UNIVERSIDAD CENFOTEC

MAESTRÍA EN CIBERSEGURIDAD

Documento Final de Proyecto de Investigación Aplicada 2

“Modelo de Mejores Prácticas en la implementación de la Ciberseguridad”.

Diego Esteban González Villachica

Agosto, 2018

Declaratoria de Derechos de Autor

Dedicatoria

Un logro más, que Dios me ha concedido, se lo dedico a mi bella esposa Graciela, ya que siempre ha sido de gran soporte en todos los retos que hemos afrontado juntos en los últimos años, quien además me sigue impulsado a esforzarme y superarme día con día.

A mis amados padres, quienes siempre me han apoyado con sus consejos y oraciones en todos mis proyectos.

Y a mi amada suegra, quien fue la me informó sobre la apertura de esta maestría y me motivó a tomar este reto, el cual hoy, tres años después, y gracias a Dios, es todo una realidad.

Agradecimientos

Ante todo, agradezco a Dios, creador y Señor de todo lo que existe, quien me dio las fuerzas, la salud, la inteligencia y el ímpetu para ganar con excelencia este grado de maestría.

Gracias a mi familia, la cual fue mi gran apoyo en todo el camino.

Cabe destacar mi agradecimiento especial a mis profesores Carlos Calvo, César Rodríguez, Alex Araya, Matías, Juan Ignacio, Miguel, que siempre fueron de lo mejor para transmitir su experiencia y gran conocimiento, lo cual valoro muchísimo.

Aprovecho también para agradecer a mis compañeros, quienes también fueron pieza clave para lograr esta preciada meta, con quienes compartí muchísimo, en todos los proyectos, al comer, en llamadas. ¡De verdad muchas gracias!

Por supuesto, mi agradecimiento especial a don Ignacio Trejos, María Eugenia Ucros, Viviana Brenes, Maureen Quirós, y todo el equipo en general de la universidad, quienes hacen posible estos logros académicos.

HOJA DEL TRIBUNAL

Tabla de contenido

Tabla de Figuras

Resumen ejecutivo

Nos encontramos viviendo en una era tecnológica, lo cual nos aporta muchísimos beneficios en nuestro diario vivir, muchos de estos se traducen en calidad de vida para las personas, ya que, como bien significa, nos mejoran la vida por todo lo que podemos lograr y en ocasiones nos cambian la vida, por cosas que en definitiva no se pudieran lograr sin esos inventos, aplicaciones, software y dispositivos que marcan definitivamente un antes y un después en la historia de la humanidad.

Como bien hemos aprendido en los últimos años, dicha tecnología también lleva de la mano toda una serie de implicaciones en todas las áreas, más allá de su aporte positivo para las personas, empresas públicas y privadas, países y organizaciones, si se emplea de una forma incorrecta.

En este documento se analizan ampliamente una serie de controles de seguridad que se aplican a varias de las más importantes áreas de la ciberseguridad, como lo son por ejemplo: infraestructura, redes, equipos de hardware, software y dispositivos que se conectan a nuestra red, entre otros. Esto permite generar un modelo de implementación de seguridad en dichas áreas, para la mayoría de empresas en el mundo, ya que estas comparten una estructura similar.

Dichos controles, que recopilamos y abordamos ampliamente en este documento, han sido propuestos por diferentes organizaciones reconocidas internacionalmente en el campo de la Ciberseguridad, tales como SANS Institute, Center for Internet Security (CIS), Tripwire, Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST).

CAPÍTULO I

INTRODUCCIÓN

1.1 Generalidades

En cuanto a la seguridad y la buena administración de las TICs, cabe destacar que ambas siempre deben ir de forma conjunta, por ejemplo, una red bien administrada, es más difícil de atacar que una mal administrada.

Para entender qué tan bien la organización está gestionando la ciberseguridad, debemos empezar por hacernos estas preguntas:

- ✓ ¿Se conoce qué está conectado a las computadoras y redes?
- ✓ ¿Se conoce qué software se está ejecutando en los sistemas y redes?
- ✓ ¿Se configuran las computadoras teniendo en cuenta la seguridad?
- ✓ ¿Se tiene una buena administración sobre quién tiene acceso a información confidencial o quién tiene privilegios adicionales?
- ✓ ¿Tiene claro su personal sobre la importancia que desempeñan en la protección de la organización contra incidentes cibernéticos?

Como podemos leer en muchas noticias, por ejemplo (Jara, 2018), En enero de 2016, la revista Forbes publicó la nota: *"Costos de delitos Cibernéticos proyectados a alcanzar 2 mil millones para el 2019".* En ese sentido, Steve Morgan considera que es atenuante llamar a esto una 'ola de crímenes' cuando se consideran los costos que las empresas están sufriendo como resultado del delito cibernético.
De hecho, Morgan afirma que 'Epidemia' es más adecuado, a la vez que el CEO y presidente de IBM Corp., Ginni Rometty, dijo recientemente que el delito cibernético puede ser la mayor amenaza para todas las compañías en el mundo.

En esa línea, es importante mencionar que, en 2015, la compañía de seguros británica Lloyd's estimó que los ciberataques cuestan a las empresas, hasta $ 400 mil millones al año, lo que incluye daños directos e interrupciones al curso normal de los negocios, posterior a los incidentes.

Por su parte, Gordon Snow, Asistente Director de la Ciberdivisión del FBI, testificó ante la comitiva judicial de Estados Unidos que las amenazas cibercriminales provocan pérdidas económicas significativas. Pero que la amenaza contra las instituciones financieras es solo una parte del problema, pues también son motivo de gran preocupación las amenazas a la infraestructura crítica, el robo de propiedad intelectual y los problemas a la cadena de suministros.

A lo largo de esta síntesis, se aborda una variedad de herramientas gratuitas o de bajo costo, así como los procedimientos que se pueden implementar para mejorar la seguridad.

1.2 Definición y descripción del problema

Según estudios de la CIS, las brechas de seguridad en las tarjetas de crédito, robo de identidad, Ransomware, robo de propiedad intelectual, pérdida de privacidad, denegación de servicio, entre otros incidentes cibernéticos, se han convertido en noticias cotidianas. Las víctimas incluyen algunas de las empresas más grandes, mejor financiadas y más conocedoras de la seguridad, como por ejemplo agencias gubernamentales, tiendas de ventas al por menor, compañías de servicios financieros, incluso vendedores de soluciones de seguridad.
Muchas de las víctimas tienen millones de dólares para destinar a la ciberseguridad, y aun así se quedan cortos en sus esfuerzos para defenderse de los ataques comunes. Lo que es aún más inquietante es que muchos ataques podrían haberse evitado mediante prácticas de seguridad bien conocidas, como parches y configuraciones seguras.

Entonces, ¿qué se supone que haga el resto de nosotros? ¿Cómo hacen las organizaciones con pequeños presupuestos? ¿El personal limitado responde al problema cibernético continuo?
En este documento se propone potenciar a propietarios de pequeñas y medianas empresas (PYME), para ayudarlos a proteger sus negocios con un número de acciones

de alta prioridad, basadas en buenas prácticas de ciberseguridad, desarrolladas por expertos en TI de distintas organizaciones.

1.3 Justificación

Según (ISACA, Resources and Threats, 2017), en el tercer estudio anual de Estado de la Seguridad Cibernética, encuentra que la ciberseguridad es cada vez más una prioridad comercial. Ocho de cada 10 organizaciones dicen que su liderazgo ejecutivo apoya la seguridad y, más organizaciones que nunca, ahora tienen un CISO a cargo de la función de seguridad de la información. Sin embargo, los recursos y las habilidades disponibles no siguen el ritmo de un panorama de amenazas que está escalando rápidamente en complejidad y volumen.

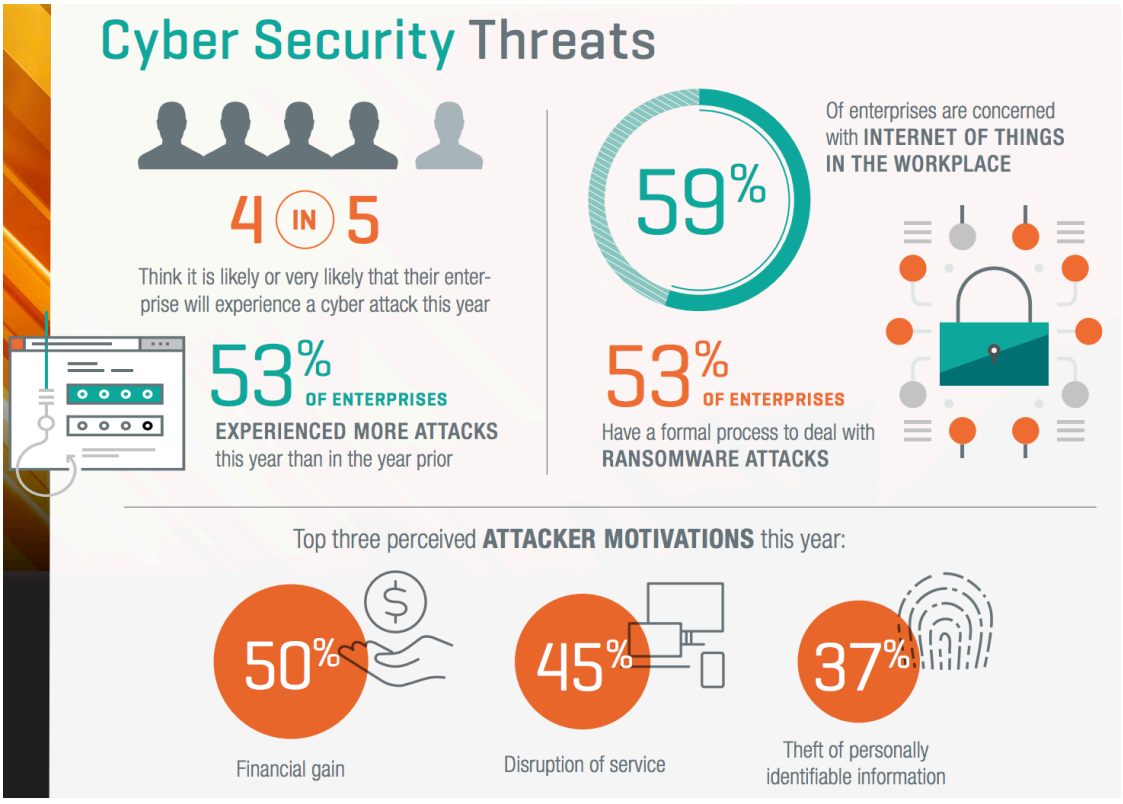


Figura # 1: ISACA's State of Cyber Security 2017: Part 2: Current Trends in the Threat Landscape

Fuente: www.isaca.org/state-of-cyber-security-2017

Según la National Association of Corporate Directors (NACD), en conjunto con la American International Group (AIG) y la Internet Security Alliance (ISA), publicaron un informe que describe los cinco principios que todas las juntas corporativas deberían considerar, a medida que buscan mejorar su supervisión de los riesgos cibernéticos.

Los cinco principios son:

1. Los directores deben entender y abordar la ciberseguridad como un riesgo para toda la empresa y gestionar el problema, ya que no es solo un problema de TI.
2. Los directores deben comprender las implicaciones legales de los riesgos cibernéticos en relación con sus circunstancias específicas de la compañía.
3. Las juntas deberían tener acceso adecuado a una buena experiencia en ciberseguridad por parte de un buen equipo, de forma que se pueda discutir sobre la gestión del riesgo cibernético de forma regular y adecuada en la agenda de reunión del consejo.
4. Los directores deben establecer la expectativa de que la administración establecerá un riesgo para toda la empresa, además de un marco de gestión acorde, con personal y presupuesto adecuados.
5. La discusión de la gerencia de la junta sobre el riesgo cibernético debe incluir la identificación de cuáles riesgos evitar, aceptar, mitigar o transferir a través de un seguro, así como planes específicos asociados con cada enfoque.

Por esta y varias razones descritas en esta síntesis, se ha elaborado un modelo de buenas prácticas para guiar con un mayor enfoque en la ardua tarea de reforzar la Ciberseguridad en las organizaciones.

1.4 Objetivos

Los objetivos de la presente investigación se basan en la taxonomía de Benjamín Bloom, ya que se ha convertido en un estándar internacional desde 1956, y que muchos profesionales de todo el mundo han utilizado esta taxonomía como herramienta para establecer los objetivos de sus investigaciones.

Según (López García, 2014), la idea de establecer un sistema de clasificación de habilidades, comprendido dentro de un marco teórico, surgió en una reunión informal al finalizar la Convención de la Asociación Norteamericana de Psicología, reunida en Boston (USA) en 1948.

Se buscaba que este marco teórico pudiera usarse para facilitar la comunicación entre examinadores, al promover el intercambio de materiales de Evaluación e ideas de cómo llevarla a cabo. Además, se pensó que estimularía la investigación respecto a diferentes tipos de exámenes o pruebas, y la relación entre estos y la educación. El proceso estuvo liderado por Benjamín Bloom, Doctor en Educación de la Universidad de Chicago (USA). Se formuló una Taxonomía de Dominios del Aprendizaje, desde entonces conocida como Taxonomía de Bloom.

1.4.1 Objetivo general

- Diseñar un modelo para la implementación de la ciberseguridad en organizaciones basados en controles y mejores prácticas de seguridad

1.4.2 Objetivos específicos

1. Describir las diferentes áreas de la tecnología en la que se aplica la ciberseguridad
2. Explicar las amenazas más comunes que afectan las áreas de la ciberseguridad.
3. Elaborar una guía de las diferentes herramientas utilizadas en la solución de problemas en las áreas de la ciberseguridad.
4. Analizar diferentes controles de ciberseguridad.
5. Construir un modelo para la implementación de los controles de ciberseguridad.

1.5 Alcances y limitaciones

Los alcances nos indican con precisión qué se puede esperar o cuáles aspectos alcanzaremos en la investigación y las limitaciones indican qué aspectos quedan fuera de su cobertura. Las limitaciones no se refieren a las dificultades de realización, como muchos creen, sino a los “límites” o fronteras, hasta donde llegan las aspiraciones de la investigación, siempre por referencia a los objetivos ya definidos.

1.5.1 Alcances

En esta investigación exploramos las diferentes áreas de la tecnología en donde las organizaciones deben prestar más atención, de hecho, se propone una clasificación en donde es más sencillo agrupar dichas áreas.
En este documento también encontramos una explicación de las amenazas cibernéticas que más están dando dolor de cabeza a las organizaciones y gobiernos en los últimos años. Al mismo tiempo que recopilamos una gran variedad de las principales herramientas que se emplean en la actualidad en todos los procesos de análisis e implementación, para asegurar dichas áreas de TI.

Esta investigación concluye con una gran síntesis de los principales controles y mejores prácticas de seguridad que existen, propuestas por diferentes organizaciones líderes en el área de Ciberseguridad, y por ende aplicables a cualquier tipo y tamaño de organización.
Así se elabora una serie de guías que contienen todos los elementos antes mencionados: áreas de tecnología, amenazas, herramientas, controles de seguridad, pasos de implementación, entre otros detalles, de manera que se propone como un modelo por seguir en el reforzamiento de la ciberseguridad.

1.5.2 Limitaciones

En el esfuerzo de reforzar la ciberseguridad en cualquier organización, entran en juego muchos procesos, políticas, software y recursos especializados, entre otros elementos, que van a determinar si existe una área de tecnología con seguridad confiable o no.
En esta investigación abordamos varios de los principales controles y mejores prácticas de seguridad que existen; sin embargo, es importante aclarar que existen otros controles que nos aseguran de mejor forma la Ciberseguridad en nuestra organización. El detalle está en que la implementación de esos controles implica la utilización de más recursos técnicos, económicos y en mayor tiempo de implementación y son, por esta razón, más caros y complejos; por ejemplo, la utilización de sistemas SIEM, sistemas de Protección de Datos o sistemas de control de monitoreo de cuentas. Por lo mencionado, no cualquier tipo de organización está en la capacidad de tener esos controles. En este documento, solamente se abordan los controles y mejores prácticas aplicables a cualquier tipo de organización y de cualquier tamaño; se deja de lado lo que tal vez sea más complejo o costoso de implementar.

1.6 Estado de la cuestión.

En cuanto a materia de ciberseguridad, diferentes organizaciones internacionales que han estado liderando esta área, han propuesto en los últimos años diferentes formas en las que se puede trabajar y reforzar la seguridad en las distintas áreas de tecnología.

Cada una de ellas ha publicado recientemente varios artículos e inclusive algunas soluciones que vienen a atacar varias de las vulnerabilidades y problemas más comunes y recurrentes de la mayoría de las organizaciones en esta área.

Organizaciones como SANS Institute, Center for Internet Security (CIS), Tripwire, Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST) han desarrollado algunas publicaciones en las que aborda la problemática actual de la ciberseguridad en la mayoría de las empresas, en donde

proporcionan también algunas recomendaciones al respecto; además, proponen algunos controles para mitigar los riesgos y reforzar la seguridad en áreas específicas de tecnología.

Según (Pescatore, 2017) podemos revisar los controles propuestos por la CIS para asegurar nuestra organización. Según (Australian_Government, 2017) encontramos la propuesta de varios controles importantes con su respectiva estrategia de mitigación.

Por otro lado, la Organización Internacional para la Estandarización ISO, propone el estándar ISO 27032, publicado en el 2012, que contiene muchos de los elementos analizados en este documento. Sin embargo, la ISO aborda estos elementos bajo una perspectiva más global y directiva; se profundiza más en controles administrativos como políticas, comunicación, capacitación. Además, no cubre los detalles aquí desarrollados en las actividades para implementar los controles, ni tampoco las herramientas por aplicar en cada control, como sí lo abordamos en este documento. De manera que, proponemos una síntesis de varias de las publicaciones mencionadas anteriormente y como resultado la integración de elementos esenciales para la creación de guías de implementación.

Como parte de la investigación a la hora de elaborar este documento, se hace referencia de la tesis hecha por el MSc. César Rodríguez Bravo, Modelo de Madurez en Ciberseguridad (ECM2), que por su naturaleza y propósito se puede aplicar en cualquier organización para evaluar el estado actual de ciberseguridad. Esto precisamente es la primera parte, ahora, como segunda parte, para complementar y continuar el hilo investigativo, este trabajo pretende establecer un modelo de ejecución. A través de diferentes guías, se brindan diferentes consejos, directrices y pasos por seguir para asegurar diferentes áreas de tecnología, que da como resultado una organización con un determinado nivel de implementación en ciberseguridad.

CAPÍTULO II

MARCO TEÓRICO

Áreas de la tecnología en la que se aplica la ciberseguridad

En la actualidad, las siguientes áreas de TI pueden variar según el tamaño de las organizaciones; sin embargo, en la gran mayoría se mantiene este esquema, que nos lleva a tomar, como base, dichas áreas, para lo propuesto en este documento.

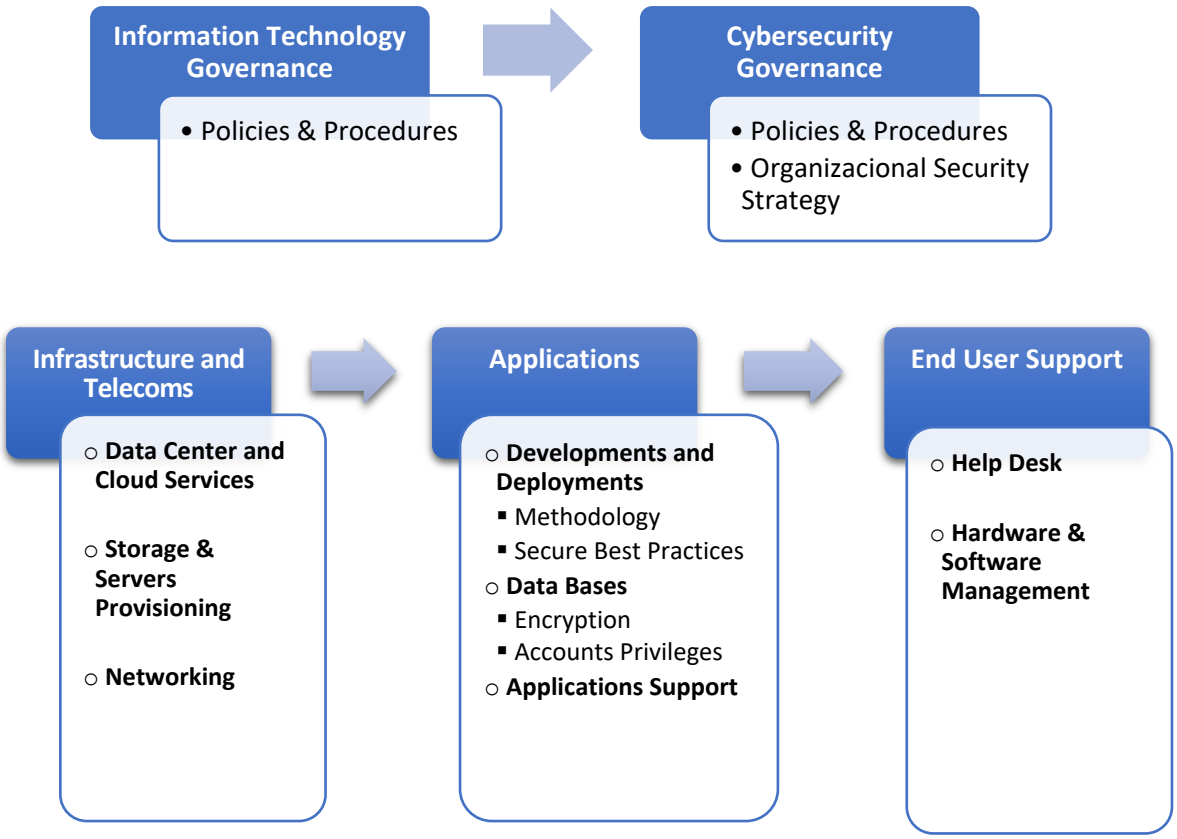


Figura # 2: Áreas de tecnologías de información en las organizaciones

El término infraestructura de TI, según (Roush, 2017) se define en ITIL v3 como un conjunto combinado de hardware, software, redes, instalaciones, etc. (incluido todo el equipo relacionado con la tecnología de la información), utilizado para desarrollar, probar, entregar, monitorear, controlar o respaldar servicios de TI. Las personas, procesos y documentación asociados, no son parte de la infraestructura de TI.

Esto incluye un amplio rango de dispositivos importantes como Firewalls, Switches, Routers, Access Points, entre otros, en el área de Networking, así como todo lo relacionado a su conectividad.
En cuanto al área de servidores, se puede mencionar todo lo referente a los servidores On Premises o físicos y también los virtuales en los Data Centers propios de la organización, además de todo lo relacionado al servicio de Cloud, donde también puedan tener otras opciones que brinde más robustez y disponibilidad, según las necesidades del negocio.

Si nos referimos al área de Aplicaciones, tenemos todo lo relacionado a las aplicaciones que se manejan en la organización, su soporte y mantenimiento, nuevos desarrollos e implementaciones, que nos lleva a mencionar puntos clave como las metodologías utilizadas para ello, además de las buenas prácticas empleadas en la seguridad y codificación.
Cabe destacar que el corazón de cualquier aplicación son las bases de datos, en donde está lo más preciado para cualquier empresa, la información debe estar con las más altas medidas de seguridad, para protegernos del acceso no autorizado y exposición de datos sensibles.

Con respecto a los servicios de usuario final, esta es posiblemente el área de mayor exposición y más fácil de vulnerar por los hackers, ya que aquí tenemos el eslabón más débil de la cadena de seguridad, las personas, las cuales manipulan las computadoras y demás equipo de usuario y por esta razón debe ser un área en la cual se empleen los controles y estrategias necesarias para mantener en buena forma todo lo referente a esto, por ejemplo, todo el hardware y software de los equipos, actualizaciones, control de inventarios, entre otros componentes inherentes a esta rama.

CAPÍTULO III

AMENAZAS

Amenazas actuales y más sobresalientes que afectan diferentes áreas de la ciberseguridad

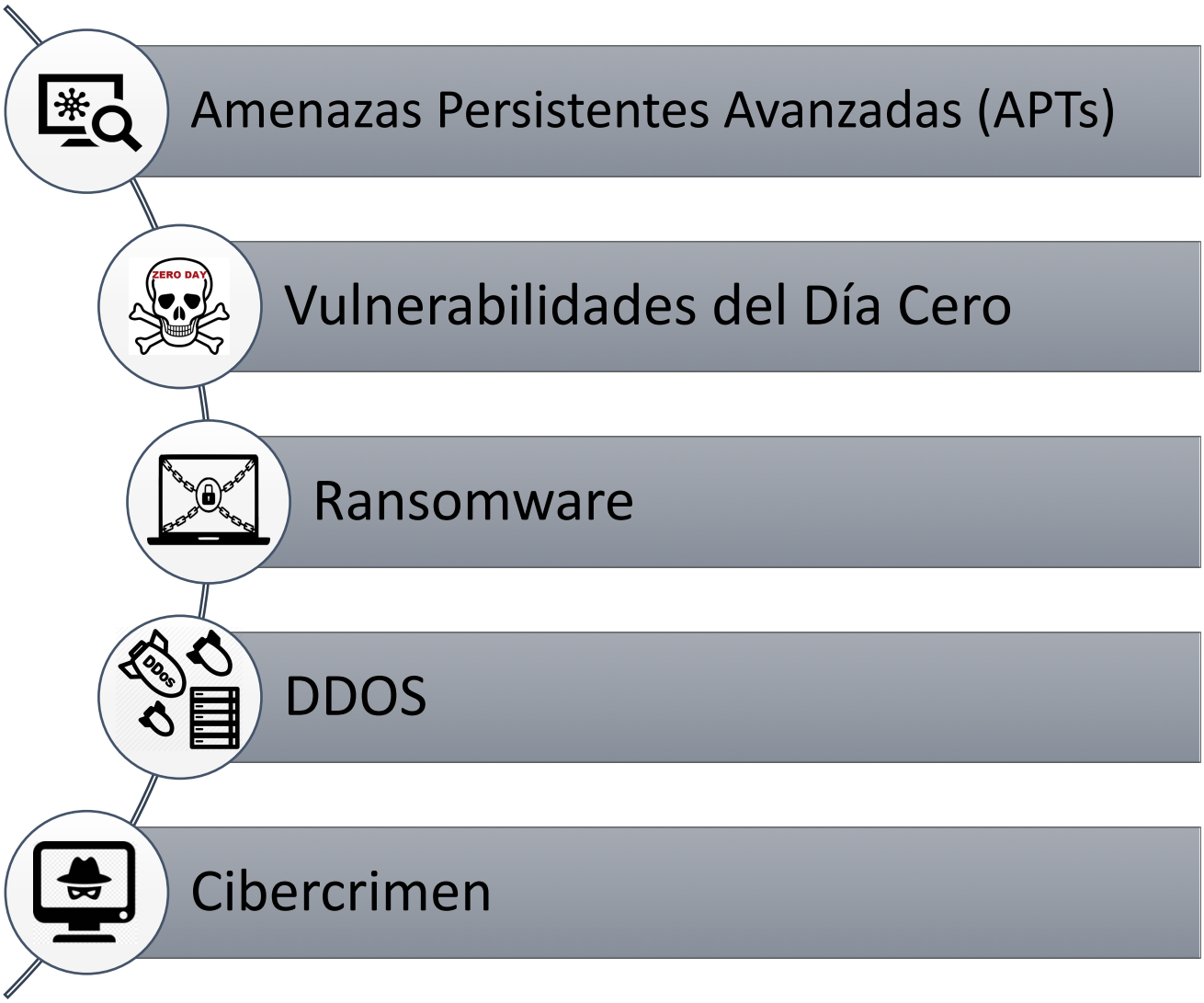


Figura # 3: Amenazas más sobresalientes en Ciberseguridad

Amenaza Persistente Avanzada (APT: Advanced Persistent Threat)

Según (Torregrosa, 2018), una amenaza persistente avanzada se trata de un conjunto de procesos informáticos sigilosos y continuos de piratería informática, a menudo orquestada por humanos, dirigido a una entidad específica, generalmente, fija sus objetivos en organizaciones o naciones por motivos de negocios o políticos.

El proceso avanzado involucra sofisticadas técnicas en las que se utiliza software malicioso para explotar vulnerabilidades en los sistemas. El término 'persistente' sugiere que existe un control y monitorización externos para la extracción de datos de un objetivo específico en una forma continua. El término 'amenaza' indica la participación humana para orquestar el ataque.

En otras palabras, las APTs son un tipo de malware creado específicamente para atacar a una empresa o gobierno, con el objetivo principal de robar su información, mantenerse oculto y en el mayor tiempo posible. Cuanto más tiempo permanezca oculto, más información será capaz de extraer.

Un ejemplo real, es el virus Stuxnet, que fue considerado como la primera "ciber-arma" del mundo; fue capaz de detener los reactores nucleares de Irán en el año 2010 y causar pérdidas de suministro eléctrico que afectaron a todo el país.

Para la creación de una APT, se requiere mucha información sobre el objetivo, sobre la cual, los desarrolladores toman toda la ventaja posible, por ejemplo, información sobre:

- Sistemas informáticos internos y externos.
- Bases de Datos que se utilizan.
- Sistemas de seguridad de la red.
- Sistemas de seguridad del puesto de trabajo.
- Socios conocidos.

- Contratos con terceros.
- Directivos.
- Empleados.

Una vez que se dispone de la máxima información posible, solo hay que diseñar un software que sea capaz de aprovechar una vulnerabilidad en alguno de dichos elementos.

Vulnerabilidad del Día Cero

Según publicación en el sitio (AVAST, 2014), cuando un proveedor de software saca al mercado un nuevo producto, con alguna brecha de seguridad de la que no son conscientes ni el proveedor ni la empresa antivirus, se denomina vulnerabilidad de día cero o exploit de día cero.

Los ataques de día cero provienen de hackers criminales que han descubierto (o conocido) una brecha en el sistema e intentan aprovecharla para realizar sus ataques. En concreto, los ataques de día cero suelen aprovechar las brechas de los navegadores web y las aplicaciones de correo electrónico, ya que gozan de una gran distribución.

Según (Myers, 2015), el nombre 0-day (día cero) se debe a que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad. Estas a veces se usan junto a los troyanos, rootkits, virus, gusanos y otros tipos de malware, para ayudarlos a propagarse e infectar más equipos. También se puede encontrar escrito como “0day“, “zeroday” y “zero-day”.

¿Cómo se reconocen los exploits de día cero?

La mala noticia es que no es posible reconocer las vulnerabilidades o exploits de día cero. Si se detecta una, ¡ya no será de día cero! Por esto, los ataques de día cero constituyen una seria amenaza para la seguridad, pero afortunadamente, hay recursos para evitarlos. Por ejemplo, algunos antivirus pueden detectar una vulnerabilidad de día cero utilizando algoritmos de seguimiento del comportamiento, al detectar patrones sospechosos o malintencionados.

¿Cómo se soluciona una vulnerabilidad de día cero?

La solución de una vulnerabilidad de día cero suele ser trabajo del proveedor de software, que deberá publicar un parche de seguridad para corregir la brecha de su software. Sin embargo, es decisión de cada usuario instalar en su dispositivo dicho parche de seguridad o actualización de software. La forma más sencilla de asegurarse de que no olvida actualizar su software es mediante una aplicación que se encargue de gestionar automáticamente sus parches.

Según los especialistas de FireEye, (Recent Zero-Day Exploits, 2018), los atacantes cibernéticos son extraordinariamente hábiles, y su malware puede pasar desapercibido en los sistemas durante meses e incluso años, lo que les da mucho tiempo para causar daños irreparables.

A continuación, se puede observar una lista de las vulnerabilidades de día cero, encontradas por el equipo de FireEye en el 2017.

CVE-2017-8759: inyección de código del analizador WSDL SOAP.	Recientemente FireEye detectó un documento malicioso de Microsoft Office RTF aprovechando CVE-2017-8759, una vulnerabilidad de inyección de código del analizador WSDL de SOAP. Esta vulnerabilidad permite a un actor malintencionado inyectar código arbitrario durante el análisis de los contenidos de definición de WSDL de SOAP.

CVE-2017-0261: EPS "restaurar" Uso-Después-Gratis	FireEye detectó una vulnerabilidad de "restaurar" uso-después-libre en Encapsulated PostScript (EPS) de Microsoft Office - CVE-2017-0261 - que se utiliza para entregar malware SHRIME de un grupo conocido como Turla, y malware NETWIRE de un actor desconocido de motivación financiera.
CVE-2017-0262: Confusión tipo en EPS.	FireEye observó APT28 utilizando una vulnerabilidad de confusión de tipo en PostScript encapsulado (EPS) de Microsoft Office (CVE-2017-0262) para entregar una carga útil GAMEFISH.
CVE-2017-0263: win32k! XxxDestroyWindow Use-After-Free.	FireEye observó APT28 utilizando CVE-2017-0263, una vulnerabilidad de uso de win32k! XxxDestroyWindow para escalar privilegios durante la entrega de una carga de GAMEFISH. Esta vulnerabilidad se usó en conjunto con CVE-2017-0262.
CVE-2017-0199: en Wild Attacks Leveraging HTA Handler.	FireEye detectó documentos maliciosos de Microsoft Office RTF aprovechando CVE-2017-0199. La vulnerabilidad permite a un actor malintencionado descargar y ejecutar un script de Visual Basic que contiene comandos de PowerShell cuando un usuario abre un documento que contiene un exploit incrustado.

Ransomware

Cuando nos enteramos de un rescate, inmediatamente pensamos que una persona está siendo rehén hasta que se cumplan ciertas demandas monetarias. Si bien tales instancias son ciertas en el mundo real, lo mismo puede decirse del ransomware en el mundo de las computadoras e Internet.

Según publicaciones sobre el ransomware por parte del equipo de (EnigmaSoftware, 2018), este representa una amenaza grave, ya que puede afectar a MS Windows, Mac OS X o Linux. La fuerza del cifrado puede bloquear archivos importantes, como imágenes, videos, audio, archivos PDF, archivos de MS Office y otros tipos de archivos y aplicaciones. El Centro de Quejas por Delitos en Internet del FBI (IC3) afirma que, entre abril de 2014 y junio de 2015, las víctimas informaron pérdidas por un total de más de $ 18 millones.

¿Qué es Ransomware?

Ransomware, también conocido como scareware, es un software malicioso que restringe el acceso a una computadora infectada mientras muestra una notificación que exige al usuario de la computadora pagar una tarifa para restaurar el acceso al sistema. Se sabe que los ransomware recientes, como CryptoLocker y CryptoWall, encriptan archivos, lo que bloquea una computadora infectada y la hace prácticamente inútil para realizar funciones básicas o navegar por Internet.

Según una investigación de (CISSecurity.org, 2018), una vez que se bloquea el acceso al sistema, el ransomware exige un rescate para desbloquear los archivos, con frecuencia $ 200 - $ 3,000 en Bitcoins, aunque otras monedas y tarjetas de regalo se informan ocasionalmente. Las variantes de ransomware casi siempre apuntan de forma oportunista a las víctimas, al infectar una variedad de dispositivos desde las computadoras hasta los teléfonos inteligentes.

Las víctimas corren el riesgo de perder sus archivos, pero también pueden experimentar pérdidas financieras debido al pago del rescate, pérdida de productividad, costos de TI, honorarios legales, modificaciones de la red y / o la compra de servicios de monitoreo de crédito para empleados / clientes.

Vectores de infección

La mayoría del ransomware se propaga a través de acciones iniciadas por el usuario, como hacer clic en un enlace malicioso en un correo electrónico no deseado o visitar un sitio web malicioso o comprometido. En otros casos, el malware se disemina a través de la publicidad maliciosa y las descargas directas, que no requieren el compromiso del usuario para que la infección sea exitosa.

Si bien casi todas las infecciones de ransomware son oportunistas, se diseminan a través de vectores de infección indiscriminada, como los discutidos anteriormente; en algunos casos muy raros, los actores de amenazas cibernéticas se dirigen específicamente a una víctima. Esto puede ocurrir después de que los actores se den cuenta de que una entidad sensible ha sido infectada o debido a intentos de infección específicos. La Oficina Federal de Investigaciones (FBI), se refiere a estas instancias como extorsión, en lugar de ransomware, ya que casi siempre hay una cantidad de rescate más alta que coincide con la focalización estratégica. Este fue el caso en la primavera de 2016, cuando varios hospitales infectados con ransomware, estratégicamente dirigidos, fueron noticia.

Capacidades adicionales

En el último año, las características de las variantes de ransomware se han ampliado para incluir la filtración de datos, la participación en ataques distribuidos de denegación de servicio (DDoS) y componentes anti-detección. Una variante elimina archivos independientemente de si se realizó o no un pago. Otra variante incluye la capacidad de bloquear copias de seguridad basadas en la nube cuando los sistemas realizan copias de seguridad de forma continua en tiempo real (por ejemplo, durante la sincronización persistente). Otras variantes apuntan a teléfonos inteligentes y dispositivos de Internet de las cosas (IoT).

Afortunadamente, según últimas investigaciones, con algunas herramientas como MALTEGO entre otras, es posible rastrear y conocer el usuario dueño con solo la dirección de billetera de Bitcoin, la cual utilizan las víctimas para depositar el monto de rescate a los cibercriminales, con el fin de liberar sus equipos.

A continuación, se describen los más recientes ataques por ransomware, los cuales dieron un fuerte dolor de cabeza a muchísimas personas, instituciones y países, según publicación de la revista en línea CSO (Fruhlinger, 2017).

CryptoLocker

Jonathan Penn, Director de Estrategia en Avast, señala que a finales del 2013 y principios del 2014, más de 500,000 máquinas fueron infectadas por CryptoLocker.

TeslaCrypt

TeslaCrypt se dirigió a los archivos auxiliares asociados con los videojuegos guardados, mapas, contenido descargable, y similares. Estos archivos son a la vez preciosos para los jugadores hardcore, pero también es más probable que se almacenen localmente, en lugar de la nube o respaldados en un disco externo. En 2016, TeslaCrypt compuso el 48% de los ataques de ransomware.

SimpleLocker

A medida que más y más archivos valiosos migran a dispositivos móviles, también lo hacen los estafadores de ransomware. Android fue la plataforma elegida para atacar, y a finales de 2015 y principios de 2016, las infecciones de ransomware de Android se cuadruplicaron.

SimpleLocker fue también el primer ransomware conocido que entregó su carga maliciosa a través de un descargador de troyanos, lo que dificultó la recuperación de las medidas de seguridad. Mientras SimpleLocker nació en Europa del Este, tres cuartas partes de sus víctimas se encuentran en los Estados Unidos, ya que los estafadores persiguen el dinero.

WannaCry

El primero de los dos ataques principales se llamó WannaCry, y "fue fácilmente el peor ataque de ransomware en la historia", según indica Jonathan Penn de Avast, cerrando hospitales en Ucrania y estaciones de radio en California, y fue entonces cuando el ransomware se convirtió en una amenaza existencial.

"El 12 de mayo, el ransomware comenzó a tomar fuerza en Europa. Solo cuatro días después, Avast había detectado más de 250,000 detecciones en 116 países".

Petya, NotPetya

Petya y NotPetya son dos piezas relacionadas de malware que afectaron a miles de computadoras en todo el mundo en 2016 y 2017. Tanto Petya como NotPetya apuntan a encriptar el disco duro de las computadoras infectadas. Pero NotPetya tiene muchas más herramientas potenciales para ayudar a difundir e infectar las computadoras, y aunque Petya es una pieza estándar de ransomware que tiene como objetivo hacer pocas Bitcoins rápidas de las víctimas, NotPetya es ampliamente visto como un ataque cibernético ruso patrocinado por el estado disfrazado de ransomware.

Ataques de Denegación de Servicio Distribuido (DDOS)

Según documentos de aprendizaje de (CloudFlare, 2018), los ataques de denegación de servicio (DoS) son los precursores de los ataques DDoS. Históricamente, los ataques DoS fueron un método principal para interrumpir los sistemas informáticos en una red. Los ataques DoS se originan en una sola máquina y pueden ser muy simples; por ejemplo se puede lograr un ataque de inundación ping básico mediante el envío de muchas solicitudes ICMP (paquetes ping) a un servidor específico. Casi cualquier persona con una máquina en red puede lanzar este tipo de ataque mediante el uso de comandos de terminal simples. Existieron también ataques DoS más complejos, los cuales usaban la fragmentación de paquetes, como el ataque Ping of Death.

Los ataques que involucran varias computadoras u otros dispositivos, todos dirigidos a la misma víctima, se consideran ataques DDoS debido a su diseño distribuido. De los dos, los ataques DDoS son más frecuentes y dañinos en la Internet moderna. Debido a la relativa simplicidad de comprar o crear un grupo de máquinas maliciosas capaces de enviar una gran cantidad de tráfico de Internet a un objetivo; estos ataques se han incrementado muchísimo en los últimos años.

Según los especialistas de en Security Planet (Rubens, 2018), los ataques DDoS son cada vez más comunes, según una investigación publicada por Corero Network Security a fines de 2017. Su informe DDoS Trends and Analysis encontró que el número de ataques aumentó en un 35% entre el segundo trimestre de 2017 y el tercero de 2017.

Una razón de su mayor prevalencia es el creciente número de dispositivos inseguros de Internet de las cosas (IoT) que están siendo infectados y reclutados en botnets como Reaper.

El volumen de datos lanzados en las víctimas de ataques DDoS también ha aumentado significativamente, en gran parte gracias a los ataques de amplificación como la técnica de ataque de amplificación de memcached. A principios de este año, los cibercriminales lanzaron unos 15,000 ataques de memcached, incluido un ataque a GitHub que alcanzó un máximo de 1,35 Tbps, por lo que evitar un ataque DDoS, cuando los actores malintencionados pueden lanzar más de 1 Tbps en sus servidores, es casi imposible.

Entre algunos de los muchos consejos que existen para detener estos ataques tenemos:

Identificar el ataque DDoS anticipadamente: Es buena idea familiarizarse con su perfil de tráfico entrante típico; cuanto más sepa sobre el tráfico normal, más fácil será detectar cuándo cambia su perfil. La mayoría de los ataques DDoS comienzan con picos pronunciados en el tráfico, y es útil poder diferenciar entre un repentino aumento de visitantes legítimos y el comienzo de un ataque DDoS. También es una buena idea nominar a un líder de DDoS en su empresa que sea responsable de actuar en caso de que sea atacado.

Sobre-provisión del ancho de banda: Por lo general, tiene sentido tener más ancho de banda disponible para su servidor web de lo que alguna vez cree que es probable que necesite. De esta forma, puede acomodar repentinas e inesperadas oleadas de tráfico que podrían ser el resultado de una campaña publicitaria, una oferta especial o incluso una mención de su empresa en los medios.
Incluso si aprovisiona en exceso en un 100 por ciento, o 500 por ciento, es probable que no detenga un ataque DDoS. Pero puede que tengas unos minutos más para actuar antes de que tus recursos se vean abrumados por completo.

Defender en el perímetro de la red (Por ejemplo, de su servidor web): Hay algunas medidas técnicas que se pueden tomar para mitigar parcialmente el efecto de un ataque, especialmente en los primeros minutos, y algunas de ellas son bastante simples. Por ejemplo, se puede:

- Limitar la tasa de tráfico del enrutador para evitar que su servidor web se vea abrumado.
- Agregar filtros para decirle a su enrutador que elimine los paquetes de las fuentes de ataque obvias.
- Agotar las conexiones semi-abiertas de forma más agresiva.
- Rechazar paquetes falsificados o malformados.
- Establecer con valores bajos los umbrales por caída de inundación de paquetes SYN, ICMP y UDP.

De igual forma, lo máximo que se puede esperar es obtener un poco más de tiempo a medida que aumenta el ataque DDoS.

Contratar a un especialista en mitigación de DDoS: Para ataques muy grandes, es probable que su mejor oportunidad de permanecer en línea sea utilizar una compañía especialista en mitigación de DDoS. Estas organizaciones tienen una infraestructura a gran escala y utilizan una variedad de tecnologías, incluida la depuración de datos, para ayudar a mantener su sitio web en línea.

Es posible que deba ponerse en contacto directamente con una empresa de mitigación de DDoS, o su compañía de alojamiento o proveedor de servicios puede tener un acuerdo de asociación con uno para manejar grandes ataques. Entre esos especialistas podemos citar:

- Akamai DDoS mitigation.
- Verisign DDoS Protection Services.
- Radware DDoS Protection.
- Cloudflare DDoS Protection.
- NetScout Arbor.
- Nexusguard.
- DOSarrest DDoS Protection.
- F5 DDoS Protection.
- Neustar SiteProtect NG.
- Imperva Incapsula.

En el sitio web http://www.digitalattackmap.com podemos encontrar un mapa del mundo que nos muestra la actividad DDoS global en un día determinado. Los ataques se muestran como líneas de puntos, se ajustan a escala y se colocan según los países de origen y de destino del tráfico de ataque cuando se conocen. Entre algunas características de la herramienta tenemos:

- Histograma en la parte inferior del mapa para explorar datos históricos.
- Poder seleccionar un país para ver la actividad DDoS desde o hacia ese país.
- Filtro de color para ver los ataques por clase, duración o puerto de origen / destino.
- Sección de noticias para encontrar informes en línea de actividades de ataque desde un tiempo específico.

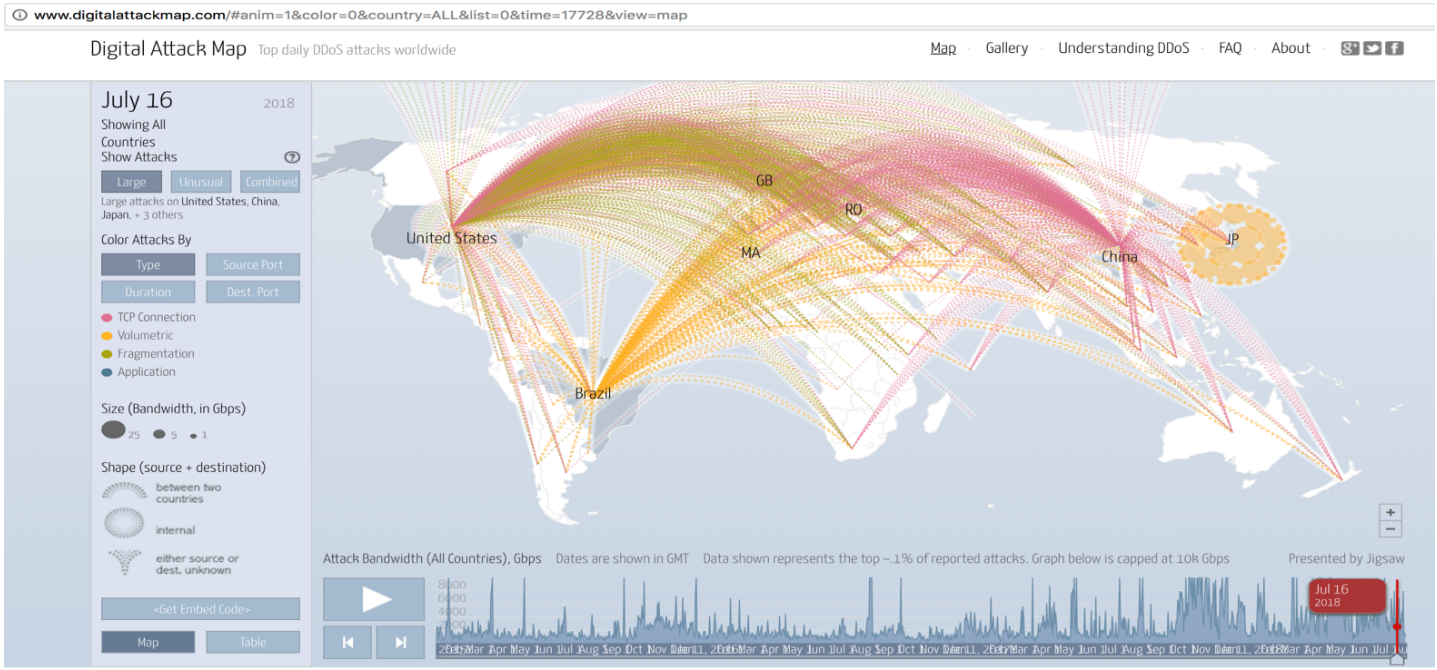


Figura # 4: DigitalAttackMap.com

Cibercrimen

Según establece el gobierno Australiano en su sitio web (ACORN.GOV.AU, 2018), el cibercrimen es un problema que afecta la vida de muchísimas personas, organizaciones y países.

Los ciberdelitos son crímenes, los cuales son:

- dirigido a computadoras u otros dispositivos (por ejemplo, piratería), y
- donde las computadoras u otros dispositivos son parte integral de la ofensa (por ejemplo, fraude en línea, robo de identidad y distribución de material de explotación infantil).

Los tipos comunes de delito cibernético incluyen piratería informática, fraudes en línea y fraude, robo de identidad, ataques a sistemas informáticos y contenido en línea ilegal o prohibida.
El efecto del cibercrimen puede ser extremadamente molesto para las víctimas y no necesariamente solo por razones financieras. Las víctimas pueden sentir que su privacidad ha sido violada y que son impotentes.

Según publicación de la Interpol (Interpol, 2018), el cibercrimen es un área de crímenes de rápido crecimiento. Cada vez más delincuentes están explotando la velocidad, la comodidad y el anonimato de Internet para cometer una amplia gama de actividades delictivas que no conocen fronteras, ya sean físicas o virtuales, causan daños graves y representan amenazas muy reales para las víctimas en todo el mundo.

La aplicación de la ley hace una distinción entre dos tipos principales de delitos relacionados con Internet:

- Cibercrimen avanzado (o crimen de alta tecnología): ataques sofisticados contra el hardware y software de la computadora.
- Delitos informáticos: muchos crímenes "tradicionales" han tomado un nuevo rumbo con el advenimiento de Internet, como los crímenes contra los niños, los delitos financieros y hasta el terrorismo.

Las nuevas tendencias en el delito cibernético están surgiendo todo el tiempo, con costos estimados para la economía mundial que ascienden a miles de millones de dólares.
En el pasado, el cibercrimen fue cometido principalmente por individuos o grupos pequeños. Hoy en día, estamos viendo redes de ciberdelincuentes altamente complejas que reúnen a personas de todo el mundo en tiempo real para cometer delitos en una escala sin precedentes.

Las organizaciones criminales recurren cada vez más a Internet para facilitar sus actividades y maximizar sus ganancias en el menor tiempo. Los crímenes en sí mismos no son necesariamente nuevos, como el robo, el fraude, el juego ilegal, la venta de

medicamentos falsos, pero están evolucionando de acuerdo con las oportunidades presentadas en línea y, por lo tanto, cada vez más generalizados y dañinos.

Según (Dennis, 2018), la mayoría de los delitos cibernéticos son ataques que no tienen lugar en un cuerpo físico, sino más bien tienen lugar en el cuerpo virtual personal o corporativo, que es el conjunto de atributos informativos que definen a las personas e instituciones en Internet. En otras palabras, en la era digital, nuestras identidades virtuales son elementos esenciales de la vida cotidiana: somos un conjunto de números e identificadores en múltiples bases de datos informáticas propiedad de gobiernos y empresas. El cibercrimen resalta la centralidad de las computadoras conectadas en red en nuestras vidas, así como la fragilidad de hechos aparentemente sólidos como la identidad individual.

Un aspecto importante del cibercrimen es su carácter no local: las acciones pueden ocurrir en jurisdicciones separadas por grandes distancias. Esto plantea graves problemas para la aplicación de la ley, ya que los delitos anteriormente locales o incluso nacionales ahora requieren cooperación internacional. Por ejemplo, si una persona accede a pornografía infantil ubicada en una computadora en un país que no prohíbe la pornografía infantil, ¿está cometiendo esa persona un delito en una nación donde dichos materiales son ilegales? ¿Dónde exactamente tiene lugar el cibercrimen? El ciberespacio es simplemente una versión más rica del espacio donde se lleva a cabo una conversación telefónica, en algún lugar entre las dos personas que tienen la conversación. Como una red que abarca todo el planeta, Internet ofrece a los delincuentes múltiples escondites tanto en el mundo real como en la propia red. Sin embargo, así como las personas que caminan por el suelo dejan marcas que un rastreador experto puede seguir, los ciberdelincuentes dejan pistas sobre su identidad y ubicación, a pesar de sus mejores esfuerzos para cubrir sus huellas. Sin embargo, para seguir esas pistas a través de las fronteras nacionales, los tratados internacionales de cibercrimen deben ser ratificados.

Afortunadamente en Costa Rica contamos con muy buena legislación en cuanto al cibercrimen, aunque como país nos encontramos aún en pañales en cuanto al desarrollo de estrategias y directrices en ciberseguridad; por lo menos contamos con un marco legal muy bueno que protege a los ciudadanos y empresas contra los delitos cibernéticos.

Con leyes como la 9048 y la 9135 sobre Delitos Informáticos, hechas con base en el documento del Convenio sobre la ciberdelincuencia, Budapest 2001, Costa Rica brinda un marco legal para luchar contra esta crisis que hoy en día ocupa más y más protagonismo en nuestro mundo. Cabe destacar además que, en nuestro país tenemos dos instituciones importantes que nos ayudan a combatir la ciberdelincuencia, entre ellas: la División de Delitos Informáticos del Poder Judicial y la Agencia de Protección de Datos de los Habitantes PRODHAB, la cual fue creada producto de la emisión de la Ley No. 8968, de Protección de Datos de la Persona frente al Tratamiento de sus Datos Personales, con el fin de orientar al ciudadano a ejercitar sus derechos y a las entidades públicas y privadas que manejan bases de datos, a cumplir con las obligaciones que establece dicha ley.

CAPÍTULO IV

HERRAMIENTAS ACTUALES

Herramientas actuales más destacadas en la solución de problemas de ciberseguridad.

Más adelante, en este documento, vamos a profundizar sobre diferentes formas de agrupar varios controles, herramientas y estrategias, aplicables para asegurar cualquier área de TI.

Por el momento, se pueden mencionar, según publicación de (CIS, 2017), tres fases para priorizar esfuerzos, o sea, un enfoque por etapas en todos los procesos relacionados para asegurar nuestra empresa.

- La *fase #1* implica saber qué hay en la red y comprender la línea base de ciberseguridad.

- La f*ase # 2* se centra en proteger la línea base de seguridad a través de la educación y la prevención.

- Finalmente, *la fase # 3* ayuda a la organización a prepararse con anticipación para eventos disruptivos.

	Fase #1 - Conoce tu Ambiente		
	Herramienta	***Descripción***	***URL / Source***
Fase #1	**Nmap**	Famoso escáner de red multipropósito, utilizado por administradores de sistemas y hackers de todo el mundo para identificar qué dispositivos están conectados a su red.	https://nmap.org/
	ZenMap	Interfaz gráfica de usuario fácil de usar para Nmap.	https://nmap.org/zenmap/
	Spiceworks	Software gratuito de inventario y gestión de activos para identificar dispositivos y software en su red.	https://www.spiceworks.com
	Applocker	Herramienta gratuita de Microsoft® Windows para identificar y restringir el software que está permitido ejecutar.	https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd759117(v=ws.11)
	Netwrix	Variedad de herramientas gratuitas para identificar información sobre el acceso administrativo en sus sistemas.	https://www.netwrix.com
	OpenAudIT	Aplicaciones de inventario y software en servidores de estaciones de trabajo y dispositivos de red.	http://www.open-audit.org/

	Fase #2 - Proteger los Activos		
	Herramienta	***Descripción***	***URL / Source***
Fase #2	**Bitlocker**	Cifrado incorporado para dispositivos con Microsoft® Windows.	https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732774(v=ws.11)
	FireVault	Cifrado incorporado para dispositivos Mac.	https://support.apple.com/en-us/HT204837
	Qualys Browser Check	Herramienta para verificar si su navegador está actualizado con todos sus parches.	https://browsercheck.qualys.com/
	OpenVAS	Herramienta para escanear sistemas para verificar las líneas de base de seguridad.	www.openvas.org
	Microsoft Baseline Security Analyzer	Herramienta gratuita de Microsoft® para comprender cómo las computadoras con Windows pueden configurarse de forma segura.	https://www.microsoft.com/en-us/download/details.aspx?id=7558

	Fase #3 - Preparar la Organización		
	Herramienta	***Descripción***	***URL / Source***
Fase #3	**Microsoft "Backup and Restore"**	Herramienta de utilidad de respaldo instalada en los sistemas operativos Microsoft®.	https://support.microsoft.com/en-us/help/17127/windows-back-up-restore
	Apple Time Machine	Herramienta de respaldo instalada en los sistemas operativos Apple®.	https://support.apple.com/en-us/HT201250
	Amanda Network Backup	Herramienta gratuita de copia de seguridad de código abierto.	http://www.amanda.org
	Bacula	Solución de copia de seguridad y recuperación de red de código abierto.	http://blog.bacula.org

	[ToolBox] Otras herramientas para el proceso…		
	Herramienta	***Descripción***	***URL / Source***
#1	**VirtualBox** by Oracle	VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico. VirtualBox no solo es un producto extremadamente rico en características y alto rendimiento para clientes empresariales, también es la única solución profesional que está disponible libremente como software de código abierto bajo los términos de la Licencia Pública General de GNU (GPL) versión 2.	https://www.virtualbox.org/
#2	**VMware Workstation Player**	VMware Workstation Player es una utilidad ideal para ejecutar una sola máquina virtual en una PC con Windows o Linux. Las organizaciones usan Workstation Player para entregar escritorios corporativos administrados, mientras que los estudiantes y educadores lo usan para el aprendizaje y la capacitación.	https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
#3	**VEGA**	Vega es un escáner de seguridad web gratuito y de código abierto y una plataforma de pruebas de seguridad web para probar la seguridad de las aplicaciones web. Vega puede ayudarlo a encontrar y validar Inyección SQL, Cross-Site Scripting (XSS), divulgación de información confidencial inadvertidamente y otras vulnerabilidades. Está escrito en Java, basado en GUI, y se ejecuta en Linux, OS X y Windows.	https://subgraph.com/vega/index.en.html
#4	**Metasploitable** Virtual Machine to Test Metasploit	Metasploitable es una máquina virtual basada en Linux que contiene varias vulnerabilidades intencionales para que pueda aprovechar. Metasploitable es esencialmente un laboratorio de pruebas de penetración en una caja, disponible como máquina virtual VMware (VMX).	https://information.rapid7.com/download-metasploitable-2017.html

	[ToolBox] Otras herramientas para el proceso…		
	Herramienta	***Descripción***	***URL / Source***
#5	**McAfee Software Free Tools** End User License Agreement **Anti-Malware Tools**	- GetSusp - Ransomware Interceptor (Pilot) - Stinger - McAfee Ransomware Recover (MR2) - RootkitRemover - Tesladecrypt - Pinkslipbot Control Server Proxy Detection and Port-Forwarding Removal Tool - Steganography Analysis Tool	https://www.mcafee.com/us/downloads/free-tools/index.aspx
#6	**SecTools.Org Top 125 Network Security Tools**	Durante más de una década, el Proyecto Nmap ha estado catalogando las herramientas favoritas de la comunidad de seguridad de red. En 2011, este sitio se volvió mucho más dinámico, ofreciendo calificaciones, revisiones, búsqueda, clasificación y un nuevo formulario de sugerencias de herramientas.	http://sectools.org/
#7	**WifiSlax**	Es una distribución GNU/Linux en formato *.iso basada en Slackware con funcionalidades de LiveCD y LiveUSB. WiFiSlax incluye una larga lista de herramientas de seguridad y auditoría como numerosos escáners de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría wireless, además de añadir una serie de útiles lanzadores. Posee una gran integración de varios controladores de red no oficiales en el kernel de Linux, y da así soporte inmediato para un gran número de tarjetas de red cableadas e inalámbricas.	http://www.wifislax.com/

	[ToolBox] Otras herramientas para el proceso…		
	Herramienta	***Descripción***	***URL / Source***
#8	**KALI Linux**	La seguridad ofensiva nació de la creencia de que la única forma real de lograr una seguridad defensiva sólida es a través de una mentalidad y un enfoque ofensivos. Kali Linux es uno de varios proyectos de Seguridad ofensiva, financiado, desarrollado y mantenido como una plataforma de prueba de penetración gratuita y de código abierto.	https://www.kali.org/
#9	**Black Arch**	BlackArch Linux es una distribución de prueba de penetración basada en Arch Linux para testers de penetración e investigadores de seguridad. El repositorio contiene 1950 herramientas. Puede instalar herramientas individualmente o en grupos.	https://blackarch.org/
#10	**Pen Test Box**	It essentially provides all the security tools as a software package and lets you run them natively on Windows. This effectively eliminates the requirement of virtual machines or dualboot environments on windows. It was created because more than 50% of penetration testing distribution users use virtual machines to run those distributions on the Windows operating system.	https://pentestbox.org/

CAPÍTULO V

Propuesta de Solución

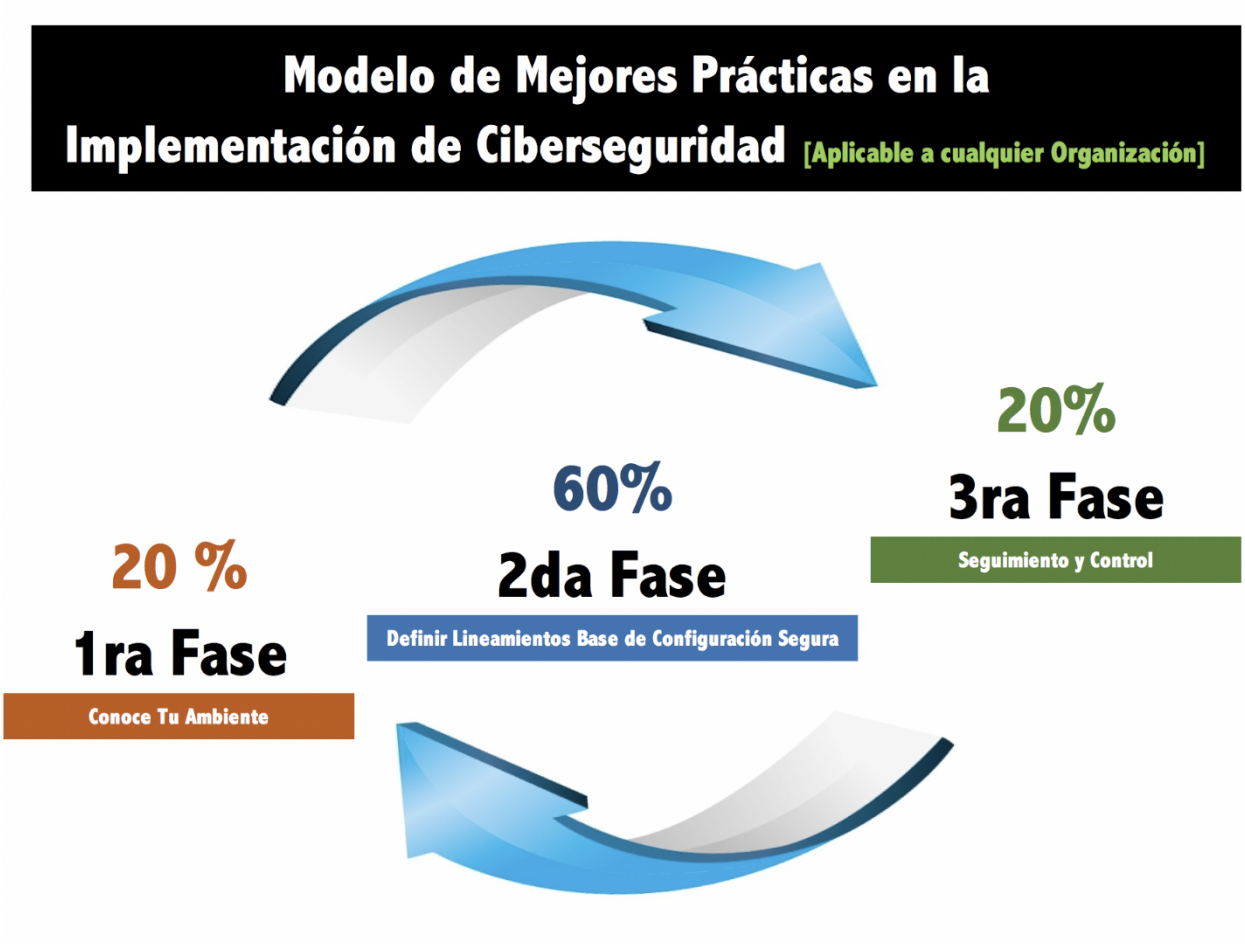


Figura # 5: Modelo de Ejecución (Ilustración de las fases que componen el modelo)

Este modelo de ejecución consta de tres fases en las que agrupamos todos los controles, evaluaciones de seguridad y guías de configuraciones base, con las que se pretende asegurar las áreas de TI más importantes y sensibles de cualquier organización.

Cada fase y cada paso en este modelo tienen un valor porcentual; más adelante se determinará el nivel en el que la organización se encuentra en cuanto a implementación de ciberseguridad. Por definición y naturaleza del proceso, este modelo se puede aplicar de manera cíclica y dotar a la organización de una mejora continua en la tarea del aseguramiento de todas sus áreas de tecnología.

En todos los controles del modelo y en cada uno de los pasos por seguir, se emplean ciertos parámetros para medir el nivel de implementación; por lo que se definen:

- (I) Implementado.
- (NN) No es necesario o No Aplica.
- (N) No se ha implementado aún.
- (P) Parcialmente implementado.

Más adelante se explicará en detalle que función tienen estos parámetros en la fase de resultados, en donde tendremos una nota de nuestro esfuerzo de implementación.

Esta primera fase agrupa dos controles básicos pero primordiales en nuestra tarea por implementar la ciberseguridad, estos requieren precisión para saber qué activos deben estar protegidos y cuál software o aplicación se ejecuta en esos activos. Se espera que, si seguimos todas las pautas en esta fase, tendríamos ya un 20% de nuestra organización asegurada.

20 %

1ra Fase

Conoce tu ambiente

SF.C01 - Inventario de dispositivos autorizados y no autorizados.

SF.C02 - Inventario de software autorizado y no autorizado.

En la segunda fase, que requiere también del mayor esfuerzo, se encuentran los controles y diagnósticos más relevantes del modelo; por ello, completar esta etapa significa un 60% del total, un porcentaje muy importante por el nivel de implementación, que se lograría en la seguridad de la compañía.

60%

2da Fase

Definir lineamientos base de configuración segura

SF.C03 - **Hardening**: Asegurar configuraciones para todo el hardware y software

SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología

- Acceso al sistema (logging) y monitoreo.
- Administración de sistemas.
- Administración de vulnerabilidades.
- Autenticación.
- Control de accesos.
- Encriptación.

SF.C03.SA02 - Lineamientos de seguridad para las bases de datos.

- Control de accesos.
- Instalación.
- Roles y permisos.
- Configuraciones de entorno.

SF.C06 - Protección para navegadores web y correo.

SF.C07 - Defensas del malware.

SF.C09 - Asegurar configuraciones para dispositivos de red.

SF.C10 - Control de accesos para las redes inalámbricas.

SF.C11 - Implementación de seguridad en las aplicaciones

SF.C11.SA04 - Evaluación de seguridad para implementación de APIs

- Arquitectura.
- Codificación de salidas (Outputs).
- Control de accesos.
- Criptografía.
- Desarrollo.
- Monitoreo y Logs.
- Sesión: Autenticación y autorización.
- Validación de entradas (INPUTS).
- Vulnerabilidades.

En esta última fase, se emplean otros controles compensatorios, e igual de primordiales en nuestra tarea, con los que cerramos nuestro ciclo de aseguramiento; esta conforma el último 20% de nuestra nota final.

Como mencionamos anteriormente, todo este proceso en general es iterativo, por lo que podemos volver a la primera fase e iniciar otra ronda; la idea es siempre estar actualizados y en total mejora de nuestra seguridad.

20%

3ra Fase

Seguimiento y Control

SF.C04 - Evaluación y Remediación Continua de Vulnerabilidades.

SF.C05 - Controlar el uso de los privilegios administrativos.

SF.C08 - Limitación y control de puertos de red, protocolos y servicios.

Los controles a continuación son un conjunto recomendado de acciones para la defensa cibernética que brindan formas específicas y accionables para detener los ataques más penetrantes y peligrosos de la actualidad.

Un beneficio principal de los controles es que priorizan en enfocar un menor número de acciones con altos resultados. Además, son efectivos porque se derivan de los patrones de ataque más comunes destacados en los principales informes de amenazas y examinados en una comunidad muy amplia de profesionales del gobierno y la industria.

Fueron creados por personas que saben cómo funcionan los ataques (equipos de la Agencia Nacional de Seguridad de los EE. UU., laboratorios de energía nuclear del Departamento de Energía de los EE. UU., organizaciones de justicia encargadas de hacer cumplir la ley y algunas de las principales organizaciones forenses y de respuesta ante incidentes).

SF.C01 - Inventario de dispositivos autorizados y no autorizados			
Control		Buenas prácticas de seguridad	Evaluación
Fase #1 - Conoce Tu Ambiente	SF.C01.1	- Implemente una herramienta de descubrimiento de inventario de activos automatizada y úsela para crear un inventario preliminar de los sistemas conectados a las redes públicas y privadas de la organización. - Deben emplearse tanto las herramientas activas que escanean los rangos de direcciones de red IPv4 o IPv6 como las herramientas pasivas que identifican hosts basados en el análisis de su tráfico.	**[I] [NN] [N] [P]**
	SF.C01.2	- Si la organización asigna dinámicamente direcciones usando DHCP, implemente entonces DHCP y use esta información para mejorar el inventario de activos y ayudar a detectar sistemas desconocidos.	**[I] [NN] [N] [P]**
	SF.C01.3	- Asegúrese de que todas las adquisiciones de equipos actualicen automáticamente el sistema de inventario, a medida que nuevos dispositivos aprobados estén conectados a la red.	**[I] [NN] [N] [P]**
	SF.C01.4	- Mantenga un inventario de activos de todos los sistemas conectados a la red y los dispositivos de red, al registrar al menos las direcciones de red, nombre (s) de la máquina, propósito de cada sistema, propietario del activo responsable de cada dispositivo y departamento asociado a cada dispositivo. - El inventario debe incluir todos los sistemas que tengan una dirección de protocolo de Internet (IP) en la red, incluidos, entre otros, *desktops, portátiles, servidores, equipos de red (routers, switches, firewalls, etc.), impresoras, equipos de almacenamientos de área de red, Teléfonos IP, equipos con direcciones virtuales, etc*. - El inventario de activos creado, también debe incluir datos sobre si el dispositivo es un dispositivo portátil y / o personal. Deben identificarse dispositivos como *teléfonos móviles, tabletas, computadoras portátiles y otros dispositivos electrónicos portátiles* que almacenan o procesan datos, independientemente de si están conectados a la red de la organización.	**[I] [NN] [N] [P]**

SF.C01 - Inventario de dispositivos autorizados y no autorizados			
Control		Buenas prácticas de seguridad	Evaluación
Fase #1 - Conoce Tu Ambiente	SF.C01.5	- Implemente la autenticación a nivel de red, a través de 802.1x, para limitar y controlar qué dispositivos se pueden conectar a la red. El 802.1x debe estar vinculado a los datos de inventario, para determinar los sistemas autorizados versus los no autorizados.	**[I] [NN] [N] [P]**
	SF.C01.6	- Utilice los certificados del cliente para validar y autenticar los sistemas antes de conectarse a la red privada.	**[I] [NN] [N] [P]**
	Herramientas	Nmap, ZenMap, SpiceWorks	

SF.C02 - Inventario de software autorizado y no autorizado			
	Control	Buenas prácticas de seguridad	Evaluación
Fase #1 - Conoce Tu Ambiente	SF.C02.1	- Diseñe una lista de software autorizado y la versión que se requiere en la empresa para cada tipo de sistema, incluidos servidores, estaciones de trabajo y computadoras portátiles de diversos tipos y usos. - Esta lista debe ser supervisada por las herramientas de comprobación de integridad de archivos, para validar que el software autorizado no ha sido modificado.	**[I] [NN] [N] [P]**
	SF.C02.2	- Implemente la tecnología de listas blancas de aplicaciones que permite que los sistemas ejecuten software, solo si está incluido en la lista blanca e impide la ejecución de todos los demás software del sistema. - La lista blanca puede ser muy extensa (como una lista de proveedores disponibles), de modo que los usuarios no tengan inconvenientes cuando utilicen un software común. O bien, para algunos sistemas de propósito especial (que requieren solo una pequeña cantidad de programas para lograr su funcionalidad comercial necesaria), la lista blanca puede ser bastante limitada.	**[I] [NN] [N] [P]**
	SF.C02.3	- Implemente herramientas de inventario de software en toda la organización que cubran cada uno de los tipos de sistemas operativos en uso, incluidos servidores, estaciones de trabajo y computadoras portátiles. - El sistema de inventario de software debe rastrear la versión del sistema operativo subyacente, así como las aplicaciones instaladas en él. - Los sistemas de inventario de software deben estar vinculados al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.	**[I] [NN] [N] [P]**
	SF.C02.4	Las máquinas virtuales y / o los sistemas de espacio aislado se deben usar para aislar y ejecutar aplicaciones que se requieren para las operaciones comerciales, pero basadas en un riesgo mayor no deberían instalarse dentro de un entorno de red.	**[I] [NN] [N] [P]**
	Herramientas	Applocker, OpenAudIT, IDS & IPS products	

sf.c03 - Hardening: asegurar configuraciones para todo el hardware y software			
Control		Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C03.1	- Establezca configuraciones seguras estándar de sus sistemas operativos y aplicaciones de software. Las imágenes estandarizadas deben representar versiones reforzadas del sistema operativo subyacente y las aplicaciones instaladas en el sistema. - Estas imágenes deben validarse y actualizarse regularmente para actualizar su configuración de seguridad a la luz de las vulnerabilidades recientes y los vectores de ataque.	**[I] [NN] [N] [P]**
	SF.C03.2	- Siga la administración de configuración estricta, al generar una imagen segura que se utiliza para crear todos los sistemas nuevos que se implementan en la empresa. Cualquier sistema existente que se vea comprometido, debería ser reimpreso con la compilación segura. - Las actualizaciones regulares o excepciones a esta imagen, deben integrarse en los procesos de gestión de cambios de la organización. Las imágenes deben crearse para estaciones de trabajo, servidores y otros tipos de sistemas utilizados por la organización.	**[I] [NN] [N] [P]**
	SF.C03.3	- Almacene las imágenes maestras en servidores configurados de forma segura, validados con herramientas de comprobación de integridad capaces de inspección continua y gestión de cambios, para garantizar que solo sean posibles los cambios autorizados en las imágenes. - Alternativamente, estas imágenes maestras se pueden almacenar en máquinas fuera de línea, separadas de la red de producción, que puedan ser copiadas a través de medios seguros para moverlas entre los servidores de almacenamiento de imágenes y la red de producción.	**[I] [NN] [N] [P]**
	SF.C03.4	- Realice toda la administración remota de servidores, estaciones de trabajo, dispositivos de red y equipos similares a través de canales seguros. - Los protocolos como telnet, VNC, RDP u otros que no sean compatibles con el cifrado seguro, solo se deben usar si se realizan a través de un canal de cifrado secundario, como SSL, TLS o IPSEC.	**[I] [NN] [N] [P]**

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software			
Control		Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C03.5	- Utilice las herramientas de comprobación de integridad de archivos para asegurarse de que los archivos críticos del sistema (incluidos el sistema sensible y los ejecutables, las bibliotecas y las configuraciones de la aplicación) no se hayan modificado. - El **sistema de informes** debe: *- Tener la capacidad de darse cuenta de los cambios de rutina y esperados.* *- Resaltar y alertar sobre alteraciones inusuales o inesperadas.* *- Muestre el historial de cambios de configuración a lo largo del tiempo e identifique quién realizó el cambio (incluida la cuenta de inicio de sesión original en el caso de un cambio de ID de usuario, como con el comando su o sudo)*. - Estas verificaciones de integridad deberían identificar alteraciones sospechosas del sistema, tales como: - Cambios de dueño y permisos a archivos o directorios. - El uso de flujos de datos alternativos que podrían usarse para ocultar actividades maliciosas. - Y la introducción de archivos adicionales en áreas clave del sistema (lo que podría indicar carga útil maliciosa dejada por atacantes o archivos adicionales añadidos inapropiadamente durante los procesos de distribución por lotes).	**[I] [NN] [N] [P]**
	SF.C03.6	- Implemente y pruebe un sistema de monitoreo de configuración automatizado que verifique todos los elementos de configuración segura comprobables remotamente y las alertas cuando ocurran cambios no autorizados. - Esto incluye *la detección de nuevos puertos de escucha, nuevos usuarios administrativos, cambios en los objetos de políticas locales y grupales (cuando corresponda) y nuevos servicios que se ejecutan en un sistema.* Siempre que sea posible, use herramientas que cumplan con el protocolo de automatización del contenido de seguridad (SCAP) para agilizar los informes y la integración.	**[I] [NN] [N] [P]**

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software			
Control		Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C03.7	- Implemente herramientas de administración de configuración del sistema, tales como Active Directory Group Policy Objects para sistemas Microsoft Windows o sistemas Puppet para UNIX que aplicarán y volverán a implementar automáticamente las configuraciones en los sistemas a intervalos regularmente programados. - Deben ser capaces de desencadenar la redistribución de la configuración de forma programada, manual o basada en eventos.	**[I] [NN] [N] [P]**
	Herramientas	- Microsoft Baseline Security Analyzer - Red Hat (Open SCAP 1) - Rapid1 (Nexpose 6) - ThreatGuard (Secutor Compliance Automation Toolkit S-CAT 5) - SPAWAR (SCAP Compliance Checker 4)	

SF.C03 - HARDENING: Asegurar Configuraciones para todo el Hardware y Software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
Código		Pregunta a evaluar	Evaluación	Fecha	Resp.
Autenticación	SF.C03.SA01.A.1	¿La autenticación está en línea con los requisitos de la política de seguridad de la compañía? - Nivel de acceso **Público**: acceso anónimo permitido. - Nivel de acceso **Interno**: autenticación de un solo factor como contraseña. - Nivel de acceso **Confidencial**: autenticación múltiple. - Nivel de acceso **Restringido**: autenticación de múltiples factores.	**[I] [NN] [N] [P]**		
	SF.C03.SA01.A.2	¿El acceso a los activos se autentica de forma centralizada para los usuarios estándar? (por ejemplo: *LDAP, Kerberos, Active Directory, RACF / Top Secret*)	**[I] [NN] [N] [P]**		
	SF.C03.SA01.A.3	¿Los ajustes del sistema están configurados para garantizar que la complejidad de la contraseña cumpla con los estándares de la compañía?	**[I] [NN] [N] [P]**		
Código		Pregunta por evaluar	Evaluación	Fecha	Resp.
Control de Accesos	SF.C03.SA01.B.1	¿Tiene cada usuario interno un identificador único (identificación de usuario, cuenta de usuario) y contraseña?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.2	¿Está prohibido el uso de identificadores genéricos de usuarios designados para el uso por usuarios múltiples o usuarios anónimos?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.3	¿Existe un proceso documentado formal para otorgar solicitudes de acceso?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.4	¿El acceso se otorga con el mínimo privilegio, es decir, con el nivel de acceso más bajo otorgado para permitir al usuario realizar un rol de trabajo?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.5	¿Se revisan los derechos de acceso de usuarios privilegiados al menos cada 3 meses para garantizar que sigan siendo válidos?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
	Código	Pregunta por evaluar	Evaluación	Fecha	Resp.
Control de Accesos	SF.C03.SA01.B.6	¿Existe un proceso formal de abandono, documentado, que elimine las cuentas redundantes?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.7	¿Se revisan los derechos de acceso de los usuarios estándar al menos una vez al año para garantizar que sigan siendo válidos?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.8	¿Hay informes de cuentas no utilizadas durante 60 días que no se hayan inhabilitado?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.9	¿Hay informes de cuentas no utilizadas durante 120 días que no se han eliminado?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.10	¿Hay informes de actividad de cuenta privilegiada?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.B.11	¿Hay informes de errores de inicio de sesión?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp.
Administración de Sistemas	SF.C03.SA01.C.1	¿Están deshabilitados todos los servicios y cuentas innecesarios? (algunos ejemplos serían: *scripts, controladores, características, subsistemas, sistemas de archivos, servidores web*)	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.2	¿Se renombraron y protegieron todas las cuentas administrativas locales con una contraseña segura?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.3	¿Se vuelven a nombrar todas las cuentas predeterminadas?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.4	¿Han cambiado las contraseñas provistas por el proveedor de sus configuraciones predeterminadas?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.5	¿El acceso a las herramientas de administración está denegado por defecto y restringido a usuarios autorizados?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.6	¿Hay contraseñas, para cuentas de usuario con privilegios y cuentas de servicio que ejecutan funciones con privilegios, de al menos 10 caracteres de largo?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.7	¿El acceso administrativo está limitado a redes internas y confiables?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.8	¿Los administradores inician sesión con autenticación de dos factores?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.9	¿Las cuentas de soporte o proveedor están habilitadas solo cuando son requeridas, y monitoreadas cuando están en uso?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.10	¿Las sesiones de las herramientas de administración expiran después de 15 minutos de inactividad?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.C.11	¿Están deshabilitadas todas las interfaces físicas innecesarias para evitar el acceso no autorizado?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp.
Encriptación	SF.C03.SA01.D.1	¿Está encriptada toda la información de la organización de acuerdo con la política de seguridad global? - Información confidencial almacenada fuera de los entornos seguros de la compañía o transmitida a través de redes inseguras debe estar encriptada. - la información restringida siempre se debe cifrar en almacenamiento y transmisión.	**[I] [NN] [N] [P]**		
	SF.C03.SA01.D.2	¿El proceso de administración de cifrado de claves incluye: i) acceso restringido al menor número de custodios necesarios ? ii) las claves de cifrado son al menos tan fuertes como las claves de cifrado de datos que protegen ? iii) almacenamiento separado de las claves de encriptación ? iv) las claves se almacenan de forma segura y en el menor número de ubicaciones posibles ? v) criptoperíodo definido para cada clave ? vi) cómo y cuándo reemplazar las llaves ?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.D.3	¿Se utilizan algoritmos y tamaños de clave que proporcionan al menos la potencia equivalente de AES256 para cifrar datos en reposo o transmisiones de datos?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar Configuraciones para todo el Hardware y Software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
	Código	Pregunta por evaluar	Evaluación	Fecha	Resp.
Acceso al Sistema (Logging) y Monitoreo	SF.C03.SA01.E.1	¿La infraestructura produce el registro al nivel adecuado para ***respaldar el análisis forense***, particularmente en el caso de cualquier acceso a los datos del titular de la tarjeta? Los siguientes eventos deben registrarse: - auditoría de usuarios de cuentas privilegiadas como root o admin - intenta usar una cuenta inactiva - entradas de contraseña inválidas - Excede el umbral - aprovisionamiento de cuenta - acceso de usuario individual a los datos de la tarjeta - intentos no autorizados de acceder a cuentas o recursos - cambios en la configuración, configuraciones de seguridad y permisos - puesta en marcha del sistema, parada, alerta o fallas - actualizaciones de versiones de código - acceso a los registros de auditoría - detener o pausar los registros de auditoría - creación y eliminación de objetos a nivel del sistema - acceso a las utilidades del sistema - actividad de terceros y soporte de proveedores	**[I] [NN] [N] [P]**		
	SF.C03.SA01.E.2	¿Están todos los relojes del sistema sincronizados?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
	Código	Pregunta por evaluar	Evaluación	Fecha	Resp.
Acceso al Sistema (Logging) y Monitoreo	SF.C03.SA01.E.3	Los registros contienen: - identidad de usuario, - tipo de evento (intentos de inicio de sesión fallidos, deshabilitación de registros de auditoría, cambios), - recurso afectado, - fecha / hora, - resultado, - motivo de la falla - Información de IP - dirección de red y protocolo	**[I] [NN] [N] [P]**		
	SF.C03.SA01.E.4	¿Se revisan los registros para detectar intrusiones, acceso no autorizado, actividades no intencionadas, software malicioso o intentos de estas u otras acciones que comprometan la seguridad de los sistemas de la compañía?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.E.5	¿Están todos los registros de eventos de seguridad de la información escritos en tiempo real en un servidor de registro centralizado y seguro?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.E.6	¿Los registros de seguridad son monitoreados y revisados por una función de seguridad central?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA01 - Evaluación de seguridad para implementación de nueva tecnología					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp.
Administración de Vulnerabilidades	SF.C03.SA01.F.1	¿Están todos los activos dentro de su área actualizados con parches de seguridad relevantes?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.F.2	¿Existen procesos efectivos para obtener lanzamientos de parches para todos los SO compatibles?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.F.3	¿Tiene un proceso en lugar de escanear el sistema de vulnerabilidades regularmente (todos los SO / dispositivos compatibles)?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.F.4	¿Utiliza un enfoque basado en el riesgo para remediar las vulnerabilidades que se encuentran en línea con los requisitos de la política de seguridad global?	**[I] [NN] [N] [P]**		
	SF.C03.SA01.F.5	¿Todos los dispositivos se someten a pruebas de penetración (internas y externas) en una base anual mínima? De ser así, ¿las vulnerabilidades son corregidas de acuerdo con los requisitos de la política de seguridad global?	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de datos					
Código		Requerimiento de seguridad	Evaluación	Fecha	Resp.
Instalación	SF.C03.SA02.A.1	Eliminar los scripts de conexión a las base de datos: Estos pueden contener combinaciones de nombre de usuario y contraseña al permitir a un atacante mucho más oportunidad de comprometer la base de datos.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.A.2	Asegurar que el inicio de sesión remota y la ejecución remota de comandos para la instancia dueña de la base de datos, esté desactivada. Dicha instancia es muy vulnerable y compromete toda la base de datos.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.A.3	Deshabilitar componentes innecesarios de la base de datos: Muchos de estos componentes predeterminados permiten el acceso remoto y además vienen con vulnerabilidades de desbordamiento de búfer, lo cual puede permitir a los usuarios autenticados obtener acceso administrativo a la base de datos subyacentes.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de datos					
Código		Requerimiento de seguridad	Evaluación	Fecha	Resp.
Control de Accesos	SF.C03.SA02.B.1	Asegurar que el acceso a los DBMS binarios y ejecutables esté restringido: Falllar en asegurar los archivos del sistema operativo DBMS pueden permitir al atacante oportunidades mucho mayores para comprometer el sistema.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.B.2	Deshabilitar métodos innecesarios de acceso a las bases de datos de producción: Medios alternativos de conectividad a las bases de datos (servidores HTTP, bases de datos XML, etc.) presentan una gran cantidad de vulnerabilidades que pueden ser potencialmente utilizadas comprometer el sistema.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.B.3	Prevenir a los usuarios de tener la capacidad de leer archivos de rastreo (Trace): Los usuarios con acceso a archivos de rastreo pueden acceder información que probablemente no deberían.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.B.4	Limitar o negar el acceso a capacidades de restauración de la base de datos: La restauración de las bases de datos puede permitir que atacantes puedan acceder a los datos de forma no controlada ni monitoreada. También puede resultar en interrupción de la base de datos debido a una accidental sobreescritura de las bases de datos actuales con copias anteriores, por ejemplo.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de datos					
Código		Requerimiento de seguridad	Evaluación	Fecha	Resp.
Control de Accesos	SF.C03.SA02.B.5	Restrinja el acceso a la red de los servidores de base de datos: No implementar controles para un acceso de red estricto aumenta la oportunidad de ataques potenciales.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.B.6	Asegurarse de que los desarrolladores no se concedan acceso sin restricciones en ambientes de producción, por ejemplo: No restringir el acceso del desarrollador al los entornos de producción aumentan el riesgo de cambios inapropiados o no autorizados a la base de datos. Algunos de estos accesos a entornos de producción pueden ser necesarios, para diferentes requerimientos o soporte, por lo que controles adicionales compensatorios deben ser utilizados para asegurar que este acceso está habilitado sólo cuando es estrictamente necesario y monitoreado de cerca.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de datos					
	Código	Requerimiento de seguridad	Evaluación	Fecha	Resp.
Roles y Permisos	SF.C03.SA02.C.1	Asegurar que la instancia dueña de la base de datos no esté en alguno de los grupos de nivel administrador o configurado como una cuenta de sistema local (Servidores con sistemas operativos Windows). No restringir los privilegios de la instancia de base de datos puede aumentar el nivel de acceso a un atacante. Los usuarios deben ser creados con perfiles apropiados para la función, el perfil predeterminado puede estar sujeto a cambiar en cualquier momento y puede tener configuraciones ilimitadas que a menudo es requerido por el usuario SYS cuando se hace un parcheo; tales configuraciones ilimitadas deben estar estrictamente reservadas y no aplicado a usuarios innecesarios.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.C.2	Cambiar el nombre de la cuenta del propietario del software (no predeterminado): El uso de nombres de cuenta predeterminados aumenta el riesgo de un ataque de fuerza bruta exitoso, dando lugar a un acceso no autorizado. Como sugerencia, se podría asignar como dueños de base de datos a los gerentes de cada proceso en especial, para así mantener un inventario claro de bases de datos.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de datos					
Código		Requerimiento de seguridad	Evaluación	Fecha	Resp.
Roles y Permisos	SF.C03.SA02.C.3	Las aplicaciones DBMS a menudo crean numerosos archivos y directorios que pueden contener información sensible. No asegurar que estos objetos de datos se crean con los permisos asegurados pueden permitir acceso no autorizado a información. Las revisiones de la gerencia proporcionarán garantías de que niveles de acceso apropiado son aplicados Revisión de acceso privilegiado (DB Administrador, propietario de DB, otro) debe realizarse al menos una vez por trimestre, todas las demás revisiones de acceso a BD se deberán realizar al menos una vez al año (recomendado una vez cada 6 meses).	**[I] [NN] [N] [P]**		
	SF.C03.SA02.C.4	Limitar el acceso otorgado al rol PÚBLICO: El rol de PUBLIC en un DMBS es a menudo privilegios concedidos muy por encima de lo que es necesario.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de Datos					
Código		Requerimiento de seguridad	Evaluación	Fecha	Resp.
Roles y Permisos	SF.C03.SA02.C.5	Controle qué usuarios pueden crear objetos dentro de esquemas: Sin controles de acceso granulares, el riesgo de acceso no autorizado aumenta. El establecimiento de políticas de RBAC (Rol Based Access Control) proporciona roles de usuario estandarizados, los cuales definen los niveles de acceso.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.C.6	Prevenir actualizaciones ad-hoc a las tablas del sistema: Las actualizaciones ad-hoc a las tablas del sistema permiten al administrador de base de datos modificar datos dentro de las tablas del sistema, posiblemente impactando la integridad y disponibilidad de datos en el entorno de producción. La función de rol ad-hoc puede permitir un usuario no autorizado para acceder potencialmente, cambiar datos confidenciales o dañar el catálogo de datos debido a potencial completo de acceso a la instancia. Se recomienda restringir la capacidad.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de datos					
	Código	Requerimiento de seguridad	Evaluación	Fecha	Resp.
Configuraciones de Entorno	SF.C03.SA02.D.1	Separar los datos de: archivos DBMS, sistema operativo, archivos de registro, copias de seguridad a la hora de configurar los servidores dedicados de base de datos. La segregación de estos componentes reduce el riesgo de acceso no autorizado a los datos. Segregación lógica y / o física de código, datos y registros es un excelente método para asegurar un DBMS en general, siempre y cuando, las credenciales no sean compartidas a través de los segmentos. Se entiende que algunas bases de datos se configuran en un entorno de nivel único, en cuyo caso este requisito no aplica.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.D.2	No usar puertos predeterminados. Las bases de datos generalmente utilizan puertos estándar que son bien conocidos, por lo que son blanco de ataques.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.D.3	Implementar protección para los enlaces de base de datos: Los enlaces de las bases de datos se crean para permitir la comunicación entre ellas, permitiendo el procesamiento distribuido. Fallar al validar y restringir estos enlaces aumenta la oportunidad de usuarios maliciosos para obtener acceso no autorizado a los datos en caso de un compromiso. Permitir a usuarios sin privilegios manipular o ver los enlaces de la base de datos puede permitir la captura de contraseña, información, etc.	**[I] [NN] [N] [P]**		

SF.C03 - HARDENING: Asegurar configuraciones para todo el hardware y software					
SF.C03.SA02 - Lineamientos de seguridad para las bases de Datos					
Código		Requerimiento de seguridad	Evaluación	Fecha	Resp.
Configuraciones de Entorno	SF.C03.SA02.D.4	Implementar vistas para la seguridad de los datos: La falta de uso de vistas aumenta el riesgo de que los datos sean accedidos o modificados por personas no autorizadas. Las restricciones en las vistas de la base de datos deben ser en función del usuario, rol, y requisitos adicionales.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.D.5	Asegurarse que todos los datos de muestra (demo) y usuarios de muestra son eliminados: Los esquemas de muestra no son necesarios para el funcionamiento de la base de datos. Los datos de muestra no son necesarios para operaciones de producción, ya que proporciona a los usuarios con valores predeterminados, contraseñas o procedimientos, esta información podría ser utilizada para generar un ataque o explotar alguna vulnerabilidad en dichos ambientes de producción.	**[I] [NN] [N] [P]**		
	SF.C03.SA02.D.6	Eliminar todas las puertas traseras (Back Doors) en bases de datos de producción: Si dejamos puertas traseras utilizadas en desarrollos y cuentas de prueba en los entornos de producción se aumenta el riesgo de acceso no autorizado. Se recomienda mantener ambientes separados, de desarrollo y pruebas (UAT), y de producción.	**[I] [NN] [N] [P]**		

SF.C04 - Evaluación y remediación continua de vulnerabilidades			
Control		Buenas prácticas de seguridad	Evaluación
Fase #3 - Seguimiento y Control	SF.C04.1	- Ejecute herramientas automatizadas de análisis de vulnerabilidades contra todos los sistemas de la red de forma semanal o más frecuente y entregue listas priorizadas de las vulnerabilidades más críticas a cada administrador del sistema responsable junto con puntajes de riesgo que comparen la efectividad de los administradores del sistema y departamentos para reducir el riesgo. - Use un escáner de vulnerabilidades validado por SCAP que busque las vulnerabilidades basadas en código (como las descritas en Common Vulnerabilities and Exposures **(https://nvd.nist.gov/config/cce/index)**) y las vulnerabilidades basadas en la configuración (según lo enumerado por el Common Configuration Enumeration Project).	**[I] [NN] [N] [P]**
	SF.C04.2	- **Correlacione registros** de eventos con información de escaneos de vulnerabilidades para cumplir dos objetivos: - En primer lugar, el personal debe verificar que la actividad de las herramientas de análisis de vulnerabilidades habituales esté registrada. - En segundo lugar, el personal debería poder correlacionar los eventos de detección de ataques con los resultados de escaneo de vulnerabilidades anteriores para determinar si el exploit dado se usó contra un objetivo conocido como vulnerable.	**[I] [NN] [N] [P]**
	SF.C04.3	- Realice la exploración de vulnerabilidades en modo autenticado, ya sea con agentes que se ejecutan localmente en cada sistema final para analizar la configuración de seguridad o con escáneres remotos a los que se les otorgan derechos administrativos en el sistema que se prueba. - Utilice una cuenta dedicada para escaneos de vulnerabilidad autenticados, que no se deben usar para ninguna otra actividad administrativa y deben estar vinculados a máquinas específicas en direcciones IP específicas. - Asegúrese de que solo los empleados autorizados tengan acceso a la interfaz de usuario de gestión de vulnerabilidades y que los roles se apliquen a cada usuario.	**[I] [NN] [N] [P]**

SF.C04 - Evaluación y remediación continua de vulnerabilidades			
Control		Buenas prácticas de seguridad	Evaluación
Fase #3 - Seguimiento y Control	SF.C04.4	- Suscríbase a los servicios de inteligencia de vulnerabilidad para mantenerse al tanto de las exposiciones emergentes y utilice la información obtenida de esta suscripción para actualizar las actividades de exploración de vulnerabilidades de la organización al menos **una vez al mes**. - De forma alternativa, asegúrese de que las herramientas de análisis de vulnerabilidades que utiliza se actualicen periódicamente con todas las vulnerabilidades de seguridad relevantes importantes.	**[I] [NN] [N] [P]**
	SF.C04.5	- Implemente **herramientas automatizadas de administración de parches y herramientas de actualización de software** para sistemas operativos y software / aplicaciones en todos los sistemas para los cuales dichas herramientas están disponibles y son seguras. Los parches se deben aplicar a todos los sistemas, incluso a los sistemas que se ventilan correctamente.	**[I] [NN] [N] [P]**
	SF.C04.6	- Controle los registros asociados con cualquier actividad de escaneo y cuentas de administrador asociadas para garantizar que esta actividad se limite a los marcos de tiempo de los escaneos legítimos.	**[I] [NN] [N] [P]**
	SF.C04.7	- Compare los resultados de los escaneos de vulnerabilidades consecutivos para verificar que las vulnerabilidades se abordaron mediante parches, implementando un **control de compensación o documentando y aceptando un riesgo comercial razonable**. - Dicha aceptación de los riesgos comerciales para las vulnerabilidades existentes debe revisarse periódicamente para determinar si los controles de compensación más recientes o los parches posteriores pueden abordar las vulnerabilidades que se aceptaron previamente, o si las condiciones han cambiado, lo que aumenta el riesgo.	**[I] [NN] [N] [P]**
	SF.C04.8	- **Establecer un proceso para evaluar** las vulnerabilidades basadas en la vulnerabilidad y el posible impacto de la vulnerabilidad, y segmentado por grupos de activos apropiados (por ejemplo, servidores DMZ, servidores de red internos, computadoras de escritorio, computadoras portátiles). - Primero **aplique parches para las vulnerabilidades más riesgosas**. - **Establezca los cronogramas** de parche esperados basados en el nivel de calificación de riesgo.	**[I] [NN] [N] [P]**

SF.C05 - Controlar el uso de los privilegios administrativos			
Control		Buenas prácticas de seguridad	Evaluación
Fase #3 - Seguimiento y Control	SF.C05.1	- Minimice los privilegios administrativos y solo use cuentas administrativas cuando sean necesarios. - Implementar auditorías enfocadas en el uso de funciones administrativas privilegiadas y monitorear el comportamiento anómalo.	**[I] [NN] [N] [P]**
	SF.C05.2	- Use herramientas automatizadas para inventariar todas las cuentas administrativas y valide que cada persona con privilegios administrativos en computadoras de escritorio, computadoras portátiles y servidores esté autorizada por un ejecutivo superior.	**[I] [NN] [N] [P]**
	SF.C05.3	- Antes de implementar cualquier dispositivo nuevo en un entorno de red, cambie todas las contraseñas predeterminadas para que las aplicaciones, los sistemas operativos, los enrutadores, los firewalls, los Access Point inalámbricos y otros sistemas tengan valores compatibles con las cuentas de nivel de administración.	**[I] [NN] [N] [P]**
	SF.C05.4	- Configure los sistemas para emitir una entrada de registro y una alerta cuando se agrega o elimina una cuenta de un grupo de administradores de dominio, o cuando se agrega una nueva cuenta de administrador local en un sistema.	**[I] [NN] [N] [P]**
	SF.C05.5	- Configure los sistemas para emitir una entrada de registro y alerta sobre cualquier inicio de sesión fallido en una cuenta administrativa.	**[I] [NN] [N] [P]**
	SF.C05.6	- Use la **autenticación multifactor** para todos los accesos administrativos, incluido el acceso administrativo del dominio. La autenticación de múltiples factores puede incluir una variedad de técnicas, que incluyen el uso de tarjetas inteligentes, certificados, tokens de contraseña única (OTP), datos biométricos u otros métodos de autenticación similares.	**[I] [NN] [N] [P]**

SF.C05 - Controlar el uso de los privilegios administrativos			
Control		Buenas prácticas de seguridad	Evaluación
Fase #3 - Seguimiento y Control	SF.C05.7	- Cuando no se admite la autenticación de múltiples factores, las cuentas de usuario deberán usar contraseñas largas en el sistema (**más de 14 caracteres**).	**[I] [NN] [N] [P]**
	SF.C05.8	- Se debe solicitar a los administradores que accedan a un sistema utilizando una cuenta totalmente registrada y no administrativa. Luego, una vez que haya iniciado sesión en la máquina sin privilegios administrativos, el administrador debería hacer la transición a privilegios administrativos utilizando herramientas como Sudo en Linux / UNIX, RunAs en Windows y otras instalaciones similares para otros tipos de sistemas.	**[I] [NN] [N] [P]**
	SF.C05.9	- Los administradores utilizarán una máquina dedicada para todas las tareas administrativas o tareas que requieran un acceso elevado. Esta máquina debe estar aislada de la red principal de la organización y no se le debe permitir el acceso a Internet. Esta máquina no debe usarse para leer correos electrónicos, componer documentos o navegar en Internet.	**[I] [NN] [N] [P]**

SF.C06 - protección para navegadores web y correo			
Control		Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C06.1	- Asegúrese de que solo los navegadores web y los clientes de correo electrónico totalmente compatibles puedan ejecutarse en la organización, lo ideal es usar la última versión de los navegadores proporcionados por el proveedor para aprovechar las últimas funciones de seguridad y correcciones.	**[I] [NN] [N] [P]**
	SF.C06.2	- Desinstale o deshabilite cualquier complemento de navegador o cliente de correo electrónico innecesario o no autorizado o aplicaciones complementarias. - Cada complemento utilizará la lista blanca de aplicaciones / URL y solo permitirá el uso de la aplicación para dominios preaprobados.	**[I] [NN] [N] [P]**
	SF.C06.3	- Limite el uso de lenguajes de scripting innecesarios en todos los navegadores web y clientes de correo electrónico. Esto incluye el uso de idiomas como **ActiveX y JavaScript** en sistemas en los que no es necesario admitir dichas capacidades.	**[I] [NN] [N] [P]**
	SF.C06.4	- Registre todas las solicitudes de URL de cada uno de los sistemas de la organización, ya sea en el sitio o en un dispositivo móvil, para identificar actividades potencialmente maliciosas y ayudar a los manejadores de incidentes a identificar sistemas potencialmente comprometidos.	**[I] [NN] [N] [P]**
	SF.C06.5	- Implemente dos configuraciones de navegador separadas para cada sistema: - Una configuración debería desactivar el uso de todos los complementos, lenguajes de scripts innecesarios y, en general, configurarse con funcionalidad limitada y utilizarse para la navegación web general. - La otra configuración permitirá más funcionalidades del navegador, pero solo se debe usar para acceder a sitios web específicos que requieren el uso de dicha funcionalidad.	**[I] [NN] [N] [P]**

SF.C06 - Protección para Navegadores Web y Correo			
Control		Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C06.6	- La organización debe mantener y aplicar filtros de URL basados en la red que limiten la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. - La organización se suscribirá a los servicios de categorización de URL para asegurarse de que estén actualizados con las definiciones de categoría de sitio web más recientes disponibles. - Los sitios no categorizados se bloquearán de manera predeterminada. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea que se encuentren físicamente en las instalaciones de una organización o no.	**[I] [NN] [N] [P]**
	SF.C06.7	- Para reducir la posibilidad de mensajes de correo electrónico falsificados, implemente el marco de políticas del remitente (SPF) desplegando registros SPF en DNS y habilitando la verificación del lado del receptor en los servidores de correo.	**[I] [NN] [N] [P]**
	SF.C06.8	- Escanee y bloquee todos los archivos adjuntos de correo electrónico que ingresen al gateway de correo electrónico de la organización si contienen códigos maliciosos o tipos de archivos innecesarios para el negocio de la organización. - Esta exploración debe realizarse antes de que el correo electrónico se coloque en la bandeja de entrada del usuario. Esto incluye el filtrado de contenido de correo electrónico y el filtrado de contenido web.	**[I] [NN] [N] [P]**

SF.C07 - Defensas del malware			
Control		Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C07.1	- Emplee herramientas automatizadas para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles con **antivirus, antispyware, firewalls personales y funcionalidad IPS basada en host.** - Todos los eventos de detección de malware deben enviarse a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos.	**[I] [NN] [N] [P]**
	SF.C07.2	- Utilice un software antimalware que ofrezca una infraestructura centralizada que recopile información sobre la reputación de archivos o haga que los administradores envíen actualizaciones manualmente a todas las máquinas. - Después de aplicar una actualización, los sistemas automatizados deben verificar que cada sistema haya recibido su actualización de firma.	**[I] [NN] [N] [P]**
	SF.C07.3	- Limite el uso de dispositivos externos a aquellos con una necesidad empresarial aprobada y documentada. - Monitoree el uso e intento de uso de dispositivos externos. Configure computadoras portátiles, estaciones de trabajo y servidores para que no ejecuten automáticamente el contenido de medios extraíbles, como tokens USB (es decir, "unidades miniatura"), discos duros USB, CD / DVD, dispositivos FireWire, dispositivos de conexión de tecnología avanzada en serie externa, y acciones de red montadas. - Configure los sistemas para que automáticamente realicen un análisis antimalware de los medios extraíbles cuando se inserten.	**[I] [NN] [N] [P]**

SF.C07 - Defensas del Malware			
Control		Buenas Prácticas de Seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C07.4	- Habilite las funciones antiexploración, como la Prevención de ejecución de datos (DEP), Aleatorización de diseño de espacio de direcciones (ASLR), virtualización / contenedorización, etc. - Para una mayor protección, implemente capacidades como Enhanced Mitigation Experience Toolkit (EMET) que se pueden configurar para aplicarlas protecciones a un conjunto más amplio de aplicaciones y ejecutables.	**[I] [NN] [N] [P]**
	SF.C07.5	- Utilice herramientas antimalware basadas en la red para identificar ejecutables en todo el tráfico de la red y utilice técnicas distintas a la detección basada en firmas para identificar y filtrar el contenido malicioso antes de que llegue al punto final.	**[I] [NN] [N] [P]**
	SF.C07.6	- Habilite el registro de consultas del sistema de nombres de dominio (DNS) para detectar búsquedas de nombres de host en dominios C2 maliciosos conocidos.	**[I] [NN] [N] [P]**

SF.C08 - Limitación y control de puertos de red, protocolos y servicios			
Control		Buenas prácticas de seguridad	Evaluación
Fase #3 - Seguimiento y Control	SF.C08.1	- Asegúrese de que solo se ejecuten puertos, protocolos y servicios con necesidades comerciales validadas en cada sistema.	**[I] [NN] [N] [P]**
	SF.C08.2	- Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.	**[I] [NN] [N] [P]**
	SF.C08.3	- Realice escaneos automáticos de puertos de forma regular contra todos los servidores de claves y en comparación con una línea de base efectiva conocida. Si se descubre un cambio que no figura en la línea de base aprobada de la organización, se debe generar y revisar una alerta.	**[I] [NN] [N] [P]**
	SF.C08.4	- Verifique cualquier servidor que sea visible desde Internet o una red que no sea de confianza, y si no es necesario para fines comerciales, muévalo a una VLAN interna y asígnele una dirección privada.	**[I] [NN] [N] [P]**
	SF.C08.5	- Opere servicios críticos en máquinas host físicas o lógicas separadas, como DNS, archivos, correo, web y servidores de bases de datos.	**[I] [NN] [N] [P]**
	SF.C08.6	- Coloque firewalls de aplicaciones frente a servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier servicio o tráfico no autorizado se debe bloquear y generar una alerta.	**[I] [NN] [N] [P]**

SF.C09 - Asegurar configuraciones para dispositivos de red			
	Control	Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C09.1	- Compare la configuración de Firewalls, Routers, Switches con configuraciones de seguridad estándar definidas para cada tipo de dispositivo de red en uso en la organización. - La configuración de seguridad de tales dispositivos debe ser documentada, revisada y aprobada por una junta de control de cambios de la organización.	**[I] [NN] [N] [P]**
	SF.C09.2	- Todas las nuevas reglas de configuración, más allá de una configuración reforzada que permita que el tráfico fluya a través de dispositivos de seguridad de red, como firewalls e IPS basados en red, deben documentarse y registrarse en un sistema de administración de configuración, con un motivo comercial específico para cada cambio, el nombre específico de la persona responsable de esa necesidad comercial y la duración esperada de la necesidad.	**[I] [NN] [N] [P]**
	SF.C09.3	- Use herramientas automatizadas para verificar configuraciones de dispositivos estándar y detectar cambios. - Todas las alteraciones en dichos archivos deben registrarse y reportarse automáticamente al personal de seguridad.	**[I] [NN] [N] [P]**
	SF.C09.4	- Administre dispositivos de red usando autenticación de dos factores y sesiones encriptadas.	**[I] [NN] [N] [P]**
	SF.C09.5	- Instale la última versión estable de las actualizaciones relacionadas con la seguridad en todos los dispositivos de red.	**[I] [NN] [N] [P]**

SF.C010 - Control de accesos para las redes inalámbricas			
	Control	Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C10.1	- Asegúrese de que cada dispositivo inalámbrico conectado a la red, coincida con una configuración autorizada y que cuente con un perfil de seguridad, con un propietario de la conexión documentado y una necesidad comercial definida. - Las organizaciones deben denegar el acceso a esos dispositivos inalámbricos que no tienen dicha configuración y perfil.	**[I] [NN] [N] [P]**
	SF.C10.2	- Configure las herramientas de exploración de vulnerabilidades de red para detectar los puntos de acceso inalámbrico conectados a la red cableada. - Los dispositivos identificados se deben conciliar con una lista de puntos de acceso inalámbrico autorizados. Los puntos de acceso no autorizados deben estar desactivados.	**[I] [NN] [N] [P]**
	SF.C10.3	- Use sistemas inalámbricos de detección de intrusos (WIDS) para identificar dispositivos inalámbricos sospechosos y detectar intentos de ataque y compromisos exitosos. - Además de WIDS, todo el tráfico inalámbrico debe ser monitoreado por WIDS a medida que el tráfico pasa a la red cableada.	**[I] [NN] [N] [P]**
	SF.C10.4	- Cuando se haya identificado una necesidad comercial específica para el acceso inalámbrico, configure el acceso inalámbrico en las máquinas del cliente para permitir el acceso solo a redes inalámbricas autorizadas. - Para dispositivos que no tienen un propósito comercial inalámbrico esencial, deshabilite el acceso inalámbrico en la configuración de hardware (sistema básico de entrada / salida o interfaz extensible del firmware).	**[I] [NN] [N] [P]**
	SF.C10.5	- Asegúrese de que todo el tráfico inalámbrico tenga, al menos, el cifrado del Estándar de Cifrado Avanzado (AES) que se utiliza al menos con la protección Wi-Fi Protected Access 2 (WPA2).	**[I] [NN] [N] [P]**

SF.C010 - Control de accesos para las redes inalámbricas			
	Control	Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C10.6	- Asegúrese de que las redes inalámbricas usen protocolos de autenticación como Protocolo de autenticación extensible: seguridad de la capa de transporte (EAP / TLS), que proporcionan protección de credenciales y autenticación mutua.	**[I] [NN] [N] [P]**
	SF.C10.7	- Inhabilite las capacidades de red inalámbrica punto a punto en clientes inalámbricos.	**[I] [NN] [N] [P]**
	SF.C10.8	- Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth), a menos que tal acceso sea necesario para una necesidad comercial documentada.	**[I] [NN] [N] [P]**
	SF.C10.9	- Cree redes de área local virtuales separadas (VLAN) para sistemas BYOD u otros dispositivos que no sean de confianza. - El acceso a Internet desde esta VLAN debe atravesar al menos el mismo límite que el tráfico corporativo. El acceso de la empresa desde esta VLAN debe tratarse como no confiable y debe filtrarse y auditarse en consecuencia.	**[I] [NN] [N] [P]**

SF.C11 - Implementación de seguridad en las aplicaciones			
	Control	Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C11.1	- Para todo el software de aplicación adquirido, verifique que la versión que está utilizando todavía sea compatible con el proveedor. De lo contrario, actualice a la versión más actual e instale todos los parches relevantes y las recomendaciones de seguridad del proveedor.	**[I] [NN] [N] [P]**
	SF.C11.2	- Proteja las aplicaciones web implementando firewalls de aplicaciones web (WAF) que inspeccionen todo el tráfico que fluye hacia la aplicación web para ataques de aplicaciones web comunes, incluidos, entre otros, scripts entre sitios, inyección SQL, inyección de comandos y ataques de directorio cruzado. - Para las aplicaciones que no están basadas en la web, se deben implementar firewalls de aplicaciones específicas si dichas herramientas están disponibles para el tipo de aplicación dado. - Si el tráfico está encriptado, el dispositivo debe sentarse detrás del cifrado o ser capaz de descifrar el tráfico antes del análisis. Si ninguna de las opciones es adecuada, se debe implementar un firewall de aplicaciones web basado en host.	**[I] [NN] [N] [P]**
	SF.C11.3	- Para el software desarrollado internamente, asegúrese de que se realice y documente la verificación de errores explícita para todas las entradas, incluidos el tamaño, el tipo de datos y los rangos o formatos aceptables.	**[I] [NN] [N] [P]**
	SF.C11.4	- Pruebe las aplicaciones web desarrolladas internamente y adquiridas por terceros para detectar debilidades de seguridad comunes mediante el uso de escáneres de aplicaciones web remotas automatizados antes de la implementación, cada vez que se realicen actualizaciones en la aplicación y de manera recurrente. - En particular, las rutinas de validación de entrada y codificación de salida del software de aplicación deben ser revisadas y probadas.	**[I] [NN] [N] [P]**
	SF.C11.5	- No muestre mensajes de error del sistema a los usuarios finales (desinfección de salida).	**[I] [NN] [N] [P]**

SF.C11 - Implementación de seguridad en las aplicaciones			
	Control	Buenas prácticas de seguridad	Evaluación
Fase #2 - Definir Lineamientos Base de Configuración Segura	SF.C11.6	- Mantener entornos separados para sistemas de producción y no producción (Desarrollo o UAT). - Los desarrolladores no deberían tener un acceso sin supervisión a los entornos de producción.	**[I] [NN] [N] [P]**
	SF.C11.7	- Para aplicaciones que dependen de una base de datos, use plantillas de Hardening, para limpiar la configuración por defecto. - Todos los sistemas que son parte de procesos comerciales críticos también deben ser probados.	**[I] [NN] [N] [P]**
	SF.C11.8	- Asegúrese de que todo el personal de desarrollo de software reciba capacitación para escribir código seguro para su entorno de desarrollo específico.	**[I] [NN] [N] [P]**
	SF.C11.9	- Para las aplicaciones desarrolladas internamente, asegúrese de que los artefactos de desarrollo (datos de muestra y scripts, bibliotecas no utilizadas, componentes, código de depuración o herramientas) no estén incluidos en el software implementado o accesibles en el entorno de producción.	**[I] [NN] [N] [P]**

SF.C11 - Implementación de seguridad en las aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Sesión: Autenticación y Autorización	SF.C11.SA04.A.1	¿Los nombres de usuario, contraseñas, tokens de sesión y claves API no pueden aparecer en la URL?	**[I] [NN] [N] [P]**		
	SF.C11.SA04.A.2	¿Las sesiones están autenticadas por un método seguro? P.ej. estableciendo un token de sesión a través de un POST o usando una clave API como un argumento de cuerpo POST o como una cookie.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.A.3	¿Se usa un protocolo seguro para autenticación y autorización? P.ej. Oauth 2.0 o OpenID Connect	**[I] [NN] [N] [P]**		
	SF.C11.SA04.A.4	¿El estado de la sesión está protegido de los ataques de reproducción? P.ej. mediante el uso de una clave de cifrado de tiempo limitado, codificada contra el token de sesión o la clave de API, la fecha y hora y la dirección IP entrante	**[I] [NN] [N] [P]**		
	SF.C11.SA04.A.5	¿Los tokens de sesión expiran después de un corto período? La duración de la sesión debe depender de la aplicación y la sensibilidad de los datos a los que se puede acceder y establecer en el menor tiempo posible.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.A.6	¿El alcance de los tokens de acceso está limitado solo a la funcionalidad que necesita el usuario?	**[I] [NN] [N] [P]**		

SF.C11 - Implementación de Seguridad en las Aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Control de Accesos	SF.C11.SA04.B.1	¿Existen límites impuestos al uso inadecuado o de alta velocidad de las API para evitar la denegación de servicio o el cultivo de datos? P.ej. esto se puede implementar en firewalls de aplicaciones web o en una puerta de enlace API. También se pueden considerar los controles contractuales, los certificados del lado del cliente, CAPTCHAS o las claves de API que limitan la tasa. Los límites de velocidad pueden ser diferentes según el verbo API, y bloquear temporalmente una clave API hasta que se haya investigado el uso.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.B.2	¿Se asegura de que el método HTTP entrante sea válido para el token de sesión o la clave API y la recolección, acción y registro de recursos asociados? P.ej. Los verbos POST, PUT y DELETE pueden no ser apropiados para todos los usuarios.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.B.3	¿Los verbos API permitidos para la API están controlados con una lista blanca? P.ej. Es importante que el servicio se asegure de que solo los verbos permitidos funcionen, mientras que los demás devolverán un código de retorno HTTP prohibido 403 .	**[I] [NN] [N] [P]**		

SF.C11 - Implementación de Seguridad en las Aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Control de Accesos	SF.C11.SA04.B.4	¿Los tokens de sesión o las claves API se envían como un parámetro de cookie o cuerpo para garantizar que las colecciones o acciones privilegiadas estén protegidas adecuadamente del uso no autorizado?	**[I] [NN] [N] [P]**		
	SF.C11.SA04.B.5	¿Las solicitudes PUT, POST y DELETE están protegidas contra la falsificación de solicitudes entre sitios? P.ej. mediante el uso de un enfoque basado en token fuerte y la eliminación de las vulnerabilidades de secuencias de comandos entre sitios.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.B.6	¿Las verificaciones contextuales de datos siempre se realizan en el servidor en cada solicitud para garantizar que sean válidas para el usuario? P.ej. Las URL o incluso un formulario POSTed nunca deben contener una " clave " de control de acceso o similar que proporcione una verificación automática.	**[I] [NN] [N] [P]**		

SF.C11 - Implementación de seguridad en las aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Validación de Entradas (INPUTS)	SF.C11.SA04.C.1	¿Están todas las entradas suministradas por el usuario validadas, desinfectadas o codificadas para evitar secuencias de comandos entre sitios o ataques de inyección?	**[I] [NN] [N] [P]**		
	SF.C11.SA04.C.2	¿Se usa un analizador seguro para los mensajes entrantes, y si se usa XML, un analizador que no es vulnerable a los ataques de entidades externas XML (XXE)?	**[I] [NN] [N] [P]**		
	SF.C11.SA04.C.3	Cuando sea posible, ¿los datos suministrados por el usuario se limitan a un número limitado de opciones lo más rápido posible? P.ej. las entradas solo pueden ser verdaderas o falsas, o un número, o uno de un pequeño número de valores aceptables	**[I] [NN] [N] [P]**		
	SF.C11.SA04.C.4	¿El servidor valida que el usuario suministró el encabezado Content-Type? P.ej. esta comprobación debería garantizar que el encabezado Content-Type y el contenido sean del mismo tipo, o si falta el encabezado Content-Type o se proporciona un encabezado inesperado de tipo de contenido.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.C.5	Si el marco API utilizado proporciona validación, ¿está habilitado?	**[I] [NN] [N] [P]**		

SF.C11 - Implementación de seguridad en las aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Codificación de Salidas (Outputs)	SF.C11.SA04.D.1	¿Está el servidor configurado para enviar siempre al cliente el encabezado de tipo de contenido y las opciones de tipo de contenido? P.ej. esto debería incluir el tipo de contenido correcto, el juego de caracteres y X-Content-Type-Options: opciones de nosniff .	[I] [NN] [N] [P]		
	SF.C11.SA04.D.2	¿Está el codificador JSON configurado de manera segura para evitar ataques? P.ej. si se usa node.js, en el servidor es vital que se use un serializador JSON adecuado para codificar los datos proporcionados por el usuario de manera adecuada. Al insertar valores en el DOM del navegador, use .value / .innerText / .textContent para protegerlo contra simples ataques DOM XSS.	[I] [NN] [N] [P]		
	SF.C11.SA04.D.3	¿Se construye todo el XML de salida utilizando un serializador XML para proteger contra la inyección de XML?	[I] [NN] [N] [P]		
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Criptografía	SF.C11.SA04.E.1	¿Se aplica TLS de forma segura para todas las API?	[I] [NN] [N] [P]		
	SF.C11.SA04.E.2	Si la API está almacenando en caché datos confidenciales o regulados, ¿está fuertemente encriptada cuando está en la memoria o en el disco? P.ej. AES 128, AES 256, etc. Los algoritmos de codificación, de cosecha propia o patentada, no se consideran fuertes ni están sometidos a pruebas industriales.	[I] [NN] [N] [P]		
	SF.C11.SA04.E.3	Si están disponibles, ¿se utilizan tokens web JSON para garantizar la integridad del mensaje?	[I] [NN] [N] [P]		

SF.C11 - Implementación de seguridad en las aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Arquitectura	SF.C11.SA04.F.1	¿La API devuelve los códigos de retorno HTTP correctos para ayudar a validar las solicitudes entrantes e identificar mejor los posibles riesgos de seguridad?	**[I] [NN] [N] [P]**		
	SF.C11.SA04.F.2	¿La documentación de la API es completa y de una calidad adecuada? P.ej. esto debería ser tanto del usuario (por ejemplo, programador de API) como de la perspectiva del administrador .	**[I] [NN] [N] [P]**		
	SF.C11.SA04.F.3	¿Están prohibidas todas las conexiones externas a los sistemas internos limitando el tráfico de Internet entrante a una DMZ? ¿segmento?	**[I] [NN] [N] [P]**		
	SF.C11.SA04.F.4	Si está expuesto a Internet, ¿la aplicación actualmente está siendo monitoreada y protegida por una aplicación web? ¿Cortafuegos? Si los servidores de la aplicación albergan o procesan información confidencial o restringida están equipados con un sistema de protección contra intrusiones basado en host o protegidos por un sistema de protección contra intrusos dedicado y	**[I] [NN] [N] [P]**		
	SF.C11.SA04.F.5	¿un firewall que se implementa para la red inmediata que contiene los servidores? "	**[I] [NN] [N] [P]**		
	SF.C11.SA04.F.6	¿Existe un diagrama de red actualizado, un diagrama de flujo de datos y una lista de activos para esta aplicación?	**[I] [NN] [N] [P]**		

SF.C11 - Implementación de seguridad en las aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Desarrollo	SF.C11.SA04.G.1	¿Las pruebas estáticas se incluyen como parte del ciclo de vida de desarrollo?	[I] [NN] [N] [P]		
	SF.C11.SA04.G.2	¿La API ha sido probada manualmente y se ha aprobado un informe de prueba?	[I] [NN] [N] [P]		
	SF.C11.SA04.G.3	¿Se mantiene un registro auditable de todas las actualizaciones del código de la aplicación de producción para que exista un seguimiento continuo de los cambios?	[I] [NN] [N] [P]		
	SF.C11.SA04.G.4	¿Se mantienen actualizadas todas las bibliotecas y componentes de aplicaciones de terceros, incluido el software de código abierto? Enumere todas las principales bibliotecas de aplicaciones y componentes que se utilizan y sus versiones en la sección de comentarios.	[I] [NN] [N] [P]		
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Monitoreo y Logs	SF.C11.SA04.H.1	¿Los registros de auditoría registran las acciones intentadas por usuarios que no están autorizados para realizarlos? P.ej. intentos fallidos de acceder, cambiar o eliminar archivos, registros, tablas o ejecutar funciones de aplicaciones restringidas.	[I] [NN] [N] [P]		
	SF.C11.SA04.H.2	¿Tiene procesos implementados para monitorear el acceso a los datos?	[I] [NN] [N] [P]		
	SF.C11.SA04.H.3	¿Los registros de auditoría registran toda la actividad de gestión de cuentas? P.ej. creación, eliminación y modificaciones de cuenta, o cambios a roles y grupos que otorgan privilegios.	[I] [NN] [N] [P]		

SF.C11 - Implementación de seguridad en las aplicaciones					
SF.C011.SA04 - Evaluación de seguridad para implementación de APIs					
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Monitoreo y Logs	SF.C11.SA04.H.4	¿Los registros de la aplicación contienen suficiente información para reconstruir eventos pasados? Para responder Sí, los registros deben contener como mínimo los siguientes detalles: Marca de tiempo Usuario / ID del sistema Descripción del evento Resultado del evento	**[I] [NN] [N] [P]**		
	SF.C11.SA04.H.5	¿Están todos los registros de eventos de seguridad de la información escritos en tiempo real en un servidor de registro seguro y centralizado?	**[I] [NN] [N] [P]**		
Código		Pregunta por evaluar	Evaluación	Fecha	Resp. / Rol
Vulnerabilidades	SF.C11.SA04.I.1	¿Los servidores que alojan esta aplicación escanean regularmente en busca de vulnerabilidades? Por ej. Escaneos de Qualys.	**[I] [NN] [N] [P]**		
	SF.C11.SA04.I.2	¿Son todas las infraestructuras del sistema? P.ej. sistemas operativos, dispositivos de red, firewalls, bases de datos, etc.), cubiertos por un proceso formal, regular y oportuno de administración de parches.	**[I] [NN] [N] [P]**		

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

1. Este trabajo logra describir las diferentes áreas de tecnología que existen en las diferentes organizaciones y cómo se integran entre ellas. Por ejemplo: Gobernanza de Tecnologías de Información, Gobernanza de Ciberseguridad, Infraestructura y Telecomunicaciones, Aplicaciones y Soporte a Usuario Final; de manera que se propone un esquema de cómo debe operar, además de algunos servicios clave de cada una. Se enfatiza también la necesidad de asegurar cada una de ellas mediante controles de seguridad, para así operar con un menor riesgo, de forma más tranquila, en un mundo empresarial competitivo y muy atacado en los últimos años en cuanto a ciberataques.

2. Esta investigación explica en detalle y con algunos ejemplos cómo operan las amenazas cibernéticas más sobresalientes de los últimos años, como lo son: Las Amenazas Persistentes Avanzadas, Vulnerabilidades del Día Cero, Ransomware, Ataques por Denegación de Servicio y Ciber-crimen. Con ello se logra informar de forma clara sobre los peligros que existen si estas nos llegan a afectar, además de mencionar algunos consejos para protegernos de ellas.

3. Como parte del aporte en esta investigación, se proporciona una gran cantidad de herramientas disponibles en el mercado para trabajar en el área de ciberseguridad, en el área preventiva y de aseguramiento, la mayoría son gratuitas y de código abierto, como también se describen otras que son de proveedores reconocidos en el medio tecnológico.

4. A través del desarrollo del modelo propuesto, se analiza y se explica en detalle cada uno de los controles propuestos en este trabajo; con ello se logra una vasta guía de mejores prácticas en la tarea de asegurar cada una de las áreas de tecnología en las empresas.

5. El principal fin de este trabajo investigativo se plasma en la elaboración del modelo para implementar la ciberseguridad en las organizaciones, de forma que se establece una forma metódica y práctica, a la vez de seguir una extensa serie de guías y evaluaciones, para las áreas críticas de tecnología. Se abarcan diferentes aspectos esenciales como arquitectura, validación de entradas, codificación de salidas, control de accesos, criptografía, monitoreo y registros de bitácoras, asegurar la sesión (autenticación y autorización), administración de vulnerabilidades, entre muchos otros. Este modelo consta de tres fases con un porcentaje de trabajo asignado a cada uno y además es cíclico, de manera que aporta un comportamiento de mejora continua en las organizaciones. Esto significa un modelo vivo, información que se actualiza constantemente y, por ende, permite a las compañías estar siempre al día en cuanto a sus TICs.

6.2 **Recomendaciones**

Se recomienda aplicar este modelo en su totalidad en cualquier organización para así dotar de una seguridad base, eficiente y efectiva para enfrentar muchas de las actuales amenazas.

Sin embargo, cabe destacar que este no abarca todos los controles ni evaluaciones que existen en el mercado, por lo que no es la última palabra para el aseguramiento total de una organización. Esto conllevaría muchísimas horas en análisis por parte de expertos y muchas horas de trabajo en la ejecución, además de contar con aplicaciones de software y equipos especializados.

CAPÍTULO VII

TRABAJOS FUTUROS

Este modelo de mejores prácticas, a través de guías y evaluaciones, se podría actualizar periódicamente, para así mantenerse vigente y efectivo en el aseguramiento de cada una de las áreas de tecnología.

Además, a este modelo se le agregó un módulo para contabilizar los puntos de evaluación de cada uno de los controles, de manera que se podría implementar un tablero principal con los resultados de cada uno. Esto podría ser de gran utilidad para las gerencias y juntas directivas a la hora de visualizar los resultados, sacar estadísticas y conclusiones para tomar mejores decisiones.

Existen muchos más controles por agregar, para formar parte de este modelo, de manera que se puede robustecer y así abarcar más áreas de tecnología, por ejemplo: Administración y respuesta a incidentes, Pruebas de penetración, Defensas de borde, Control y monitoreo de cuentas, Entrenamiento y capacitación en temas de ciberseguridad para los colaboradores, entre otros.

BIBLIOGRAFÍA

ACORN.GOV.AU. (04 de 08 de 2018). Obtenido de Learn about Cybercrime: https://www.acorn.gov.au/learn-about-cybercrime

Australian_Government. (02 de 2017). *Strategies to Mitigate CyberSecurity Incidents [White Paper].* Australia: Australian Signals Directorate. Obtenido de Australian Government Department of Defense.

AVAST. (11 de 04 de 2014). Obtenido de Avast: https://www.avast.com/es-es/c-zero-day

CIS. (2017). *CIS Controls - Implementation Guide for Small and Medium Sized Enterprises [WhitePaper].* NY: CIS.

CISSecurity.org. (14 de 07 de 2018). *Ransomware: Facts, Threats, and Countermeasures*. Obtenido de https://www.cisecurity.org/ransomware-facts-threats-and-countermeasures/

CloudFlare. (14 de 07 de 2018). Obtenido de How to DDoS | DoS and DDoS attack tools: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/

Dennis, M. A. (03 de 08 de 2018). *Encyclopedia Britannica*. Obtenido de Cybercrime: https://www.britannica.com/topic/cybercrime

EnigmaSoftware. (14 de 07 de 2018). Obtenido de THE FIGHT AGAINST DIGITAL EXTORTION: https://www.enigmasoftware.com/fight-ransomware/

Filkins, B. (2016). *Reducing Attack Surface: SANS Second Survey on Continuous Monitoring Programs [WhitePaper].* SANS Institute.

Fruhlinger, J. (01 de 08 de 2017). Obtenido de The 5 biggest ransomware attacks of the last 5 years: https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html

Interpol. (04 de 08 de 2018). Obtenido de Cybercrime: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

ISACA. (2017). *NIST CyberSecurity Framework Using COBIT 5 [White Paper].* IL: ISACA.

ISACA. (2017). *Resources and Threats*. Obtenido de State of Cyber Security 2017: https://cybersecurity.isaca.org/static-assets/documents/State-of-Cybersecurity-part-2-infographic_res_eng_0517.pdf

Jara, E. (11 de 04 de 2018). *¿Cuánto dinero podría perder su empresa por un ciberataque?* Obtenido de WIDEFENSE: https://www.widefense.com/noticias/

López García, J. C. (2014). Obtenido de Eduteka: http://www.eduteka.org/articulos/TaxonomiaBloomCuadro

Myers, L. (25 de 02 de 2015). Obtenido de ESET: https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/

Pescatore, J. (2017). *Back to Basics: Focus on the First Six CIS Critical Security Controls.* SANS Institute & Tripwired.

Rai, S. (2014). *CYBERSECURITY - What the Board of Directors needs to ask? [White Paper].* Florida: The Institute of Internal Auditors Research Foundation.

Recent Zero-Day Exploits. (14 de 07 de 2018). Obtenido de FireEye: https://www.fireeye.com/current-threats/recent-zero-day-attacks.html

Roush, J. (02 de 05 de 2017). Obtenido de BMC: http://www.bmc.com/blogs/what-is-it-infrastructure-and-what-are-its-components/

Rubens, P. (26 de 06 de 2018). *How to Stop DDoS Attacks: 6 Tips for Fighting DDoS Attacks*. Obtenido de eSecurity Planet: https://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html

Torregrosa, J. M. (30 de 03 de 2018). Obtenido de IBM: https://www.ibm.com/blogs/think/es-es/2015/02/24/cuidado-con-las-apts/

TripWired. (2015). *Responding to High Impact Vulnerabilites: Are You Prepared? [WhitePaper].* TripWired Inc.

ANEXOS

1. Módulo Estadístico

A manera de ilustración, ejecutamos el modelo propuesto y lo aplicamos en una empresa, para reunir en los siguientes cuadros los resultados, con el fin de mostrar los posibles gráficos estadísticos que llevaría un reporte gerencial.

Cabe destacar que asignamos un puntaje a cada uno de los parámetros que miden el nivel de implementación de cada control:

- (I) Implementado **= 10 puntos**
- (NN) No es necesario o No Aplica **= 10 puntos**
- (N) No se ha implementado aún **= 0 puntos**
- (P) Parcialmente implementado **= 5 puntos**

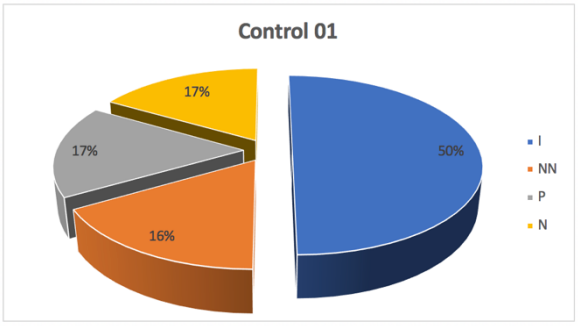
	Control	Evaluación	Puntaje
Fase #1	SF.C01.1	I	10
	SF.C01.2	I	10
	SF.C01.3	I	10
	SF.C01.4	NN	10
	SF.C01.5	P	5
	SF.C01.6	N	0
	SF.C02.1	I	10
	SF.C02.2	I	10
	SF.C02.3	I	10
	SF.C02.4	I	10
Fase #2	SF.C03.1	NN	10
	SF.C03.2	P	5
	SF.C03.3	P	5
	SF.C03.4	N	0
	SF.C03.5	P	5
	SF.C03.6	P	5
	SF.C03.7	P	5
Autenticación	SF.C03.SA01.A.1	I	10
	SF.C03.SA01.A.2	I	10
	SF.C03.SA01.A.3	I	10
Control de Accesos	SF.C03.SA01.B.1	NN	10
	SF.C03.SA01.B.2	P	5
	SF.C03.SA01.B.3	N	0
	SF.C03.SA01.B.4	I	10
	SF.C03.SA01.B.5	I	10
	SF.C03.SA01.B.6	I	10
	SF.C03.SA01.B.7	I	10
	SF.C03.SA01.B.8	NN	10
	SF.C03.SA01.B.9	P	5
	SF.C03.SA01.B.10	P	5
	SF.C03.SA01.B.11	N	0

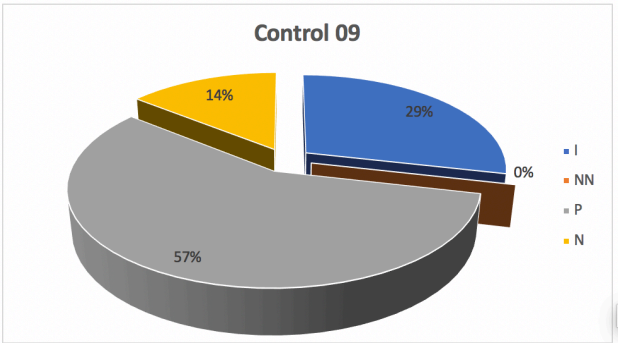
En el siguiente cuadro, podemos ver cuántas veces se obtuvo cada parámetro de evaluación en cada control y por fase, además del total de puntos acumulados de acuerdo a cada parámetro. No puede faltar al final, el porcentaje de cumplimiento en cada fase, según el porcentaje meta de esta.

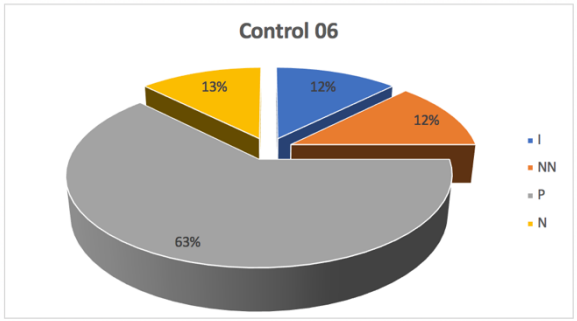
Fase	Control	I	NN	P	N	TOTAL	VALOR	Cumplimiento %	Meta x Fase
Fase#1: Conoce Tu Ambiente	C01	3	1	1	1	**6**	45	**17%**	20%
	C02	4	0	0	0	**4**	40		
Fase#2: Definir Lineamientos Base de Configuración Segura	C03	27	8	24	8	**67**	470	**42%**	60%
	C06	1	1	5	1	**8**	45		
	C07	3	1	1	1	**6**	45		
	C09	2	0	4	1	**7**	40		
	C10	5	2	1	1	**9**	75		
	C11	20	5	18	6	**49**	340		
Fase#3: Seguimiento y Control	C04	1	1	5	1	**8**	45	**15%**	20%
	C05	6	1	1	1	**9**	75		
	C08	4	1	1	0	**6**	55		

A partir de este cuadro principal de resultados se puede graficar lo siguiente:

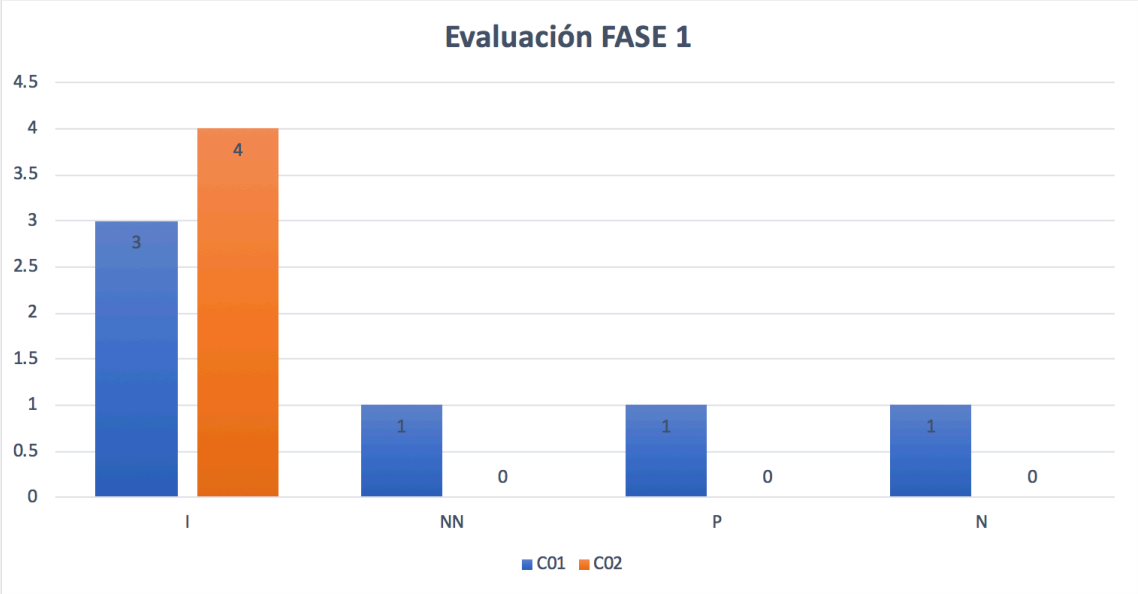
- Porcentajes de implementación y demás parámetros de evaluación por cada control.

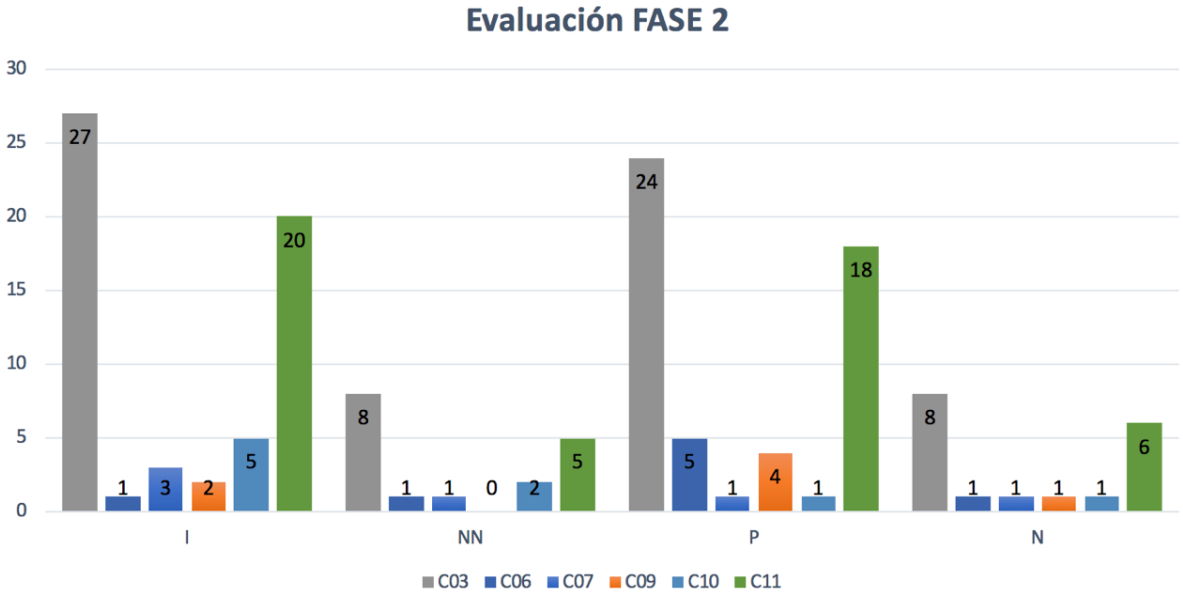






- Porcentajes de implementación y demás parámetros de evaluación de cada control por cada fase.





- Gráfico Macro: Porcentajes de cumplimiento en cada fase del modelo y su posición con respecto al porcentaje meta.