la herramienta se procede a hacer la evaluación de Ciberseguridad que nos permita identificar las necesidades de seguridad que está teniendo la Organización, para esto pasamos a la pestaña **"Assessment"**

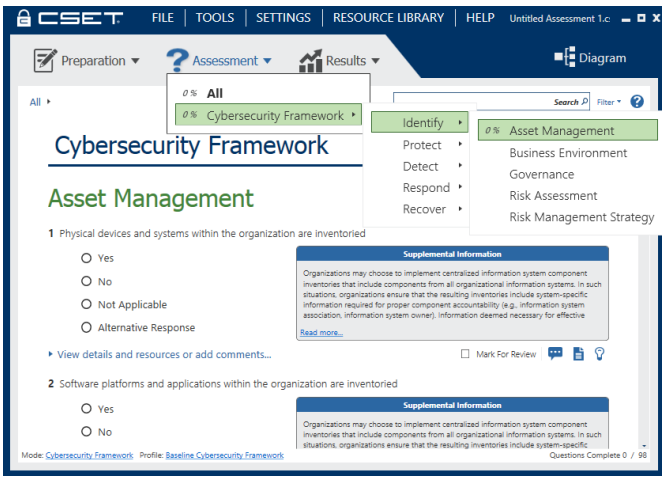


Figura 32. Cuestionario de evaluación ciberseguridad – CSET®

Luego de respondidas todas las preguntas del Marco de Ciberseguridad, en la pestaña "Results" se obtiene el resultado de la evaluación y al final se puede personalizar la generación del reporte completo

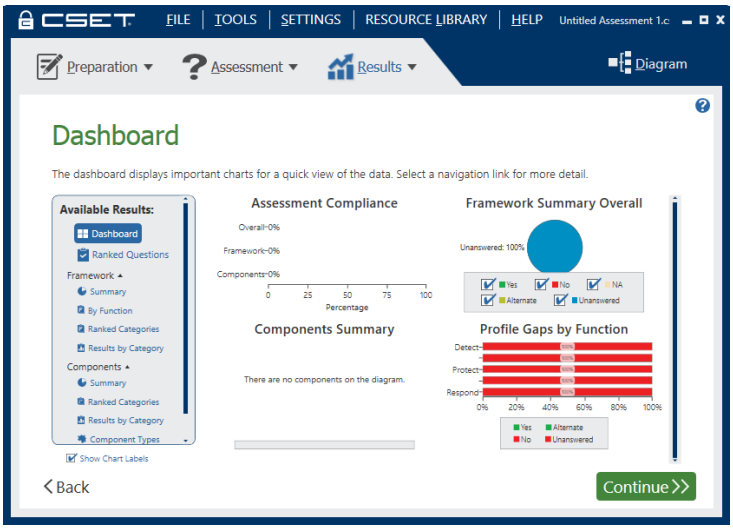


Figura 33. Resultados de la evaluación – CSET®

La pestaña RESOURCE LIBRARY contiene una completa librería de estándares, reportes, plantillas, guías de ciberseguridad, recomendaciones, etc. disponibles para ser aprovechadas por los usuarios de la herramienta.

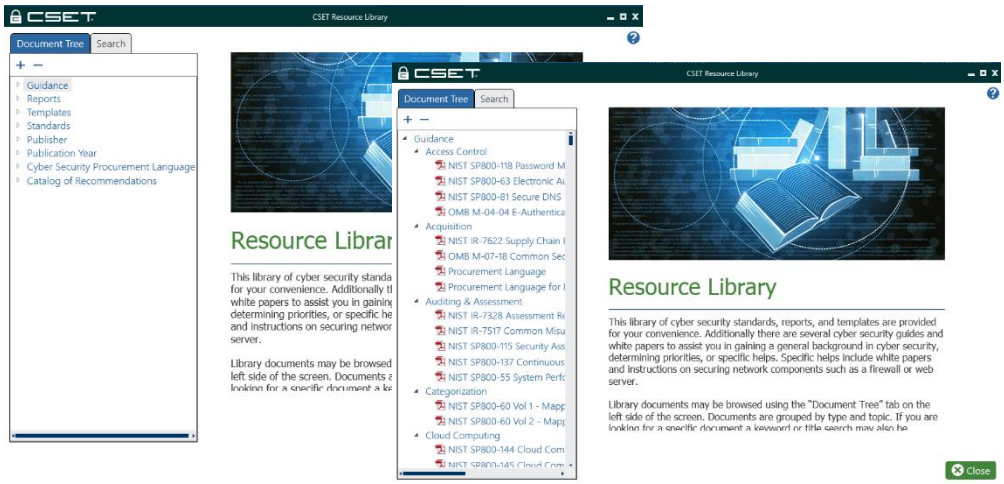


Figura 34. Librería – CSET®

Una vez identificadas las necesidades de seguridad de la Organización, se procede a complementar el levantamiento de información detallada de controles tecnológicos y procedimentales que soportan los procesos críticos del negocio que se van a proteger:

- Levantamiento de necesidades de control por host (server).
- Canales de Comunicación requeridos para el transporte y recolección de eventos (anchos de banda).
- Configuraciones de los equipos a integrar al SIEM (Correlacionador de Eventos).
- Arquitectura y funcionamiento de las plataformas contempladas en el alcance.
- Validación de requerimientos funcionales.
- Validación de requerimientos técnicos.
- Levantamiento de necesidades para la generación de reportes.
- Usuarios por notificar (notificación y escalamientos).
- Las demás que resulten necesarias.

Se incluye también el entendimiento del entorno de operación y flujos de información, de tal manera que se pueda identificar y definir los casos de uso, punto focal para la definición del modelo de Indicadores de Compromiso – IoC. Durante esta fase se realizará la documentación detallada de:

- Conocimiento de la Organización - Cadena de Valor
- Procesos críticos de negocio
- Flujos de información e información crítica
- Aplicaciones que soportan los procesos críticos de negocio
- Actores relevantes en el flujo de la información
- Usuarios/Roles que intervienen en los procesos
- Identificaciones de Actividades consideradas como anómalas (Condiciones de alerta)
- Requerimientos legales y regulatorios
- Entendimiento del modelo de operación de TI

6.2. MODELAMIENTO DE LA ARQUITECTURA DE CIBERSEGURIDAD PARA LA IDENTIFICACIÓN DE LOS INDICADORES DE COMPROMISO – IOC

Luego de realizado el entendimiento de necesidades y levantamiento detallado de información, se realizará el modelamiento y/o afinamiento de la arquitectura de ciberseguridad que tenga implementada la Organización, que brinde la capacidad necesaria para una proactiva identificación de los IoC que permita incrementar y optimizar la eficiencia en la gestión de incidentes de ciberseguridad a las infraestructuras críticas de la Organización para su análisis, investigación y/o respuesta, que nos lleve a obtener respuesta al "Qué, Quién, Cómo, Cuándo, Dónde y Por qué" de dicho incidente.

Debido a la proliferación de vectores de ataque, el crecimiento acelerado de la cantidad de ciberamenazas a las infraestructuras críticas, la dificultad en la detección de las nuevas ciberamenazas, su complejidad y alto impacto cuando se materializa el ciberataque, han llevado a los líderes en la industria de la Ciberseguridad a evolucionar los modelos de Ciberseguridad, especialmente en lo relacionado con el monitoreo y correlación de eventos y la gestión de incidentes de ciberseguridad, hacia un nuevo modelo denominado SOAPA por sus siglas en inglés: **S**ecurity **O**perations and **A**nalytics **P**latform **A**rchitecture (Enterprise Strategy Group - ESG , 2018)

6.2.1. ARQUITECTURA SOAPA

Algunos de los más importantes factores que impulsaron la evolución del concepto tradicional de SOC a una arquitectura SOAPA es el incremento exponencial en el volumen de logs y eventos en las organizaciones y el crecimiento en la implementación de tecnologías de información y comunicaciones para apalancar los negocios, haciéndose cada vez más difícil su procesamiento, análisis y gestión, lo que conlleva a una mayor complejidad de las redes de datos con una gran dependencia de los procesos de negocio de las tecnologías TIC.

Todo esto puso en evidencia la necesidad de:

- **Centralización y normalización de los datos de seguridad internos y externos:** esto conducirá a mejores análisis para una mejor identificación de Identificadores de Compromiso – IoC y la toma de decisiones más asertiva. Decisiones basadas en análisis de inteligencia.

- **Automatización y flujos de trabajo:** para que los equipos de ciberseguridad resuelvan simultáneamente las presiones de los ataques y maximicen la eficiencia del personal, deben contar con automatizaciones y flujos de trabajo repetibles y documentados.

SOAPA es una arquitectura dinámica, que integra diferentes tecnologías para procesar datos, crear inteligencia, automatizar tareas rutinarias, organizar complejos procesos de seguridad y en última instancia, ofrecer información que apoye una toma de decisiones mejor y más rápida para mitigar los riesgos de nuestros clientes.

El dinamismo de SOAPA permite que se agreguen incrementalmente en la medida que se vayan requiriendo nuevas fuentes de datos y controles de seguridad como:

- SIEM – Security Information and Event Management
- EDR – End Point Detecction and Response
- IRP – Incident Incident Response Platform
- TIP – Threat Intelligence Platform
- UEBA – User and Entity Behavior Analytics
- VM – Vulnerability Management
- Sandboxes

A continuación, se presenta de manera esquemática el modelo de arquitectura SOAPA: (Enterprise Strategy Group, Inc, 2017)

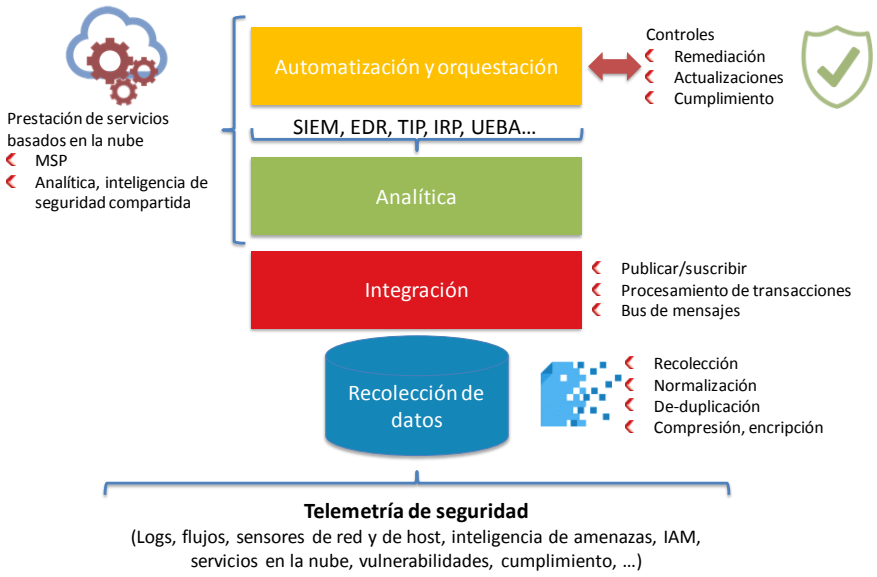


Figura 35. Arquitectura SOAPA

El servicio inicia con la recolección, normalización, de-duplicación (eliminación de registros redundantes), compresión y/o encripción de los datos recibidos cuando se requiera, de los datos de telemetría de seguridad (logs, eventos, información no estructurada del cliente, disponibilidad, políticas, clasificación de información, mapas de riesgo, etc).

Toda esta información recolectada es entregada en la siguiente capa de integración, denominada Bus de Seguridad o Bus de Integración de Servicios; esta capa está diseñada para recibir toda la telemetría recolectada proveniente de cualquier tipo de plataforma de cualquier fabricante que tenga implementada la Organización y realiza un proceso de traducción, para que todas las plataformas se entiendan, permitiendo que estas se puedan comunicar entre sí, logrando de esta forma identificar mucho más rápido cuando un incidente de seguridad se está presentando y de esta forma generar el correspondiente Indicador de Compromiso – IoC.

Este bus de integración también se alimenta de publicaciones y subscripciones a distintas fuentes de información y plataformas de inteligencias de seguridad de los líderes de la industria de Ciberseguridad como XForce, Threat Cloud, First, etc. Igualmente se hace el procesamiento de transacciones.

La siguiente capa de analítica, permite modelar la forma en que queremos ver la información que está en el correlacionador de eventos, en las plataformas de análisis de amenazas, respuestas a incidentes, análisis de comportamiento, etc. e inclusive apoya la realización de análisis forenses. Para esto es necesario hacer la orquestación y automatización de todas las plataformas de seguridad con las que cuenta la Organización, para poder analizar de una manera más eficiente los exponenciales volúmenes de información estructurada y no estructurada que se generan, Indicadores de Compromiso – IoC, eventos de seguridad etc.

Esta arquitectura SOAPA se constituye en un gran apoyo en la identificación de los Indicadores de Compromiso – IoC ya que su objetivo final consiste en identificar proactivamente cuando se presenta una amenaza real de ciberataque o se está presentando un problema que aunque no obedece a un ciberataque si puede generar un incidente de ciberseguridad, identificar más fácilmente cuando se está presentando un ciberataque, donde se inició, que lo generó, como lo hizo, hasta donde llegó, que impacto tuvo y por qué se produjo.

6.2.2. CENTRO DE INTELIGENCIA DE SEGURIDAD

El Centros de Inteligencia de Seguridad – SIC por sus siglas en inglés son parte integral de las arquitecturas SOAPA; reúne el conjunto de plataformas fuentes de eventos, procesos operativos y profesionales en seguridad de la información, tienen

como función la protección en tiempo real frente a ciberamenazas nuevas y conocidas y actúa como Centro de Respuesta a Incidentes de Seguridad – CSIRT.

Permite tomar todos los eventos de seguridad que se están presentando en la infraestructura de la Organización, analizar dichos eventos y poder definir si corresponden a un intento de ataque o un incidente de seguridad que se está presentando.

Para realizar esto, es necesario entender cuál es el flujo de información de la infraestructura crítica de la Organización, a partir de sus procesos críticos de negocio.

Utilizando metodologías de gestión de riesgos descrita en el capítulo anterior, se busca entender cuál es el flujo de información de los procesos críticos del negocio del cliente; se identifica que usuarios interactúan con el proceso, cuales es la plataforma tecnológica asociados el proceso, que infraestructura de seguridad tiene el proceso para protegerlo y el inventario de activos críticos. Todo esto se identifica y se documenta en la CMDB para poder tener un entendimiento completo del proceso.

Si la Organización no tiene plenamente identificados cuales son los activos asociados a sus procesos críticos, será necesario hacer este inventario, siguiendo los pasos descritos en el capítulo 5, posteriormente hacer la identificación de vulnerabilidades y realizar el parcheo de dichas vulnerabilidades.

Con toda esta información se hace la identificación de los Indicadores de Compromiso – IoC, se definen las líneas base de comportamiento y se construyen los casos de uso que permitan identificar proactivamente posibles incidentes de seguridad y prevenir que estos incidentes se materialicen.

Entre las actividades más importantes que debe realiza un SIC – CSIRT están:

- Servicios reactivos (Tratamiento de incidentes y mitigación de daños)
- Alertas y advertencias
- Tratamiento de incidentes
- Análisis de incidentes
- Apoyo a la respuesta de incidentes
- Coordinación de la respuesta a incidentes
- Respuesta a incidentes en sitio
- Análisis de la vulnerabilidad
- Tratamiento de la vulnerabilidad

- Respuesta a la vulnerabilidad
- Coordinación de la respuesta a la vulnerabilidad
- Servicios proactivos (Orientados a la prevención)
- Comunicados
- Observatorio de tecnología
- Evaluaciones o auditorias de seguridad
- Configuración y mantenimiento de la seguridad
- Difusión de información relacionada con la seguridad
- Manejo de Instancias (Incluye el análisis de cualquier archivo u objeto encontrado en un sistema que pueda intervenir en acciones maliciosas, como restos de virus, gusanos, secuencias de comandos, troyanos, ransomware, etc.)
- Análisis de instancias
- Respuestas a las instancias
- Coordinación a las respuestas a las instancias
- Gestión de la calidad de la seguridad (Tienen objetivos a más largo plazo e incluyen servicios adicionales de consultoría y las medidas de tipo educativo).
- Análisis de riesgos
- Continuidad del negocio y recuperación tras un desastre
- Consultoría de Seguridad
- Sensibilización
- Educación / Formación
- Evaluación o certificación de productos
- Servicios de inteligencia en Deep web y Dark web para protección de marca

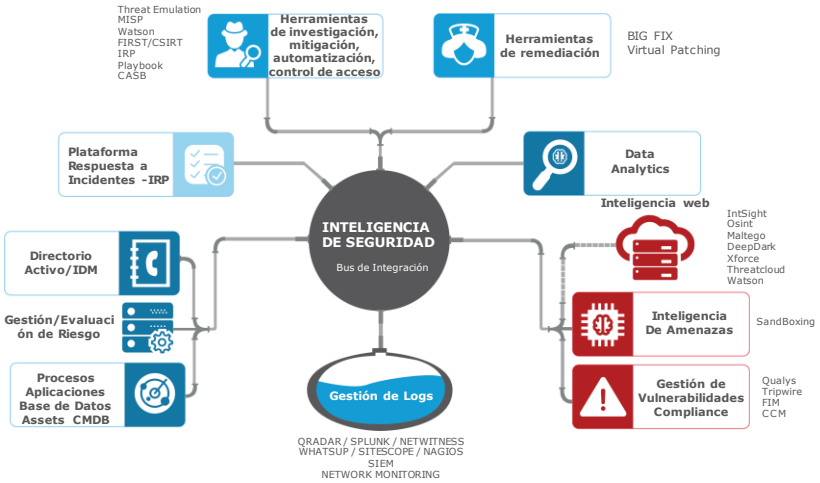


Figura 36. Esquema Centro Inteligencia de Seguridad

6.3. DEFINICIÓN DE LOS CASOS DE USO

Una vez identificados los Indicadores de Compromiso – IoC que pueden afectar las Infraestructuras Críticas de la Organización, se procede al modelamiento de los casos de uso que permitirán a la Organización prevenir proactivamente la identificación y/o neutralización de los intentos de ciberataques, optimizando el proceso de gestión de incidentes.

Los casos de uso son la descripción paso a paso de actividades asociadas a los procesos de negocio donde intervienen personas y tecnologías; permiten la perfilación de los diferentes Indicadores de Compromiso – IoC que se pueden presentar en una organización, mediante la parametrización de los eventos considerados anómalos, lo que y permite identificar el tipo de ataque para el cual se está definiendo el caso de uso, de tal forma que se pueda detectar, prevenir y neutralizar proactivamente dicho ataque cuando se esté presentando.

A continuación, se presentan algunos ejemplos de casos de uso:

Caso de Uso 1	**Violación de políticas de acceso y uso correcto de credenciales de acceso**
Descripción	Controlar el acceso autorizado a los sistemas y aplicaciones de la Organización desde uno o varios ambientes geográficos
Objetivo	Detectar incumplimiento de políticas de control de acceso de usuarios
Condiciones de alerta	Alertar sobre múltiples autenticaciones simultaneas de un mismo usuario Inicio de sesión desde ubicaciones geográficas no autorizadas Alerta por intentos fallidos de conexión
Fuentes de Datos	Logs del Directorio Activo, firewalls, IPS, Proxy, Endpoint, IDM

Caso de Uso 2	**Detección eventos salida internet**
Descripción	Cuando un equipo interno de la compañía genere un alto número de peticiones hacia internet este indicará en el FW e IPS que es posible que una máquina este contaminada con malware o esté enviando ataques a externos
Objetivo	Detectar incumplimiento de políticas de control de acceso de usuarios
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea:

	-FW: Múltiples conexiones hacia redes externas -IPS: Detección de firma que involucre la misma IP destino en las conexiones de FW.
Fuentes de Datos	Firewall, IPS

Caso de Uso 3	**Detección reconocimiento objetivos**
Descripción	Reconocimiento de servicios críticos
Objetivo	Detectar un posible ataque interno de reconocimiento de puertos a los servidores principales
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea: -FW: Detecta conexiones fallidas y satisfactorias hacia los diferentes servidores -IPS: Se detectan firmas relacionadas con reconocimiento hacia la granja de servidores con destino de direcciones críticas para el negocio
Fuentes de Datos	Firewall, IPS, topología de la infraestructura, EPO

Caso de Uso 4	**Detección de ataques específicos**
Descripción	Alto número de conexiones hacia un servicio especifico
Objetivo	Identificar ataques internos realizados hacia los servidores principales
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultánea: -FW: Detecta conexiones satisfactorias hacia los servidores críticos -IPS: Se detecta una firma de un servicio: Web, SSH, Correo; Base de dato, etc. Con destinos de direcciones críticas para el negocio
Fuentes de Datos	Firewalls, IPS, topología de la infraestructura

Caso de Uso 5	**Detección DOS**
Descripción	Denegación de servicios hacia servidores internos
Objetivo	Detectar ataques que puedan llegar a afectar la disponibilidad del servicio
Condiciones de alerta	Alertar cuando ocurran los siguientes eventos de forma simultanea: -FW: Detecta un alto numero de conexiones permitidas hacia redes internas

	-IPS: Detecta firmas relacionadas con DoS con destino de direcciones críticas para el negocio
Fuentes de Datos	Firewall, IPS

Caso de Uso 6	**Detección Usuario VPN**
Descripción	Detección conexiones VPN con un mismo usuario desde orígenes diferentes
Objetivo	Detectar conexiones VPNs establecidas por un mismo usuario desde sitios múltiples orígenes
Condiciones de alerta	Alertar cuando el origen de la primera conexión y el origen de la segunda conexión sean diferentes.
Fuentes de Datos	Firewall

Caso de Uso 7	**Detección de amenazas externas sobre infraestructura crítica**
Descripción	Detectar actividades anómalas provenientes de fuentes externas que puedan afectar la disponibilidad de las aplicaciones críticas de negocio
Objetivo	Identificar ataques que puedan afectar la disponibilidad de las aplicaciones críticas
Condiciones de alerta	Flujos de tráfico desde una misma dirección IP o hacia uno o múltiples puertos
Fuentes de Datos	Firewalls, switches, routers, access point, IPS, topología de la infraestructura

Caso de Uso 8	**Detección de incidentes específicos**
Descripción	Detección de un alto número de conexiones concurrentes desde un mismo destino hacia servicios específicos
Objetivo	Identificación de ataques de denegación de servicio hacia servidores Web
Condiciones de alerta	Un alto número de peticiones originadas desde una misma dirección IP origen por el puerto 80 o 443
Fuentes de Datos	Firewall

Caso de Uso 9	**Autenticaciones fallidas sobre los FW**
Descripción	Detección de intentos de conexiones fallidas sobre el fw por medio del protocolo SSH
Objetivo	Identificación de posibles ataques de fuerza bruta sobre el protocolo SSH
Condiciones de alerta	Se detectan 3 intentos de conexión fallidas sobre los modulos y managment del fw
Fuentes de Datos	Firewall

Caso de Uso 10	**Caidas principales VPN´s Site to Site**
Descripción	Detección de errores en la comunicación VPN
Objetivo	Identificar indisponibilidad sobre las principales VPN´s
Condiciones de alerta	El estado de la VPN es down debido a errores en la comunicación
Fuentes de Datos	Firewall

6.4. PROCESO GESTIÓN DE INCIDENTES

La administración de incidentes, habilita a la Organización para administrar y responder de manera efectiva cuando un incidente ocurre, con el fin de minimizar el impacto que las brechas de seguridad de la información tengan sobre la confidencialidad, integridad y disponibilidad de la información.

6.4.1. ALCANCE

El alcance de este procedimiento incluye los procesos de:

- Detección y registro de incidentes de seguridad
- Clasificación o Tipificación del incidente
- Seguimiento y diagnóstico del incidente
- Notificación,
- Contención y solución, y
- Cierre del incidente

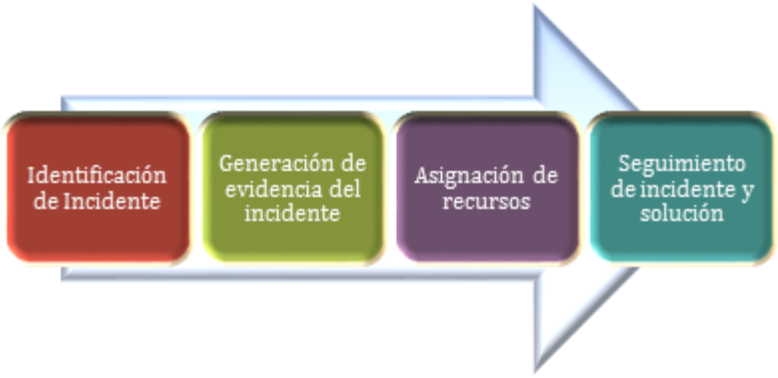
6.4.2. MEDIOS DE ATENCIÓN

Los medios a utilizar para el reporte de incidentes son:

- Teléfono (extensión)
- Intranet Corporativa

6.4.3. DESCRIPCIÓN DEL PROCESO

Siguiendo los lineamientos de las mejores prácticas de gestión de incidentes proporcionadas por ITIL y los requisitos asociados e la norma ISO 20000. A continuación, se muestra el proceso en diagrama de bloques:



El reporte del incidente se realizará a través de los ingenieros de monitoreo y operaciones quienes informarán de fallas a raíz del análisis y monitoreo de la plataforma o debido a reportes directos de incidentes por parte de persona de la Organización. Se asignará un número de ticket en el cual quedará consignada toda la información del desarrollo y solución del incidente y se tomarán los datos necesarios para ingresar la solicitud al sistema de soporte. A partir de este momento se dará inicio al estudio y solución del caso.

El analista de monitoreo que atiende la solicitud de servicio mantendrá informada a la Organización sobre el progreso de las solicitudes reportadas y consignará el caso para que la Organización tenga el registro de los casos. Adicionalmente, los ingenieros de operación y monitoreo tendrán el conocimiento apropiado para realizar un troubleshooting inicial en pro de encontrar una solución en un periodo menor de tiempo el cual estará claramente definido.

Se elaborará una guía donde se definirán todos los contactos, teléfonos, correos y demás instrumentos necesarios para garantizar que el servicio de soporte sea prestado de manera eficiente. Además, ese documento tendrá el detalle del procedimiento en caso que la Organización requiera mayor atención en alguna situación puntual o requiera realizar seguimiento de los casos reportados por el mismo.

Una vez el registro del caso se haya realizado, se notifica a los ingenieros de soporte quienes inician la labor de revisión y diagnóstico. Se buscará en la base de conocimiento local y del fabricante para encontrar la solución final o una medida alterna (solución temporal) que le permita a la Organización continuar con su operación. En caso que el analista de soporte no encuentre una solución definida previamente en la base de conocimiento, se procede a escalar al soporte en tercer nivel (fabricante) para continuar con el manejo y seguimiento del caso. A todos los casos se les hará seguimiento por un

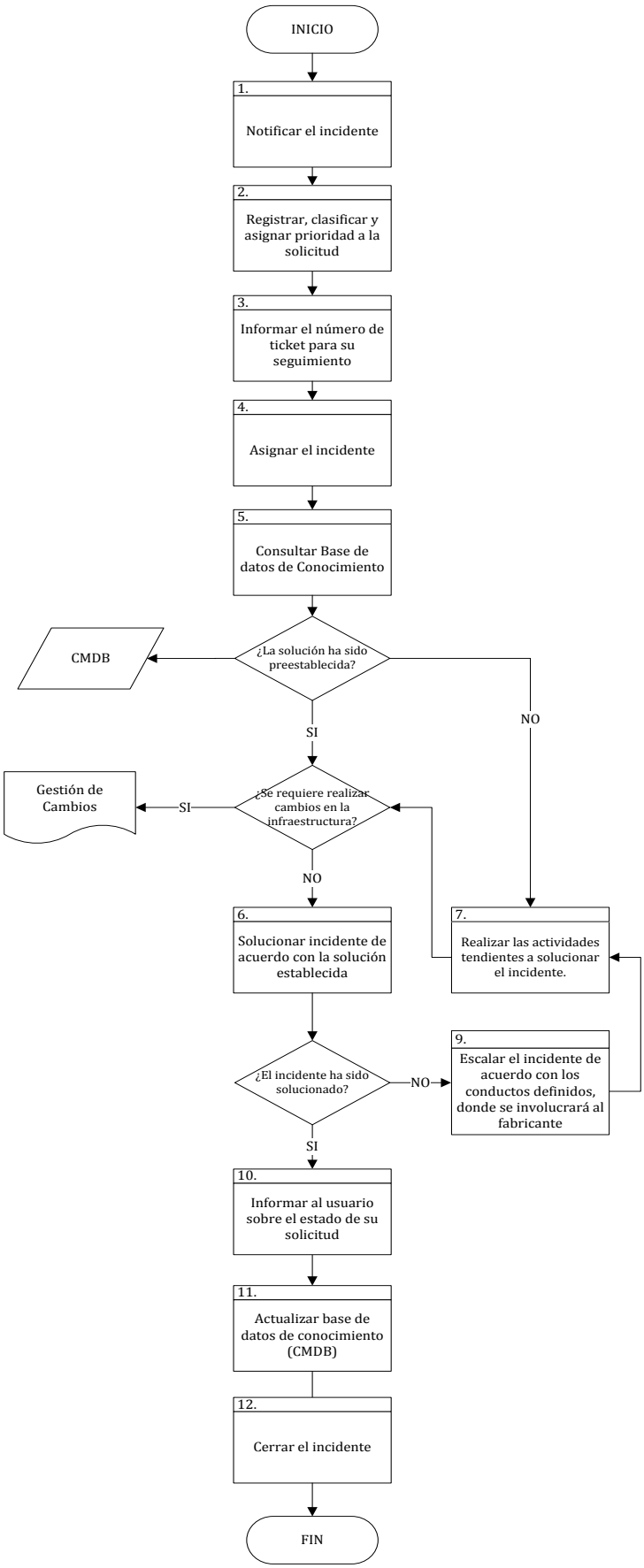
grupo dedicado de ingenieros los cuales tienen la responsabilidad de hacer el seguimiento, realizar actualizaciones y facilitar los medios para solucionar rápidamente los incidentes de la Organización.

Se elaborará un procedimiento de solicitud de aprobación donde se encontrará plasmado el procedimiento mediante el cual la Organización comunica el método para solicitar información, autorización y todo lo relacionado con procesos internos. La finalidad es que todos los procesos de la Organización sean adoptados por el grupo que brinde el soporte de la plataforma, realizándolo de la manera más transparente posible.

El caso será cerrado de común acuerdo con la Organización, cuando el problema sea corregido y la solución sea aceptada.

6.4.4. DIAGRAMA DE FLUJO DEL PROCESO

A continuación se presenta el diagrama de flujo del proceso:


INICIO
1.
Notificar el incidente
2.
Registrar, clasificar y asignar prioridad a la solicitud
3.
Informar el número de ticket para su seguimiento
4.
Asignar el incidente
5.
Consultar Base de datos de Conocimiento
¿La solución ha sido preestablecida?
CMDB
NO
SI
¿Se requiere realizar cambios en la infraestructura?
Gestión de Cambios
SI
NO
6.
Solucionar incidente de acuerdo con la solución establecida
7.
Realizar las actividades tendientes a solucionar el incidente.
¿El incidente ha sido solucionado?
NO
9.
Escalar el incidente de acuerdo con los conductos definidos, donde se involucrará al fabricante
SI
10.
Informar al usuario sobre el estado de su solicitud
11.
Actualizar base de datos de conocimiento (CMDB)
12.
Cerrar el incidente
FIN

6.4.5. FORMATO REPORTE DE INCIDENTES

Fecha del Incidente	
Incidente No.	
Número de identificación del incidente o evento relacionado:	

IDENTIFICACIÓN PERSONAL Y MESA DE AYUDA

Nombres y Apellidos:	
Cargo:	
Teléfono:	
Dirección:	
e-mail:	

IDENTIFICACIÓN PERSONAL ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD

Nombres y Apellidos:	
Cargo:	
Teléfono:	
Dirección:	
e-mail:	

DESCRIPCIÓN DEL INCIDENTE DE SEGURIDAD

¿Qué ocurrió?

¿Cómo ocurrió?

¿Por qué ocurrió?

¿Componentes afectados?

¿Impactos adversos en el negocio?

¿Vulnerabilidades identificadas?

DETALLES DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN

Fecha y hora en que ocurrió el evento	
Fecha y hora en que se descubrió el evento	
Fecha y hora en que se reportó el evento	

¿Ha terminado el evento? (marque según sea adecuado) Si ☐ No ☐

Si es afirmativo, ¿cuánto ha durado el evento en:	Días:	Horas:	Minutos:
Si no, especifique cuanto a durado hasta ahora:			

6.4.6. TIPIFICACIÓN DE INCIDENTES

TIPO 1. CONTINUIDAD DE NEGOCIO – DISPONIBILIDAD (indique los tipos de amenaza implicados)			
Falla del hardware (FH)		Falla del software (FS)	
Incendio (IN)		Falta de personal (FP)	
Inundación (ID)		Error de operaciones (EO)	
Error de usuario (EU)		Error de mantenimiento de hardware (EH)	
Error de diseño (ED)		Error de mantenimiento de software (ES)	
Especifique:			

TIPO 2. ACCESO NO AUTORIZADO (indique los tipos de amenaza implicados)			
Acceso lógico o físico sin permiso a una red (AR)		Acceso lógico o físico sin permiso a una aplicación (AA)	
Acceso lógico o físico sin permiso a los datos (AD)		Acceso lógico o físico sin permiso a un Sistema (AS)	
Acceso lógico o físico sin permiso a otro recurso. (SO)			
Especifique:			

TIPO 3. USO INAPROPIADO DE RECURSOS (indique los tipos de amenaza implicados)		
Violación de una política de uso aceptable de recursos (VI)		
Especifique:		

TIPO 4. CÓDIGO MALICIOSO (CM) (indique los tipos de amenaza implicados)			
Virus (VI)		Gusano (GU)	
Troyano (TR)		Cualquier código malintencionado que infecte un sistema (OC)	
Especifique:			

TIPO 5. MÚLTIPLES COMPONENTES (MC) (indique los tipos de amenaza implicados)	
Continuidad del negocio	Código malicioso
Acceso no autorizado	Múltiples componentes
Especifique:	

7. RESULTADOS

Una vez definidos e implementados los casos de uso que soportan los Indicadores de Compromiso – IoC, se procede a la recolección de evidencias de compromiso, análisis de las evidencias de compromiso y presentación de informes.

A continuación, se presentan algunos ejemplos de reportes de evidencias de compromiso y análisis de dichas evidencias:

1. MSSQL: SQL Server Worm Slammer

IP Origen	Categorización	País registrador	Total Diciembre	Total Noviembre
	IPs de escaneo (100%)	Vietnam	578	70
	IPs de escaneo (100%)	China	519	48
	IPs dinámicas (71%)	Ucrania	372	41
	IPs de escaneo (100%)	China	291	9
	IPs de escaneo (100%)	China	287	11
	IPs de escaneo (100%)	China	238	10
	No sospechoso	China	207	21
	No sospechoso	China	18	0
	Arte / Museos / Teatros	Rusia	9	2
	IPs de escaneo (71%)	China	8	0
	IPs de escaneo (100%)	Estados Unidos	7	0
	IPs de escaneo (86%)	China	7	2

- Se registraron 2606 eventos de la firma MSSQL: SQL Server Worm Slammer desde diferentes orígenes registrados en Vietnam, China y Ucrania principalmente, hacia los pool públicos de xxxxxx(xxxx.xxx.x y xx.xx.x.x). En comparación con los eventos recibidos en el mes de Noviembre, en Diciembre se recibieron 2206 eventos más de este tipo.

- Esta firma hace referencia a la detección de un gusano que busca generar denegación de servicios en los equipos publicados en Internet. Este tipo de exploit se aprovecha de una vulnerabilidad de desbordamiento de búfer en productos Microsoft® SQL Server™ 2000 y Microsoft Desktop Engine 2000.

- **Acciones por realizar:**

  ⇨ Se recomienda instalar los últimos parches de seguridad sobre todos los productos Microsoft que estén publicados en Internet de acuerdo al boletín MS02-039 (https://technet.microsoft.com/library/security/ms02-039).

- ⇨ Bloquear las IPs origen involucradas en estas conexiones.
- ⇨ Bloquear en el Firewall todo tráfico entrante por el puerto 1434 UDP.

2. Detección de uso de cifrado débil

Dirección IP	URL registrada	Total eventos
		411
		169
		36
		34
		31
		20
		2
		2
		2
		1
		708

- Se detectan 708 eventos de la firma *SSL: OpenSSL Weak cipher use detected* que involucra direcciones IP registradas bajo el dominio de xxxx.
- Esta firma indica que se realizó una detección del uso de métodos de cifrado débiles en los portales web relacionados en la presente tabla y que sin las debidas protecciones en cada una de las aplicaciones locales, podrían verse expuestos a un gran número de vulnerabilidades existentes sobre OpenSSL.
- **Acciones por realizar:**
  - ⇨ Se recomienda contactar a cada uno de los administradores de los servicios web relacionados en la tabla presentada, y solicitarles el reforzar los métodos de cifrado usados en estas aplicaciones.
  - ⇨ Evitar el uso de protocolos de cifrado como DES y RC4.
  - ⇨ Deshabilitar SSL 2.0 y SSL 3.0
  - ⇨ Deshabilitar TLS 1.0

3. Infección de equipos de red

Nombre del Equipo	IP Origen	Nombre de Usuario	Nombre de la Amanaza	Nombre del archivo infectado	Total
		SYSTEM	none	null	7
		SYSTEM	none	null	6
		SYSTEM	none	null	4
		Administrador	none	null	1
		SYSTEM	none	null	2
		SYSTEM	none	null	2
		SYSTEM	none	null	2
		NT AUTHORITY\SYSTEM	Artemis!60524DE4D95D	C:\Users\joslina0\AppData\Roaming\alFSVWJB\helppane.exe	1
		NT AUTHORITY\SYSTEM	Artemis!93A46F303B65	C:\Users\joslina0\AppData\Roaming\alFSVWJB\splwow64.exe	1
		SYSTEM	none	null	1
		SYSTEM	none	null	1
					28

- Se detectaron 28 eventos de archivos infectados encontrados que no pudieron ser eliminados por la herramienta de VirusScan.

- **Acciones por realizar:**

  - ⇨ Se recomienda correr nuevos escaneos manuales completos sobre cada uno de los equipos relacionados en la tabla anterior para descartar presencia de virus en el equipo y evitar una posible infección a otros equipos en la red.

  - ⇨ En el equipo LPG-JOSLINA01 puede haber presencia del ackDoor.Andromeda.662. Se recomienda realizar escaneos completos con más de una herramienta de AntiVirus para garantizar una detección más precisa.

4. Autenticaciones exitosas ROOT

Servidor Linux	IP Origen	Total
LinuxServer @		13
		12
		11
		8
		5
		4
		3
		3
		2
		1
		1
Total general		*63*

- Se registraron 63 conexiones exitosas hacia el servidor 50.0.0.43 usando el usuario root desde 11 máquinas diferentes.

- Se recomienda el control del usuario root. El uso del usuario root debería ser restringido por políticas de FW o directamente dentro de las configuraciones del servidor únicamente para los equipos administradores. Adicionalmente, teniendo en cuenta que este usuario posee privilegios completos del sistema, no debería intentar ser usado para actividades regulares de administración, si no sólo para actividades especiales que lo requieran bajo un control adecuado, tales como instalación de software o cambios críticos del sistema. Se recomienda también asegurar la contraseña del usuario root para que no pueda ser fácilmente obtenida por métodos de fuerza bruta.

- **Acciones por realizar:**

  ⇨ Confirmar si las direcciones IP relacionadas en la tabla están autorizadas para acceder con usuario root al servidor linux 50.0.0.43.

5. Autenticaciones al servidor ZIGMA

Desde las siguientes direcciones IP origen se registraron autenticaciones SSH no exitosas hacia el servidor ZIGMA (10.50.0.195).

Usuario	IP Origen	Total
magcast0		298
gabherr0		212
andcoch0		204
angrisc0		184
dierodr0		120
yaigrad0		114
		2
fiorome0		106
		10
frarome0		104
		4
mereraz0		106
catmele2		85
		10
		4
		2
		2

- Los usuarios **andcoch0**, **yaigrad0**, **fiorome0, frarome0**, **mereraz0** y **catmele2** registraron un número alto de conexiones fallidas SSH hacia el servidor Zigma cuando en meses anteriores no habían reportado un número tan alto.

- En el Anexo D se puede ver el detalle de estas conexiones.

- **Acciones por realizar:**

  ⇨ Confirmar si se realizaron las validaciones recomendadas en meses anteriores sobre las actividades ejecutadas por cada uno de estos usuarios con el fin de descartar intentos de fuerza bruta por agentes externos.

6. Svchost.exe

ID: 4625 - An account failed to log on	
Detectado en el equipo:	**WindowsAuthServer @ 50.0.0.70**
Cuenta en la que falló la autenticación:	**sysadmin**
Razón de la falla:	**Usuario correcto, contraseña incorrecta**
Proceso invocado:	**C:\Windows\System32\svchost.exe**
Conteo de eventos:	**8886**

- Continúa registrándose un número muy alto de fallos de autenticación en el equipo SRVDC00 usando la cuenta de usuario sysadmin. El proceso que generó este tipo de registros recibe el nombre de svchost.exe.

- Svchost.exe es un proceso de Windows relacionado al uso de los archivos DLL*. Es usual encontrar muchos procesos svchost activos en una máquina para segmentar los servicios del sistema, sin embargo, debido a que el equipo 50.0.0.70 ha mantenido valores un poco altos de rendimiento es importante descartar la presencia de virus en el dispositivo ya que muchos virus y malware se aprovechan del proceso SvcHost.exe para tomar control del equipo.

- **Acciones por realizar:**

  ⇨ Correr escaneos sobre el equipo SRVDC00 para descartar presencia de virus.

  ⇨ Identificar los servicios relacionados con el proceso svchost.exe que esté ralentizando el ordenador y reiniciar estos servicios.

***Archivo DLL:** Un archivo DLL es una biblioteca que contiene el código y datos que pueden ser utilizados por más de un programa al mismo tiempo. Estos archivos tienen el propósito de simplificar el desarrollo y reutilizar y optimizar fuentes del sistema.

8. CONCLUSIONES Y TRABAJO FUTURO

8.1. CONCLUSIONES

Aplicando los conocimientos adquiridos a lo largo de la maestría y durante la preparación del presente trabajo de grado, se observa la consecución de los objetivos planteados, proponiendo una metodología clara para la identificación de IoC, a través de una guía detallada con unas actividades claras y definidas, de fácil comprensión y que llevan al lector paso a paso en los puntos a seguir: definición de los flujos de información, inventario y clasificación de activos, identificación de tipos de ataque, análisis de riesgos, que serán los insumos necesarios para la identificación de los indicadores de compromiso que permitirán de manera proactiva contar con una adecuada protección de las Infraestructuras Criticas Cibernéticas que soportan los procesos corporativos y de negocio de las Organizaciones.

Independientemente del tipo o tamaño del negocio, todas las organizaciones son vulnerables en algún grado a las amenazas constantes que se presentan contra la información importante y que pueden comprometer cualquiera de sus principales propiedades: Confidencialidad, Integridad y Disponibilidad.

Considerando que el tema central del trabajo fue la Identificación de los Indicadores de Compromiso – IoC con un enfoque más estratégico que técnico, mostramos que para lograr este enfoque estratégico es necesario ir más allá de simplemente instalar herramientas tecnológicas y desarrollar actividades como:

- Entender los flujos de información de las infraestructuras críticas. En este primer paso, es importante tener en cuenta los flujos de información, entendidos como el recorrido que sigue la información desde su origen hasta su destino, los cuales están representados en diagramas de flujo de datos, que se pueden dividir en 5 capas (Red, Tecnología, Usuarios, Aplicaciones, Información), permitiendo la organización y contextualización de los elementos que intervienen en el flujo de información identificada como objeto de protección dentro de los procesos críticos de negocios para los cuales se pretende identificar los Indicadores de Compromiso – IoC; por otra parte, se diseñaron unos pasos para la elaboración de mencionados diagramas de flujo de datos, con el fin de mantener una organización en la caracterización de los activos y la construcciones de los diagramas.

- Identificación de los activos de información críticos a proteger según el flujo de información. En este punto, se plantea un análisis para el establecimiento de la información que se va a proteger, incluyendo datos electrónicos o impresos y los medios o equipos que almacén o procesan la información, dentro de este se proponen

los siguientes aspectos: Valoración en impacto y clasificación de los activos, Alcances de la solución, Requerimientos de negocio.

- Clasificación de los tipos de ataque que afecten Integridad, Confidencialidad y Disponibilidad. En este paso, es importante tener en cuenta los ataques más relevantes contra los principios de la Seguridad de la Información, con el fin de observar los métodos y técnicas que utilizan los atacantes y de esta forma generar conciencia acerca de la necesidad de contar con medidas que garanticen la seguridad en todo momento.

- Definición de indicadores de compromiso. A través del desarrollo de los pasos anteriores, utilizando metodologías para el análisis de riesgo, se busca entender cuál es el flujo de información de los procesos críticos del negocio de la Organización, identificando los usuarios que interactúan con el proceso, la plataforma tecnológica asociada a los procesos críticos, al igual que la infraestructura de seguridad con la que cuentan los procesos para protegerlos, con el fin de definir los Indicadores de Compromiso – IoC, que permitan perfilar un incidente, crear una línea base para la identificación de diferentes variables asociadas a ese incidente en particular y comparar un dispositivo potencialmente afectado contra dichos parámetros para dar una respuesta rápida y efectiva.

8.2. TRABAJO FUTURO

La tecnología continuará evolucionando, las empresas seguirán siendo cada vez más dependientes de las Tecnologías de la Información y las Telecomunicaciones y las vulnerabilidades inherentes a la tecnología se mantendrán e inclusive podrían aumentar debido producto de malas configuraciones, inadecuada gestión o falta de capacidades y competencias técnicas de los operadores de las tecnologías.

Todo esto conlleva a que las Organizaciones deben seguir trabajando en madurar sus modelos de seguridad donde el enfoque estratégico sea tanto o más importante que el técnico, ya que el enfoque estratégico al estar basado en los procesos de negocio, misionales y corporativos, define el norte a seguir basado en las estrategias de crecimiento y desarrollo de las organizaciones.

Otro aspecto a considerar para desarrollar como trabajo futuro es el fortalecimiento de la cultura y generación de conciencia en Seguridad de la información; las personas son el eslabón más débil en la cadena de la seguridad, por lo tanto, no importa cuánto se invierta en la implementación de tecnologías de seguridad, en la capacitación técnica de los operadores y administradores de seguridad, todos los esfuerzos pueden perderse .si el usuario final no conoce y respetas las políticas de seguridad corporativas y no es consciente que la responsabilidad del cuidado de la información es de todos en la Organización.

9. BIBLIOGRAFÍA

International Standards Organization, ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la Información (SGSI) – Requisitos.

International Standards Organization, ISO/IEC 27002: Tecnología de la Información – Técnicas de Seguridad – Código de práctica para la gestión de la seguridad de la información.

International Standards Organization, ISO/IEC 27005: Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la seguridad de la información.

International Standards Organization, ISO/IEC 20000-1: Tecnología de la Información – Gestión del Servicio - Requisitos de los sistemas de gestión de servicios.

International Standards Organization, ISO/IEC 20000-2: Tecnología de la Información – Gestión del Servicio - Guía de implementación de los sistemas de gestión de servicios.

Computer Security Division of the National Institute of Standards and Technology, NIST 800-30: Risk Management Guide for Information Technology Systems

Computer Security Division of the National Institute of Standards and Technology, NIST 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

Computer Security Division of the National Institute of Standards and Technology, NIST 800-34: Contingency Planning Guide For Information Technology Systems

10. WEBGRAFÍA

Albors, J. (17 de Abril de 2015). *¿Sabes qué es un backdoor y en qué se diferencia de un troyano?* Obtenido de http://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/

Albors, J. (09 de Febrero de 2017). *Ataques al DNS: cómo intentan dirigirte a páginas falsas*. Obtenido de https://www.welivesecurity.com/la-es/2017/02/09/ataques-al-dns/

Andrés Mendez Barco y Centro Criptológico Nacional. (Octubre de 2015). Obtenido de https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1090-ccn-stic-423-indicadores-de-compromiso/file.html

Aranda Software. (2017). *LAS 15 PRINCIPALES ESTADÍSTICAS DE 2017 PARA IT*. Obtenido de https://arandasoft.com/las-quince-principales-estadisticas-it/

Ciberseguridad al día. (4 de Septiembre de 2013). *10 indicadores de compromiso (IOC)*. Obtenido de https://cibersecurity.wordpress.com/2013/09/05/10-indicadores-de-compromiso-ioc/

crhoy.com. (29 de Noviembre de 2017). *Ataques informáticos para el 2018 serán más destructivos, según estudio*. Obtenido de https://www.crhoy.com/mundo/ataques-informaticos-para-el-2018-seran-mas-destructivos-segun-estudio/.

Enterprise Strategy Group - ESG . (2018). *SOAPA: Security Operations and Analytics Platform Architecture*.

Enterprise Strategy Group, Inc. (2017). *SOAPA: Security Operations and Analytics Platform Architecture*. Obtenido de http://www.esg-global.com/hubfs/pdf/SOAPA-architecture-slide-Sept17.pdf?t=1523046067986

ETEK International Corporation. (2017). *ETEK International Corporation.* Obtenido de https://www.etek.com.co/Pages/monitoreo-y-correlacion-eventos.aspx

G. Soto, M. (27 de Junio de 2016). *¿Qué es el envenenamiento ARP o ataque ARP Spoofing y ¿Cómo funciona?* Obtenido de https://medium.com/@marvin.soto/que-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-como-funciona-7f1e174850f2

Infobae. (9 de Noviembre de 2017). *Las cinco principales ciberamenazas para 2018 y como combatirlas*. Obtenido de https://www.infobae.com/tendencias/innovacion/2017/12/09/las-cinco-principales-ciberamenazas-para-2018-y-como-combatirlas/

International Standard Organization. (s.f.). *American National Standard Insituta*.

Mora, o. F. (14 de Junio de 2002). *Computer World* . Obtenido de http://www.computerworld.es/movilidad/la-gestion-de-los-flujos-de-informacion-de-la-empresa-desde-la-movilidad

NIST. (13 de Febrero de 2017). *Cybersecurity Framework - Draft Version 1.1* . Obtenido de https://www.nist.gov/cyberframework/draft-version-11

NIST. (10 de Junio de 2017). Framework for Improving Critical Infrastructure Cybersecurity.

NIST. (13 de Marzo de 2018). *Cybersecurity Framework - New to Framework* . Obtenido de https://www.nist.gov/cyberframework/new-framework#components

OBAMA, B. (12 de Febrero de 2013). *The White House* . Obtenido de https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Optical News. (26 de Enero de 2018). *Tipos de ataques informáticos y previsiones para el 2018*. Obtenido de https://www.optical.pe/tipos-de-ataques-informaticos-y-previsiones-para-el-2018/

Ramiro, R. (20 de Enero de 2018). *25 Tipos de ataques informáticos y cómo prevenirlos*. Obtenido de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Ramiro, R. (03 de Enero de 2018). *Algunos tipos de ataques informáticos*. Obtenido de https://ciberseguridad.blog/algunos-tipos-de-ataques-informaticos/

Securelist. (28 de Septiembre de 2017). *Península Ibérica y Latinoamérica: estadística de las amenazas para sistemas de automatización industrial, primer semestre de 2017*. Obtenido de https://securelist.lat/threat-landscape-for-industrial-automation-systems-in-h1-2017/85531/

Securelist. (28 de Septiembre de 2017). *Threat Landscape for Industrial Automation Systems in H1 2017*. Obtenido de https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2017/82660/

US - CERT. (18 de Septiembre de 2017). *CSET Download*. Obtenido de https://www.us-cert.gov/forms/csetiso

11. LISTADO DE FIGURAS