INVESTIGACIÓN

# Metodología para la implantación de la suite de seguridad informática para la gestión de la ciberseguridad

## Methodology for the implementation of the computer security suite for the management of cybersecurity

Daniel Morales Blanco[1*]

Recibido: 03/2023 | Aceptado: 05/2023 | Publicado: 12/2023


## RESUMEN

En el presente trabajo se realiza una metodología como solución para la implantación de la Suite de Seguridad Informática para la gestión de ciberseguridad, la Suite de Seguridad Informática (SSI), permite dar una respuesta integral a la seguridad informática, creando capacidades para detectar y gestionar eventos e incidentes y fortaleciendo la resiliencia. Lo que contribuye a la reducción de riesgos y vulnerabilidades. La SSI, en su arquitectura está integrada por dos componentes tecnológicos: la Plataforma de Monitoreo y el Sistema de Diagnóstico y Supervisión, y responde al marco legal vigente de Seguridad Informática, lo cual facilita la generación de reportes para la gestión de ciberseguridad. Donde se analizan las funcionalidades y herramientas que las componen. El proceso de implantación de la Suite de Seguridad Informática es un proceso complejo debido a que se involucran diversos sistemas que convergen, los amplios conocimientos que se requieren y la participación directa de los usuarios finales. Siendo este la base para que todo el sistema se implante de forma correcta y entendible. La metodología desarrollada permitió facilitar el proceso


1* Empresa de Aplicaciones Informáticas Desoft, División Territorial, La Habana, Cuba. daniel.morales@desoft.cu

de implantación y utilización de la SSI para la gestión de la ciberseguridad. Como aporte una metodología para la implantación y utilización de la SSI elaborada por Desoft consta con los procedimientos para la implantación por los especialistas, los manuales de utilización por los clientes y la descripción de las opciones y funciones de la SSI.

**Palabras clave:** Ciberseguridad; gestión; metodología; seguridad informática

## ABSTRACT

*In the present work a methodology is carried out as a solution for the implementation of the Computer Security Suite for cybersecurity management, the Computer Security Suite (SSI), allows a comprehensive response to computer security, creating to detect and manage events and incidents and strengthening resilience. This contributes to the reduction of risks and vulnerabilities. The SSI in its architecture is integrated by two technological components: the Monitoring Platform and the Diagnosis and Supervision System and responds to the current legal framework of Information Security, which facilitates the generation of reports for cybersecurity management. Where the functionalities and tools that compose them are analyzed. The implementation process of the Information Security Suite is a complex process due to the fact that various converging systems are involved, the extensive knowledge required and the direct participation of end users. This being the basis for the entire system to be implemented correctly and understandably. The methodology developed made it possible to facilitate the process of installing and using the SSI for cybersecurity management. As a contribution to a methodology for the implementation and use of the SSI prepared by Desoft, it consists of the procedures for the implementation by specialists, the user manuals for clients and the description of the options and functions of the SSI.*

**Keywords:** *Cybersecurity; management; methodology; computer security*

## Introducción

En la actualidad las Tecnologías de la Información y las Comunicaciones (TIC), han estado en constante perfeccionamiento desde su surgimiento. El uso creciente ha constituido un alto beneficio para la

sociedad, pero estos vienen asociados con grandes problemas de seguridad, los cuales se agravan, si no se gestiona de manera eficiente la ciberseguridad.

La Ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio. En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes y el fortalecimiento de la resiliencia (Consejo_de_Ministros, 2019).

El Decreto-Ley No. 370, "Sobre la Informatización de la Sociedad en Cuba" dispone las regulaciones generales aplicables a las Tecnologías de la Información y las Comunicaciones (TIC) y recoge los principios a seguir y las acciones y medidas para la determinación, desarrollo y mejoramiento de las condiciones de fiabilidad, estabilidad y seguridad de las TIC que respalden la informatización de la sociedad y la soberanía de la nación, la investigación, el desarrollo, la asimilación tecnológica y los soportes de soluciones para su seguridad de forma sostenible; acciones que requieren ser implementadas mediante las normas complementarias que resulten necesarias (Consejo_de_Ministros, 2018).

El Decreto-Ley No. 360, "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional" establece el marco legal que ordene el empleo seguro de las Tecnologías de la Información y la Comunicación, en lo adelante TIC, para la informatización de la sociedad, la defensa del Ciberespacio Nacional (Consejo_de_Ministros, 2019).

La metodología para la Gestión de la Seguridad Informática (SGSI) descrita en la Resolución 129/2019 promueve la adopción de un enfoque basado en procesos, con el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI de una organización; para ello adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI en correspondencia con la NC-ISO-IEC 27001"Requisitos de los Sistema de Gestión de la Seguridad de la Información" y adecuada

a la NC-ISO-IEC 17799 (27002) “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”(Ministerio_de_Comunicaciones, 2019).

El número de ciberataques está creciendo, aunque también es verdad que las empresas están dando pasos en la mejora de su gestión de la ciberseguridad, por lo que también están siendo capaces de detectar y contener un mayor número de ataques. Hay diferentes razones que explican este incremento, como son las vulnerabilidades de los sistemas y la incertidumbre socio económica. Aunque, sin duda, una realidad a tener muy en cuenta es que las empresas están en pleno proceso de digitalización y su espacio de ataque está creciendo. Por lo tanto, deben ser conscientes de que todo proceso de digitalización conlleva la implementación de medidas de ciberseguridad.

La ciberseguridad empresarial como es la capacidad organizacional definida para defender y anticipar las amenazas digitales propias del ecosistema donde la organización opera, con el fin de proteger y asegurar la resiliencia de las operaciones y la reputación de la empresa (Cano, 2021), se convierte en la nueva frontera de las corporaciones modernas, que demanda ir más allá de las prácticas conocidas en seguridad y control, para conectar con la dinámica de los riesgos cibernéticos, que no solamente reconocen los tradicionales activos claves como los datos, la infraestructura, las aplicaciones, los procesos y las personas, sino los terceros de confianza (cadena de suministro) y los adversarios como fuente natural de su accionar y reconocimiento de patrones de amenaza latentes y emergentes (Cano, 2021).

La seguridad de la información para las empresas se ha convertido en una de las principales preocupaciones desde que comenzaron a usarse los softwares de gestión empresarial para organizar y gestionar datos.

Para ser considerado seguro, el sistema informático de una empresa debe ser íntegro y confidencial (accesible sólo para personas autorizadas), irrefutable (las acciones realizadas no se pueden negar) y tener buena disponibilidad (estable y disponible en el tiempo).

## Materiales y métodos

Para la realización del estudio se establecieron las siguientes preguntas de investigación:

¿Qué componentes, contenidos y procedimientos debe tener una metodológica para la implantación y utilización de la Suite de Seguridad Informática?

¿Qué resultados tendrá la implementación de la metodológica para facilitar el proceso de implantación y utilización de la Suite de Seguridad Informática para la gestión de la ciberseguridad?

## Métodos de investigación utilizados:

### Teóricos

Analítico-Sintético: permitió interpretar, procesar y analizar los antecedentes de la ciberseguridad, para conformar el marco teórico que sustenta la propuesta de la investigación.

Histórico - Lógico: utilizado para el estudio de los antecedentes de los sistemas de gestión de la ciberseguridad en el mundo y particularmente en Cuba. De igual modo se utilizó en el estudio de los referentes teóricos relacionados con la gestión de la seguridad informática.

Método Sistémico Estructural Funcional: utilizado para expresar la lógica o sucesión de procedimientos seguidos en la elaboración de la metodología para la implantación y utilización de la Suite de Seguridad Informática para la gestión de la ciberseguridad.

### Empíricos

Observación descriptiva: se utilizó para analizar los procesos desde un marco exterior, o sea, sin profundizar en el problema, permite percibir lo que acontece realmente en el ámbito en que se encuentra enmarcada la investigación.

Análisis documental: permitió el estudio de diferentes documentos relacionados con las guías y manuales para caracterizar el proceso de implantación y utilización por parte de los especialistas y clientes.

Consulta a expertos: para la obtención de criterios especializados acerca de la propuesta y de su validación a través de la técnica Iadov.

Encuestas y entrevistas para conocer las causas que generan el problema y la valoración de la metodología propuesta.

## Aporte

Una metodología para la implantación y utilización de Suite de Seguridad Informática (SSI) elaborada por Desoft con los procedimientos para la implantación por los especialistas, manual de utilización por los clientes y la descripción de las opciones y funciones de la suite.

## Resultados y discusión

Existen una variedad de herramientas de seguridad, tales como: herramientas de monitoreo de tráfico de red, scanner de vulnerabilidades, detectores de anomalías, *Intrusion Detection System and Intrusion Prevention System* (IDS/IPS, por sus siglas en inglés), Información de seguridad y gestión de eventos (SIEM), cortafuegos, antivirus, inventarios de equipos, entre otros, que ayudan a minimizar los problemas de seguridad. Para la gestión de la ciberseguridad se integran varias de estas herramientas de seguridad, con el fin de recoger, ordenar y correlacionar la información sobre el estado de la red, los comportamientos de sistemas y usuarios, y la información del estado de las máquinas.  La información que se registra, sirve a los administradores de seguridad, para encontrar indicios de ataques que hayan ocurrido o que puedan suceder en un futuro. La implantación de esta tecnología involucra un conocimiento claro de la infraestructura que se maneje, el flujo de datos, servicios que presta, funcionamiento de las herramientas, determinación de una arquitectura de monitoreo, y la evaluación de funcionalidad y rendimiento.

La Suite de Seguridad Informática (SSI), ofrece un enfoque sistémico para la gestión de la ciberseguridad, la cual está destinada a todas las entidades del país con el objetivo de gestionar la ciberseguridad. La Suite de Seguridad Informática no escapa de necesitar una buena solución para su implantación, además de darle posteriormente un adecuado soporte que garantice su continua calidad y funcionamiento.

El proceso de implantación de la SSI es un proceso complejo debido a que se involucran diversos sistemas que convergen, los amplios conocimientos que se requieren y la participación directa de los usuarios finales. Siendo este la base para que todo el sistema se implante de forma correcta y entendible.

La incorporación de la SSI para la gestión de la ciberseguridad, debe ser un proceso bien planificado y coordinado, debido a que se debe analizar con profundidad la adaptabilidad del sistema a las características de la entidad, acorde a los procedimientos y normativas vigente en el marco legal, además de estudiar la preparación de la entidad para el proceso de gestión de la ciberseguridad. Por otra parte, sin una solución para implantar y dar soporte al software, se pondría en riesgo el completo éxito del sistema.

Cada estrategia de implantación tiene sus méritos de acuerdo con la situación que se considere dentro de la empresa. Sin importar cuál sea la estrategia utilizada, los encargados de implantar el sistema procuran que el uso del sistema se encuentre libre de problemas. Cuando el proceso de implantación no se realiza con todo el éxito que requiere, las consecuencias llegan a hacer fatales. Un ejemplo de esto lo constituyen, la mala preparación que pueden tener los encargados de implantar la SSI, como los conocimientos de los usuarios, y que no documentan los incidentes y buenas prácticas como manera habitual, si esto ocurre, entonces no se puede implantar y explotar de forma exitosa el sistema, lo cual provoca un mal funcionamiento del mismo y a la vez un descontento para el cliente. Por otra parte, si no se les brinda una correcta ayuda a los usuarios sobre cómo se debe trabajar con el sistema obtenido, se les hace muy difícil interactuar con el sistema y explotar al máximo todas sus funcionalidades.

La gestión de los proyectos ejecutados, ha requerido la necesidad de la creación de una Metodología que rija como debe ser realizado el proceso de implantación que documente las mejores prácticas y guíe a los implantadores y especialistas responsables.

La Suite de Seguridad Informática (SSI) es una aplicación que garantiza la seguridad de la información en el contexto de un Sistema Informático especifico, gestionando las vulnerabilidades de los componentes que integran dicho sistema: infraestructura, sistemas operativos, aplicaciones, servicios telemáticos y personal.

Su arquitectura está compuesta por 2 componentes tecnológicos: Sistema de Control y Supervisión (Thor) y Plataforma de Monitoreo (Syn).

**Sistema de Control y Supervisión**

Radica en la sede central de la entidad y permite gestionar las vulnerabilidades existentes en todos los componentes y partes que integran el Sistema Informático mediante su identificación en Variables de Seguridad. Está integrado por los componentes: Módulo de Set Point [MSP], Módulo de Diagnóstico [MD], Módulo de Control [MC], Módulo de Supervisión [MS].

**Plataforma de Monitoreo**

Radica en cuántas redes locales se decidan gestionar. A esta plataforma se conectan los sensores (herramientas de seguridad definidas en la resolución 126/2019 de MINCOM) son los encargados de monitorear el estado real de las Variables de Seguridad. El Sistema de Control y Supervisión está integrado por el componente de normalización [CN] y el componente de transmisión [CT].

La Suite de Seguridad Informática es una solución basada en Software Libre y desarrollada para un entorno multicompañía, con tecnología Odoo.

La Suite de Seguridad Informática integra los procesos de automatización de Chequeos, Monitoreo del Sistema Informático e Informatización del Proceso de Ciberseguridad.

**Sus funcionalidades:**

Gestión Documental para los componentes del Sistema Informático:

Definición de Usuario (Altas y Bajas)

Definición de Perfiles de Usuario (Agrupación de Usuarios por características comunes)

Definición de Locales

Definición de Terminales (Ficha Técnica del Equipo)

Asignación de Terminales (Asignar Responsables de un Equipo)

Movimiento de Terminales

Definición de Catalogo de Software

Definición de Lista de Software Autorizado

Definición de Perfil de Software (Solicita de Software de la Entidad)

Definición de Servidores

Definición de Servicios

Definición de Accesos a Sistemas

Definición de Datos

Definición de Perfiles de Servicios (Consumo de Servicios)

Registro de Incidencias

Registro de Auditorias

Definición del Plan de Mantenimiento y Reparaciones

Definición de Documentos Legales Requeridos (Ambiente de Control)

Reportes Estadísticos e Informativos del Sistema Informático

**Representación de Sistemas Informáticos:**

Tablero de Indicadores (Conteo de Objetos)

Visualización de Componentes del Sistema Informático por Tipo

Tableros de Monitoreo

**Controles Automáticos:**

Detección y Captura de Hardware

Detección y Captura de Software

Detección y Captura de Host en la red

Detección y Captura de Puertos Abiertos

Detección y Captura de Vulnerabilidades en Puertos Abiertos

**Diagnóstico:**

Pérdida de Componentes Internos en Hardware

Terminales no Controlados

Software No Autorizado

Host No Autorizado

Puerto Abierto No Autorizado

Vulnerabilidades de Puertos Abiertos

**Monitoreo:**

Uso del Canal de Navegación

Métricas de Servidores

Disponibilidad de Servicios

Vulnerabilidades de Puertos

Disponibilidad de Agentes (Agentes de Monitoreo)

**Para el funcionamiento de la suite de seguridad informática, es necesario contar con las siguientes herramientas:**

Docker

Odoo

Módulo de Odoo (l10n_cu_ssi)

Módulo de Odoo (l10n_cu_ssi_asset)

Postgresql

Python

Celery

Pip

RabbitQM

Nmap

Traefik

OCSInventory

ElasticSearch

Grafana

Filebeat

Heartbeat

Metricbeat La suite de seguridad informática responde al marco legal vigente de Seguridad Informática, lo cual facilita la generación de reportes para la gestión de ciberseguridad. Uno de los principales que brinda es el reporte de cumplimiento de la normativa, que es capaz de simular una auditoría automática de los eventos de seguridad activos, ayudando a las entidades en la toma de decisiones.

## Conclusiones

La metodología para la Gestión de la Seguridad Informática (SGSI) promueve la adopción de un enfoque basado en procesos, con el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar la ciberseguridad. En función de ello, en el presente trabajo se definió la metodología para la implantación de la Suite de Seguridad Informática para la gestión de la ciberseguridad, definiéndose como debe ser realizado el proceso de implementación que documente las mejores prácticas y guíe a los implementadores y especialistas responsables.

## Referencias

Bojorquez Huanca, J. S. (2022). Ciberseguridad.

Cano, J. (2021). Ciberseguridad empresarial. Reflexiones y retos para los ejecutivos del siglo XXI. Bogotá, Colombia: Lemoine Editores.

Carrillo, J. J. M., Zambrano, N. A., Zambrano, T. J. L., & Bravo, M. Z.

(2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. Revista Ibérica de Sistemas e Tecnologias de Informação(E29), 41-50.

Consejo_de_Ministros. (2018). Decreto No. 370 SOBRE LA INFORMATIZACION DE LA SOCIEDAD EN CUBA.

Consejo_de_Ministros. (2019). Decreto No. 360 SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LA DEFENSA DEL CIBERESPACIO NACIONAL.

Díaz, R. M. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe.

Hernández, W. C. C., Payés, M. A. L., & Acosta, J. I. Y. Guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto.

Hidalgo Pereda, L. A. (2019). Revisión de metodologías para evaluación y selección de un ERP.

Ministerio_de_Comunicaciones. (2019). Resolución 129 Metodología para la Gestión de la Seguridad Informática.

Ranchal Tomás, E. Estudio e implantación de un sistema ERP en una empresa.