Diseño de una arquitectura de seguridad basada en la metodología SABSA para el Ejército Nacional

Luis Wilmar Cárdenas Moreno

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD BASADA EN LA METODOLOGÍA SABSA PARA EL EJÉRCITO NACIONAL

ALUMNO: LUIS WILMAR CÁRDENAS MORENO

MAESTRÍA DE CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

Bogotá – Colombia

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD BASADA EN LA METODOLOGÍA SABSA PARA EL EJÉRCITO NACIONAL

ALUMNO: LUIS WILMAR CÁRDENAS MORENO

DIRECTOR: MSc. Carlos Arturo Martínez Forero

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2020

Aceptación del Trabajo

Nota de Aceptación:

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Agradecimientos

En primer lugar, agradezco a Dios por darme la gracia de culminar otra etapa de mi vida tanto personal como profesional. A mi familia por su apoyo y acompañamiento en todo mi proceso de formación.

A la Escuela Superior de Guerra por permitirme participar en este proceso pedagógico y los docentes quienes me brindaron las herramientas necesarias en la formación como Magíster en Ciberseguridad y Ciberdefensa, en especial al señor MSc. Carlos Arturo Martínez Forero como tutor del presente trabajo por sus valiosos aportes.

Finalmente, a mis compañeros por transmitirme sus conocimientos y experiencias y a todas las personas que de una u otra forma colaboraron en la realización del presente proyecto.

Contenido

Índice de Ilustraciones

Índice de tablas

Lista de Abreviaturas

BIA: Business Impact Analysis. Análisis de Impacto de Negocios.

ADM: Architecture Development Method. Método de Desarrollo de la Arquitectura

TI: Tecnología de la Información

SGSI: Sistema de Gestión de la Seguridad de la Información

TIC: Tecnologías de la Información y la Comunicación

CERT: Computer Emergency Response Team. Equipo de Respuesta para Emergencias Informáticas

ACL: Access Control List. Lista de Control de Acceso

SOC: Security Operations Center. Centro de Operaciones de Seguridad

CSIRT: Computer Security Incident Response Team. Equipo de Respuesta a Incidentes

API: Application Programming Interface. Interfaz de Programación de Aplicaciones

DNS: Domain Name Server. Servidor de nombres de dominio.

ICMP: Internet Control Message Protocol. Protocolo de Control de Mensajes de Internet

SNMP: Simple Network Management Protocol. Protocolo Simple Administración de Red

RAID: Redundant Array of Independent Disks. Matriz Redundante de Discos Independientes

VPN: Virtual Private Network. Red Privada Virtual

IP: Internet Protocol. Protocolo de Internet

IPsec: Internet Protocol Security. Seguridad del Protocolo de Internet

GUI: Graphical User Interface. Interfaz Gráfica de Usuario

SSL: Secure Sockets Layer. Capa de Puertos Seguros

CA: Certification Authority. Autoridad de Certificación

RA: Registration Authority. Autoridad de Registro

MLS: Multiple Level of Security. Seguridad Multinivel

VAR: Value at Risk. Valor en riesgo

FTP: File Transfer Protocol. Protocolo de Transferencia de Archivos

IRC: Internet Relay Chat.

BCM: Business Continuity Management. Administración de la Continuidad del Negocio

1. Resumen

Este documento introduce conceptos que permitirán estructurar un proyecto a partir de investigaciones y experiencias que servirán de base para desarrollar una estrategia más sólida a la hora de presentar nuevas soluciones para cubrir las brechas y riesgos de seguridad que existen actualmente en la institución Ejército Nacional.

Para este proyecto de grado en particular se buscará la documentación y definición de una arquitectura de seguridad, teniendo como referente las diferentes metodologías que sirven de apoyo para poder estructurar este tipo de arquitecturas. De esta manera, se pretende dar una visión de la arquitectura de seguridad deseada y conveniente para la institución, generando los mecanismos necesarios para una futura implementación de tal manera que se pueda dar respuesta oportuna y eficiente a los diferentes ciberataques, con base en las necesidades de ciberseguridad para así proteger la información digital de la institución.

Es por lo anterior, que se presenta la propuesta del diseño de una arquitectura de seguridad de la información SABSA, donde se dará a conocer esta metodología de manera específica definiendo un esquema de acción estratégico, mediante el cual se establecen las directrices en materia de ciberseguridad para la institución.

Así mismo, aborda un conjunto de lineamientos que ayudará a los profesionales de seguridad a ser capaces de adaptarse a los nuevos desafíos cibernéticos y estar preparados para hacer frente a cada uno de los retos que puedan presentarse en el futuro.

2. Abstract

This document introduces concepts that will allow it structuring a project based on research and experiences that will serve as the basis for developing a more solid strategy at the moment to present new solutions to cover the gaps and security risks that currently exist in the Army institution.

For this degree project, the documentation and definition of a security architecture will be sought, taking as a reference the different methodologies that serve as support to be able to structure this type of architecture. In this way, it is intended to give a vision of the desired and convenient security architecture for the institution, generating the necessary mechanisms for a future implementation in an efficient and timely way that can be given response to the different cyberattacks, this based on the cybersecurity needs in order to protect the institution's digital information.

For this reason the design of a SABSA information security architecture is presented, where this methodology will be made known in a specific way, defining a strategic action scheme through the guidelines on cybersecurity to be established for the institution.

Likewise, it addresses a set of guidelines that will help to the security professionals to be able to adapt it to the new cyber challenges and be prepared to face each one in the future.

3. Palabras clave

Arquitectura de Seguridad - Ciberseguridad - Ciberdelincuentes - Ciberataque, Vulnerabilidades - Ciberamenazas - Tecnología - Modelos - Estándares - Riesgos – Información - Organización - Institución - Comunicaciones - Fraude.

4. Keywords

Security Architecture - Cybersecurity - Cybercriminals - Cyberattack, Vulnerabilities - Cyberthreats - Technology - Models - Standards - Risks - Information - Organization - Institution - Communications - Fraud.

5. Introducción

El gobierno Colombiano en cabeza del Ministerio de Tecnologías de la Información y las Comunicaciones, está en busca de mejores prácticas en materia de ciberseguridad y ciberdefensa, por ello ha hecho la gestión necesaria para que el país se adhiera al convenio sobre la ciberdelincuencia, conocido como el primer tratado internacional en la materia y el cual se enfoca principalmente en dos frentes: fortalecer el marco nacional que regule la ciberdelincuencia y la cooperación internacional, convirtiéndose en un compromiso del país tanto a nivel nacional como internacional. (Consejo de Europa, 2001).

Con la intención de seguir los protocolos internacionales, Colombia ha generado "unos lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país". (Departamento Nacional de Planeación, 2011).

> La problemática central se fundamenta en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas, presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. (Departamento Nacional de Planeación, 2011).

El Ejército Nacional como entidad gubernamental encargada de la defensa nacional, conocida como infraestructura crítica, ha sido blanco de ataques cibernéticos en repetidas ocasiones, lo cual ha generado traumatismos en los procesos desarrollados por la institución, amenazando la estabilidad, seguridad y soberanía del país. Es por esto que la identificación temprana de ataques cibernéticos, juega un papel importante en la protección de la información. Poder identificar la intrusión en el momento que se produce y prevenir la ocurrencia de ataques, son valores agregados que aportaría al logro de los objetivos

estratégicos de la organización, mejorando su competitividad y apoyando en términos generales la continuidad del negocio. Así mismo, se evitará la ocurrencia de ciberataques a la Fuerza.

Actualmente el Ejército Nacional, no cuenta con un alineamiento estratégico entre sus procesos de negocio y la protección de la información digital que vive en los sistemas interconectados de la institución. Es por ello, que sus procesos más importantes en la mayoría de los casos, se realizan sin tener en cuenta los riesgos que pueden acarrear al no tener las medidas de seguridad necesarias para evitar posibles ciberataques.

Teniendo como referencia la norma ISO 27001, el recurso más importante para cualquier organización son los sistemas de información, los cuales comprenden los conocimientos y los datos. Es por ello, que la adopción de un sistema de gestión de seguridad de la información, debería ser una decisión estratégica de la organización. Donde la implementación de la misma sea acorde a las necesidades de la institución en seguridad, tamaño, empleados y estructura, entre otros. (Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, 2006).

Por lo anterior, el Ejército Nacional debe tener la capacidad desde todos los ámbitos, de reducir los riesgos asociados a la información digital, tomando en consideración que cuenta con una infraestructura tecnológica capaz de almacenar, tratar y modificar la información que da respaldo a su operación hasta un nivel que sea aceptable para los interesados, mitigando amenazas latentes y protegiendo todas aquellas actividades encaminadas a resguardar la información de algún tipo de riesgo tanto interno como externo, con el propósito de evaluar que los resultados cumplan los requisitos y expectativas. (Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, 2006).

Aunado a lo anterior, el aumento de las redes de cómputo de la Fuerza y de las organizaciones alrededor de esta, el crecimiento de aplicaciones que funcionan

permanentemente en línea y el incremento acelerado de ciberdelincuentes, amplían las probabilidades de que se produzca un número mayor de ataques cibernéticos imperceptibles para los profesionales de seguridad. Así mismo, el no alineamiento entre la misión, la visión, los procesos, los datos que soportan esos procesos y la ciberseguridad del Ejército Nacional, conlleva a concluir que se debe tener en cuenta un modelo que permita integrarlos de manera tal que se puedan dar mejores soluciones a la institución, protegiéndola de riesgos y amenazas cibernéticas.

En razón a lo anteriormente expuesto y teniendo en cuenta la creciente dependencia del ciberespacio y los riesgos asociados a este, donde los ciberataques están siendo cada vez más utilizados como armas digitales, los cuales son más difíciles de detectar, se hace indispensable la implementación de métodos de ciberseguridad y ciberdefensa.

Así las cosas, la entidad tiene la necesidad de contar con una metodología integral y organizada para el cumplimiento de los objetivos en términos de aseguramiento de la información, siguiendo y ejecutando los lineamientos, políticas de defensa y protección electrónica para desarrollar una estrategia que contrarreste el incremento de las ciberamenazas que pueden afectar directamente la misión de la Fuerza, logrando implementar el desarrollo tecnológico, electrónico e informático para prever el comando y control, mediante el uso de tecnología moderna y segura en todas sus actividades. (Ejército Nacional de Colombia, 2016).

En la búsqueda de reducir los riesgos por fuga de información se debe identificar aquella información generada y manejada al interior de la organización que es considerada confidencial para la misma, teniendo en cuenta cuál sería el impacto en caso de que dicha información terminara en manos de cibercriminales que pudiesen obtener algún tipo de beneficio con ella, se aborda un esquema de metodologías que ayudan a detectar los diferentes riesgos y posteriormente entrar a mitigarlos o eliminarlos. Esto consiste en realizar un análisis que al ser aplicado a la institución, cubre sus necesidades particulares y contempla buenas prácticas de seguridad de la información. Lo anterior, con el fin de tomar

las medidas necesarias para mantener la confidencialidad, disponibilidad e integridad y de esa forma garantizar que los procesos internos no se vean amenazados en caso de posibles ciberamenazas.

Dentro de este contexto, se debe permitir la integración de la ciberseguridad con las tecnologías de la información, los usuarios y los procesos de negocio donde se reconoce la información digital como el activo principal de la institución.

6. Objetivos

6.1. Objetivo general

Diseñar una arquitectura de seguridad basada en una metodología capaz de integrar los procesos para estar a la vanguardia de la seguridad digital para el Ejército Nacional.

6.2. Objetivos específicos

- Realizar una valoración detallada de la metodología seleccionada para la propuesta de la arquitectura de seguridad, articulándola a las necesidades del Ejército Nacional.

- Analizar la arquitectura de seguridad actual del Ejército Nacional.

- Definir los planes a seguir para llegar a la arquitectura de seguridad objetivo y las herramientas de seguridad necesarias propuestas para esta.

7. Metodología

El presente proyecto de investigación "Diseño de una arquitectura de seguridad basada en la metodología SABSA para el Ejército Nacional" se realiza bajo una metodología descriptiva cualitativa, al hacer un análisis de las diferentes clases de arquitecturas de seguridad y exponer las razones por las cuales se elige una de estas. Donde se emplearán conocimientos asociados a la seguridad de la información, la ciberseguridad y la ciberdefensa desarrollados en clase, en el ámbito laboral y en la investigación realizada a las fuentes literarias a las que se hace referencia. De acuerdo a Meyer (2006), "Los investigadores recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento". (Deobold B. Van Dalen y William J. Meyer., 2006).

De acuerdo a los objetivos específicos se desarrollarán los temas relacionados con el proyecto y la relevancia de los mismos para el cumplimiento del objetivo general y la resolución a la pregunta problema de esta investigación: ¿Cómo proteger la información digital del Ejército Nacional a través de la arquitectura de seguridad SABSA?, llevando a cabo un análisis y descripción de la teoría que se expone llamada arquitectura de seguridad SABSA.

Con la ejecución del objetivo específico número uno, se pretende hacer una valoración detallada de la metodología SABSA como arquitectura de seguridad, dando a conocer el paso a paso para realizarla y las bondades de esta para la institución a la cual se le pretende aplicar. Este modelo y metodología se utiliza para desarrollar el manejo de riesgo en una arquitectura de seguridad empresarial, teniendo como propósito la entrega de soluciones de infraestructura de seguridad que soporten las iniciativas críticas para la misión de la organización, donde la característica principal del modelo de SABSA consiste en que todo se deriva de un análisis de los requerimientos para seguridad del negocio. (John Sherwood, Andrew Clark, David Lynas, 2005).

Para el desarrollo del objetivo específico número dos, se pretende hacer un diagnóstico y análisis del nivel de gestión de seguridad de la información con el que cuenta actualmente el Ejército Nacional y el cual ha sido el punto de partida para la gestión y aseguramiento de la información al interior y exterior de la organización y los riesgos asociados a los que se pretende dar solución a través de la arquitectura de seguridad de SABSA.

El objetivo específico número tres, busca definir planes, estrategias, diseño y operación del modelo seleccionado, el cual permitirá evaluar, establecer políticas de seguridad, implementar herramientas y medidas de ciberseguridad que mitiguen en gran porcentaje las vulnerabilidades y riesgos protegiendo la información digital de los actuales y nuevos ataques cibernéticos dirigidos hacia la Fuerza.

Se hará una descripción detallada del modelo en sus etapas de aplicabilidad y se llegará a las conclusiones definitivas, las cuales darán a conocer las ventajas de que la institución tome esta arquitectura como parte de su estrategia no sólo para el aseguramiento de la información, sino también para el aseguramiento del cumplimiento de su misión a cabalidad.

Es importante mencionar que para la elaboración de este trabajo, se presentarán las cuatro fases de la metodología SABSA, sin embargo, para cumplir el objetivo propuesto del proyecto, se tendrán en cuenta de manera específica las dos primeras fases (Estrategia – Concepto y Diseño) y el desarrollo de las fases, (Implementación y Gestión - Medición) planteando la oportunidad para que se lleve a la práctica estas dos últimas.

8. Justificación

¿Por qué SABSA?

Muchas metodologías existen actualmente para desarrollar arquitecturas de seguridad en una organización, el desafío es adoptar e implementar aquella arquitectura que sea efectiva para las necesidades de la empresa a la que se va a aplicar.

Todas las metodologías tienen diferentes perfiles, cada una tiene su propio enfoque y fortalezas, por ello, es posible que ninguna metodología se adapte cien por ciento a los desafíos de seguridad que maneja una organización.

Por lo anterior, es importante hacer una selección adecuada del tipo de metodología que se quiere implementar en la institución, la cual logre acercarse lo más posible al estado óptimo de seguridad y permita cumplir con los objetivos trazados no solo en esta materia de seguridad sino en todos los procesos de la organización.

De acuerdo a la investigación realizada a lo largo de este proyecto, la arquitectura de seguridad SABSA, al estar orientada a la seguridad empresarial que tiene un enfoque holístico, es decir, que toma en consideración todos y cada uno de los procesos sin dejar ninguna actividad excluida de esta, no solo se enfoca en el "cómo" si no en el "qué" priorizando la razón por la cual la arquitectura de seguridad es necesaria para el éxito de la organización.

La razón de usar SABSA es que hace un mapeo directo de los objetivos del negocio con drivers de seguridad, cambiando la perspectiva de seguridad como un costo y convirtiéndola en un habilitador del negocio. Esta metodología, es la única que mapea los objetivos de negocio contra la seguridad y sus distintos componentes divididos en capas lógicas.

SABSA garantiza que las necesidades de la organización se integren por completo y que los servicios de seguridad se diseñen, entreguen y respalden de manera sistemática como parte integral de la empresa con la infraestructura tecnológica.

Por otro lado, la metodología de arquitectura de seguridad SABSA al dividirse en capas, es considerada como una arquitectura solida debido a su simplicidad y fácil comprensión, además, al ser una metodología de uso abierto y no un producto comercial podrá ser desarrollada por el equipo de seguridad e implementada al interior de la organización.

Así mismo, esta metodología permite el compromiso de todas las personas que hacen parte de la organización, pues la misma está directamente relacionada con el cumplimiento los objetivos institucionales y las partes interesadas, logrando una integración en todos los niveles jerárquicos de la misma.

SABSA al ser una metodología estándar aplicada en varias partes del mundo, ha evolucionado y también se ha incorporado como un marco y estándar de arquitectura gubernamental aplicada en sectores de defensa e inteligencia, es por esto que esta metodología se podrá adaptar a las necesidades de una institución como el Ejército Nacional.

9. Marco teórico y conceptual

9.1. Concepto de seguridad

La seguridad tiene que ver con la protección de los objetivos y los activos del negocio, significa proporcionar un conjunto de controles que se ajustan a las necesidades las cuales a su vez se derivan de una evaluación y análisis de riesgos. El objetivo en la evaluación de riesgos es priorizar los mismos para enfocarse en los que más requieren mitigación. (John Sherwood, Andrew Clark, David Lynas, 2005).

La seguridad debe considerarse como una actividad que permite reducir los riesgos a niveles aceptables y así permitir a la organización hacer uso de las nuevas tecnologías para una mayor ventaja en el cumplimiento de su misión.

9.2. Seguridad de la información

Al hablar de seguridad de la información se dice que dicha información tiene un valor específico en un contexto determinado y por tanto, hay que proteger.

Se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información.

Existen también diferentes definiciones del término seguridad de la información. De ellas nos quedamos con la entregada por el estándar ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC). "La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras

propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio." (International Organization for Standardization (ISO) , 2005).

La seguridad de la información, se compone de medidas tomadas para proteger una red del acceso no autorizado, interferencia accidental o intencionada con operaciones normales, o con la destrucción, inclusive la protección de facilidades físicas, del software, y de la seguridad del personal.

9.3. Concepto de ciberseguridad

De acuerdo al Conpes 3854 definen la ciberseguridad como: "El conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio". (Departamento Nacional de Planeación, 2016).

Otro concepto relevante es el presentado por ISACA (Information Systems Audit and Control Association) quienes definen ciberseguridad como la "protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". (ISACA Information Systems Audit and Control Association, 2015).

9.4. El significado de la arquitectura

Arquitectura hace referencia a diseñar; dependiendo del contexto, se pueden encontrar diseños de tipo eléctrico, electrónico, de red de datos, diseño de máquinas, diseño industrial, entre otros. El proceso de diseño permite la definición de un esquema en el cual se vislumbre la armonía entre cada uno de los componentes del mismo y la forma como

estos interactúan para proporcionar la funcionalidad dentro del sistema a construir (John Sherwood, Andrew Clark, David Lynas, 2005).

9.5. Arquitectura de seguridad.

El término latín de la palabra arquitectura, hace referencia a diseñar y construir. Para la norma ISO/IEC 27001 seguridad de la información se define como el "proceso de proteger la información contra una gama amplia de amenazas, busca asegurar la continuidad del negocio, disminuir los posibles daños y maximizar el retorno de inversión" (Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, 2006).

Si miramos las dos definiciones no tienen ninguna relación directa, pero para crear una arquitectura de seguridad de la información y teniendo en cuenta la creciente demanda de los términos, definiciones y procesos en este entorno, es indispensable darle forma a esta, de acuerdo a una estructura que facilite su correcta implementación, gestión y administración.

> La arquitectura de seguridad es el arte y la ciencia de diseñar y supervisar la implementación de sistemas de negocios, generalmente sistemas de información de negocios que están: libres de peligro, daños, libres de miedo, cuidado, en custodia segura, no es probable que falle, se puede confiar en ellos y a salvo de ataque. Un arquitecto de seguridad es una persona calificada para diseñar y supervisar la implementación de sistemas de negocios seguros. (John Sherwood, Andrew Clark, David Lynas, 2005).

Pero si nos preguntamos ¿cuál sería la mejor opción de poder trabajar de forma ordenada, con sentido de apoyo y proporcionando el normal funcionamiento de la organización?; de esta manera se debe pensar en un esquema o modelo que garantice la administración (entendida como el estudio de las organizaciones y la técnica empleada de la planificación, organización, dirección y control, con el fin de obtener el máximo

beneficio posible), donde existirá la integración y equilibrio de los esfuerzos que hace cada elemento en la materialización de la seguridad de la información para la misión de la organización; dicho modelo se conoce como arquitectura de seguridad de la información.

Así las cosas, se puede concluir que la arquitectura de seguridad de la información es la correlación de los elementos que permiten diseñar y construir un esquema que organice, administre y gestione los procesos de la organización bajo los fundamentos de las buenas prácticas de la seguridad de la información, alineados con las expectativas de la alta gerencia (Killmeyer, Jan, 2006).

La alineación de procesos de seguridad y expectativas del negocio se puede manifestar a través de la comunicación clara, concisa y concreta que se establece entre el encargado de la seguridad y la alta gerencia del negocio; esta comunicación es posible mediante dicha arquitectura de seguridad de la información la cual maneja tres tipos de lenguaje:

1. Estratégico: expresar de forma clara y precisa las expectativas del negocio, creando los lineamientos generales de la arquitectura de seguridad de la información.

2. Táctico: utilizar estándares y normas para que a través de estas se pueda llegar a construir la arquitectura de seguridad de la información.

3. Operacional: definición del comportamiento de los usuarios, alta gerencia, clientes, proveedores, entre otros; en la ejecución de sus funciones, detallando cómo se realizan los procesos definidos en la arquitectura de seguridad de la información.

Según Sherwood (2005) "la arquitectura de seguridad es una herramienta utilizada para describir el estado actual de una organización o empresa basada en los activos de información que posee, sistemas de información y de las personas que pertenecen a la empresa en general". Con el análisis realizado a la situación actual de seguridad de dicha empresa, se debe diseñar y documentar una arquitectura de seguridad objetivo, de manera

que se minimicen los riesgos y vulnerabilidades que presenta actualmente en sus activos, mediante la implementación de herramientas de seguridad que protejan la información.

Una organización puede asegurar su información y las personas que pertenecen a la misma minimizando el riesgo al que están expuestos a través de una arquitectura de seguridad, para ello es importante realizar un análisis minucioso del riesgo e identificar los activos de información y recursos indispensables y relevantes para la organización con el propósito de detectar toda clase de amenazas que se puedan dar, las cuales pueden ir desde interceptaciones de un recurso hasta interrupción del mismo, generando una denegación del servicio a los usuarios. (John Sherwood, Andrew Clark, David Lynas, 2005).

Inicialmente la arquitectura de seguridad fue propuesta por Gartner Inc. empresa especializada en el desarrollo de frameworks de trabajo para varios tipos de arquitecturas incluida la empresarial y de seguridad en su publicación incorporando seguridad en el proceso de arquitectura empresarial publicada en el año 2006. (Gregg Kreizman, Bruce Robertson, 2006).

Sin embargo, existen varios modelos o marcos de trabajo que indican metodologías para la definición e implementación de la arquitectura de seguridad las cuales serán abordadas a continuación de manera resumida para luego sumergirnos en el modelo SABSA, metodología seleccionada para el caso de estudio.

9.6. Arquitecturas, marcos de referencia y estándares de seguridad

Después de revisar los conceptos de forma general que incluyen los componentes de un estándar de arquitectura de seguridad, a continuación se presentaran algunas arquitecturas, marcos de referencia y estándares de seguridad que nos permiten contextualizar el tema presentado.

Arquitectura de seguridad según Jan Killmeyer

Este modelo describe los elementos que a consideración de Jan Killmeyer (2006) deben ser parte de una arquitectura de seguridad de la información, tal como se muestra en la Ilustración 1:

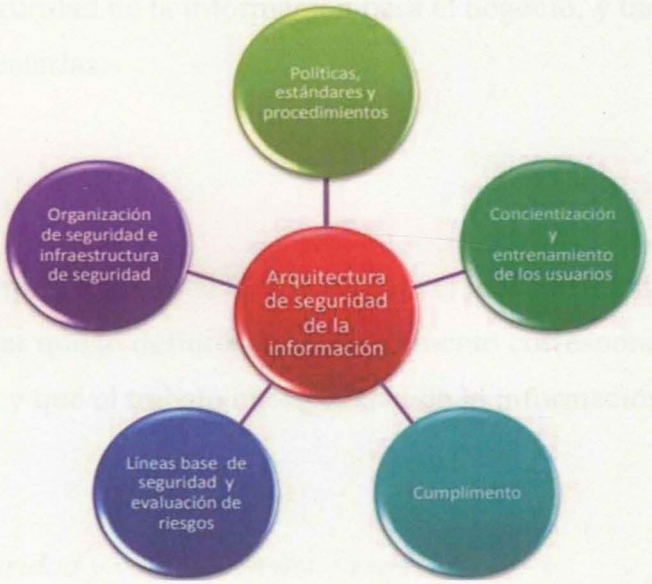

Ilustración 1 Componentes de la arquitectura de seguridad según Jan Killmeyer

Fuente: Recuperado de (Killmeyer, Jan, 2006)

Políticas, estándares y procedimientos:

- Política: definida en términos de los objetivos del negocio, los cuales son los que llevan el detalle para el comportamiento de los usuarios.
- Estándares: son las buenas prácticas en seguridad de la información.
- Procedimientos: especifican el paso a paso y la forma como se desarrollan las actividades por las personas encargadas de su ejecución.

Capacitación y entrenamiento de los usuarios:

Según el autor en mención, el objetivo fundamental del proceso de concienciación y sensibilización de los usuarios encargados de llevar el proceso de la gestión en seguridad de la información; es dar a conocer la importancia de las políticas, estándares, normas y buenas prácticas de seguridad de la información para el negocio, y también las graves consecuencias de no acatarlas.

Cumplimiento:

Para el autor, el cumplimiento es el elemento para el mecanismo de revisión que tiene como propósito verificar que lo definido en cada elemento corresponda a lo que la alta gerencia tenía previsto y que el trabajo en seguridad de la información este aportando a su ejecución.

Líneas base de seguridad y valoración del riesgo:

Debido a la gran demanda de esfuerzo en tiempo y dinero en pruebas de vulnerabilidad en los dispositivos, Jan Killmeyer (2006) recomienda la definición de los siguientes elementos:

- Las líneas base para la configuración de dispositivos.
- La educación a los administradores y usuarios en el uso de las políticas de seguridad.
- La evaluación de los controles, teniendo en cuenta que se debe tener realimentación continúa.

Organización de la seguridad e infraestructura:

Al hacer necesario la alineación de los procesos del negocio con la seguridad de la información, se propone la persona que va a ser la encargada de su ejecución y gestión, la cual debe ser parte o miembro de la alta gerencia en la organización, con el fin de lograr la alineación entre la alta gerencia y el área de seguridad de la información. (Killmeyer, Jan, 2006).

Arquitectura de seguridad según Jeimy Cano

El modelo de arquitectura de seguridad de Jeimy Cano (2008) "Entre la Administración y el Gobierno de la Seguridad de la Información" define tres elementos dentro de su presentación de acuerdo a los procesos fundamentales que componen la seguridad de la información, como se muestra en la Ilustración 2.

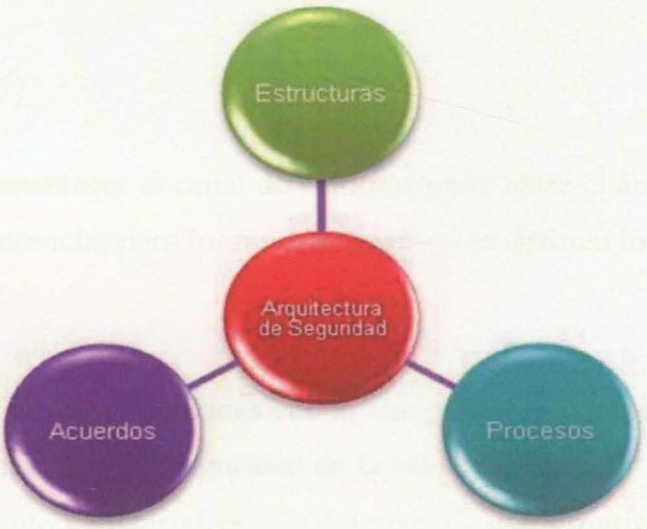

Ilustración 2 Componentes de la arquitectura de seguridad según Jeimy Cano

Fuente: Recuperado de (Jeimy Cano, 2008)

Estructuras:

- La información: reconocida como un activo.
- Las estrategias del negocio: procesos que generan valor en la organización en su operación.
- Los fundamentos de la seguridad de la información: basados en los principios de confidencialidad, integridad y disponibilidad como características de la información.
- La administración de riesgos: implementación de alguna metodología para descubrir vulnerabilidades y las estrategias para tratarlas y mitigar las amenazas.

Procesos:

Llevar a cabo la implementación de las buenas prácticas de seguridad propuesta basadas en la norma internacional ISO 27002.

Acuerdos:

Tiene por objetivo establecer el canal de comunicación entre el área de seguridad de la información y la alta gerencia; para lograr este objetivo se definen los siguientes aspectos a tener en cuenta:

- Establecimiento de prioridades con la alta gerencia, competencias y habilidades requeridas en el área de seguridad de la información.
- Establecimiento y materialización del nivel de compromiso de la alta gerencia en los proyectos definidos en el área de seguridad de la información.
- Definir los acuerdos de nivel de servicio y niveles de inversión en infraestructura de seguridad de la información.
- Compartir y alinear la agenda interna de la alta gerencia, con la agenda interna del área de seguridad de la información.

Arquitectura de seguridad por el SANS INSTITUTE

SANS (SysAdmin Audit, Networking and Security Institute) esta institución la cual trabaja en temas de seguridad de la información, cuenta con un modelo denominado "Information Systems Security Architecture: A Novel Approach to Layered Protection (2004)" cuyo autor es George Farah, quien con base en la definición de cinco fases explica cómo se desarrolla una arquitectura de seguridad de la información en un entorno donde existen pocas medidas de seguridad, mediante el establecimiento de algunas directrices como se muestra en la Ilustración 3:

Ilustración 3 Componentes de la arquitectura de seguridad por el SANS Institute

Fuente: Recuperado de (SANS, 2004).

Realización de evaluaciones de la seguridad:

El fin de dicha fase es encontrar vulnerabilidades al sistema de información, independiente de que se hayan aplicado o no controles. Esta fase se realiza mediante cinco procesos:

- Realización de entrevistas con los dueños de los procesos.
- Elaboración de inventario de activos.
- Implementación de un análisis del impacto del negocio (BIA).
- Identificación de amenazas sobre el inventario de activos.
- Implementación de un análisis de riesgos.

Formulación del diseño de los objetivos de la arquitectura de seguridad:

Tiene su fundamento en la realización de las evaluaciones de seguridad contempladas en el paso anterior, de tal manera que se definan con acierto los objetivos de la arquitectura de seguridad de la información, para ello se tiene en cuenta la definición de la arquitectura lógica y física del sistema de información.

Implementación de políticas y procedimientos:

En este punto se comienza a crear una política apropiada para el negocio a través de su conocimiento, esta debe ser definida en su estructura teniendo en cuenta el marco de la política corporativa y conducir a los usuarios internos y externos sobre la forma en la cual se debe utilizar los sistemas de información.

Implementación del diseño de los objetivos de la arquitectura de seguridad:

Habiendo seguido la secuencia en el cumplimiento de las fases anteriores, se establecen los plazos, la financiación y los recursos necesarios para implementar la arquitectura de seguridad de la información.

Integración de las prácticas de seguridad para mantener el estado de seguridad:

Es la forma de mantener el trabajo realizado en las fases anteriores en un ambiente de trabajo seguro, se logra estableciendo el personal idóneo y con las capacidades necesarias para la evaluación y actualización de la arquitectura de seguridad del sistema de información, para esta fase se debe tener en cuenta:

- Gestión de cambios de los elementos o dispositivos que conforman la arquitectura.
- Gestión de proyectos de tecnologías de la información, donde se definan los requisitos y etapas en la ejecución de proyectos que realimenten el estado de la arquitectura de seguridad de la información y sus posibles actualizaciones.

Arquitectura de seguridad TOGAF

El Open Group Architecture Framework (TOGAF, por sus siglas en inglés), es un estándar diseñado por la organización Open Group, el cual está probado como arquitectura empresarial y es utilizado por las organizaciones líderes del mundo para mejorar la eficiencia empresarial con un nuevo enfoque modernizado en su última versión acercándose a los nuevos retos de las organizaciones en el mundo actual. (The Open Group, 2018).

El estándar TOGAF en su última versión 9.2 (2018), ha sido de provecho para muchas organizaciones pues el mismo abarca temas de interés y pueden ser aplicados de manera sencilla utilizando guías separadas para poner en práctica en relación a cómo usar la metodología de la arquitectura al interior de la organización. Con este estándar las empresas lograrán identificar las necesidades de transformación en lo referente a la protección de la información digital acorde a sus necesidades específicas, utilizando la guía de arquitectura de negocios, arquitectura de seguridad, mapeo de otros modelos de referencia y la guía práctica de implementación.

De acuerdo al Open Group (2018), este modelo de arquitectura de seguridad tiene un enfoque que se basa en la implementación de políticas de seguridad que una empresa u organización debe tener para proteger el recurso de la información. La estructura de su arquitectura está compuesta en ocho fases, alienadas de principio a fin. Tienen como propósito proteger el valor de los sistemas de información y los bienes de la empresa, de manera que cumplan con los criterios de aceptación de autenticación, autorización, auditoria, aseguramiento, disponibilidad, protección de activos, administración y gestión del riesgo.

El estándar que es denominado como Método de Desarrollo de la Arquitectura (ADM, por sus siglas en inglés) se divide en ocho partes como se ve en la Ilustración 4:

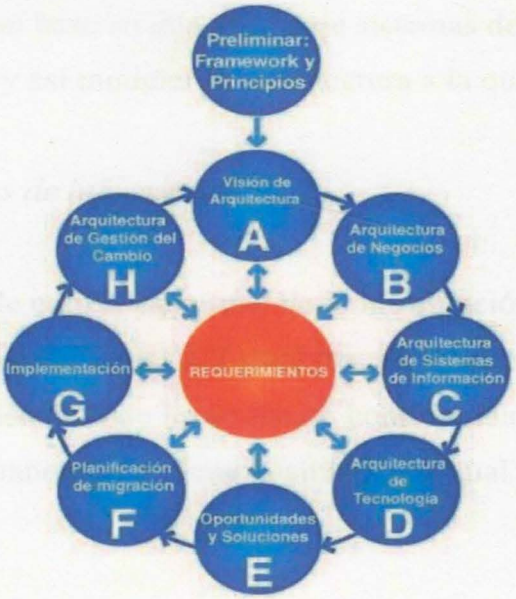

Ilustración 4 Fases del framework TOGAF

Fuente: Recuperado de (The Open Group, 2018).

A - Visión de la arquitectura:

Específica cual es el alcance, restricciones y las expectativas para llevar a cabo la arquitectura, así mismo busca definir los objetivos de la empresa identificando los requerimientos clave para empezar a plantear la estrategia de la organización.

B - Arquitectura de negocios:

Dentro de este componente se desarrollan los objetivos de la línea base de la arquitectura, describiendo las funciones y procesos, la información, los aspectos geográficos del entorno del negocio, basado en los principios y los objetivos estratégicos desarrollados en la visión de la arquitectura. Se debe realizar una evaluación para conocer el desempeño de la empresa con base en una norma de sistemas de gestión, definiendo la situación actual de la empresa y así modelar la arquitectura a la que se quiere llegar.

C - Arquitectura de sistemas de información:

Determina cual es el nivel de confidencialidad de la información contenida en los sistemas de información, estableciendo las obligaciones a sus propietarios, para que se genere responsabilidad sobre este tipo de información considerada la más sensible analizando brechas y de esta manera se obtiene la situación actual logrando plantear la arquitectura objetivo.

D - Arquitectura de tecnología:

Se basa en la creación de las especificaciones técnicas en los sistemas en los cuales se implementarán los requisitos de seguridad definidos en las arquitecturas anteriores, se debe identificar primero el estado actual de la seguridad en los sistemas específicos para definir la arquitectura objetivo, mediante la implementación de estándares, normas y directrices aplicables en la empresa.

E - Oportunidades y soluciones:

Decidir sobre el enfoque que se le dará a la arquitectura dentro de la organización y como se implementará la arquitectura de la Fase D, con la solución a preguntas tales como si se debe hacer, comprar o reusar; si se requiere un proceso de tercerización donde se debe definir que se contrata y que no es necesario hacerlo. Es importante conocer el mercado existente de soluciones que puedan asegurar un óptimo funcionamiento de la arquitectura. Mirar soluciones híbridas entre una global y local.

F - Planificación de migración:

Aborda la planificación de la migración; es decir, cómo moverse desde la arquitectura de la línea de base a la arquitectura de destino finalizada con un plan de implementación y migración en detalle el cual proporcione alineación con los objetivos principales de la organización para la gestión e implementación de cambios de ser necesarios.

G - Implementación:

Hacer el plan de implementación y especificar cómo se van a llevar a cabo esas soluciones es la parte importante de esta fase. Saber exactamente cómo se va a ejecutar el proyecto de la arquitectura para construir las soluciones de TI y determinar si se va a pasar de un punto A a un punto B de modo incremental o de un solo paso.

H - Arquitectura de gestión del cambio:

Tiene que ver con el monitoreo y evaluación de los sistemas existentes para determinar cuándo iniciar un nuevo ciclo de ADM. En esta fase es importante:

- Proveer un continuo monitoreo y un proceso de gestión de cambio.

- Asegurarse que los cambios a la arquitectura sean gestionados de una manera cohesiva.
- Monitorear el negocio y la capacidad de gestión.
- Garantizar que el cambio es coherente con todo el proyecto y que todo el proyecto permanece coherente.

OSA Arquitectura de seguridad

La Arquitectura de Seguridad OSA (Open Security Architecture) tiene una definición de arquitectura de seguridad compuesta por dos componentes fundamentales, seguridad de tecnologías de la información y arquitectura de tecnologías de la información "Diseño de artefactos que describe la estructura de los compontes de la organización, sus interrelaciones, principios y directrices que gobiernan su diseño y evolución". En esencia consiste en el diseño de herramientas o artefactos que describen como los controles de seguridad están posicionados y como se relacionan en general con la arquitectura TI; los controles tienen como propósito mantener los atributos de calidad del sistema tales como confidencialidad, integridad, disponibilidad, responsabilidad y seguridad. (Open Security Architecture, 2020).

Inicialmente se realiza un análisis de riesgo que tiene como objetivo identificar las vulnerabilidades a las que están expuestos los sistemas y medir el impacto que tiene en los procesos de negocio en caso de presentarse un incidente, busca mitigar estas vulnerabilidades con la implementación de controles, que básicamente definen un conjunto de políticas (principios y objetivos) que van ligados a las leyes y regulaciones que debe cumplir la empresa dependiendo de su razón de ser, el cumplimiento de estas leyes y regulación es soportado por estándares y directrices que son probadas y tienen como resultado la emisión de certificados. (Open Security Architecture, 2020).

La taxonomía de este modelo según sus autores describe las entidades y relaciones que son relevantes para ella, también ayuda a comprender cómo se relaciona este modelo con otros conceptos de seguridad, y permite considerar cómo la desarrollará en el futuro.

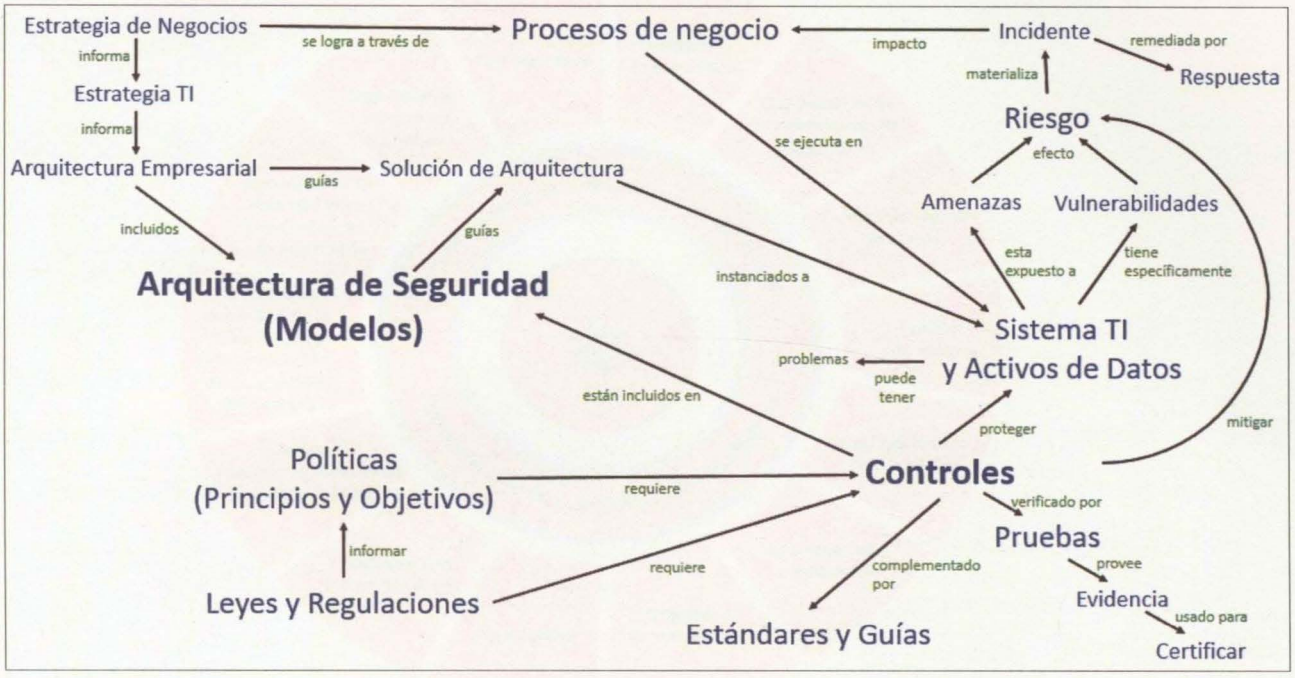

Ilustración 5 Taxonomía del modelo OSA

Fuente: Recuperado de (Open Security Architecture, 2020)

ISO/IEC 27000

Es un conjunto de estándares y normas desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de la seguridad de la información (SGSI). Tiene la posibilidad de integrarse con otros sistemas de gestión, baja en costos, mejora en los procesos de servicio y por último el

aumento de la seguridad en base a la gestión de procesos en lugar de la compra de productos y tecnologías. (International Organization for Standarization, 2018).

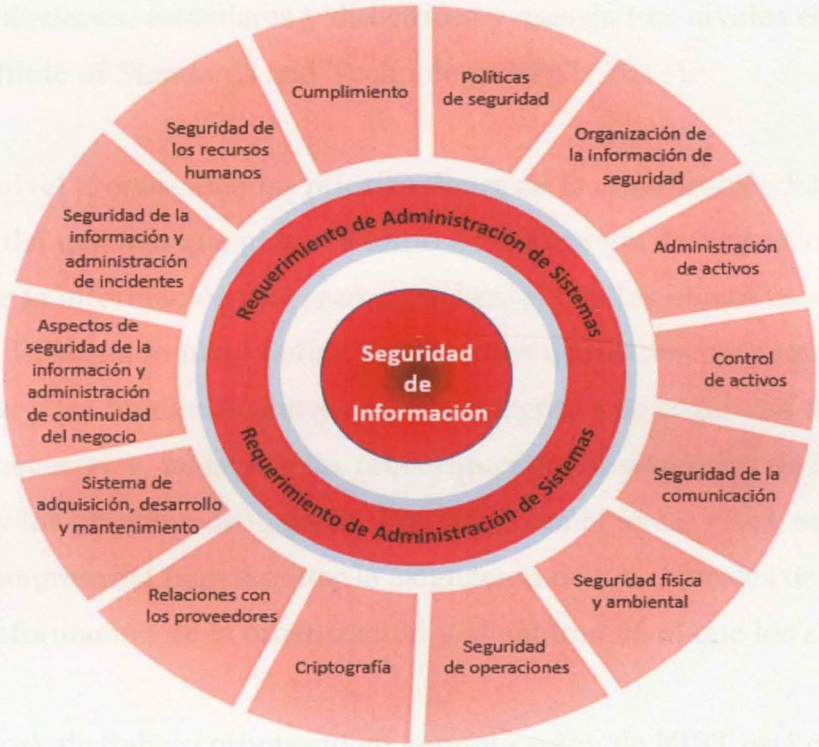

Ilustración 6 Requisitos del sistema de gestión ISO 27001

Fuente: Recuperado de (International Organization for Standarization, 2018).

Este estándar es el utilizado al interior de la organización objetivo de estudio en este proyecto, cuestión que se dará a conocer con más detalle con el desarrollo del segundo objetivo específico del trabajo.

NIST

El NIST (National Institute of Standards and Technology) es un instituto especializado en medidas y estándares tecnológicos regulado por la agencia del departamento de comercio de los Estados Unidos, en abril de 2013 realizó una publicación acerca de la

seguridad y controles de privacidad donde muestra que el manejo de riesgo está compuesto por la selección y la especificación de los controles de seguridad para un sistema de información, los controles pueden ser leyes federales, órdenes ejecutivas, directivas, políticas, regulaciones, estándares y directrices y maneja tres niveles en particular. (National Institute of Standards and Technology NIST, 2013).

El primer nivel proporciona las priorizaciones de la organización basadas en la misión y las funciones del negocio que giran en torno a la estrategia de inversión en soluciones en tecnologías de la información que sean consistentes con los objetivos estratégicos de la organización. El segundo nivel define los procesos necesarios para soportar la misión organizacional y las funciones, determina las categorías de seguridad de los sistemas de información necesarios, incorpora los requerimientos de seguridad de la información dentro de la misión y los procesos de negocio. Por ultimo en el tercer nivel, se establece una arquitectura empresarial para facilitar la asignación de los controles de seguridad a los sistemas de información de la organización y el entorno en el que los sistemas operan.

El framework de trabajo propuesto en la publicación de NIST está compuesto de 6 pasos:

1. Categoriza los sistemas de información.

2. Selecciona los controles de seguridad aplicables a los resultados de la categorización del paso 1.

3. Implementa los controles de seguridad y la genera la documentación del diseño y del desarrollo de dichos controles.

4. Evalúa los controles de seguridad para determinar cuáles controles fueron implementados de manera correcta en base a los requerimientos de seguridad.

5. Autoriza la operación de los sistemas de información.

6. Monitoreo de los controles de seguridad implementados en los sistemas de información y en el ambiente de operación basado en los cambios en el sistema.

Ilustración 7 Framework gestión de riesgos NIST

Fuente: Recuperado de (National Institute of Standards and Technology NIST, 2013)

10. Marco legal

Las normas y regulaciones en ciberseguridad y ciberdefensa son importantes a la hora de desarrollar este proyecto, puesto que las mismas hacen parte fundamental de las medidas a las cuales se debe acoger una organización a la hora de incorporar una arquitectura de seguridad al interior de la misma, sea cual sea la que se ajustará al desarrollo de los objetivos propuestos. De igual manera, existen actualmente normas, leyes y tratados a los cuales Colombia se rige para incluir la ciberseguridad y ciberdefensa como pilar fundamental para la administración de la información digital de las organizaciones.

10.1. Normatividad a nivel nacional

- Ley 1273 de 2009 "Protección de la información y de los datos"

Esta Ley emitida por parte del gobierno nacional de Colombia es aquella "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Esta Ley garantizará la confidencialidad, integridad y la disponibilidad de los datos informáticos. (Congreso de la República , 2009).

- CONPES 3701 de 2011 "Lineamientos de política para ciberseguridad y ciberdefensa"

Es el documento por medio del cual el gobierno colombiano a través del Departamento Nacional de Planeación (DNP), establece los lineamientos de políticas para la ciberseguridad y ciberdefensa del país, con el objetivo principal de fortalecer las capacidades del Estado para contrarrestar el incremento de las amenazas informáticas que afectan al mismo que permitan la prevención y control de estos ciberataques a las infraestructuras críticas del país. Para el desarrollo de este documento, el gobierno nacional se basó en la legislación que se ha reglamentado a través de los años y que han sido un

esfuerzo para la realización de este marco que pretende prevenir y mitigar el riesgo y el cual va dirigido a las entidades que de manera directa o indirecta están involucradas en el sector de las TIC. (Departamento Nacional de Planeación, 2011).

- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"

Con la creación de esta Ley, el gobierno nacional desarrolló el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales, así como el derecho a la información. (Congreso de la República, 2012).

- CONPES 3854 "Política nacional de seguridad digital"

El documento CONPES 3854 aprobado el 11 de abril de 2016, fue diseñado por el gobierno nacional con el objetivo de dar a conocer la necesidad que tiene el país de fortalecer las capacidades para identificar, tratar y mitigar los riesgos asociados a la información digital, lo cual contribuya a la expansión de la economía digital nacional a través de la ejecución de un conjunto de estrategias con un enfoque de gestión del riesgo, especificando objetivos y trazando un plan de acción para el cumplimiento de los mismos. (Departamento Nacional de Planeación, 2016).

- Norma Técnica Colombiana NTC – ISO/IEC 27001 Tecnología de la información, técnicas de seguridad y el sistemas de gestión de la seguridad de la información (SGSI)

La NTC-ISO/IEC 27001 fue ratificada por el Consejo Directivo del Instituto Colombiano de Normas Técnicas (ICONTEC) en el año 2006 con el objetivo de establecer los requisitos para crear, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos de la organización. El

SGSI está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas. (Instituto Colombiano de Normas Técnicas (Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, 2006).

El establecimiento y gestión del SGSI de acuerdo a la norma técnica 27001 se lleva a cabo a través de los pasos que se mencionan a continuación:

- Definir el alcance y límites del SGSI.
- Definir la política del SGSI.
- Definir el enfoque organizacional para la valoración del riesgo.
- Identificar los riesgos.
- Analizar y evaluar los riesgos.
- Identificar y evaluar las opciones para el tratamiento de los riesgos.
- Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
- Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
- Obtener autorización de la dirección para implementar y operar el SGSI.
- Elaborar una declaración de aplicabilidad. (International Organization for Standardization (ISO), 2013).

- Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad"

El estándar 27032 publicado en el año 2012 por la ISO/IEC, tiene como objetivo dar unos lineamientos generales de orientación para que las empresas logren fortalecer la ciberseguridad en la misma, utilizando puntos técnicos estratégicos, principalmente aquellos relacionados con:

- La seguridad en las redes.
- Seguridad en internet.
- Seguridad de la información.
- Seguridad en las aplicaciones.

Con ello, se pretende que las organizaciones hagan frente al cibercrimen de manera efectiva, así como lograr una cooperación entre las partes interesadas para minimizar los riesgos que puedan derivarse de la utilización del ciberespacio. (The International Organization for Standardization, 2012).

- Oficio 05289 de 2012 "Creación de unidades de ciberdefensa en las Fuerzas Militares"

El Comandante General de las Fuerzas Militares de Colombia para el año 2012, imparte instrucciones a los señores Generales Comandantes de las Fuerzas Militares de Colombia (Ejército Nacional, Armada Nacional y Fuerza Aérea), con el fin de realizar un cronograma de actividades para dar cumplimiento a la creación de unidades de ciberdefensa al interior de cada una de las Fuerza. Esta instrucción se desprende de la necesidad del gobierno por implementar planes, proyectos y programas encaminados a prevenir y contrarrestar ataques cibernéticos a la infraestructura crítica del país. Con base en el documento CONPES 3701 de 2011. (Comando General Fuerzas Militares de Colombia, 2012).

- Directiva Permanente Ministerial DIR2014-18 "Políticas de seguridad de la información para el sector defensa"

Con esta Directiva el Ministerio de Defensa Nacional de Colombia, dicta instrucciones con el objetivo de establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios y en general cualquier persona que tenga relación contractual con el sector defensa o que tenga acceso a los activos de información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información, protegiendo

adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de la información. (Ministerio de Defensa Nacional, 2014).

- Directiva Permanente 00201/2017 "Lineamientos de ciberseguridad y ciberdefensa para el Ejército Nacional"

Por medio de la cual el Departamento de Comunicaciones del Ejército Nacional imparte instrucciones, órdenes y lineamientos con el fin de actualizar políticas que permitan la aplicación de las capacidades en el ciberespacio respecto a la ciberseguridad y ciberdefensa logrando identificar y determinar responsabilidades, que deben cumplir la unidad de ciberdefensa del Ejército Nacional a través del Comando de Apoyo de Combate de Inteligencia Militar (CAIMI), el Comando de Apoyo de Combate de Contrainteligencia Militar (CACIM) y el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa (CAOCC), articulando los esfuerzos para ejercer seguridad y defensa de las infraestructuras tecnológicas propias y asignadas en el ciberespacio. (Departamento de Comunicaciones CEDE6 del Ejército Nacional, 2017).

- Directiva estructural de ciberdefensa CCOCI 2019

De acuerdo al documentos directiva permanente estructural del Comando General de las Fuerzas Militares, la finalidad del mismo está enfocado en impartir órdenes e instrucciones al Comando General de las Fuerzas Militares y los Comandos de las Fuerzas a articular esfuerzos en el planeamiento, desarrollo, ejecución, evaluación y seguimiento de las operaciones militares cibernéticas conjuntas, coordinadas, combinadas e interinstitucionales, teniendo en cuenta el rol de cada Fuerza y del Comando Conjunto Cibernético (CCOCI). (Comando General de las Fuerzas Militares, 2019).

10.2. Normatividad a nivel internacional

- Convenio sobre ciberdelincuencia del consejo de Europa – CCC (convenio sobre cibercriminalidad de Budapest)

Este convenio fue adoptado en noviembre de 2001 y entró en vigor desde el 1° de julio de 2004. Es el principal convenio en relación a la ciberdelincuencia y tiene como objetivo fundamental la adopción de una legislación que facilite la prevención de las conductas delictivas en el ciberespacio y contribuya con herramientas eficientes en materia penal y de cooperación internacional, que permitan detectar, investigar y sancionar las conductas antijurídicas. (Consejo de Europa , 2001).

- Resolución AG/RES 2004 (XXXIV- O/04) de la Asamblea General de la Organización de los Estados Americanos (OEA)

La Resolución para la adopción de una estrategia interamericana integral de seguridad cibernética tiene un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética firmada por los Estados miembro de la OEA consideraron importante la adición a la Convención del Consejo de Europa sobre la ciberdelincuencia y la aplicación de sus principios, medidas legales y de otra naturaleza necesarias para su implementación. De igual manera, tienen la plena intención de continuar realizando actividades de cooperación técnica mediante las cuales se logre combatir las amenazas a la seguridad cibernética y asegurar una estrategia interamericana integral de seguridad cibernética. (Organización de Estados Americanos OEA, 2012).

- Decisión 587 de la Comunidad Andina "Lineamientos de la política de seguridad externa común andina"

Adoptada el 10 de julio de 2004, esta decisión fue considerada entre los Jefes de Estado de los países miembro de la Comunidad Andina de Naciones, reafirmando su interés y

compromiso por afianzar la paz, la seguridad y la cooperación entre los mismos estableciendo los lineamientos y políticas en materia de ciberseguridad para combatir y erradicar las nuevas amenazas que atenten contra la Comunidad Andina. (Organización de Estados Americanos OEA, 2004).

- Resolución 64/25 "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"

Esta Resolución fue adoptada en la 55° sesión plenaria de la Asamblea General de las Naciones Unidas en el año 2009, mediante la cual se exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y medidas que limiten las amenazas que surjan en ese ámbito. (Organización de Naciones Unidas, 2009).

11. El modelo SABSA

El modelo SABSA (Sherwood Applied Business Security Architecture) fue creado por el instituto SABSA entre los años 1995 y 2018 con locación en Inglaterra y Gales - Reino Unido. El modelo es definido como "una metodología probada para desarrollar arquitecturas de seguridad orientadas al negocio, centradas en el riesgo y en las oportunidades, tanto a nivel empresarial como de soluciones, que respaldan de manera rastreable los objetivos comerciales". (Instituto SABSA CIC, 2020).

Según el instituto SABSA (2020), en la actualidad esta metodología es utilizada en diferentes organizaciones de todo el mundo de manera exitosa convirtiéndose en una de las metodologías preferidas en organizaciones de diferentes tipos como bancos, energía nuclear, servicios de la información, tecnología de las comunicaciones y el gobierno.

Tomando como referencia la metodología SABSA, esta comprende seis capas y se aplican a lo largo del ciclo de vida del proceso desde la ingeniería de requisitos hasta la gestión de las soluciones entregadas, cuyo resumen se encuentra en la Tabla 1.

Cada capa representa la vista de un diferente sujeto en el proceso de especificar, diseñar, construir y utilizar este modelo.

Tabla 1 Vistas de la arquitectura en capas del modelo SABSA

La vista del negocio	→	Arquitectura contextual
La vista del arquitecto	→	Arquitectura conceptual
La vista del diseñador	→	Arquitectura lógica
La vista del implementador	→	Arquitectura física
La vista del comerciante	→	Arquitectura de componente
La vista del administrador	→	Arquitectura operacional

Fuente: Recuperado de (Instituto SABSA CIC, 2020)

Según Sherwood uno de los autores de la metodología SABSA, existe otra distribución de las seis capas anteriormente mencionadas que quizás podría considerarse más útil para algunas organizaciones, tal como se muestra en la Ilustración 8, mostrando la capa de la arquitectura de seguridad operativa verticalmente a lo largo de las otras cinco capas. Esto se debe a que surgen problemas de seguridad operacional en todas y cada una de las cinco capas.

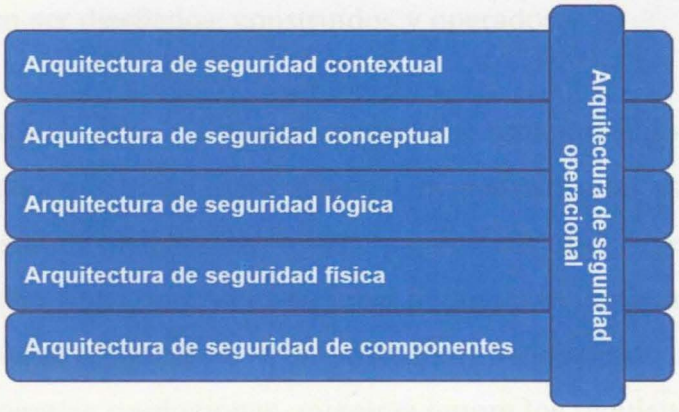

Ilustración 8 El modelo SABSA para el desarrollo de la arquitectura de seguridad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

11.1. La vista del negocio

Al diseñar un sistema de información seguro, se debe aplicar el enfoque arquitectónico más adecuado que será impulsado desde una clara comprensión de los requisitos de negocio para el sistema, para ello es indispensable que la organización se plantee lo siguientes interrogantes:

- ¿Qué tipo de sistema de información es y para qué se utilizará?
- ¿Por qué será utilizado?
- ¿Cómo se utilizará?
- ¿Quién lo usará?
- ¿Dónde será utilizado?
- ¿Cuándo se utilizará?

Estas son las preguntas características que se deben tener en cuenta al hacer el análisis para comprender los requisitos de un sistema seguro. A partir de ellos, se debe poder resumir una arquitectura de seguridad que cumpla con esos requisitos específicos.

En el modelo SABSA este punto de vista de la organización se llama la arquitectura de seguridad contextual, es una descripción del contexto organizacional en el que los sistemas seguros deben ser diseñados, construidos y operados.

Cualquier intento de definir una arquitectura que tome un atajo y evite este paso esencial es poco probable que tenga éxito. Aun así, de acuerdo a las estadísticas del instituto SABSA una simple observación revela que muchas organizaciones arquitectónicas no se toman en serio esta etapa, lo cual es un error al iniciar la implementación. Es muy común que el trabajo de la arquitectura de seguridad comience desde una perspectiva técnica, mirando tecnologías y soluciones, mientras ignora los requisitos esenciales del negocio.

En el modelo SABSA presentado, la arquitectura de seguridad contextual debe responder a las siguientes preguntas:

¿Qué?

- La organización, los activos a proteger y las necesidades de seguridad de la información (seguridad como facilitador de negocios, operaciones electrónicas seguras, continuidad operativa y estabilidad, cumplimiento de la ley, etc.).

¿Por qué?

- Los riesgos de la organización expresados en términos de activos, objetivos, factores de éxito y las amenazas, impactos y vulnerabilidades que los ponen en riesgo, impulsando

la necesidad de seguridad (protección de marca, prevención de fraudes, prevención de pérdidas, obligaciones legales, continuidad del negocio, etc.).

¿Cómo?

- Los procesos de la organización que requieren seguridad (interacciones y transacciones operacionales, comunicaciones, etc.).

¿Quién?

- Los aspectos organizativos de la seguridad (estructuras de gestión, suministros, estructuras de cadena, relaciones de subcontratación, asociaciones estratégicas).

¿Donde?

- La geografía y los aspectos relacionados con la ubicación de la seguridad (mercado global, sitios corporativos distribuidos, trabajo remoto, etc.).

¿Cuando?

- Los aspectos relacionados con el tiempo de la seguridad organizacional tanto en términos de rendimiento como de secuencia (rendimiento de transacciones operacionales, tiempos de vida y fechas límite, operaciones justo a tiempo, etc.).

11.2. La vista del arquitecto

Según el modelo SABSA, un arquitecto es una persona creativa con una gran visión, prosperan en acciones desafiantes, reúnen sus habilidades y experiencias para crear una imagen inspirada de cómo será la organización, proporcionan descripciones de alto nivel, preparando el camino para llevar a cabo el trabajo detallado más adelante.

Esta capa del modelo arquitectónico también se conoce como la arquitectura de seguridad conceptual definiendo los principios y conceptos fundamentales que guíen la selección y organización de los elementos lógicos y físicos de la misma.

Al describir la arquitectura de seguridad de la empresa según Sherwood (2005), menciona que este es el momento en que la organización debe describir la seguridad conceptual y los principios que se utilizaran. Éstos incluyen:

¿Qué se quiere proteger expresado en el Modelo SABSA en términos de los atributos del perfil del negocio?

- Los atributos de la metodología SABSA proporcionan la herramienta principal para que las necesidades de la organización sean tomadas en una forma sistematizada.

¿Por qué la protección es importante en términos de objetivos de control?

- Los objetivos de control se derivan directamente de un análisis de los riesgos operacionales de la organización y son una conceptualización de la motivación de la empresa para la seguridad.

¿Cómo lograr la protección en términos de alto nivel técnico y de gestión de estrategias de seguridad?

- Estas estrategias establecen el marco conceptual por capas para integrar tácticas individuales y elementos en los niveles más bajos, asegurando que estos encajen de manera significativa para cumplir con el conjunto de objetivos estratégicos del negocio.

Tales estrategias incluyen: la estrategia para la seguridad de las aplicaciones, de seguridad de la red, de infraestructura criptográfica, el control de acceso basado en roles, y así sucesivamente para cada área importante de las necesidades de la organización

identificadas en la arquitectura de seguridad contextual, habrá una estrategia de seguridad (o grupo de estrategias) que lo apoya.

¿Quién está involucrado en la gestión de la seguridad en términos de modelos de relación de entidad y cuál es el marco de confianza dentro del cual las entidades interactúan entre sí?

- Los conceptos de confianza importantes se refieren a las diversas autoridades políticas que gobiernan la confianza dentro de un dominio, las políticas que establecen para gobernar el comportamiento de las entidades en cada uno de esos dominios, y las relaciones de confianza entre ellos.

¿Dónde lograr la protección conceptualizada en términos de dominios de seguridad?

- Los conceptos importantes aquí son los dominios de seguridad tanto lógicos como físicos, límites de dominio y asociaciones de seguridad.

¿Cuándo es relevante la protección en términos de tiempo y plazos?

- Los conceptos importantes son la vida útil y los plazos de caducidad (de claves, certificados, contraseñas, sesiones, etc.), y el uso del tiempo de confianza y las transacciones operacionales sensibles al tiempo. También son importantes los criterios de rendimiento relacionados con el tiempo: la rapidez con que deben ocurrir las cosas.

11.3. La vista del diseñador

Siguiendo la referencia de Sherwood (2005), el diseñador interpreta las ideas conceptuales del arquitecto, visualiza y convierte una estructura lógica que pueda diseñarse. El arquitecto es el artista y visionario, el diseñador es el ingeniero.

En el mundo de la era digital y las comunicaciones de datos, este proceso de diseño implica la identificación y especificación de la arquitectura lógica. Esta vista modela la organización como un sistema con componentes mostrando los principales elementos de seguridad arquitectónica en términos de servicios de seguridad lógica, y describe el flujo lógico de control y las relaciones entre estos elementos lógicos. Por lo tanto, también se conoce como la arquitectura de seguridad lógica.

En términos de descomposición arquitectónica a través de las capas, la arquitectura de seguridad lógica debe reflejar y representar todas las principales estrategias de seguridad en la arquitectura de seguridad conceptual.

La arquitectura de seguridad lógica se ocupa de:

¿Qué?

- La información de la organización es una representación lógica del negocio real. Es la información de operaciones que necesita ser asegurada.

¿Por qué?

- Especificación de los requisitos de la política de seguridad (política de seguridad de alto nivel, política de autoridad de registro, política de autoridad de certificación, políticas de dominio físico, políticas de dominio lógico, etc.) para asegurar la información de la organización.

¿Cómo?

- Especificando los servicios de seguridad lógica (autenticación de entidad, confidencialidad, integridad, no repudio, garantía del sistema, etc.) y que encajen como

bloques reutilizables comunes en un sistema de seguridad complejo que cumple con los requisitos operacionales.

¿Quién?

- Especificando las entidades (usuarios, administradores de seguridad, auditores, etc.) y sus interrelaciones, atributos, roles autorizados y perfiles de privilegios.

¿Donde?

- Especificación de los dominios de seguridad y las relaciones entre dominios (dominios de seguridad lógica, dominios de seguridad física, asociaciones de seguridad).

¿Cuando?

- Especificando el ciclo de seguridad de procesamiento (registro, certificación, inicio de sesión, sesión de gestión, etc.).

11.4. La vista del implementador

De acuerdo a la metodología, el diseñador entrega el proceso de trabajo al implementador. Este toma las descripciones lógicas, los diseños y los convierte en un modelo tecnológico que se puede utilizar para construir el marco de seguridad. Aquí es tarea del implementador elegir y ensamblar los elementos físicos que harán que el diseño lógico cobre vida. Esta vista por lo tanto se conoce como la arquitectura de seguridad física.

La arquitectura de seguridad física, describe el modelo de tecnología real y específica los requisitos funcionales de los diversos componentes del sistema. Los servicios de seguridad lógica se expresan ahora en términos de mecanismos de seguridad física y equipos que se utilizarán para prestar estos servicios.

La arquitectura de seguridad física se ocupa de:

¿Qué?

- Especificar el modelo de datos de negocio y las estructuras de datos relacionadas con la seguridad (tablas, mensajes, certificados, firmas, etc.).

¿Por qué?

- Especificar reglas que impulsan la toma de decisiones lógicas dentro del sistema (condiciones, prácticas, procedimientos y acciones).

¿Cómo?

- Especificando mecanismos de seguridad (cifrado, control de acceso, firmas digitales, escaneo de virus, firewall, etc.) y los equipos físicos en los que se alojarán estos mecanismos.

¿Quién?

- Especificando la dependencia de personas en la forma de los usuarios, las aplicaciones que uso y la interfaz de seguridad del usuario.

¿Donde?

- Especificando infraestructura de tecnología de seguridad (diseño físico del hardware, software y líneas de comunicación).

¿Cuando?

- Especificando la dependencia temporal en forma de estructuras de control de ejecución (secuencias, eventos, tiempos de vida e intervalos de tiempo).

11.5. La vista del comerciante

Cuando se planifica el proceso de implementación según SABSA, se necesita reunir una serie de productos, proveedores especializados y un equipo con las habilidades de integración para unirse a estos productos durante una implementación del diseño.

Cada uno de los integradores es el equivalente de un comerciante que trabaja con productos especializados y componentes del sistema. Los comerciantes trabajan con una serie de componentes que son elementos de hardware, software, especificaciones y normas de interfaz. De ahí que esta capa del modelo también se llame la arquitectura de seguridad de componentes.

La arquitectura de seguridad de componentes se refiere a:

¿Qué?

- Especificaciones de campos de datos, de direcciones y otra estructura de datos detallados en el presupuesto.

¿Por qué?

- Normas de seguridad.

¿Cómo?

- Productos y herramientas tanto de hardware como de software.

¿Quién?

- Identidades de usuario, privilegios, funciones, acciones y listas de control de acceso.

¿Donde?

- Procesos informáticos y protocolos entre procesos.

¿Cuando?

- Pasos de seguridad y secuenciación.

11.6. La vista del administrador

El trabajo del administrador es ocuparse de la operación y sus diversos servicios, manteniéndolos en buen estado de funcionamiento y controlando su desempeño en el cumplimiento de los requisitos. El marco para hacer esto se llama arquitectura de seguridad operacional.

La arquitectura de seguridad operacional se ocupa de lo siguiente:

¿Qué?

- Asegurar la continuidad operativa de los sistemas de la organización, información, procesamiento y mantenimiento de la seguridad de los datos e información de negocios

operativos (confidencialidad, integridad, disponibilidad, auditabilidad y responsabilidad).

¿Por qué?

- Gestionar los riesgos operacionales minimizando las fallas operativas e interrupciones.

¿Cómo?

- Realizar operaciones especializadas relacionadas con la seguridad (administración de seguridad de usuarios, administración de seguridad del sistema, copias de seguridad de datos, monitoreo de seguridad, respuesta de emergencia a procedimientos, etc.).

¿Quién?

- Proporcionar soporte operativo para las necesidades relacionadas con la seguridad de todos los usuarios y sus aplicaciones (usuarios, operadores, administradores, etc.).

¿Donde?

- Mantener la integridad y seguridad del sistema de todas las plataformas operativas y redes (aplicando estándares de seguridad operacional y auditando la configuración en contra de estas normas).

¿Cuando?

- Programación y ejecución de un calendario de operaciones relacionadas con la seguridad.

11.7. La vista del auditor

Hay otra vista de la seguridad en el modelo SABSA y es la vista del auditor, que se preocupa por garantizar que la arquitectura sea completa, consistente, robusta y que se ajuste al propósito en todos los sentidos. En el ámbito de la seguridad, este es el proceso de auditoría de seguridad realizada por personal de control de calidad en el área.

Sin embargo, el modelo SABSA no reconoce esto como una vista arquitectónica separada. El enfoque de la auditoría revisa que el modelo de arquitectura en su totalidad satisface las necesidades. La existencia de tal arquitectura es una de las formas en que los auditores establecerán que la seguridad se aplica de forma sistemática y adecuada, además, se aborda la auditoría y la revisión de seguridad como uno de los principales programas estratégicos dentro de la arquitectura de seguridad operacional asociada con la capa conceptual.

Tabla 2 La arquitectura de seguridad operacional

En la capa contextual	Elaboración de políticas empresariales, proceso de evaluación de riesgos empresariales del negocio. Recogida y especificación de requisitos y necesidades organizacionales y culturales, etc.
En la capa conceptual	Principales programas de formación, sensibilización, continuidad empresarial, gestión, auditoria y revisión, desarrollo de procesos de registro, autorización, administración y manejo de incidencias, desarrollo de normas y procedimientos, etc.
En la capa lógica	Políticas de seguridad, clasificación de la información, sistema. Clasificación, gestión de servicios de seguridad, seguridad de servicio. Gestión, negociación de estándares de seguridad interoperables. Servicios, seguimiento de auditorias e invocación de acciones, etc.
En la capa física	Desarrollo y ejecución de normas de seguridad, practicas y procedimientos, incluyendo: manejo de claves criptográficas, comunicación de parámetros de seguridad entre las partes, mantenimiento y distribución de ACL (listas de control de acceso) de ACE (entrada de control de acceso), gestión de copias de seguridad (almacenamiento, etiquetado, indexación, etc.), mantenimiento de búsqueda de patrones de virus, gestión de archivos de registro de eventos, etc.
En la capa componente	Productos, tecnología, evaluación, selección de estándares y herramientas, gestión de proyectos, gestión de implementación, operación y administración de componentes individuales, etc.

Fuente: Recuperado de: (John Sherwood, Andrew Clark, David Lynas, 2005)

11.8. La matriz SABSA

Cada una de las seis capas horizontales que contempla el modelo de arquitectura SABSA (contextual, conceptual, lógica, física, componente y operacional) ha sido examinada por los autores del modelo, donde cada una de las secciones también ha introducido una serie de cortes verticales a través de cada capa horizontal.

De esta manera proporciona una matriz de celdas de 6 x 6, que representa el modelo completo para la arquitectura de seguridad, llamada matriz de SABSA (Tabla 3). Lo ideal es que una organización logre abordar los temas planteados por todas y cada una de estas celdas, para así cubrir toda la gama de preguntas a ser respondidas, y se podrá tener un alto nivel de confianza de la arquitectura de seguridad. El proceso del desarrollo de la arquitectura de seguridad es el proceso de completar todas estas 36 celdas.

Tabla 3 La matriz de 36 celdas de SABSA

	Bienes (Qué)	Motivación (Por qué)	Proceso (Cómo)	Personas (Quien)	Ubicación (Dónde)	Hora (Cuando)
Contextual	El negocio	Modelo de riesgo empresarial	Modelo de proceso de negocio	Organización de negocios y relaciones	Geografía empresarial	Dependencias de tiempo de negocios
Conceptual	Perfil de atributos comerciales	Objetivos de control	Estrategias de seguridad y capas arquitectónicas	Modelo de entidad de seguridad y marco de confianza	Modelo de dominio de seguridad	Vidas y fechas límite relacionadas con la seguridad
Lógico	Modelo de información comercial	Políticas de seguridad	Servicios de seguridad	Esquema de entidad y perfiles de privilegio	Definiciones y asociaciones de dominios de seguridad	Ciclo de procesamiento de seguridad
Físico	Modelo de datos comerciales	Reglas de seguridad, prácticas y procedimientos	Mecanismos de seguridad	Usuarios, aplicaciones y la interfaz de usuario	Infraestructura de plataforma y red	Ejecución de estructura de control
Componente	Estructuras de datos detalladas	Normas de seguridad	Productos y herramientas de seguridad	Identidades, funciones, acciones y ACL	Procesos, modos, direcciones y protocolos	Paso de seguridad Tiempo y secuencia
Operacional	Aseguramiento de la continuidad operacional	Manejo de riesgos operacionales	Servicio de seguridad de gestión y soporte	Soporte de aplicaciones y gestión de usuarios	Seguridad de sitios, redes y plataformas	Programa de operaciones de seguridad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

11.8.1. Matriz SABSA para la capa operativa

Cuando se examina la capa más baja (arquitectura de seguridad operacional) de la Tabla 3, queda claro que esta capa operativa puede dividirse aún más en la matriz SABSA a cada una de las cinco capas anteriores, en otras palabras, hay aspectos operacionales asociados a cada una de las capas contextuales, conceptuales, lógicas, físicas y de componentes. La arquitectura de seguridad de operación se proporciona en la Tabla 4 con más detalle.

Tabla 4 La matriz de la arquitectura de seguridad operacional

	Bienes (Qué)	Motivación (Por qué)	Proceso (Cómo)	Personas (Quien)	Ubicación (Dónde)	Hora (Cuando)
Contextual	Colección de requisitos comerciales; Clasificación de información	Evaluación de riesgos comerciales; Elaboración de políticas corporativas	Programa de gestión de seguridad de la información orientado a los negocios	Gestión de la organización de seguridad empresarial	Gestión de operaciones de campo de negocios	Calendario de negocios y gestión de horarios
Conceptual	Gestión de continuidad del negocio	Auditoría de seguridad y niveles de garantía; Medición, métrica y evaluación comparativa	Respuesta al incidente; Recuperación de desastres; Programa de control de cambios	Capacitación en seguridad, sensibilización y desarrollo cultural	Gestión del dominio de seguridad	Gestión de horarios de operaciones de seguridad
Lógico	Seguridad de información; Integridad del sistema	Elaboración detallada de políticas de seguridad; Cumplimiento de la política; Supervisión; La recogida de información	Detección de intrusiones; Monitoreo de eventos; Proceso de desarrollo; Gestión de servicios de seguridad; Controles de desarrollo del sistema; Gestión de la configuración	Control de acceso y administración del perfil de privilegios	Administración y Administración de Seguridad de Aplicaciones	Gestión de plazos de entrega y corte
Físico	Integridad del software de seguridad de bases de datos	Evaluación de vulnerabilidad; Pruebas de penetración; Evaluación de amenazas	Definición de reglas; Gestión de claves; Mantenimiento de ACL; Administrador de respaldo; Informática forense; Administrador de registro de eventos; Administrador de antivirus	Soporte al usuario y mesa de ayuda	Gestión de seguridad de red; Administración de seguridad del sitio	Envejecimiento de la cuenta de usuario; Envejecimiento de contraseña; Administrar el tiempo de Windows para el control de acceso
Componente	Seguridad e integridad de productos y herramientas	Notificaciones CERT; Investigación sobre amenazas y vulnerabilidades	Adquisición de productos; Gestión de proyectos; Jefe de operaciones	Examen de personal; Administración de Usuario	Gestión de seguridad de plataformas, estaciones de trabajo y equipos	Configuración de tiempo de espera; Secuencia de operación detallada

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

11.9. Metodología SABSA como guía

El propósito principal de este proyecto es proporcionar una guía práctica para desarrollar una arquitectura de seguridad dentro del Ejército Nacional, señalando algunos de los pasos

clave y describiendo cómo planificar y ejecutar el proceso en sí, basado en los autores de la metodología SABSA.

Por lo anterior, es importante tener en cuenta:

- El proceso de desarrollo de SABSA y cómo se deriva directamente del modelo SABSA.
- El ciclo de vida de SABSA para el desarrollo de la arquitectura de seguridad y la forma en que se asigna al modelo SABSA.
- Los procesos y subprocesos detallados que comprenden la descomposición de arriba hacia abajo de las cuatro fases individuales del ciclo de vida de SABSA.
- Los flujos de proceso detallados que debe seguir al aplicar la metodología SABSA.
- La forma en que las distintas capas del modelo SABSA se integran al final en la arquitectura de seguridad para la institución.

Uso del modelo SABSA para definir un proceso de desarrollo

El flujo de proceso implícito es que las capas se desarrollan en secuencia, a excepción de la capa operativa de arquitectura de seguridad, esta se desarrolla en paralelo en lugar de secuencialmente, aunque esta actividad no puede comenzar realmente hasta que la capa conceptual se haya definido, así se verá la combinación secuencial y el flujo paralelo como se muestra en la Ilustración 9.

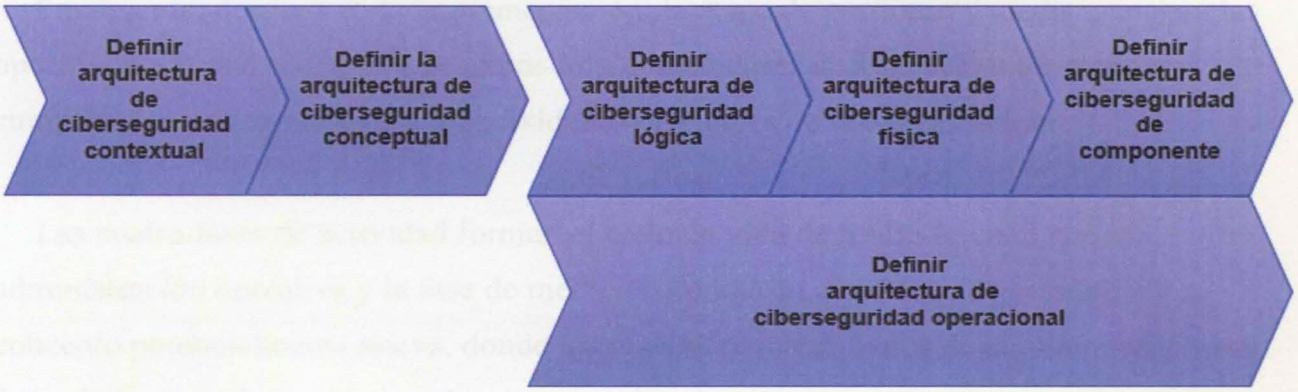

Ilustración 9 Proceso de desarrollo

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Para llevar el proceso un paso más allá, hay una ruptura natural en la continuidad del flujo entre la capa conceptual y lógica, la arquitectura de seguridad conceptual (la visión del arquitecto) es la conclusión de lo que se llama la fase de estrategia y concepto, dentro de la cual la estrategia es desarrollada y acordada siendo esencial obtener la aprobación de estas estrategias y visiones antes de comprometer fuertemente los recursos para las siguientes fases.

Una vez que la arquitectura de seguridad contextual (la vista del negocio) y la arquitectura de seguridad conceptual (la vista del arquitecto) se han concertado y hay una clara aceptación por parte de todas las partes interesadas, entonces estos conceptos se pueden materializar a través de una fase de diseño. Esto abarca la definición de las capas lógica, física, de componentes y operativa del modelo SABSA.

La finalización del diseño constituye otro hito importante, con la aprobación y el acuerdo de ser necesario antes de pasar a la fase de implementación en la que construye los sistemas y procesos que han sido diseñados.

Finalmente, después de la implementación, la etapa de gestionar y medir manejará las operaciones de los sistemas y procesos implementados y dirá si están o no realmente cumpliendo con los requisitos y necesidades originales de la organización.

Las cuatro fases de actividad forman el ciclo de vida de SABSA, en el que la administración operativa y la fase de medición conducen a una fase de estrategia y concepto potencialmente nueva, donde los nuevos requerimientos de la organización son formulados basados en la experiencia operacional.

Por lo tanto, el diagrama que se muestra en la Ilustración 10 representa el ciclo de vida de SABSA para la arquitectura de seguridad.

Ilustración 10 El ciclo de vida de SABSA

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

A continuación se examina cada una de las cuatro fases del ciclo de vida de SABSA con mayor detalle, observando los pasos del proceso en cada una con sus productos y entregables. Sin embargo, es importante mencionar que para el desarrollo de los objetivos

de este proyecto únicamente se tendrá en cuenta la primera y segunda fase del ciclo de vida, para el caso de la tercera y cuarta fase del ciclo se mencionará solo de manera conceptual.

11.9.1. Fase de estrategia y concepto

La fase de estrategia y concepto del ciclo de vida de SABSA comienza con la recopilación de requisitos operacionales completos y entendiendo la infraestructura tecnológica existente. La información recopilada se basa en las respuestas a las preguntas identificadas en el contexto de la organización y su infraestructura actual como se muestra en la Tabla 5.

Tabla 5 Las filas contextuales y conceptuales de la matriz SABSA

	Bienes (Qué)	Motivación (Por qué)	Proceso (Cómo)	Personas (Quien)	Ubicación (Dónde)	Hora (Cuando)
Contextual	El negocio	Gestión de riesgos empresariales	Modelo de proceso de negocio	Organización de negocios y relaciones	Geografía empresarial	Dependencias de tiempo de negocios
Conceptual	Perfil de atributos comerciales	Objetivos de control	Estrategias de seguridad y capas arquitectónicas	Modelo de equidad de seguridad y marco de confianza	Modelo de dominio de seguridad	Vidas y fechas límite relacionadas con la seguridad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Productos de la arquitectura de seguridad contextual

- El modelo de la institución: impulsores de la institución, incluidos los activos, metas y objetivo, asignados a los atributos de SABSA de la misma.

- El modelo de riesgo SABSA de la institución: en forma de una matriz de evaluación de riesgos, impulsado desde los atributos del modelo SABSA.

- El modelo de proceso de la organización.

- El modelo de organización y relaciones empresariales.

- El modelo de geografía organizacional.

- El modelo de dependencia del tiempo en la organización.

Entregables de arquitectura de seguridad conceptual

- El perfil de atributos de negocios de SABSA, sus definiciones detalladas dentro del contexto de la organización, la métrica, los enfoques de medición que se utilizarán y los objetivos de rendimiento para cada métrica.

- El modelo de riesgo SABSA, para incluir una declaración del control de objetivos.

- Una evaluación del estado actual de la seguridad en relación con los atributos de negocio de SABSA y los objetivos de control asociados.

- Una descripción de las capas arquitectónicas que se emplearán, la estrategia de seguridad principal y conceptos mapeados a los objetivos de control.

- Una serie de documentos donde se describe la estrategia de seguridad.

- El modelo de entidad de seguridad y el marco de confianza.

- El modelo de dominio de seguridad.

- Una lista de tiempos de vida relacionados con la seguridad y fechas límite que deben abordarse en las capas inferiores.

¿Cómo encajan la fase de estrategia y concepto?

Para el autor de la metodología, es absolutamente esencial que se entienda lo que está pasando en este nivel de la arquitectura ya que gran parte de lo que se está tratando de lograr en el desarrollo de esta, depende de los bases que se construyan en esta etapa, en la Ilustración 11 se puede comprender mejor cómo se articula.

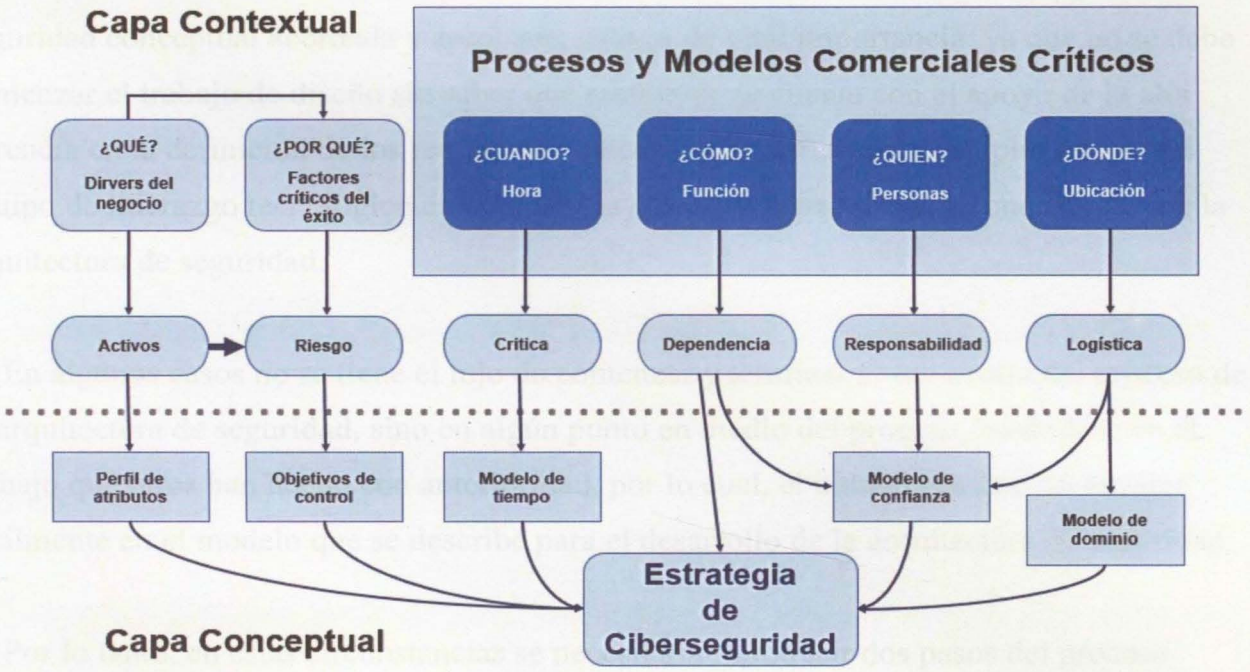

Ilustración 11 Integración de la fase de estrategia y concepto

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

La descripción de lo que está tratando de proteger a nivel organizacional está incorporada en los elemento de valor de la organización, estos son vistos como los activos cuando se realiza una evaluación de riesgo, esta última examina cuales están en riesgo, también está estrechamente vinculado a los factores críticos de éxito para la organización.

Las preguntas sobre cuándo, cómo, quién y dónde se refieren a una serie de procesos críticos y modelos de negocio, estos ponen de manifiesto aspectos del modelo de negocio que se ocupan de temas como la criticidad, la dependencia, la responsabilidad y la logística.

11.9.2. Fase de diseño

De acuerdo a Sherwood (2005), la fase de diseño se debe iniciar con una arquitectura de seguridad conceptual acordada y aprobada, esto es de vital importancia, ya que no se debe comenzar el trabajo de diseño sin saber que realmente se cuenta con el apoyo de la alta gerencia en la definición de los requisitos y necesidades, así como, el amplio apoyo del equipo de liderazgo tecnológico en acordar los enfoques estratégicos y conceptuales de la arquitectura de seguridad.

En algunos casos no se tiene el lujo de comenzar y terminar el desarrollo del proceso de la arquitectura de seguridad, sino en algún punto en medio del proceso, basándose en el trabajo que otros han hecho con anterioridad, por lo cual, el trabajo puede o no encajar fácilmente en el modelo que se describe para el desarrollo de la arquitectura de seguridad.

Por lo tanto, en estas circunstancias se necesitaría introducir dos pasos del proceso adicionales:

- Revisar y validar los requisitos de la organización (arquitectura de seguridad contextual).

- Revisar y validar la arquitectura de seguridad conceptual.

Una vez más, es el momento de recordar los elementos de la matriz de SABSA que deben abordarse en la fase de diseño. Estos se reproducen en la Tabla 6.

Tabla 6 Las capas lógica, física, de componentes y operativa de la matriz SABSA

	Bienes (Qué)	Motivación (Por qué)	Proceso (Cómo)	Personas (Quién)	Ubicación (Dónde)	Hora (Cuándo)
Lógico	Modelo de información comercial	Políticas de seguridad	Servicios de seguridad	Esquema de entidad y perfiles de privilegio	Definiciones y asociaciones de dominios de seguridad	Ciclo de procesamiento de seguridad
Físico	Modelo de datos comerciales	Reglas de seguridad, prácticas y procedimientos	Mecanismos de seguridad	Usuarios, aplicaciones y la interfaz de usuario	Infraestructura de plataforma y red	Ejecución de estructura de control
Componente	Estructuras de datos detalladas	Normas de seguridad	Productos y herramientas de seguridad	Identidades, funciones, acciones y ACL	Procesos, modos, direcciones y protocolos	Paso de seguridad Tiempo y secuencia
Operacional	Aseguramiento de la continuidad operacional	Manejo de riesgos operacionales	Servicio de Seguridad de Gestión y Soporte	Soporte de aplicaciones y gestión de usuarios	Seguridad de sitios, redes y plataformas	Programa de operaciones de seguridad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Entregables de arquitectura lógica

- Arquitectura de políticas de seguridad: un modelo jerárquico de la documentación de políticas y cómo encajan.

- Las políticas de seguridad individuales, las plantillas y directrices para su elaboración.

- Una lista y una descripción de los servicios de seguridad lógicos que se proporcionarán dentro de la arquitectura de seguridad con un mapeo a los objetivos de control y las principales estrategias de seguridad.

- El esquema de la organización que se aplicará en el directorio (lógico), con modelos para perfiles de privilegios, autorizaciones, atributos de autenticación, etc.

- Los dominios de seguridad específicos con una descripción de su composición lógica, sus características individuales de las políticas de seguridad y las asociaciones de seguridad que existen dentro del dominio.

- Una descripción del ciclo de procesamiento de seguridad lógica.

- Un programa de mejoras para obtener ventajas a corto plazo del programa de arquitectura de seguridad.

Entregables de arquitectura de seguridad física

- Un modelo de datos operacionales actualizado que describa los nuevos tipos de datos requeridos por la arquitectura de seguridad (como contraseñas, nombres de usuario, certificados, etc.).

- Una declaración de las reglas de seguridad, prácticas y procedimientos que serán requeridos, en esta etapa no se escribirán los detalles de los procedimientos y prácticas; solo aquellos que serán necesarios para implementar las políticas definidas en la capa lógica.

- Una lista de los mecanismos de seguridad que se necesitarán para implementar la seguridad lógica, se utilizarán en diferentes contextos para el mismo servicio y una indicación de dónde se debe seleccionar cada mecanismo utilizado. Sin embargo, el número de tipos de mecanismos de seguridad debe minimizarse para evitar la complejidad y para proporcionar genéricos, reutilizables, aproximaciones modulares a la implementación de nuevas infraestructuras y aplicaciones.

- Una lista de aplicaciones y usuarios con un diseño de interfaz de usuario de seguridad para cada tipo. En el futuro a medida que se agreguen más aplicaciones, es posible que deba actualizarse. Como con los mecanismos de seguridad, se debe minimizar el número de tipos de interfaz de usuario. Un módulo de interfaz de usuario con una aplicación definida sería un buen enfoque arquitectónico.

- El diseño físico de las plataformas y redes, probablemente en una forma esquemática, que defina el número de cajas físicas, líneas de comunicaciones físicas y elementos de equipos de redes físicas: cuántos, qué tipo y dónde.

- Una declaración de la planificación de la capacidad, dado el rendimiento de los dispositivos, el procesamiento, el poder de las computadoras y el ancho de banda de las líneas de comunicaciones.

- Una descripción del modelo de resiliencia proporcionado por la redundancia de cajas y conexiones, el modelo de resiliencia es integral al modelo de diseño físico, proporcionando capacidad redundante en configuraciones resilientes.

- El modelo de ejecución de la estructura de control necesario para ejecutar el procesamiento lógico de seguridad.

Entregables de la arquitectura de seguridad de componentes

- Un diccionario de datos actualizado que define las reglas de sintaxis de todas las estructuras de datos requeridas por la arquitectura de seguridad.

- Un marco para los estándares de seguridad y una lista de todos los que se requieren.

- Una lista con descripciones y especificaciones de todas las tecnologías, productos y herramientas que se han seleccionado, con orientación para los equipos de proyecto sobre cómo, por qué, dónde y cuándo deben ser utilizados.

- Un esquema de nombres y un marco para definir roles, identidades, perfiles de privilegios de acceso (también conocido como permisos o autorizaciones), funciones y acciones autorizadas, orientación sobre la construcción de listas de control de acceso que representan estos parámetros.

- Diseño detallado de la infraestructura de seguridad, incluidos los procesos de aplicación a ejecutar, los nodos de la plataforma en los que se alojarán, el manejo de ambos esquemas de direccionamiento lógicos, físicos y los protocolos que se utilizarán en los procesos.

- Especificación detallada de pasos de procedimiento y secuencias necesarias para implementar el modelo de ejecución de la estructura de control.

Entregables de arquitectura de seguridad operacional

- Marco para la garantía de continuidad operativa:

    - Proceso de recolección de requerimientos del negocio.
    - Esquema de clasificación de la información.
    - Proceso o programa de gestión de la continuidad del negocio.
    - Proceso de gestión de la seguridad de la información.
    - Proceso de gestión de integridad de sistemas.
    - Proceso de gestión de la seguridad de la base de datos.
    - Proceso de gestión de la integridad del software.
    - Proceso de gestión de integridad y seguridad de productos y herramientas.

- Marco de gestión del riesgo operacional:

    - Proceso de evaluación de riesgos empresariales.
    - Proceso de formulación de políticas corporativas.
    - Proceso de medición, métricas.
    - Marco de garantía de seguridad.
    - Proceso de auditoría de seguridad.
    - Proceso detallado de formulación de políticas.

- Seguimiento del cumplimiento de políticas.
- La recolección de información.
- Evaluación de vulnerabilidades.
- Evaluación de amenazas.
- Pruebas de penetración.
- Investigación en curso sobre amenazas y vulnerabilidades.
- Proceso de gestión de notificaciones CERT.

- Gestión de servicios de seguridad y marco de soporte:
  - Programa de gestión de seguridad de la información.
  - Proceso de respuesta a incidentes.
  - Proceso de recuperación de desastres.
  - Proceso de control de cambios.
  - Servicio de detección de intrusos.
  - Servicio de seguimiento de eventos.
  - Programa de desarrollo de procesos de seguridad.
  - Proceso de gestión del servicio de seguridad.
  - Programa de controles de desarrollo.
  - Proceso de gestión de la configuración.
  - Procedimientos operacionales, incluyendo.
    - Definición de la regla.
    - Gestión de claves.
    - Mantenimiento de ACL.
    - Administración de respaldo.
    - Información forense.
    - Administración de registro de eventos.
    - Administración de antivirus.
  - Proceso de adquisición de productos.

- Proceso de gestión operativa.
- Proceso de gestión de proyectos.

- Gestión de aplicaciones y marco de soporte de usuarios:

  - Estructura de la organización de gestión de la seguridad empresarial:
    - Roles
    - Estructura de informes.
    - Responsabilidades.
  - Programa de formación en seguridad, sensibilización y desarrollo cultural.
  - Marco de gestión de privilegios de acceso (permisos):
    - Definiciones de perfiles basadas en roles.
    - Gestión de identidad de usuario y registro.
    - Administración de cuentas de usuario y privilegios.
    - Revisiones de personal.

- Sitios, redes y plataformas del marco de gestión de seguridad:

  - Gestión de operaciones de campo de negocios.
  - Gestión de dominio de seguridad.
  - Administración y gestión de seguridad de aplicaciones.
  - Gestión de la seguridad de la red.
  - Gestión de la seguridad del sitio.
  - Gestión de plataformas, estaciones de trabajo y equipos de seguridad.

- Marco para la gestión del calendario de operaciones de seguridad:

  - Calendario de negocios y gestión de horarios.
  - Gestión de horarios de operaciones de seguridad.

- Gestión de plazos de entrega y de corte.
- Gestión de la dependencia del tiempo:
  - Ciclo de vida de la contraseña.
  - Ciclo de vida de la cuenta.
  - Clave criptográfica del ciclo de vida.
  - Definición del contexto dependiente del tiempo para el control de acceso.
- Secuenciación de operaciones.

A continuación la Ilustración 12, muestra como el autor de la metodología cómo se integran la estrategia y el proceso de concepto con la fase de diseño (seguridad lógica, física, componentes y operacional):

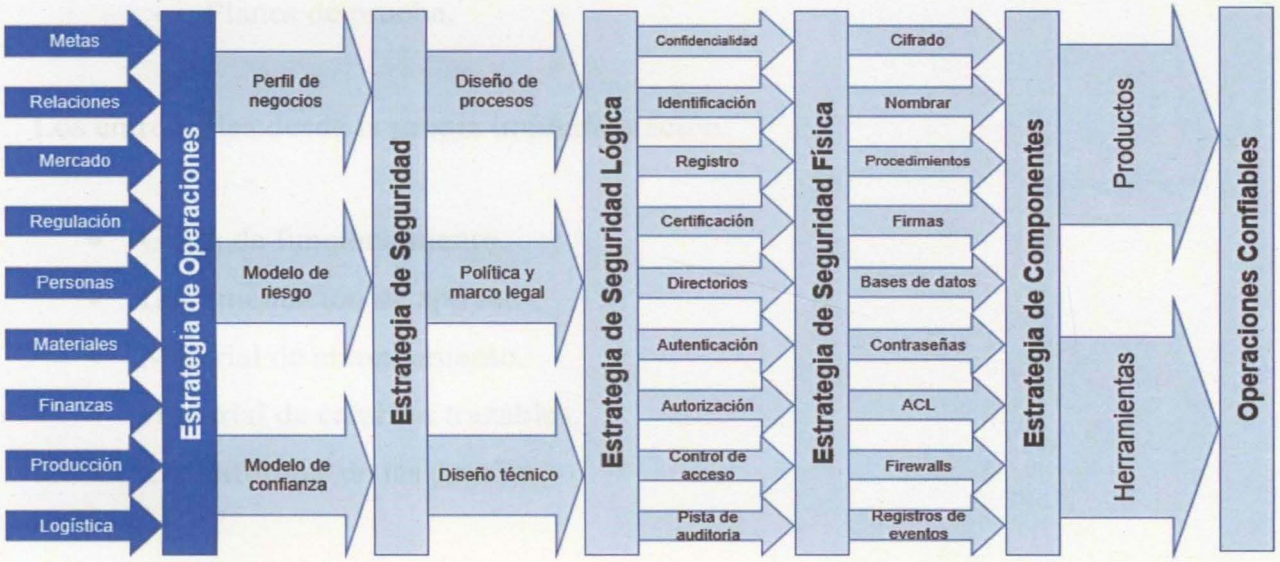

Ilustración 12 Cómo se integran la estrategia y el proceso de concepto / diseño

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

11.9.3. Fase de implementación

Sherwood plantea dentro de la fase de implementación el problema de la gobernanza de la arquitectura, garantizando el cumplimiento de la misma.

- Los entregables claves incluyen:
    - Los planes de implementación:
        - Planes de adquisiciones.
        - Planes de gestión del cambio.
        - Planes de proyecto.
        - Planes de calidad.
        - Planes de prueba.

- Los entregables desde la propia implementación:
    - Guías de funcionamiento.
    - Documentación de apoyo.
    - Material de entrenamiento.
    - Historial de cambios trazables.
    - Los informes de las pruebas.

11.9.4. Fase de gestión y medición

La fase final del ciclo de vida de SABSA es administrar y medir, aquí es donde se ve la arquitectura en operación de acuerdo al modelo de Sherwood (2005).

Cuando observa el costo total de la arquitectura de seguridad, aquí es donde la mayor parte del costo se encuentra. En grandes organizaciones, el costo de administrar es alto.

Cuando el arquitecto diseña algo, quizás la pregunta más importante que debe hacer la dirección es: ¿cuánto costará operar esto? por lo general, será mucho más de lo que costará diseñarlo y construirlo.

La "medida" de esta fase también es de importancia crítica, parte de las operaciones de la arquitectura de seguridad debe ser un proceso mediante el cual puede medir el rendimiento en relación con el diseño de objetivos incorporados en el perfil de atributos de la organización, el propósito de estas medidas es proporcionar retroalimentación al equipo directivo superior.

- Para los subprocesos más importantes en la fase de gestión y medición los entregables clave son:

    - Informes operacionales.
    - Informes de eventos.
    - Informes de incidentes.
    - Informes de ensayos de penetración.
    - Informes de análisis de brechas.
    - Plan de mejoras del programa.

Finalmente, la arquitectura de seguridad debe mantenerse, a medida que el tiempo avance habrá nuevos negocios, requisitos, imprevistos, novedades, entre otros.

También habrá lecciones aprendidas de la experiencia que muestran en retrospectiva si se podría haber hecho las cosas de manera diferente para una mejor ventaja, y en algunos casos esto impulsará cambios en el pensamiento y en las soluciones elegidas; para adaptar todo esto, también se necesitará un proceso de mantenimiento de la arquitectura.

12. Análisis de la arquitectura de seguridad actual del Ejército Nacional

El Ejército Nacional es una entidad del Estado que tiene como misión "conducir operaciones militares orientadas a defender la soberanía, la independencia y la integridad territorial y proteger a la población civil y los recursos privados y estatales para contribuir a generar un ambiente de paz, seguridad y desarrollo, que garantice el orden constitucional de la nación". (Ejército Nacional de Colombia, 2020).

Para ello, la institución tiene dentro de sus pilares organizacionales generar planes, proyectos y programas, encaminados a la protección de la información en todos los niveles de la organización para proteger el desarrollo de las operaciones militares propias de la organización las cuales tienen como propósito el cumplimiento de la misión y visión en el corto, mediano y largo plazo.

Derivado de lo anterior, el Ejército Nacional a través de la Directiva Permanente 00201/2017 imparte instrucciones y lineamientos de ciberseguridad y ciberdefensa para la Fuerza con el fin de actualizar políticas que permitan la aplicación de las capacidades en el ciberespacio. (Departamento de Comunicaciones CEDE6 del Ejército Nacional, 2017).

Con la creación del Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa (CAOCC), surge el Grupo de Apoyo Operacional de Comunicaciones y Ciberdefensa (GAOCC), el cual tiene como propósito "emplear las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales". (Grupo de Apoyo Operacional de Comunicaciones y Ciberdefensa, 2020).

Aunado a lo anterior, el Área de Ciberseguridad hace parte del GAOCC, desde esta unidad de capacidad de gestión de ciberdefensa se pretende defender los activos informáticos ejecutando acciones que permitan minimizar los riesgos y proteger la

infraestructura y la información digital que viaja a través de la red institucional del Ejército Nacional.

Con la intención de evaluar el estado actual de la seguridad en la institución, se realiza una identificación de los controles adoptados y aplicados en el sistema de seguridad de la información del Ejército Nacional de Colombia para sus procesos.

La selección de los objetivos de control y sus controles se apoyan en los resultados y conclusiones del proceso de valoración y tratamiento de riesgos, requisitos legales o reglamentarios, obligaciones contractuales y requisitos misionales del Ejército Nacional de Colombia en cuanto a la seguridad de la información.

La metodología del Ejército Nacional se basa en lo definido por el Departamento Nacional de la Función Pública en la Guía para la Administración del Riesgo. (Departamento Administrativo de la Función Pública (DAFP), 2011).

De acuerdo a esta metodología el manejo de los riesgos está dado por la ejecución de las siguientes actividades y las políticas de administración del riesgo, la ilustración 13 muestra estas actividades:

Ilustración 13 Metodología de gestión de riesgos

Fuente: Recuperado de (Organización Internacional de Normalización (ISO), 2018)

Para evaluar los riesgos en la institución se realizó una calificación inicial, correspondiente a los riesgos inherentes, es decir sin controles, teniendo en cuenta las matrices de impacto y probabilidad definidas por la institución. A continuación se presenta un resumen del ejercicio:

Tabla 7 Evaluación de la probabilidad e impacto de los riesgos Ejército Nacional

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)					
Improbable (2)				8 12	
Posible (3)			13	5 11 17	
Probable (4)			4	9 10 14 15	
Casi seguro (5)		19	16 18	1	2 3 6 7

Fuente. Elaboración propia

En la matriz del riesgo adoptada se observa la exigencia de llevar los riesgos a niveles mínimos de probabilidad e impacto, para que sean aceptados por la institución, evidenciando una postura conservadora ante el riesgo, lo cual es consecuente con la misión del Ejército y su contexto; teniendo en cuenta principalmente los factores gubernamentales donde existen muchas fuentes de amenazas y regulatorios que exigen el cumplimiento de mejores prácticas en seguridad de la información.

La evaluación del riesgo arroja como resultado, riesgos ubicados en los cuadrantes: catastrófico, mayor / casi seguro - probable, lo que evidencia que la probabilidad y el

impacto de la materialización de un riesgo comprometería en gran medida el cumplimiento de los objetivos de la institución, razón para colocar controles eficientes para llevar a un nivel aceptable dichos riesgos.

Los objetivos de control y controles que se seleccionaron para el ejercicio se eligieron con base en el Anexo A de la norma ISO 27001:2013, así:

Tabla 8 Evaluación controles Ejército Nacional

CONTROLES	COMENTARIO / JUSTIFICACION
A.5 POLÍTICA DE SEGURIDAD	
A.5.1 Política de Seguridad de la Información Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos misionales, con las leyes y reglamentos pertinentes.	
A.5.1.1 Conjunto de políticas para la seguridad de la información.	El Ejército Nacional identificó los grupos de activos de información y los riesgos de seguridad de la información para el alcance, en tal sentido es necesario establecer una política de seguridad de la información para informar y sensibilizar a todos el personal militar, civil y partes interesadas sobre los riesgos a los que están expuestos los activos, así como los controles implementados para evitar la materialización de estos riesgos sobre los activos de información.
A.5.1.2 Revisión de las políticas para la seguridad de la información.	La política de seguridad de la información del Ejército Nacional deberá ser periódicamente revisada por la dirección, para asegurar su idoneidad con respecto a los activos de información y los riesgos identificados. Está política debe ser comunicada a todas las partes interesadas.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
A.6.1 Organización Interna Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la institución.	
A.6.1.1 Asignación de roles y responsabilidades para la seguridad de la información	El Ejército Nacional por medio de la política de seguridad de la información establece su compromiso, distribución y asignación de responsabilidades para su cumplimiento, velando por mantener protegidos sus activos de información a través de la separación de funciones, salvaguardando el contacto con las autoridades y con grupos de interés especiales, en razón de lo expuesto, es importante establecer controles para la alineación interna de seguridad de la información.
A.6.1.2 Separación de deberes / tareas	
A.6.1.3 Contacto con las autoridades.	
A.6.1.4 Contacto con grupos de interés especiales	
A.6.1.5 Seguridad de la información en la gestión de proyectos	

CONTROLES	COMENTARIO / JUSTIFICACION
A.6.2.1 Política para dispositivos móviles	El Ejército Nacional desarrolla actividades misionales y en pro de su cumplimiento ha para el desarrollo de sus actividades, en razón de lo expuesto, es necesario establecer controles para asegurar y acreditar la seguridad de la información de la institución al momento de utilizan dispositivos móviles. Adicionalmente se permite al personal el ingreso de dispositivos móviles que pueden ser utilizados para conectarse a los servicios de la red o almacenar información, requiriéndose controles para garantizar la seguridad de la información.
A.6.2.2 Teletrabajo	El Ejército Nacional dentro del desarrollo de sus actividades misionales requiere que el personal labore fuera de las instalaciones y demanda una conexión remota para acceder a la información, en razón de lo expuesto, es necesario establecer controles de seguridad para el trabajo remoto.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	
A.7.1 Antes de asumir el empleo Objetivo: Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.	
A.7.1.1 Selección e investigación de antecedentes	Para el desarrollo de las actividades del Ejército Nacional se requiere contratar personal militar y civil, el cual va a tener acceso a los activos de información de la institución, por tanto es importante implementar controles basándose en los reglamentos, la ética y las leyes pertinentes, que aseguren un proceso de investigación y verificación de antecedentes, asignación de roles y responsabilidades, términos de la contratación y condiciones laborales previo acceso a los activos de información. Las condiciones se establecerán en un contrato que incluirán, pero sin estar limitado, acuerdos de confidencialidad, propiedad intelectual para los trabajos realizados y devolución de activos de información.
A.7.1.2 Términos y condiciones del empleo	
A.7.2 Durante la ejecución del empleo Objetivo: Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.	
A.7.2.1 Responsabilidades de la dirección	El personal del Ejército Nacional en el desarrollo de las actividades para las cuales fueron contratados interactúan permanentemente con los activos de información, por tal motivo es necesario establecer controles para asegurar que son conscientes de los riesgos, responsabilidades y deberes relacionados con la seguridad de la información; igualmente es necesario capacitar y generar conciencia al personal permanentemente en temas de seguridad de la información según sea pertinente para sus funciones laborales. Además es preciso establecer un proceso disciplinario que permita a la institución conocer la forma de actuar en caso de la violación de la seguridad por parte del personal y/o contratistas, sin embargo para evitar al máximo que se presenten incidentes el área de talento humano exigirá a los colaboradores el cumplimiento de las políticas y procedimientos establecidos por la Fuerza.
A.7.2.2 Toma de conciencia, educación y capacitación en seguridad de la información	
A.7.2.3 Proceso disciplinario	
A.7.3 Terminación y cambio de empleo Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.	

CONTROLES	COMENTARIO / JUSTIFICACION
A.7.3.1 Terminación o cambio de responsabilidades de empleo	El Ejército Nacional en el desarrollo normal de sus actividades vincula, desvincula o cambia de cargo, ocupación o empleo a personal militar y civil, y contratistas, por esta razón es necesario establecer controles que permitan asegurar la protección de la información para que los permisos y derechos de acceso sean actualizados, cuando se presentan estas circunstancias.
A.8 GESTION DE ACTIVOS	
A.8.1 Responsabilidad de los activos Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	
A.8.1.1 Inventario de activos	El Ejército Nacional identificó los activos de información que le permiten desarrollar su misión, por este motivo es importante identificar sus propietarios, realizar un inventario de los más importantes y certificar su uso apropiado a través de reglas documentadas e implementadas. Por tanto es necesario establecer controles para proteger y asignar responsabilidad sobre sus activos de información.
A.8.1.2 Propiedad de los activos	
A.8.1.3 Uso aceptable de los activos	
A.8.1.4 Devolución de activos	El Ejército Nacional en desarrollo normal de sus actividades vincula, desvincula, cambia de cargo, ocupación o empleo a funcionarios y contratistas, por esta razón es necesario establecer controles que permitan la devolución de los activos al presentarse desvinculación o cambios de empleo o contrato.
A.8.2 Clasificación de información Objetivo: Certificar que la información recibe el nivel de protección adecuado de acuerdo al nivel de importancia asignado por la institución.	
A.8.2.1 Clasificación de la información	El Ejército Nacional en el desarrollo de sus actividades misionales, tiene información de diferentes tipos, esta información no comparte el mismo nivel de importancia, por ejemplo la información financiera o del personal no tiene el mismo nivel de protección que la información concerniente a planeación y estrategia militar, operaciones de inteligencia o acciones del sector defensa, por lo anterior se deben implementar controles y procedimientos que permitan catalogar la información, en el nivel correcto de protección, etiquetado y manejo, con base en la clasificación de la información apoyado en su valor, requisitos legales, importancia y sensibilidad para la Institución.
A.8.2.2 Etiquetado de la información	
A.8.2.3 Manejo de activos	
A.8.3 Manejo de medios Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios	
A.8.3.1 Gestión de medios removibles	El Ejército Nacional en el desarrollo de sus actividades misionales, de inteligencia, de investigación y defensa utiliza medios para el almacenamiento de la información, por ejemplo: correo electrónico institucional, servicios de mensajería, USB, DVD, CD, discos externos entre otros, en razón de lo expuesto, es necesario constituir controles para evitar la materialización de eventos como la divulgación, la modificación, el retiro o la destrucción de los activos sin autorización. Es necesario definir un procedimiento para el manejo de la información contenida en documentos, redes, servidores, PC, correo, correos de voz, fax, entre otros de acuerdo a su clasificación.
A.8.3.2 Disposición de los medios	
A.8.3.3 Transferencia de medios físicos	

CONTROLES	COMENTARIO / JUSTIFICACION
A.9 CONTROL DE ACCESO	
A.9.1 Requisitos misionales para el control de acceso. Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de información.	
A.9.1.1 Política de control de acceso.	El Ejército Nacional en el desarrollo de sus actividades misionales, utiliza activos de información y es necesario definir una política de control de acceso que constituya la normativa para: disuadir el acceso no autorizado a los sistemas de información, bases de datos, servicios de información y documentos físicos. Utilizar técnicas de autenticación y autorización en los accesos de usuarios y protección física que impida el acceso no autorizado. Concientizar a los usuarios respecto a su responsabilidad frente al uso de contraseñas y equipos; sobre otras normativas que avalen la seguridad en el control de acceso lógico y en coordinación con la normativa del acceso físico.
A.9.1.2 Acceso a redes y a servicios de red	El Ejército Nacional para su operación cuenta con redes LAN y WAN, las cuales soportan las actividades de los diferentes usuarios, estableciendo la necesidad de implantar controles de seguridad para certificar que los usuarios solo tienen acceso a las redes y servicios para los cuales están autorizados.
A.9.2 Gestión de acceso de usuarios Objetivo: Asegurar el acceso de los usuarios facultados y evitar el acceso no autorizado a sistemas y servicios.	
A.9.2.1 Registro y cancelación del registro de usuarios.	Los funcionarios o contratistas del Ejército Nacional manejan diferentes tipos de activos de información, determinando la necesidad para definir los controles que establezcan las actividades necesarias para la creación y la eliminación de usuarios, la asignación de privilegios, la administración de contraseñas y la revisión periódica de los derechos de acceso de los usuarios.
A.9.2.2 Suministro de acceso de usuarios.	
A.9.2.3 Gestión de derechos de acceso privilegiado.	
A.9.2.4 Gestión de información de autenticación secreta de usuarios.	
A.9.2.5 Revisión de los derechos de acceso de usuarios	
A.9.2.6 Retiro o ajuste de los derechos de acceso	El Ejército Nacional en el desarrollo de sus actividades misionales vincula, desvincula o cambia de cargo, ocupación o empleo a funcionarios y contratistas, por esta razón es necesario establecer controles que permitan retirar o ajustar los derechos de acceso a la información al presentarse una desvinculación o cambio.
A.9.3 Responsabilidades de los usuarios Objetivo: Establecer las compromisos y responsabilidades de los usuarios en la protección de su información de autenticación	

CONTROLES	COMENTARIO / JUSTIFICACION
A.9.3.1 Uso de información de autenticación secreta.	El personal del Ejército Nacional es responsable de los activos de información que se encuentran a su cargo, así como de la protección de estos activos en correlación con los principios de confidencialidad, integridad y disponibilidad. En razón de lo expuesto, es necesario definir responsabilidades claras en cuanto a la información para autenticarse, la cual es secreta para evitar el acceso de usuarios no autorizados y el uso inadecuado de la información.
A.9.4 Control de acceso a sistemas, aplicaciones y a la información Objetivo: Evitar el acceso no autorizado a la información, sistemas y aplicaciones.	
A.9.4.1 Restricción de acceso a la información.	El Ejército Nacional tiene información que se encuentra almacenada en servidores, conformada por archivos y bases de datos, en razón de lo expuesto, es necesario restringir el acceso a la información por parte de los usuarios conforme con la política de control de acceso y establecer controles para la administración de los accesos y la definición de una política para el uso de programas que podrían ser peligrosos para la seguridad de la información. El Ejército Nacional también cuenta con información física sobre la cual es necesario definir controles de acceso.
A.9.4.2 Procedimiento de ingreso seguro	
A.9.4.3 Sistema de gestión de contraseñas.	
A.9.4.4 Uso de herramientas de administración de sistemas utilitarios privilegiados	
A.9.4.5 Control de acceso a códigos fuente de programas	El Ejército Nacional desarrolla interna y externamente software para la gestión de su información y mantiene el código fuente en servidores que deben ser protegidos de accesos no autorizados. También cuenta con proveedores de desarrollo quienes tienen a su cargo la custodia del código fuente y deben definirse acuerdos contractuales para su adecuada gestión y aseguramiento.
A.10 CIFRADO Y CRIPTOGRAFIA	
A.10.1 Controles criptográficos Objetivo: Asegurar el uso correcto y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.	
A.10.1.1 Política sobre el uso de controles criptográficos.	El Ejército Nacional en el desarrollo de sus actividades misionales, maneja información que puede tener un alto grado de criticidad y es necesario proteger la integridad y confidencialidad de la misma por medio de la implementación y gestión de controles criptográficos. Las claves para descifrar la información deben ser salvaguardadas para evitar un acceso no autorizado y también para evitar que las mismas se extravíen imposibilitando la recuperación de la información cifrada para hacerla legible.
A.10.1.2 Gestión de claves o llaves.	
A.11 SEGURIDAD FÍSICA Y AMBIENTAL	
A.11.1 Áreas seguras Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la institución.	

CONTROLES	COMENTARIO / JUSTIFICACION
A.11.1.1 Perímetro de seguridad física	El Ejército Nacional para el desarrollo de sus actividades misionales cuenta con una infraestructura física, donde se ubican los activos de información susceptibles de daño y tiene áreas de mayor confidencialidad, por lo expuesto anteriormente es importante establecer los controles de seguridad para evitar el acceso físico no autorizado, el daño a la infraestructura y activos de información de la institución.
A.11.1.2 Controles de acceso físico.	
A.11.1.3 Seguridad de oficinas, despachos, recursos, recintos e instalaciones.	
A.11.1.4 Protección contra amenazas externas y ambientales.	
A.11.1.5 Trabajo en áreas seguras.	
A.11.1.6 Áreas de carga, descarga y acceso público.	Los Complejos Militares tienen un área de carga y despacho especializada para ingresar los pedidos de los proveedores. Por lo tanto es necesario contar con controles para controlar el acceso a esta área y evitar accesos no autorizados a otras áreas.
A.11.2 Seguridad de los Equipos Objetivo: Prevenir la pérdida, daño, robo o compromiso de los activos y la interrupción de las operaciones de la institución.	
A.11.2.1 Ubicación y protección de los equipos.	El Ejército Nacional en el desarrollo de sus actividades misionales, utiliza equipos como servidores, computadores de escritorio, portátiles, impresoras, fotocopiadoras, faxes, escáneres, entre otros, como también redes de comunicaciones, en estos equipos y servicios de red se procesa y transmite la información de la institución, por esta razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo de cableado y equipos, tanto dentro como fuera de la institución.
A.11.2.2 Servicios de suministro	
A.11.2.3 Seguridad del cableado.	
A.11.2.4 Mantenimiento de equipos.	
A.11.2.5 Salida de activos o retiro de equipos fuera de las instalaciones	
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	
A.11.2.7 Disposición segura o reutilización de equipos y dispositivos de almacenamiento.	
A.11.2.8 Equipos de usuario desatendido	El Ejército Nacional en el desarrollo de sus actividades misionales, maneja información en equipos de usuario final o impresos, que puede tener un alto grado de criticidad, por tanto es necesario proteger la confidencialidad, integridad y disponibilidad de la misma por medio de controles que impidan su uso indebido o inadecuado a causa de negligencia o descuido.
A.11.2.9 Política de puesto o escritorio limpio y bloqueo de pantalla o pantalla limpia	
A.12 SEGURIDAD OPERATIVA	
A.12.1 Responsabilidades y Procedimientos operacionales Objetivo: Asegurar el correcto funcionamiento de las operaciones en las instalaciones de procesamiento de información.	

CONTROLES	COMENTARIO / JUSTIFICACION
A.12.1.1 Procedimientos de operación documentados	El Ejército Nacional en el desarrollo de sus actividades misionales, opera diferentes sistemas para el procesamiento de la información, en razón de lo expuesto, es importante establecer controles de seguridad, procedimientos de operación, control de cambios que incluyan identificación, planificación, evaluación, aprobación, comunicación, pruebas y contingencias. Conjuntamente es necesario establecer y monitorear los límites mínimos de capacidad de los dispositivos y la separación de las actividades de desarrollo y pruebas de los ambientes de producción.
A.12.1.2 Gestión de cambios.	
A.12.1.3 Gestión de capacidad.	
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.	
A.12.2 Protección contra código malicioso Objetivo: Asegurar que la información y los sistemas de procesamiento de información estén protegidas contra código malicioso.	
A.12.2.1 Controles contra código malicioso.	El Ejército Nacional en el desarrollo de sus actividades misionales, utilizan servicios como internet, medios extraíbles, los cuales son susceptibles de introducir código malicioso, afectando el correcto funcionamiento de los activos de información, en razón de lo expuesto, es importante establecer controles de seguridad que permitan identificar y evitar la acción de los códigos maliciosos, conjuntamente se debe tener un procedimiento de concientización de los funcionarios y usuarios.
A.12.3 Copias de respaldo Objetivo: Proteger a la Institución contra la pérdida de información y datos.	
A.12.3.1 Copias de respaldo de la información	La información del Ejército Nacional se encuentra ubicada en los equipos asignados a los funcionarios, archivadores, escritorios y servidores, en razón de lo expuesto, es importante establecer controles de seguridad que certifiquen la ejecución de los procedimientos de copias de respaldo y recuperación, y faciliten su restauración de la información en un tiempo acorde con las necesidades, ante la materialización de una amenaza y permitir a la institución continuar con sus actividades diarias, perdiendo la mínima información posible.
A.12.4 Registro de actividades y Monitoreo Objetivo: detectar actividades de procesamiento de la información no autorizadas.	
A.12.4.1 Registro y gestión de eventos.	El Ejército Nacional para el desarrollo de sus actividades cuenta con funcionarios que tienen acceso a los diferentes activos de información, en razón de lo expuesto, es importante establecer controles de seguridad que permitan la identificación oportuna de actividades no autorizadas de procesamiento de información y herramientas para las investigaciones de incidentes de seguridad de la información.
A.12.4.2 Protección de los registros de información.	
A.12.4.3 Registros de actividad del administrador y del operador.	
A.12.4.4 Sincronización de relojes.	
A.12.5 Control de software en producción Objetivo: Asegurar de la integridad de los sistemas en producción	
A.12.5.1 Instalación de software en producción	El Ejército Nacional en desarrollo de sus actividades, utiliza diferentes sistemas operativos sobre los cuales instala software, en razón de lo expuesto, es importante establecer los controles de seguridad para avalar la protección, control y correcta operación de los sistemas en producción.

CONTROLES	COMENTARIO / JUSTIFICACION
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas	
A.12.6.1 Gestión de las vulnerabilidades técnicas	El Ejército Nacional tiene activos de información tecnológicos, los cuales pueden tener vulnerabilidades de tipo técnico y estar a expuestos a que estas sean explotadas, por esta razón es necesario establecer controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas.
A.12.6.2 Restricciones sobre la instalación de software	En la institución es posible la instalación de software por parte de los usuarios, sobre todo aquellos que tienen permisos especiales, por lo que es necesario definir controles para esta actividad, evitando comprometer la seguridad de la información
A.12.7 Consideraciones sobre auditorias de los sistemas de información Objetivo: Certificar la ejecución segura de las actividades de auditoria sobre los sistemas de información y minimizar su impacto	
A.12.7.1 Controles de auditorías de sistemas de información	El Ejército Nacional tiene sistemas de información que pueden ser objeto de auditoria, como resultado de esta actividad es posible originar un compromiso en la disponibilidad y confidencialidad de la información, en razón de lo expuesto, es importante establecer controles de seguridad que garanticen un apropiado nivel de protección, para minimizar los riesgos interrupción de los sistemas y fuga de información asociados a procesos de auditoría.
A.13 SEGURIDAD DE LAS TELECOMUNICACIONES	
A.13.1 Gestión de la seguridad de las redes Objetivo: Asegurar la protección de la información en las redes e instalaciones de procesamiento de información.	
A.13.1.1 Controles de las redes.	El Ejército Nacional en el desarrollo de sus actividades misionales, tiene redes que soportan todas las actividades ejecutadas por los usuarios, en razón de lo expuesto, es importante establecer controles de seguridad para proteger las redes, la información y su infraestructura de amenazas.
A.13.1.2 Mecanismos de Seguridad de los servicios de red.	
A.13.1.3 Separación de las redes	El Ejército Nacional tiene redes de diferentes tipos, al mismo tiempo, si no están segmentadas o separadas pueden proporcionar accesos no autorizados, creando riesgos en la seguridad de la información, en razón de lo expuesto, es necesario implementar controles para segmentar las redes y proteger estos segmentos de acuerdo a criterios establecidos.
A.13.2 Transferencia o intercambio de la información Interna y con partes Externas Objetivo: Proteger la seguridad de la información transferida dentro y fuera de la Institución.	
A.13.2.1 Políticas y procedimientos de transferencia de información.	El Ejército Nacional en el desarrollo de sus actividades misionales, tiene operaciones de intercambio de información con funcionarios, entidades externas y terceras partes, en razón de lo expuesto, es importante establecer controles de seguridad para certificar que se cumplen las políticas y procedimientos para el intercambio de información.
A.13.2.2 Acuerdos sobre transferencia de información.	El Ejército Nacional, intercambia información entre sus funcionarios, entidades externas y terceras partes para la transferencia de información, en razón de lo expuesto, es necesario establecer acuerdos para mantener la confidencialidad, el no repudio y la integridad de la información durante su transferencia.

CONTROLES	COMENTARIO / JUSTIFICACION
A.13.2.3 Mensajería electrónica.	El Ejército Nacional en el desarrollo de sus actividades misionales, reconoce es necesario tener acceso al correo electrónico y a aplicaciones de mensajería electrónica y redes sociales únicamente para los funcionarios debidamente autorizados.
A.13.2.4 Acuerdos de confidencialidad o no divulgación.	El Ejército Nacional, tiene convenios internos con sus funcionarios, acuerdos con entidades externas y terceras partes para la transferencia de información, en razón de lo expuesto, es necesario establecer acuerdos de confidencialidad para proteger la información.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	
A.14.1 Requisitos de seguridad de los sistemas de información Objetivo: Asegurar que la seguridad sea parte integral de los sistemas de información durante todo su ciclo de vida. Conjuntamente incluye los requisitos para los sistemas de información que prestan servicios sobre redes públicas.	
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información.	El Ejército Nacional ejecuta actividades de desarrollo de software y sistemas de información, que de no examinar los requisitos de seguridad de la información, podría dejar brechas de seguridad que pueden ser aprovechadas por atacantes.
A.14.1.2 Seguridad de las comunicaciones en los servicios y aplicaciones accesibles por redes públicas	El Ejército Nacional comparte información con otras entidades a través de la red, en razón de lo expuesto, es necesario implementar controles para certificar la integridad y confidencialidad de la información. También cuenta con aplicaciones Web, que son accedidas desde la internet y deben ser protegidas contra accesos no autorizados y ataques de negación de servicios.
A.14.1.3 Protección de transacciones y aplicaciones en redes telemáticas	
A.14.2 Seguridad en los procesos de desarrollo y soporte Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de los sistemas de información.	
A.14.2.1 Política de desarrollo seguro	El Ejército Nacional en el desarrollo de sus actividades misionales, contrata o desarrolla software, en razón de lo expuesto, es necesario definir los estándares de desarrollo seguro que apliquen a todo el ciclo de vida del software.
A.14.2.2 Procedimientos de control de cambios en sistemas.	El Ejército Nacional en el desarrollo de sus actividades misionales, contrata o desarrolla software, en razón de lo expuesto, es necesario establecer controles de seguridad para certificar que todos los cambios se controlan, se revisan y se someten a pruebas y no comprometen la seguridad del sistema ni el entorno operativo.
A.14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación.	
A.14.2.4 Restricciones en los cambios a los paquetes de software.	
A.14.2.5 Uso de principios de construcción seguros.	El Ejército Nacional en el desarrollo de sus actividades misionales, contrata o desarrolla software, en razón de lo expuesto, es necesario establecer controles que apliquen los principios de construcción seguros dentro de un ambiente de desarrollo seguro.
A.14.2.6 Ambiente de desarrollo seguro	
A.14.2.7 Desarrollo contratado externamente.	

CONTROLES	COMENTARIO / JUSTIFICACION
A.14.2.8 Pruebas de seguridad durante el desarrollo de los sistemas.	El Ejército Nacional contempla como parte esencial de un desarrollo seguro, dentro de un ambiente seguro, la realización de las pruebas funcionales y de aceptación de los sistemas desarrollados, con procedimientos y criterios establecidos, que incluyen la seguridad de la información.
A.14.2.9 Prueba de aceptación de sistemas	
A.14.3 Datos de prueba Objetivo: Asegurar la protección de los datos usados para pruebas	
A.14.3.1 Protección de datos de prueba	Los datos de prueba para los sistemas en desarrollo normalmente (por su dificultad en la generación) provienen de los ambientes de producción, si no se controlan apropiadamente pueden generar riesgos de revelación no autorizada de la información por tanto es necesario establecer controles sobre los datos de prueba a utilizar.
A.15 RELACIONES CON LOS PROVEEDORES	
A.15.1 Seguridad de la información en las relaciones con los proveedores Objetivo: Asegurar la protección de los activos de información accesibles a los proveedores.	
A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	El Ejército Nacional debe definir normas que aseguren la seguridad de la información por parte de sus proveedores no solo de tecnología si no todos aquellos que tengan acceso a activos de información y las instalaciones.
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	El Ejército Nacional en el desarrollo de sus actividades misionales, debe contratar servicios o adquirir bienes con proveedores, en razón de lo expuestos se deben acordar los requisitos de seguridad entre las partes.
A.15.1.3 Cadena de suministro de tecnología de información y comunicación	El Ejército Nacional en el desarrollo de sus actividades misionales, debe tratar con proveedores que le suministren elementos de tecnología de información y comunicación y a su vez dependan de otros proveedores, deben establecer controles en toda la cadena de suministro incluidos aquellos que subcontraten.
A.15.2 Gestión de la prestación de servicios por proveedores Objetivo: Custodiar el nivel de seguridad de la información y de prestación del servicio en línea a través de acuerdos con proveedores	
A.15.2.1 Seguimiento y revisión de los servicios con proveedores	El Ejército Nacional en el desarrollo de sus actividades utiliza servicios ofrecidos por proveedores, por tal razón se debe asegurar la el monitoreo del cumplimiento de los acuerdos relacionados la seguridad de la información, así como gestionar formalmente los cambios del servicio, considerando los requisitos de los contratos firmados por las partes.
A.15.2.2 Gestión de cambios en los servicios prestados por los proveedores	
A.16 GESTION DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACION	
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad que incluya la comunicación sobre los eventos de seguridad y debilidades.	

CONTROLES	COMENTARIO / JUSTIFICACION
A.16.1.1 Responsabilidades y procedimientos.	El Ejército Nacional tiene activos de información que son susceptibles a tener incidentes de seguridad de la información, en razón de lo expuesto, es importante establecer controles que aseguren que los eventos y debilidades de seguridad de la información son comunicados oportunamente a través de los canales de gestión apropiados al área de seguridad de la información, para su respectiva gestión, en el menor tiempo posible, de acuerdo a las responsabilidades y procedimientos establecidos.
A.16.1.2 Reporte de eventos de seguridad de la información	
A.16.1.3 Reporte de debilidades de seguridad de la información.	
A.16.1.4 Evaluación de eventos de seguridad de la información y sus decisiones	
A.16.1.5 Respuesta a incidentes de seguridad de la información	
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información.	
A.16.1.7 Recolección de evidencia.	
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
A.17.1 Continuidad de la seguridad de la información Objetivo: La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la institución.	
A.17.1.1 Planificación de la continuidad de la seguridad de la información	El Ejército Nacional en el desarrollo de sus actividades misionales, debe gestionar la continuidad de la seguridad de la información para minimizar el impacto generado por un evento disruptivo que disminuya la capacidad de ejecución de sus actividades, en razón de lo expuesto, es necesario establecer controles para la planeación, implementación, verificación, revisión y evaluación de la continuidad de la seguridad de la información.
A.17.1.2 Implementación de la continuidad de la seguridad de la información	
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
A.17.2 Redundancias Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información.	
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	El Ejército Nacional considera conveniente implementar instalaciones de procesamiento de información con elementos redundantes que aseguren la disponibilidad de la información y los servicios ante eventos disruptivos, para no interrumpir la ejecución de sus actividades misionales.
A.18 CUMPLIMIENTO	
A.18.1 Cumplimiento de requisitos legales y contractuales Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	

CONTROLES	COMENTARIO / JUSTIFICACION
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.	El Ejército Nacional en el desarrollo de sus actividades misionales, está obligado a actuar bajo el marco del cumplimiento de la legislación Colombiana, los convenios internacionales, los requisitos contractuales y los propios, en razón de lo expuesto, es importante establecer controles de seguridad que certifiquen el cumplimiento de todos los requisitos legales, convenios internacionales, contractuales y reglamentarios. La evidencia del cumplimiento se mantendrá en registros, los cuales deben ser identificados para su almacenamiento, protección, recuperación, retención y disposición.
A.18.1.2 Derechos de propiedad intelectual.	
A.18.1.3 Protección de registros.	
A.18.1.4 Protección de los datos y privacidad de la información relacionada con los datos personales.	
A.18.1.5 Reglamentación de controles criptográficos.	El Ejército Nacional utiliza técnicas de encriptación para el intercambio de información, en Colombia estas técnicas no están reglamentadas por lo tanto no hay restricciones para usar cualquier técnica disponibles.
A.18.2 Revisiones de seguridad de la información Objetivo: Certificar que la seguridad de la información se implementa y usa de acuerdo con las políticas y procedimientos operacionales.	
A.18.2.1 Revisión independiente de la seguridad de la información	El personal del Ejército Nacional interactúa continuamente con los activos de información que están sujetos a las políticas y controles en materia de la seguridad de la información, en razón de lo expuesto, es importante establecer controles propendan por la revisión del diseño y efectividad de los controles de seguridad de la información y el cumplimiento de las políticas y normas de seguridad tanto técnicas como de gobierno.
A.18.2.2 Cumplimiento con las políticas y normas de seguridad.	
A.18.2.3 Revisión de cumplimiento técnico.	

Fuente. Elaboración propia

Presentando un resumen de la evaluación de los controles y teniendo como referente la información que refleja el mismo, del 100% de la evaluación el 32% de los controles no son efectivos y deben revisados en su diseño, cobertura, aplicación y seguimiento. Así mismo, otro 32% funcionan de manera irregular y deben ser mejorados. El 36% restante de los controles son adecuados tanto en su diseño como en su efectividad.

De acuerdo a lo anterior, a continuación se mencionan algunos de los controles no efectivos, los que deben ser mejorados, y los evaluados como adecuados:

- Controles no efectivos:
    - Cruces periódicos de los usuarios de los servicios informáticos del Ejército Nacional, respecto de los privilegios que tienen en las diferentes plataformas.
    - Extravío de elementos de almacenamiento: revistas periódicas de inventario para PC, servidores y portátiles, y si estos se extravían se implementan las sanciones dispuestas.
    - Capacitación al usuario final para el uso de las herramientas informáticas.
    - Estudio de seguridad para contratación de personal directo o contratistas.
    - Estar a la vanguardia de leyes y regulaciones aplicables para el Ejército.
    - Controles de acceso a los centros de cableado.
    - Cierta información crítica está protegida mediante herramientas para prevención de perdida de información.
    - Centro de cómputo alterno donde sean replicados los activos críticos.
    - Cifrado de información en algunos dispositivos de almacenamiento y en transmisión de correo.
    - Filtro para impedir el ingreso dispositivos electrónicos a las instalaciones.
    - Todos los proyectos TIC deben tener un visto bueno, donde hay un integrante de seguridad que evalúa el proyecto.

- Controles que pueden mejorarse:
    - Pruebas de penetración.
    - Campañas de sensibilización para usuarios finales.
    - Campañas de sensibilización para funcionarios de las áreas de tecnología y seguridad.
    - Capacitación al usuario final para el uso de las herramientas informáticas.
    - Entrenamiento al personal técnico en las herramientas que administra y de acuerdo a su perfil.
    - Funcionarios y terceros que tengan acceso a la información firman acuerdos de confidencialidad.
    - Políticas para el manejo seguro de la información.
    - Planes para renovación tecnológica.
    - Revisiones periódicas de conexiones no autorizadas e inspecciones físicas.
    - Pruebas de ethical hacking a las aplicaciones en la web.

- Controles eficaces: se identificaron controles con calificación satisfactoria, sin embargo estos deben revisarse permanentemente:
    - Seguridad perimetral.
    - Controles de ciberseguridad (correlacionador de eventos, antivirus).
    - Análisis periódico de vulnerabilidades.
    - Bloqueo a usuarios finales para navegar a sitios catalogados como riesgos o no autorizados.
    - Parcheo y actualizaciones.
    - Controles de acceso a las instalaciones.
    - Controles de acceso a los centros de cómputo.
    - Esquema de backups.

Existen más controles preventivos orientados a disminuir la probabilidad, que aquellos correctivos, lo cual es acertado, no obstante para garantizar la mejora continua es recomendable seguir implementando controles preventivos que disminuyan la probabilidad de que ocurra un evento no deseado, cuando esto sea posible, los controles correctivos minimizaran el impacto (en vidas, económico, operativo, cumplimiento, imagen, entre otros).

Dentro de los riesgos residuales calificados con más impacto, se detallan algunos entre ellos los mencionados a continuación:

Tabla 9 Detalle de riesgos Ejército Nacional

Detalle del riesgo	Efectividad controles
El personal técnico no conoce y aplica aspectos de seguridad en el manejo de la información y no tiene conocimientos técnicos para el manejo de activos informáticos correctamente.	No cuenta con controles efectivos
Pérdida/Revelación no autorizada de información sensible, a través de sistemas informáticos y/o en su tratamiento (almacenamiento, procesamiento, borrado), a causa de personal interno de forma accidental o intencional.	No cuenta con controles efectivos
El usuario final de TI no conoce y aplica aspectos de seguridad en el manejo de la información y no tiene conocimientos para el manejo de los activos informáticos con los que interactúa, correctamente.	Cuenta con controles pero no son suficientes
Pérdida/Revelación no autorizada de información sensible, a través de sistemas informáticos o medios análogos, por ataques externos	Cuenta con controles pero no son suficientes
Cambios no controlados en la infraestructura tecnológica y en el software, que afecta la seguridad de la información.	No cuenta con controles efectivos
Se ingresan a las instalaciones y se conectan a las redes de datos de las unidades militares, portátiles, tabletas, etc., personales de los funcionarios.	No cuenta con controles efectivos
Conexión no autorizada de dispositivos a las redes, internet de banda ancha, en unidades militares introduciendo brechas de seguridad o degradando el servicio	No cuenta con controles efectivos

Fuente. Elaboración propia

De acuerdo a lo anterior se evidencia que los controles o no son efectivos, o no se cuenta con los mismos; observando que todavía el Ejército Nacional se encuentra distante de una gestión del riesgo acorde y falta de un sistema de gestión que ayude a proteger sus activos informáticos y por ende la información digital que viaja a través de ellos.

Así mismo, se presenta una matriz DOFA proporcionando una visión amplia del estado de la ciberseguridad del Ejército Nacional, donde se dará a entender los puntos fuertes internos, las características o elementos externos que se pueden aprovechar, los aspectos internos que juegan en contra de la institución y los riesgos externos que deben afrontar la Fuerza.

Tabla 10 Matriz DOFA ciberseguridad Ejército Nacional

DEBILIDADES	OPORTUNIDADES
1. Falta de políticas de seguridad en el dominio, para evitar cambios no autorizados en los equipos. 2. Uso de software para omitir las herramientas de seguridad implementadas. 3. Falta de sensibilización a los usuarios. 4. Falta de personal capacitado para el manejo de las herramientas. 5. Falta de capacitación de ciberseguridad al personal orgánico de la unidad. 6. Falta de coordinación entre las áreas que componen el c5, para el mejoramiento continúo de los procesos. 7. Falta de presupuesto para adquisición y mantenimiento de las herramientas. 8. Falta de continuidad en el personal que se desempeña en el área de ciberdefensa. 9. Los equipos de cómputo de la unidad ya están obsoletos.	1. Realizar revistas a las unidades con el fin de verificar las políticas de ciberseguridad. 2. Dar prioridad al personal de ciberdefensa y ciberseguridad para que se capaciten en los diferentes cursos disponibles. 3. Integrar las herramientas adquiridas para organizar y fortalecer el SOC del Ejército. 4. Crear el CSIRT para la gestión de incidentes. 5. Integrar las capacidades con las unidades cibernéticas de las fuerzas. 6. Participar en los eventos nacionales e internacionales de seguridad en pro de mejorar capacidades del personal que labora en la unidad. 7. Ampliar capacidades del laboratorio forense (herramientas para análisis de vulnerabilidades y pentesting)
FORTALEZAS	**AMENAZAS**
1. Se cuenta con herramientas de ciberseguridad y ciberdefensa para la protección de la infraestructura tecnológica del Ejército. 2. Se cuenta con laboratorio forense para el análisis de malware, análisis de vulnerabilidades, ethical hacking. 3. Integración de los activos informáticos del Ejército con el correlacionador de eventos. 4. El personal con el que cuenta la unidad es idóneo para operar las herramientas adquiridas. 5. La unidad cuenta con soportes legales (directivas) para el cumplimiento de las políticas de seguridad.	1. Falta de doctrina para la implementación de procesos en ciberseguridad y ciberdefensa. 2. Falta de soporte jurídico para realizar operaciones en el ciberespacio. 3. La constante evolución de software malicioso. 4. Falta de infraestructura para garantizar la protección de los activos informáticos de la unidad. (acceso de personal no autorizado) 5. Cumplimiento de las políticas de seguridad en todos los niveles del mando.

Fuente: Elaboración propia.

De acuerdo a lo anterior se llega a varias conclusiones las cuales se presentan a continuación:

1. Es necesario lograr una mayor visibilidad del proceso de seguridad de la información y conseguir el apoyo y compromiso de los altos mandos de la institución para garantizar la obtención de recursos y el apoyo de todas las otras áreas del Ejército Nacional. Es clave transmitir las implicaciones que tiene la seguridad de la información a nivel estratégico y de gobierno corporativo en la Fuerza.

2. El Ejército Nacional requiere la implementación de un sistema de gestión de seguridad de la información que cumpla con los requisitos mínimos. Esto permitirá que los esfuerzos se orienten a los riesgos de acuerdo a su valoración, y estos se mitiguen de forma sistemática, estructurada, repetible y eficiente, adicionalmente se adapten a los cambios internos, externos y las nuevas tecnologías.

3. Muchos de los controles observados y calificados como efectivos se han orientado a proteger los activos de información contra ciberataques o ataques externos, no obstante se observa la necesidad de implementar controles orientados a mitigar los riesgos provenientes de factores de amenazas internas. No sobra citar artículos que transmiten las principales preocupaciones de los profesionales de la seguridad de la información sobre la materialización de riesgos debido a acciones negligentes o por desconocimiento de los empleados de las políticas de seguridad de la información. (Help Net Security, 2015).

4. Las unidades militares del Ejército Nacional, por su cantidad y dispersión geográfica carecen de muchos de los controles que deberían funcionar efectivamente, por lo que se sugiere trabajar para lograr un diseño de una arquitectura de ciberseguridad integral que permita proteger de forma organizada los activos; y así, mitigar los riesgos identificados de la institución.

13. Propuesta arquitectura de seguridad objetivo

13.1. Estrategia y concepto

Es el desarrollo de las dos primeras capas (contextual y conceptual) del modelo de arquitectura de ciberseguridad propuesta basada en el modelo SABSA de Sherwood (2005), la estrategia y concepto significa comprender los problemas de ciberseguridad del Ejército Nacional para crear una visión estratégica y un conjunto de esquemas, métodos e ideas para resolverlos.

13.1.1. Arquitectura de seguridad contextual

La arquitectura de ciberseguridad contextual se relaciona y depende del contexto en que se creará y utilizará, las condiciones y circunstancias en que se necesita teniendo en cuenta la misión del Ejército Nacional, esto significa que se deberá investigar, examinar y analizar todos los aspectos del contexto de la institución que crean la necesidad de tener una óptima ciberseguridad.

La estrategia de negocios, los objetivos, las relaciones, los riesgos, las restricciones y los habilitadores dicen mucho sobre qué tipo de arquitectura de ciberseguridad necesita la institución.

Necesidades del Ejército Nacional para la ciberseguridad

Dentro de las actividades que lleva a cabo actualmente el Ejército Nacional, las cuales están encaminadas al cumplimiento de los objetivos misionales, estratégicos, operacionales y de apoyo de la institución; las tecnologías de la información y las comunicaciones se han convertido en un medio importante a la hora de desarrollar los mismos, donde los medios tecnológicos e informáticos empleados son cada día más indispensables para el óptimo

desempeño de la Fuerza y por ende representan un aspecto importante a ser asegurado por parte de los altos mandos.

- Esto dice que: la institución depende en un gran porcentaje de las TIC.
- Lo que debe significar que: la institución depende en su gran mayoría del uso de la información digital.

Para proteger esta información digital y las capacidades de procesamiento de la misma, se necesitara gestión de la ciberseguridad. Para ello, es importante conocer la definición de la misma de acuerdo al Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC):

> Conjunto de respuestas que un Estado y/o entidad estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social, con el fin de garantizar la protección de los intereses esenciales de los mismos y de los derechos de los residentes en el territorio bajo su jurisdicción. En otras palabras, su objetivo es gestionar los riesgos que vienen del ciberespacio, relacionados con la información digital y sus sistemas interconectados, donde el ciberespacio se relaciona con internet. (Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, 2014).

La ciberseguridad en esta etapa protege algo que tiene valor claro para la institución. Por lo tanto, para comenzar el proceso de definición de la arquitectura de ciberseguridad de la información para el Ejército Nacional, se debe identificar primero los activos informáticos que se consideran valiosos o que puedan verse afectados por ciberdelincuentes, los cuales deben protegerse proporcionando una seguridad adecuada.

Dependencias críticas para la ciberseguridad

Los sistemas críticos para la ciberseguridad pueden ocasionar perdidas económicas significativas, daños físicos o en el peor de los casos amenazas a la vida humana, implican subsistemas controlados por sistemas informáticos o electrónicos, y son estos los que interesan en esta sección.

Comunicaciones remotas a sistemas críticos para la ciberseguridad

Un aspecto muy importante es asegurar los sistemas de control remoto en la institución, cualquier aplicación de control de procesos que implique el uso de datos remotos, sus comunicaciones corren el riesgo de que un ciberatacante las intercepte y secuestre el control, esto también se aplica a la gestión remota de sistemas informáticos y dispositivos de red, por lo tanto, cualquier aplicación admitida en una computadora o comunicaciones de datos gestionadas de forma remota, es vulnerable a ciberataques.

Los medios para asegurar las comunicaciones remotas y evitar este tipo de ataques se encuentran en el uso de técnicas criptográficas para asegurar la completa autenticidad, algunos protocolos tienen características opcionales estándar para implementar estos mecanismos de seguridad, pero la capacidad de hacerlo depende entonces del soporte del proveedor para aquellos mecanismos que han sido integrados en los dispositivos gestionados.

Aseguramiento de sistemas

Otro aspecto importante de la ciberseguridad con respecto a los sistemas críticos es el de los sistemas de garantía, esto se refiere a alcanzar altos niveles de seguridad de que el sistema ha sido implementado correctamente y funcionará como se espera y como se establece en las especificaciones funcionales. Las áreas de aplicación para el caso de la Fuerza incluyen los sistemas de defensa de seguridad nacional.

Los requisitos de ciberseguridad para las dependencias críticas son exigentes, las TIC's se utilizarán cada vez más para estos tipos de aplicaciones, y es necesario comprender cómo garantizar que los sistemas no están peligro de ser atacados.

Objetivos de negocio, factores de éxito y riesgos operacionales

A continuación se analizarán algunas de las áreas clave donde la institución enfrentará riesgos y es motivado a desarrollar una respuesta de ciberseguridad.

Protección de imagen institucional

La imagen del Ejército Nacional lleva un mensaje de fiabilidad y calidad la cual está estrechamente relacionada con la reputación, esta es una inversión y por lo tanto, debe considerarse como un activo importante a ser protegido. La gestión de la ciberseguridad para este campo juega un papel importante al apoyar el desarrollo global estratégico, táctico y operacional de la institución. Si hay fallas en la seguridad de esto puede llevar a daños en la imagen de la misma.

Prevención del fraude

El fraude está presente en todas partes al mismo tiempo, ocurre en todas las industrias, en todos los tamaños de la organización, en todos los niveles de la jerarquía de gestión, y ha existido durante todo el tiempo que ha habido servicios, transacciones, operaciones, entre otros. Así, un fraude en el cual se hace uso de la de información digital de la institución puede ser solo otra manifestación de un problema antiguo como manipular la información digital para ocultar la deshonestidad y el robo.

El fraude relacionado con las computadoras se comete abusando de los sistemas informáticos de la institución que apoyan sus operaciones (transacciones, aplicaciones institucionales, operaciones cibernéticas, etc.). Los efectos de estos fraudes puede que sean

grandes o pequeños, desde robo de información digital ultrasecreta a gran escala hasta problemas de reclamación, también varían desde el fraude único hasta la colección sistemática fraudulenta de pequeñas y desapercibidas cantidades de información digital.

Los sistemas informáticos son una de las muchas herramientas que pueden usar los ciberdelincuentes para cometer fraude, y en ese sentido, el fraude informático es igual que cualquier otro tipo de fraude, usualmente ocurre en situaciones donde hay una oportunidad (acceso, habilidad y tiempo) combinado con la motivación (necesidad, justificación y posiblemente el desafío).

La ciberseguridad es una de las principales estrategias corporativas y será esencial en el universo de los negocios digitales en contra de los cibercriminales con planes de negocio como el intento de fraude, la extorsión o el robo de propiedad intelectual. (Ciberseguridad L, Estrategia De Negocio C, Gabriela P, Rey G, 2016)

La prevención del fraude debe ser relevante para el Ejército Nacional y se necesita de la ciberseguridad para evitar el abuso de los sistemas informáticos de la institución.

Prevención de pérdidas

Las posibles pérdidas surgen de muchas áreas diferentes de riesgo operacional, la gestión de la ciberseguridad en este punto es una de las áreas de competencia clave y ayudará a gestionar y mitigar una amplia gama de estos riesgos.

Continuidad del negocio

El riesgo más temido con respecto al uso de los sistemas informáticos de la Fuerza, es la falla que lleva a la interrupción de las operaciones, puede conducir a retrasos o en algunos casos, incumplimiento total de las expectativas de nivel de servicio de los clientes (para el caso de la institución, la población civil), proveedores, empleados, operaciones, etc. Si los

servicios de información clave de la institución son interrumpidos, entonces también lo son los procesos que dependen de ellos.

Las interrupciones en el servicio pueden ser causadas por fallas accidentales del sistema, por negligencia intencional, prácticas de mal funcionamiento, o ciberdelincuentes que propician interferencias y sabotajes. Toda la arquitectura de seguridad se debe centrar en respetar el conjunto de requisitos que pueden clasificarse colectivamente en "continuidad del negocio".

Obligaciones legales

El Ejército Nacional tiene muchas obligaciones legales, y el incumplimiento de estas obligaciones representa una importante área de riesgo operacional. Muchas de las leyes y reglamentos tienen una vinculación indirecta con la gestión de la ciberseguridad.

Áreas que se necesitan examinar en los dominios de operación de la institución:

- Cumplimiento del derecho penal.
- Cumplimiento de la ley constitucional.
- Cumplimiento normativo relevante para la defensa nacional.
- Cumplimiento de obligaciones contractuales.
- Gestión y mitigación de responsabilidades legales.

Con el fin de asegurar que la arquitectura de ciberseguridad para el Ejército Nacional tenga en cuenta todos los aspectos legales y controladores regulatorios, se deberá crear un perfil de atributo de negocios que especifique los atributos y métricas relevantes para describir las necesidades de la institución, al hacer esto se necesitará representantes legales que puedan brindar asesoramiento detallado.

Evaluación de riesgo operacional

Modelación de riesgos

El riesgo es un concepto complejo para describir sin un análisis teórico. Por lo tanto es importante conocer la definición de riesgo operacional según J.P Morgan como:

> Riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas o bien aquellas que sean producto de eventos externos. El objetivo de la gestión del riesgo operacional es la identificación, evaluación, seguimiento, control y mitigación de este riesgo. La entidad ha establecido un marco para la gestión del riesgo operacional que comprende las políticas, prácticas, procedimientos y estructura con que cuenta la entidad para su adecuada gestión. Se definen, entre otros aspectos, los procedimientos que utilizará la unidad de riesgo operacional para evaluar la vulnerabilidad de la entidad ante la ocurrencia de eventos de pérdida, comprender su perfil de riesgo operacional y adoptar las medidas correctivas que sean pertinentes. Dado que la efectiva gestión de este riesgo contribuye a prevenir futuras pérdidas derivadas de eventos operativos, la entidad no sólo gestiona el riesgo operacional inherente a productos, actividades, procesos y sistemas vigentes, sino también el correspondiente a nuevos productos, inicio de actividades, puesta en marcha de procesos o sistemas en forma previa a su lanzamiento o implementación. (J.P.Morgan, 2014).

El modelo de riesgo que se deberá adoptar a la institución implicara algunos conceptos básicos:

- Activos cibernéticos: información digital que es de valor y que se desea proteger para en la Fuerza.
- Ciberamenazas: eventos potencialmente dañinos que ponen los activos cibernéticos en peligro.

- Impactos: el resultado potencial de una ciberamenaza que se materializa y causa daños a los activos cibernéticos.
- Vulnerabilidades: debilidades en los procedimientos que harán que la ciberamenaza se materialice y explote un activo cibernético, causando un impacto.

La probabilidad de que ocurra un evento de riesgo es una combinación compleja de:

- Nivel de amenaza (la probabilidad de que el evento de una ciberamenaza se materialice en un período de tiempo determinado).
- Nivel de vulnerabilidad o debilidad (la probabilidad de que un evento de ciberamenaza tenga éxito explotando los activos cibernéticos causando un impacto).

Evaluación de riesgos

Para administrar el riesgo, primero se deberán identificar las fuentes de riesgo (ciberamenazas) y evaluar su importancia (la probabilidad del evento de riesgo y el impacto en los activos cibernéticos, en caso de que se materialicen). La evaluación de riesgos es una parte importante del modelo SABSA, por lo tanto, la institución deberá adoptar una metodología de evaluación de riesgos para desarrollar este modelo.

La evaluación del nivel de amenaza es difícil, en la era de la información digital el mundo es simplemente un lugar peligroso, se deberá reconocer las ciberamenazas, identificarlas y sus fuentes (agentes de amenaza). El acceso a datos fiables, coherentes y completos sobre eventos anteriores, y el análisis estadístico proporciona una guía útil sobre la probabilidad de una ciberamenaza.

Otra forma de evaluar las ciberamenazas es reunir información de la ciberinteligencia y procesar esa información, como se hace en las agencias de aplicación de la ley y de

seguridad nacional, donde se pueden identificar ciertos tipos de amenazas planteadas por ciberdelincuentes, ciberterroristas y similares, ayudará con una amplia gama de riesgos operativos que se basaran en intenciones maliciosas.

La evaluación de las vulnerabilidades (debilidades en la forma en que se opera la institución) y el impacto asociado (el nivel de daño que sufriría si un evento de ciberamenaza explotara con éxito) es mucho más fácil, ya que ambas cosas están dentro del alcance. Así, las metodologías de evaluación de riesgos se centrarán en evaluar aspectos cualitativamente como bajo, medio y alto.

Los pasos para la metodología de evaluación de riesgo deberán ser:

Paso 1: ¿Cuáles son los activos cibernéticos de la institución a proteger?

- Identificar y valorar estos activos cibernéticos.

Paso 2: ¿Qué posibles ciberamenazas ponen en riesgo los activos cibernéticos de la institución?

- Identificar las posibles ciberamenazas.

Paso 3: Para cada amenaza, si se materializa, ¿cuál sería el impacto en los activos cibernéticos en la Fuerza?

- Identificar y cuantificar los impactos al relacionarse con la lista de activos cibernéticos.

Paso 4: Si el impacto es lo suficientemente significativo como para preocuparse, ¿Podría haber algo que permita que esta ciberamenaza explote en los activos cibernéticos causando un impacto?

- Identificar y cuantificar las vulnerabilidades o debilidades.

Paso 5: ¿Puede reducir las vulnerabilidades o debilidades introduciendo control e información adicional?

- Identificar las posibles estrategias de control y cuantificar el costo.

Paso 6: ¿Cuál es el análisis costo / beneficio derivado del nivel de reducción del potencial?

- Cuantificar los beneficios y costos.

Marco de modelado de ciberamenazas

Se necesita una técnica de modelado para ayudar a estructurar la comprensión de las ciberamenazas y que sea lo más informativa posible al intentar enfrentar y preverlas, para lograr esto, se necesita un marco de clasificación de modo que se pueda abordar una lista de verificación de todas las posibles áreas de ciberamenazas reales que se enfrentan, este esquema de clasificación permitirá crear una base de datos de amenazas conocidas y usar esto como un medio para impulsar en síntesis ejercicios específicos de evaluación de riesgos.

Dominios de ciberamenazas

El modelo SABSA de evaluación de riesgos sugiere tres dominios como una primera clasificación de las ciberamenazas y los agentes de amenaza que son relevantes para la evaluación del riesgo operacional. La tabla 11 proporciona más detalles.

- Personas - Procesos - Sistemas

Tabla 11 Dominios de ciberamenazas y agentes de amenazas

Dominio de Ciberamenaza	Descripción del Dominio	Agentes de Amenazas
Personas	Pérdidas causadas por: Violación maliciosa de políticas internas Violación negligente de políticas internas Errores humanos	Empleados actuales Empleados anteriores Personas bajo consideración para empleo Terceros
Procesos	Pérdidas causadas por: Deficiencia en un procedimiento existente Ausencia de un procedimiento adecuado No seguir un procedimiento definido	Empleados Clientes Proveedores Proveedores de servicio Agentes Socios Miembros del público
Sistemas	Pérdidas causadas por: Desglose imprevisto de los sistemas técnicos Insuficiente resistencia en los sistemas técnicos	Falla técnica por mal manejo Falla por malaadministración Falla técnica por inadecuada diseño o implementación deficiente

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Categorías de ciberamenazas

El modelo SABSA sugiere utilizar una serie de categorías de amenazas, la selección de estas categorías se basa únicamente en la experiencia práctica del autor y podrán ser cambiadas sin violar ningún principio teórico específicamente para la institución.

Cada categoría se asigna a uno o más de los dominios de ciberamenaza, no hay una asignación lógica específica de una categoría a los dominios. La categoría y dominio se indican en las columnas 2 a la 5 en la Tabla 12. Si la Fuerza considera necesario agregar nuevas categorías podría hacerlo.

Tabla 12 Taxonomía de las ciberamenazas: la base de datos de amenazas

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Personas	Procesos	Sistemas			
Instalaciones y entorno operativo	*		*	Pérdida o daño a las capacidades operativas causadas por problemas con las instalaciones, instalaciones, servicios o equipos	Interrupción comercial por uno de los muchos posibles escenarios de ciberamenazas	Gestión inadecuada de la continuidad del negocio y recuperación de desastres de las TIC
					Interrupción del servicio de procesamiento de datos	Interrupciones de los sistemas de TIC por recuperación inadecuada
					Interrupción de comunicaciones	Interrupciones de los sistemas de TIC por recuperación inadecuada
Salud y Seguridad	*	*	*	Amenazas a la salud y seguridad personal del personal, contratistas, proveedores, agentes, clientes y miembros del público	Entornos operativos inseguros con riesgos de seguridad no gestionados	Instalaciones deficientes y gestión operativa en salas de operaciones de TIC
					Ciberataques contra individuos	Débil seguridad física y lógica que conduce a la divulgación no autorizada de detalles de direcciones privadas, itinerarios de viaje, etc.
					Falla de sistemas críticos de seguridad	Protección inadecuada para sistemas de control de procesos para procesos automatizados de fábrica, máquinas herramienta, generación de energía, etc., incluidas otras maquinaria especializada

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Persona	Proceso	Sistema			
Seguridad de información	*	*	*	Divulgación o modificación no autorizada de la información, pérdida de disponibilidad de información o uso inapropiado de la información	Divulgación no autorizada de información corporativa confidencial o privada del cliente	Seguridad lógica débil, seguridad física débil y procedimientos operativos débiles
					Modificación, eliminación, duplicación o reproducción no autorizada de información	Seguridad lógica débil, seguridad física débil y procedimientos operativos débiles
					Uso no autorizado o inapropiado de la información corporativa o del cliente	Seguridad lógica débil, seguridad física débil y procedimientos operativos débiles
					Uso no autorizado o inapropiado de la información personal de los empleados	Seguridad lógica débil, seguridad física débil y procedimientos operativos débiles
					Pérdida de disponibilidad de información interna corporativa o del cliente	Inadecuada capacidad de recuperación, respaldo y recuperación en sistemas TIC
					Ciberataques de denegación de servicio que causan pérdida de servicios	Inadecuada seguridad física y lógica
					Incapacidad para responsabilizar a las personas por sus acciones	Políticas y directrices inadecuadas y logs de auditoría inadecuadas en los sistemas

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Personas	Procesos	Sistemas			
Marcos de control		*	*	Diseño o rendimiento inadecuados de la infraestructura de gestión de riesgos existente	Falta de medición de la eficiencia	Medición inadecuada y eficiencia de informes de sistemas y procesos
					Robo y fraude	Control inadecuado de la actividad no autorizada en los sistemas
Cumplimiento legal y regulatorio	*	*	*	El incumplimiento de las leyes de los países en los que se llevan a cabo las operaciones comerciales, o el incumplimiento de las normas reguladoras, de informes y fiscales, o el incumplimiento de los contratos, o el incumplimiento de los contratos para proteger los intereses comerciales	Un cambio en la ley o las regulaciones de la industria en uno o más países conduce a una violación de la ley o las regulaciones de la industria en todo o parte del mundo	Arquitectura inadecuada para permitir la actualización, la extensión, el cambio, la mejora de los sistemas para hacer frente a los cambios en las regulaciones y la investigación inadecuada de alerta temprana
					Las inconsistencias en el marco legal y regulatorio conducen a infringir la ley o las regulaciones de la industria en todo o parte del mundo	Inadecuada investigación del entorno legal para esta iniciativa empresarial
					Se encuentra que las reglas de operación de un servicio infringen la ley o las regulaciones de la industria en todo o parte del mundo	Investigación y redacción inadecuadas de las normas de funcionamiento del servicio

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Personas	Procesos	Sistemas			
Gobierno corporativo	*	*	*	Incumplimiento por parte de los directores de sus obligaciones legales personales en la gestión de la empresa y la protección de los intereses de los accionistas	Falta de política interna	Liderazgo y establecimiento de políticas inadecuados desde los niveles superiores
					No tomar medidas oportunas cuando un proyecto estratégico importante se encuentra en dificultades	Falta de diligencia debida y oportuna, informes inadecuados a la alta gerencia y falta de liderazgo para resolver problemas operativos
					Incumplimiento de las políticas internas	Mala implementación de sistemas y procesos y auditoría interna inadecuada
Procesamiento y transacciones	*	*	*	Problemas con el servicio o la entrega del producto causados por fallas en los controles internos, sistemas de información o por debilidades en los procedimientos operativos	Falta de pensamiento conceptual en la planificación de sistemas	Arquitectura inadecuada de sistemas
					Operaciones no autorizadas	Autorización, identificación, autenticación y control de acceso inadecuados en sistemas
Comportamiento	*			Problemas con el servicio o la entrega del producto causados por la falta de integridad del empleado, o por errores y fallas	Operaciones de servicios	Inadecuadas operaciones de TIC procedimientos y operaciones administración

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Personas	Procesos	Sistemas			
Tecnología		*	*	No planificar, gestionar y supervisar el rendimiento de la tecnología, proyectos, productos, servicios, procesos, personal y canales de entrega	Arquitectura técnica inadecuada	Arquitectura inadecuada de los sistemas TIC para garantizar flexibilidad en respuesta a los requisitos cambiantes
					Falta de normas técnicas para la implementación	Sistemas TIC mal diseñados e implementados
Actos penales e ilícitos	*			Pérdida o daño causado por fraude, robo, negligencia intencional, negligencia grave, vandalismo, sabotaje, extorsión, etc.	Fraude por personal interno	Prevención inadecuada de troyanos, puertas traseras, etc., introducida por desarrolladores de TIC
					Fraude por terceros	Debilidad en la seguridad lógica, la seguridad física y en los procedimientos operativos
					Robo de equipos	Debilidad en la seguridad física y en los procedimientos
					Destrucción de activos corporativos	Debilidad en la seguridad lógica, la seguridad física y en los procedimientos
					Extorsión	Protección inadecuada de la información privada y confidencial obtenida del acceso no autorizado a los sistemas

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Personas	Procesos	Sistemas			
Terrorismo, guerra y eventos similares		*	*	Pérdida o daño causado por un ataque físico malicioso por parte de fuerzas hostiles	Pérdida de centros de operaciones y capacidad operativa	Redundancia y resistencia inadecuadas en el diseño e implementación de sistemas y centros de datos
Recursos humanos	*	*		No reclutar, desarrollar o retener empleados con las habilidades y conocimientos apropiados, o gestionar las relaciones con los empleados	Dependencia de persona clave	Pobre transparencia de los procesos y falta de capacitación
Información de gestión	*	*	*	Suministro de información inadecuada, inexacta, incompleta o inoportuna para apoyar el proceso de toma de decisiones de gestión	Sistemas de información de gestión deficientes	Informes inadecuados de todos los sistemas
Ética	*	*		Daño causado por prácticas comerciales poco éticas; Los problemas incluyen la discriminación racial y religiosa, la explotación del trabajo infantil, la contaminación, el medio ambiente, el acoso sexual, etc.	Publicación no controlada bajo el nombre de la organización.	Gestión de contenido inadecuada para evitar materiales ofensivos en correos electrónicos, sitios web, etc.

Categoría de ciberamenaza	Mapeo de Dominio			Descripción	Ejemplos	Mapeo de ciberseguridad
	Personas	Procesos	Sistemas			
Geopolítico	*			Pérdida o daño en algunos países, causado por la inestabilidad política, por la mala calidad de la infraestructura en las regiones en desarrollo o por diferencias culturales y malentendidos.	Desglose de la vida laboral normal	Resistencia inadecuada y recuperación ante desastres para evitar que se interrumpan las operaciones de TIC
					Desglose de la infraestructura nacional o local.	Plan inadecuado para lidiar con cortes de energía y de telecomunicaciones
Cultural	*	*	*	Incapacidad para tratar asuntos culturales que afectan a los empleados, clientes u otras partes interesadas; incluyendo idioma, religión, moral, códigos de vestimenta y otras costumbres y prácticas de la comunidad	Acoso sexual	Políticas y procedimientos inadecuados para desalentar y, si es posible, prevenir contenido inapropiado o pornográfico en correos electrónicos

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Escenarios de amenaza

El marco de clasificación de taxonomía de ciberamenazas se puede utilizar para generar ideas sobre escenarios de amenazas, proporcionando un conjunto mucho más rico de

información para realizar la gestión de riesgos. Cada escenario está descrito por un número de parámetros cualitativos, como se muestra en la Ilustración 14.

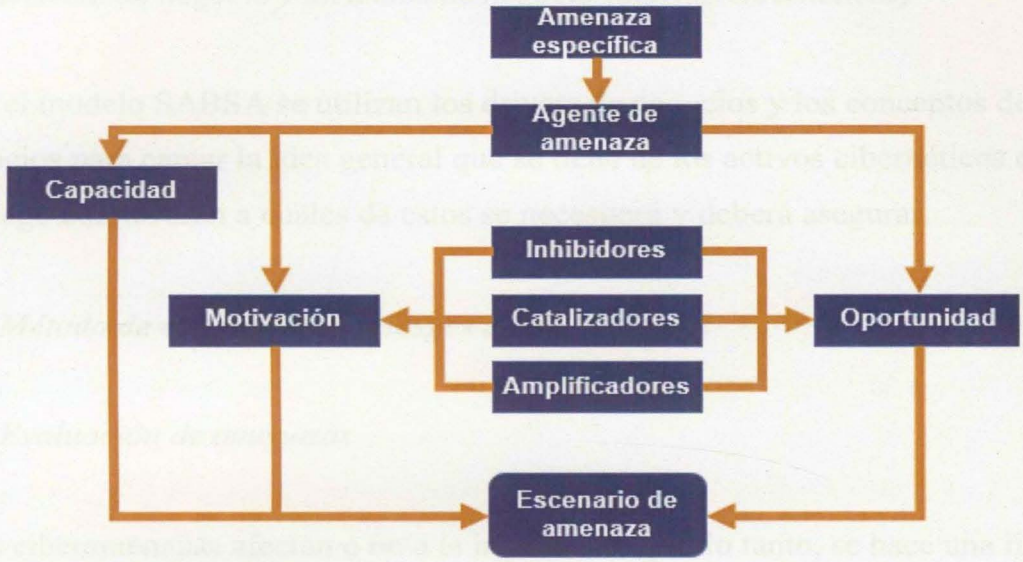

Ilustración 14 : Marco para un escenario de amenaza

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Priorización de riesgos

La institución necesita saber en este punto cuales riesgos son los más peligrosos y por lo tanto en cuáles se debería enfocar la mitigación y gestión. El principal motivo para realizar una evaluación de riesgos es establecer el ranking de importancia y llegar a una lista clasificada de riesgos que muestren el orden de prioridad.

Método de evaluación de riesgos SABSA

Con el enfoque de SABSA la institución puede evaluar los riesgos adoptando un método de medición cualitativo lo que permite clasificarlos en una serie de pasos los cuales deben ser aplicados a la Fuerza.

Método de evaluación de riesgos SABSA: Paso 1

Drivers de negocio y atributos de negocio (activos cibernéticos)

Con el modelo SABSA se utilizan los drivers de negocios y los conceptos de atributos de negocios para captar la idea general que se tiene de los activos cibernéticos de la Fuerza, estos luego conllevaran a cuales de estos se necesitará y deberá asegurar.

Método de evaluación de riesgos SABSA: Paso 2

Evaluación de amenazas

¿Las ciberamenazas afectan o no a la institución? por lo tanto, se hace una lista de estas que se consideran ser el modelo relevantes para la institución. Los requisitos o necesidades derivadas en el paso 1 son las que se utilizan para ayudar a enmarcar la declaración de una ciberamenaza que evitará que se cumpla esa necesidad o requisito.

Se debe recordar que para un negocio determinado, en un requisito puede haber varias ciberamenazas que lo pongan en riesgo, y cada una debe ser reportada y tenida en cuenta.

Método de evaluación de riesgos SABSA: Paso 3

Evaluación de impacto

Una vez que se establecen los requisitos y las ciberamenazas, el siguiente paso deberá ser evaluar lo que sería el impacto en la institución que resultaría de cada ciberamenaza materializada, esto se establece primero de manera descriptiva y luego se califica en una escala cualitativa simple, así:

- Impacto alto: podría causar daño potencial a la institución.

- Impacto medio: podría causar daño significativo a la institución.
- Impacto bajo: podría causar mínimo impacto a la institución.

Método de evaluación de riesgos SABSA: Paso 4

Evaluación de las vulnerabilidades

A pesar de todos los controles adicionales que se hayan implementado en la organización se debe seguir evaluando las vulnerabilidades como si no se hubiera hecho nada especial. Esto se llama evaluación de vulnerabilidad de campo verde, a menudo es difícil porque las personas siempre quieren explicar cómo ya han hecho lo suficiente para evitar que la ciberamenaza se materialice, pero ayuda en el desarrollo de la arquitectura de ciberseguridad para evaluar la contribución de todos los controles planificados sobre una situación superior antes de cualquier seguridad construida.

El propósito de la institución en este punto será establecer algunos objetivos de control a nivel de la arquitectura de seguridad conceptual y utilizarlos para conducir a través del diseño detallado de los controles a nivel de arquitectura de seguridad lógica, física, de componentes y operativa, este método de desarrollo arquitectónico se puede aplicar para llevar a cabo las revisiones de seguridad.

Método de evaluación de riesgos SABSA: Paso 5

Priorización del Riesgo

En el enfoque SABSA, la priorización del riesgo se basa en cuatro categorías de riesgo. Estas categorías se calculan directamente a partir de la calificación del impacto y la calificación de vulnerabilidad.

También es muy útil codificar por colores el fondo de la celda de la tabla de acuerdo con la gravedad del riesgo, produciendo un sistema de semáforos de informes de riesgos que sea fácil de entender. Los códigos de color se muestran en la Ilustración 15 y en la tabla 13.

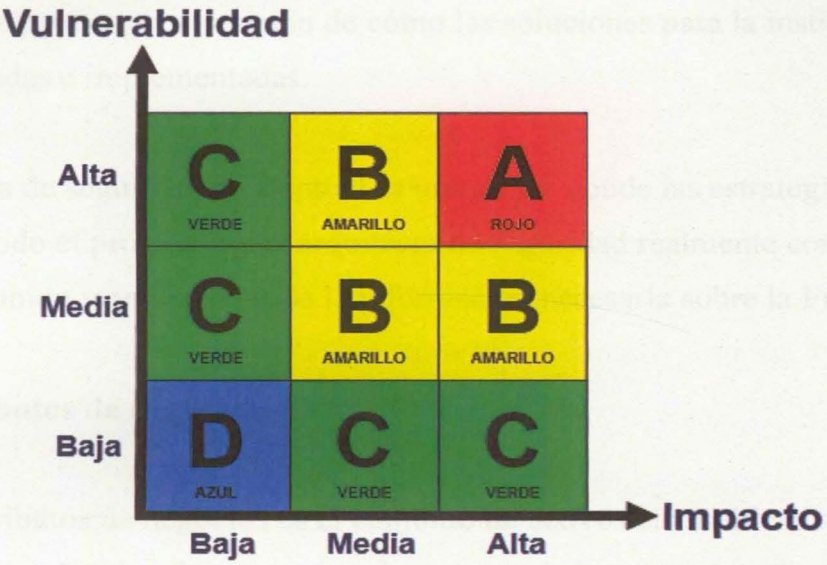

Ilustración 15 Asignación de la categoría de riesgo al impacto y la vulnerabilidad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Tabla 13 Categorías del riesgo

Categoría	Código de color	Descripción	Acciones requeridas
A	Rojo	Riesgo severo	Se requieren acciones correctivas para reducir la vulnerabilidad o para reducir el nivel de impacto, o ambos. Estos riesgos son de la máxima prioridad.
B	Amarillo	Riesgo significativo	Se deben planificar y ejecutar acciones correctivas apropiadas para reducir la vulnerabilidad o el nivel de impacto.
C	Verde	Riesgo Aceptable	Estos riesgos son aceptables porque la vulnerabilidad se encuentra en el nivel mas bajo posible o el impacto es menor, pero se deben monitorear para asegurarse de que no entren en a categoría B.
D	Azul	Riesgo insignificante	No se necesita acción.

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

13.1.2. Arquitectura de seguridad conceptual

Tras la recopilación de información digital y el análisis de esta que caracteriza a la capa contextual, en esta capa el arquitecto de seguridad sintetiza nuevas ideas y desarrolla los hechos materiales para crear una visión de cómo las soluciones para la institución serán planeadas, diseñadas e implementadas.

La arquitectura de seguridad conceptual es una de las donde las estrategias y los planes se deciden para todo el programa y el arquitecto de seguridad realmente comienza a agregar valor, pues ha reunido y analizado toda la información necesaria sobre la Fuerza.

Perfil de atributos de negocio

El perfil de atributos de negocios es el conjunto de activos cibernéticos que representan la institución, asignado a los factores y los riesgos asociados, con un enfoque de medición para producir métricas y objetivos de desempeño específicos definidos para cada uno.

Por lo tanto, la actividad de gestionar y medir en el ciclo de vida de SABSA se basa en los atributos de perfil expuestos durante la fase de actividad de estrategia y concepto que ha sido personalizado específicamente para conceptualizar esta clasificación.

Objetivos de control

Según SABSA un objetivo de control es una declaración de un resultado o propósito deseado que se logrará al implementar controles dentro de una determinada actividad. Los controles se implementan a través de políticas, estructuras organizativas, procesos, prácticas y procedimientos, a través de sistemas técnicos.

Un objetivo de control puede establecerse en respuesta a requisitos estratégicos, misionales, de evaluación y de apoyo específicos para el control, o puede ser una

declaración genérica de "buenas prácticas de ciberseguridad" que debe aplicarse a toda la institución, son un medio para tomar un sistema y normalizarlo en terminología común y conceptos genéricos que se pueden utilizar para impulsar trabajos de diseño más detallados.

Al igual que el perfil de atributos de negocios, los objetivos de control forman una importante conceptualización real de la misión de la institución, y también son una parte central de la arquitectura de seguridad conceptual.

Estrategias de ciberseguridad y estratificación arquitectónica

Hay muchas estrategias de seguridad que se pueden adoptar y muchas formas en las que se puede colocar las capas de la arquitectura de seguridad.

Seguridad de múltiples capas

El objetivo de este tipo de seguridad es brindar defensa en profundidad mediante la superposición de controles de ciberseguridad para reducir el riesgo de los activos que se protegen, se construye capa sobre capa de defensa una encima de otra. Este concepto se muestra con más detalle en la Ilustración 16. Donde los activos de información son los que se desean proteger. Alrededor de eso hay varias capas de seguridad, cada una con un nivel de detalle diferente. Más cerca de los activos están los controles de seguridad que actúan directamente sobre los activos de información: controles criptográficos. Como se mueva hacia afuera, los controles se vuelven cada vez más genéricos, hasta que en la capa exterior tiene responsabilidades, organización y política. (Andy Wood, Ying He, Leandros A Maglaras, Helge Janicke, 2009).

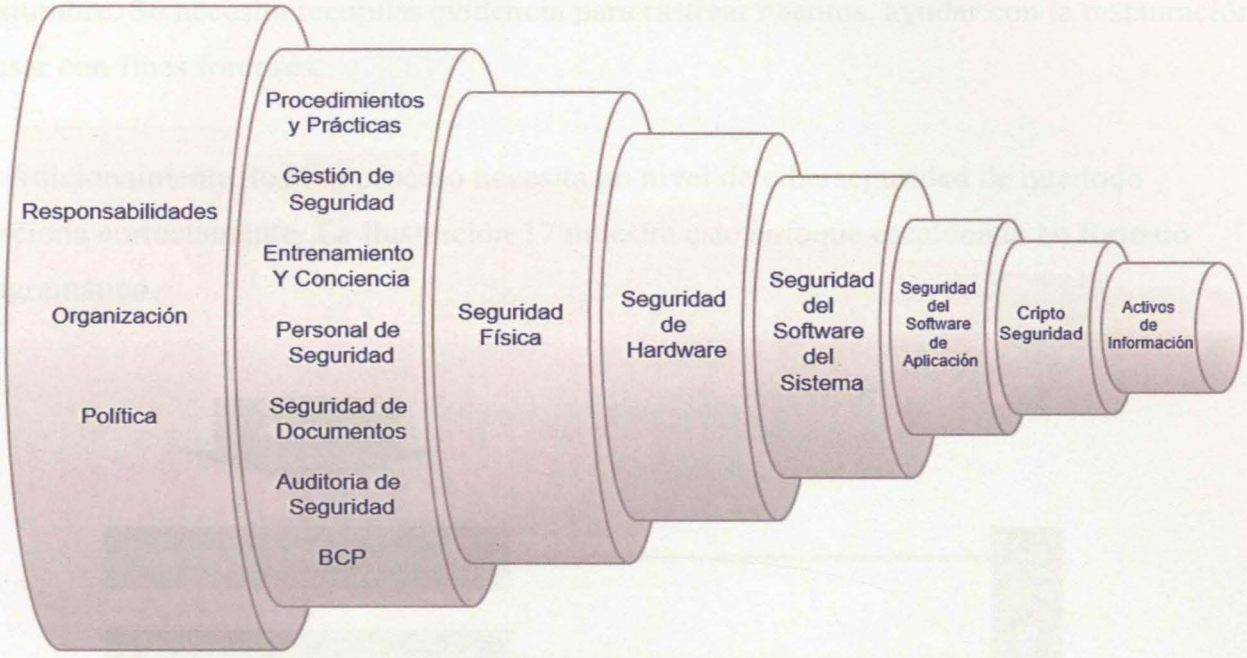

Ilustración 16 Capas múltiples de seguridad

Fuente: Recuperado de (Andy Wood, Ying He, Leandros A Maglaras, Helge Janicke, 2009)

La razón principal de este enfoque de múltiples capas es garantizar que no haya un único punto de fallo en las medidas de ciberseguridad. Si una medida no logra detener un incidente de seguridad, entonces hay otras que hacen el trabajo de una manera diferente. Las capas múltiples proporcionan un nivel razonable de seguridad de que existen múltiples formas de prevenir las brechas de seguridad.

Este es un principio fundamental que se recomienda se adopte en la arquitectura de ciberseguridad a realizar en la institución. El manejo de incidentes de múltiples niveles es otra forma de mejorar la eficacia de la seguridad y es la forma para el tratamiento de posibles incidentes de seguridad. Primero se intenta prevenirlos, si falla, se necesita contener los efectos, también detectar un incidente y dar la alarma, luego reaccionar ante el incidente para recuperarse de los efectos y restaurar el estado de las operaciones como de

costumbre. Se necesita recopilar evidencia para rastrear eventos, ayudar con la restauración y usar con fines forenses.

Adicionalmente, todo el proceso necesita un nivel de ciberseguridad de que todo funciona correctamente. La Ilustración 17 muestra este enfoque escalonado en formato diagramático.

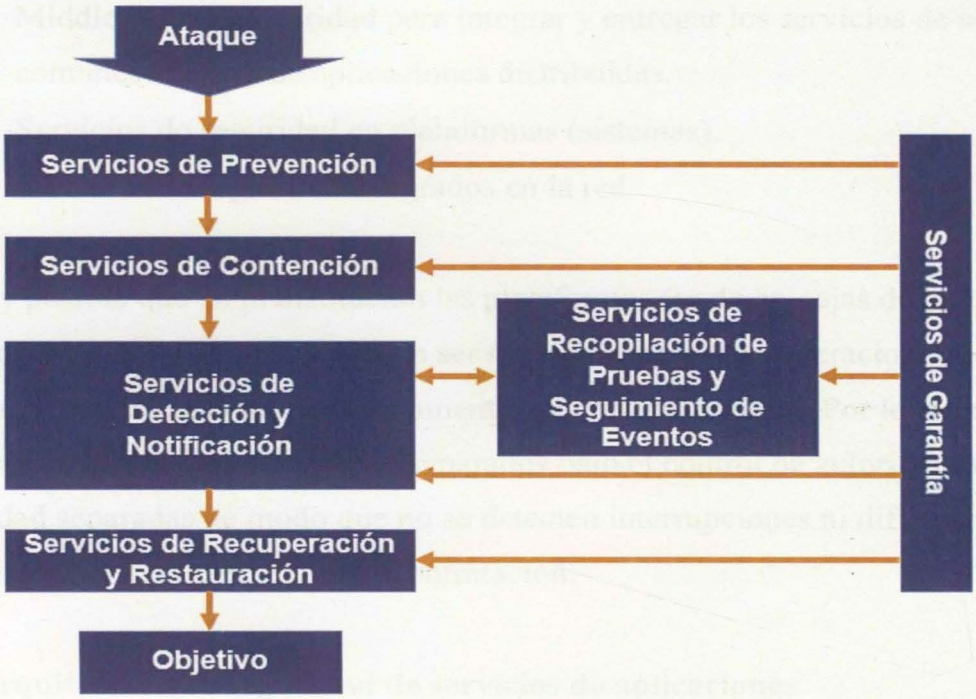

Ilustración 17 Servicios de seguridad de múltiples niveles

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

El Ejército Nacional al crear la arquitectura de ciberseguridad debe aspirar a tener una combinación de servicios de seguridad que proporcione una cobertura adecuada en cada uno de los niveles de este modelo conceptual por capas.

Arquitectura de ciberseguridad de infraestructura en capas

La prestación de servicios para la institución requiere una infraestructura de ciberseguridad. Esto debería comprender:

- Servicios de seguridad comunes entregados a través de las aplicaciones.
- API de servicios de seguridad.
- Middleware de seguridad para integrar y entregar los servicios de seguridad comunes a través de aplicaciones distribuidas.
- Servicios de seguridad en plataformas (sistemas).
- Servicios de seguridad integrados en la red.

Es muy posible que en la institución las plataformas (es decir, cajas de hardware y sus sistemas operativos) y las redes puedan ser subcontratadas para operaciones por un tercer proveedor de servicios, si no inmediatamente, en una fecha futura. Por lo tanto, deben ser tratados como dominios de seguridad separados bajo el control de autoridades de políticas de seguridad separadas de modo que no se detecten interrupciones ni dificultades operativas importantes en el momento de la subcontratación.

Arquitectura de seguridad de servicios de aplicaciones

Cada aplicación es única, y esta singularidad se muestra especialmente en la forma en que se aseguran estas aplicaciones. Cada una de estas tiene su propia base de datos y su propio registro de usuarios, y que estas son muy difíciles de compartir con otras aplicaciones, por lo tanto se requiere una arquitectura de ciberseguridad fuerte y diferenciada para cada aplicación.

Colocación de servicios de ciberseguridad en las capas de la arquitectura

En el modelo de arquitectura de infraestructura los servicios de ciberseguridad comunes proporcionados a las aplicaciones juegan un papel importante al interior del Ejército Nacional pues se cuenta con varias aplicaciones. Sin embargo, existen otras capas de seguridad en este modelo que pueden ser útiles a la hora de asegurar el servicio proporcionado. Éstos incluyen:

- Servicios de seguridad de middleware: dentro de la propia capa de middleware.
- Servicios de seguridad de gestión de datos provistos dentro de las bases de datos y posiblemente considerado como parte de los servicios de seguridad de middleware.
- Servicios de seguridad de red dentro de la red.
- Servicios de seguridad de plataforma dentro de las plataformas individuales.

Servicios de ciberseguridad en la capa de aplicaciones

El objetivo principal de la seguridad de la aplicación es abordar la cuestión de quién puede hacer qué dentro de la aplicación, y cuánto. Esas autorizaciones deben ser creadas a través de algún proceso de gestión adecuado donde los usuarios de estas aplicaciones obtienen algunos privilegios. Estos privilegios incluyen:

- Funciones de aplicación que pueden usar.
- Los datos de la aplicación se les permite leer, actualizar y crear.
- Límites en las transacciones de aplicación que están autorizados a realizar.
- Control dual en algunas transacciones sensibles donde también se necesita una segunda persona para autorizar la transacción.

- A veces hay un conjunto de reglas basadas en el contexto que rige la ubicación del usuario para ciertas actividades específicas, como la hora o día de la semana en la que se realiza la actividad.

El sistema debería aplicar las autorizaciones a través de un servicio de control de acceso lógico, como una interfaz para el control de acceso, también necesita autenticación para probar que el reclamante realmente es el autorizado, como back-end para el control de acceso, también necesita logs de auditoría para decirle históricamente quién hizo qué y cuándo, así mismo, son necesarias herramientas para crear y editar las autorizaciones y revisar el seguimiento de auditoría. Esta actividad debe llevarse a cabo por un experto que haga parte del equipo de administración de ciberseguridad.

Los servicios de seguridad de aplicaciones se pueden resumir en:

- Autorización (el proceso de otorgar un privilegio).
- Autenticación (el proceso de verificación de identidad).
- Control de acceso (el proceso de toma de decisiones de acceso basado en la verificación de autorizaciones y autenticando la identidad).
- Auditoría (el proceso de escritura, almacenamiento y revisión de registros de todos los intentos de acceso, decisiones y resultados).
- Administración (privilegios de administración y todas las actividades asociadas).
- Seguridad de comunicaciones.

Los servicios de ciberseguridad necesarios son:

- Confidencialidad.
- Integridad.
- Autenticidad.
- No repudio.

Servicios de ciberseguridad de gestión de datos

La gestión de datos tiene una doble función, por un lado proporciona acceso a los recursos de información de la aplicación y por otro protege estos recursos de información.

La clave para lograr los objetivos son la autorización y la provisión de servicios de seguridad adecuados dentro de esta capa, pues es fundamental para el éxito de la arquitectura de las aplicaciones. La función de gestión de datos abarca los siguientes componentes:

- Gestión de metadatos.
- Gestión de bases de datos relacionales.
- Base de datos orientada a objetos.
- Sistemas de gestión.
- Acceso a la base de datos.
- Almacenamiento de datos.
- Minería de datos.
- Procesamiento de transacciones de seguimiento.

Servicios de seguridad en la capa de transferencia de información (Red)

La institución deberá proporcionar administración de red que se aborde desde una perspectiva de ciberseguridad colectivamente con administración de sistemas.

Las topologías de red incluyen:

- Redes de área local.
- Redes de área de campus.
- Redes de área metropolitana.

- Redes de área amplia.
- Internet.
- Intranet.

Los objetivos de seguridad en la capa de transferencia de información son:

- Proporcionar conectividad de alta calidad, confiable y disponible a los usuarios.
- Proteger estos atributos de confiabilidad, calidad y disponibilidad.
- Protección de los flujos de gestión de red (DNS, ICMP, SNMP, etc.).
- Evitar el robo de ancho de banda por usuarios no autorizados.

Los servicios de seguridad de red que se deben implementar para proporcionar seguridad dentro de la capa de transferencia de información son:

Política de seguridad de la red:

- Definición de dominios de red.
- Asignación de propiedad de dominio.
- Configuración de la política de seguridad del dominio.
- Sensibilización sobre la política de seguridad de red y su implementación.

Segregación de dominio de red:

- Firewalls en los límites del dominio.
- Reglas de seguridad para que los firewalls reflejen la política de dominio.

Redundancia de componentes de red y resistencia:

- Enrutamiento diverso.

- Artículos de equipos redundantes.
- Múltiples puntos de acceso.
- Ancho de banda bajo demanda.

Autentificación de la entidad de red:

- Autenticación mutua de nodo a nodo dentro de la red (enrutador a enrutador).
- Autenticación de entidad externa en el límite de la red.
- Autenticación del operador para la gestión del servicio de red.

Autorización de entidad de red:

- Roles asociados con entidades de red externas.
- Perfiles de servicio para roles.

Control de acceso a los límites de la red:

- Puertas de enlace de seguridad (firewalls) para controlar los flujos de tráfico dentro y fuera de los dominios de la red.
- Reglas de restricción de servicios.

Control de conectividad:

- Autorización para conexiones.
- Cambio de control.
- Estándares de seguridad físicos y lógicos para todos los nodos de la red.

Seguridad de gestión de red:

- Entidades operadoras autorizadas.
- Control de acceso.
- Protocolos seguros 'get' y 'set'.
- Autenticación remota de entidades operadoras.
- Integración con la arquitectura de gestión del sistema.
- Integración con la infraestructura y organización de gestión existente.

Protección de integridad de recursos de red:

- Controles de ciclo de vida de desarrollo de software.
- Controles de producción.
- Controles de entrega e instalación.
- Control de configuración.
- Ciclo de vida operacional.
- Integridad de los datos de configuración.
- Integridad de la tabla de enrutamiento.
- Gestión del cambio.

Monitorización de seguridad de red y detección de intrusos:

- Detección de intrusiones basada en firmas.
- Registro y análisis de eventos en enrutadores, firewalls, gateways, servidores y otros dispositivos de red.

Manejo de incidentes de seguridad de red:

- Informes.

- Confirmación.
- Respuesta.
- Recuperación.
- Análisis y lecciones aprendidas.

Investigación de vulnerabilidad de red:

- Recopilación, cotejo y análisis de avisos del CERT.
- Pruebas de intrusión.
- Recopilación de inteligencia en internet.

Servicios de ciberseguridad para la capa de procesamiento de información

Esta capa está relacionada con la arquitectura y los estándares de las plataformas de procesamiento de la institución, las operaciones de servicios de sistema y periféricos.

Los tipos de plataforma y periféricos incluyen:

- Computadoras personales.
- Impresoras y plotters.
- Varios dispositivos de E/S: escáneres de documentos, cámaras digitales (imágenes fijas y video), audio digital, grabadores, lectores de códigos de barras, tarjetas inteligentes y dispositivos biométricos.
- Dispositivos de interfaz de red.
- Computadoras en red.
- Dispositivos de red de datos: concentradores, enrutadores.
- Terminales de red de voz, celulares y otros dispositivos.
- Dispositivos de seguridad especializados.
- Dispositivos de control de procesos, consolas de sala de control.

- Estaciones de trabajo móviles (computadoras portátiles).
- Asistentes digitales personales o computadoras de mano, a veces con dispositivos integrados con capacidad de telefonía móvil.
- Servidores de rango medio: servidores de archivos, servidores de bases de datos, servidores multimedia, servidores de inserción de datos, servidores de aplicaciones, servidores de correo.
- Dispositivos de almacenamiento: discos magnéticos, matrices RAID, discos ópticos.
- Servidores de mainframe.

Los principios estratégicos para proporcionar servicios de ciberseguridad en la capa de procesamiento de información para los diferentes sistemas operativos de las diversas plataformas de hardware son:

- Reducir las vulnerabilidades en las plataformas de procesamiento de información e infraestructura.
- Separar y aislar plataformas, y entornos de producción de aquellos utilizados para desarrollo y pruebas.
- Proporcionar y mantener entornos de ejecución altamente confiables para personas altamente sensibles, procesamiento de datos.
- Suministrar entornos de almacenamiento seguros para datos almacenados no volátiles altamente sensibles.

Los principales servicios de ciberseguridad que se proporcionarán en la capa de procesamiento de información son:

- Autenticación de usuarios locales con contraseñas y posiblemente tarjetas inteligentes u otros tokens, y posiblemente dispositivos biométricos.

- Control de acceso de usuarios locales, basado en autorizaciones locales, proporcionado por el sistema operador.
- Logs de auditoría locales.
- Servicios criptográficos proporcionados por subsistemas criptográficos locales (hardware y software).
- Interacción remota con servicios de seguridad central, como la gestión de claves criptográficas, certificados digitales, control de acceso basado en roles.
- Servicios antivirus para prevención, contención, detección, informe, restauración, recuperación de virus y otros ciberataques de software malicioso.
- Servicios de filtrado de contenido para apoyar la implementación de políticas de uso aceptables con respecto a la pornografía, mensajes raciales abusivos y otros socialmente inaceptables.
- Cambio de control.
- Control de configuración.
- Escaneo regular para detectar cambios no autorizados en la configuración.
- Planificación de copia de seguridad y recuperación.
- Gestión de sistemas (incluida la gestión de operaciones, administración de ciberseguridad y muchos otros servicios).

Estrategia de gestión de servicios de ciberseguridad

La gestión de los servicios de ciberseguridad incluye:

- Aprovisionamiento de parámetros de seguridad y privilegios para los usuarios.
- Provisión de parámetros de seguridad para sistemas de aplicaciones.
- Provisión de parámetros de seguridad para sistemas embebidos en equipos tales como enrutadores.
- Operaciones de seguridad de rutina para mantener los sistemas corporativos en un estado de cumplimiento con políticas y normas de seguridad.

    - Monitoreo de seguridad y detección de intrusos para detectar incidentes de seguridad y recopilar información relevante para el proceso de gestión de problemas.
    - Gestión de incidencias y problemas de seguridad para recuperar y restaurar operaciones seguras después de un incidente de seguridad.
- Investigación de vulnerabilidad de seguridad:
    - Recopilación, verificación y análisis de avisos del CERT.
    - Pruebas de intrusión.
    - Recopilación de inteligencia en internet.
- Autorización de entidades operadoras que realizarán funciones de gestión de servicios especiales. Se deben crear roles de administración de servicios y el servicio de control de acceso, basado en roles para imponer un dominio de seguridad lógica separado para la gestión del servicio, con subdominios aplicados por cada rol individual.
- Segregación de tareas críticas para proteger el entorno de los sistemas de información corporativos contra las acciones maliciosas de cualquier individuo trabajando solo. Esto debería lograrse a través de la definición de roles de gestión de servicios para segregar tareas entre roles mutuamente excluyentes.
- Autenticación local y remota de entidades operadoras.
- Control de acceso a aplicaciones de gestión de servicios para la gestión de:
    - La capa de transferencia de información.
    - La capa de procesamiento de información.
    - La capa de middleware.

    - La capa de aplicaciones.

- Protocolos de gestión de servicios seguros, protegiendo tanto:
    - La autenticidad de una fuente de mensajes de gestión de servicios.
    - La autenticidad de los contenidos del mensaje de gestión de servicios.
    - La confidencialidad de los contenidos del mensaje de gestión de servicios.

- Monitoreo independiente y auditoría de gestión de operaciones de seguridad.

- Integración con la arquitectura global de gestión de sistemas.

- Integración con la infraestructura y organización de gestión de servicios existentes.

Estrategia de aseguramiento del sistema

La garantía del sistema se ocupa de la corrección, la fiabilidad y el correcto funcionamiento del sistema. Hay una serie de áreas estratégicas de control a las cuales la organización se puede acoger y ayudarán a la institución a proporcionar el nivel requerido de garantía:

- Control sobre el desarrollo de sistemas.
- Control sobre operaciones de sistemas operacionales.
- Protección de la integridad del software y controles antivirus.
- Filtrado de contenido para evitar la divulgación de datos no autorizados e ilegales.
- Proteger la integridad del código móvil (como applets de java, activeX, scripts).
- Pruebas funcionales.
- Pruebas de penetración.

- Auditoria de seguridad.

Para la implementación de sistemas con altos niveles de ciberseguridad, como en el caso de sistemas críticos siendo uno de los objetivos principales de la institución, hay una serie de herramientas y enfoques adicionales importantes, los cuales incluyen:

- Redundancia de componentes.
- Arquitecturas tolerantes a fallas.
- Métodos formales de especificación y prueba.
- Evaluación probabilística de riesgos y análisis de fallas.
- Modelado de sistemas usando modelos de máquina de estado finito y modelo exhaustivo comprobación.
- Resistencia a la manipulación para defenderse de ciberataques.
- Análisis de factores humanos, mirando la interfaz de usuario.

Modelo de dominio de ciberseguridad

Para el modelo SABSA, un dominio de ciberseguridad es un conjunto de elementos sujetos a una política de seguridad común definida y ejecutada por una sola autoridad. Las actividades de un dominio de ciberseguridad involucran uno o más elementos de ese dominio de seguridad, y posiblemente elementos de otros dominios de seguridad.

Concepto de virtual private network (VPN)

Según el Instituto Nacional de Ciberseguridad de España – INCIBE (2015), una VPN es un servicio que permite el acceso remoto a la red interna de la organización y a los recursos corporativos. Este acceso se realiza a través de internet de forma segura, permitiendo la movilidad del trabajador o incluso interconectar sedes separadas geográficamente. Una VPN crea un túnel a través de internet mediante cifrado seguro, de forma que se puede acceder desde cualquier lugar a los servicios y documentos internos de la compañía.

Las VPN garantizan que toda la información que se transmite va a estar segura. Concretamente la confidencialidad, ya que en caso que fuese interceptada durante la transmisión, no podría ser decodificada; su integridad, pues la información viaja cifrada, por lo que no pueden ser modificada o alterada durante la transmisión. Además garantiza que la información está siendo transmitida solo desde dispositivos autorizados. (Instituto Nacional de Ciberseguridad de España – INCIBE, 2015).

El Ejército Nacional actualmente maneja las redes privadas virtuales (VPN) como una forma de proporcionar un servicio seguro en el entorno externo de la institución, pero hay algunas limitaciones que debe tener en cuenta.

Una VPN utiliza cifrado punto a punto dentro de la capa de red para proporcionar una serie de canales seguros a lo largo del cual los datos privados de la institución pueden ser transmitidos sin ser capaces de ser leídos por un espía. Además, en virtud del hecho de que el flujo de datos de la aplicación está completamente encriptado, por lo que tampoco es factible que un extraño realice cambios en los datos transmitidos sin que esto sea detectado.

Normalmente, una VPN se crea mediante el uso de cifrado y descifrado incrustados en los firewall que proporcionan la interfaz segura a una red hostil como el internet. El enfoque estandarizado para lograr esto es utilizar protocolos IPsec, una versión segura del protocolo IP que proporciona cifrado y/o autenticación dentro del protocolo de nivel de paquete IP.

Concepto de firewall

Hoy en día las organizaciones mantienen un flujo constante de la información digital con su entorno y a través de este flujo puede entrar en riesgo el propio negocio por las diversas ciberamenazas, a partir de estos riesgos surge la necesidad de desarrollar ambientes confiables de protección. Por esta razón, se han desarrollado enfoques de seguridad como la defensa en profundidad, que tiene como propósito proteger la información a través de la

aplicación de controles en distintas capas. Una de estas capas es el perímetro, el límite lógico que separa la red corporativa de otras redes (la frontera con el entorno, con ambientes externos), en las metodologías de seguridad de esta capa, el firewall tiene protagonismo como el mecanismo de protección de las redes y debe ser un elemento imprescindible dentro de cualquier institución. (ESET, 2014).

Un firewall es la puerta de enlace de seguridad que se encuentra en el límite entre dos dominios de red, aplicando la política de seguridad de uno de esos dominios (generalmente el dominio institucional interno), y la regulación del flujo de tráfico de red que entra y sale de ese dominio. Los firewall tienen como objetivo prevenir que los flujos de tráfico no autorizados, sean detectados y bloqueados en la seguridad límite creada alrededor del dominio protegido.

Cuando se trata de proteger los entornos de redes de datos, especialmente aquellos en los que la red institucional que deben conectarse a una red externa, la Fuerza deberá optar por usar un firewall. Sin embargo, estos equipos tienen ciertas limitaciones, considerando algunos de los temas clave se encuentran:

En primer lugar, internet es tan generalizado que rodea efectivamente el dominio de la institución, por lo tanto, se vuelve obvio que solo el firewall hará poco, porque solo puede regular el tráfico que se dirige a través de él. Si el límite alrededor del resto del dominio tiene fugas, y si el tráfico fluye dentro y fuera del dominio que no sea a través del firewall, entonces este no será cien por ciento efectivo.

Esta barrera en su mayoría no será solo un tema técnico, es una combinación de política, procedimiento, comportamiento, conciencia; sin la cual, el firewall no puede ser efectivo. Para implementar unos buenos cortafuegos de seguridad de la red, la Fuerza necesitará implementar una buena cultura de seguridad en toda su institución.

El propio firewall también debe estar correctamente configurado y gestionado. Estos permiten cierto tráfico (porque se requiere para fines operacionales legítimos) y no permitir otro tráfico (porque no es requerido para fines operacionales legítimos). Por lo que debe ser claro acerca de lo que permitirá y lo que bloqueará en el firewall. Esta es la política de seguridad del firewall, y sin una declaración de políticas correcta, el firewall probablemente no ofrezca la protección adecuada.

Objetivos de tiempo de recuperación de desastres

La recuperación ante desastres se refiere a la recuperación de los sistemas de información después de un incidente importante, eso provoca una interrupción en el servicio. Es importante que la institución haga un análisis cuidadoso de las necesidades de recuperación de los servicios, de modo que se pueden desarrollar diseños apropiados que mantendrán estos objetivos de tiempo.

Existe una considerable compensación entre el costo de proporcionar la recuperación y el tiempo objetivo para ser logrado si es realmente necesario, se puede mantener el servicio de 365 días a 24 horas sin parar, pero se elevan los costos a un nivel muy alto.

13.2. Diseño

Según SABSA, en la fase de diseño del ciclo de vida de la arquitectura de ciberseguridad es donde se trabaja la estructura y forma de los aspectos técnicos y de gestión de los sistemas de seguridad que se van a implementar en la institución, lo que se creará a través de esta actividad de diseño es un patrón coherente y resuelto por el cual todos los elementos de los sistemas seguros encajan.

13.2.1. Arquitectura de seguridad lógica

La arquitectura de seguridad lógica describe las relaciones y la interdependencia entre varios elementos de los sistemas de operación, trata el flujo lógico y razonado de un paso a otro en el procesamiento de toda la información digital de la institución.

La arquitectura de seguridad lógica se ocupa en gran medida de la vista funcional de la ciberseguridad definiendo un conjunto completo de requisitos funcionales, en esta etapa no se presta atención a los mecanismos de seguridad que se utilizarán para entregar esas funciones, son parte de la arquitectura de seguridad física.

Arquitectura informacional

En la capa de arquitectura lógica se tiene información digital de la operación que se debe asegurar en la Fuerza, esta información tiene las siguientes propiedades:

- La información digital es una representación lógica de algo real. Esta información incluye todo lo que necesita saber sobre cada usuario y cada detalle de su relación con la institución.

- La información es estructurada y organizada en campos, registros, archivos, tablas, bases de datos.

- Las estructuras de información están relacionadas entre sí tanto en forma jerárquica como entre pares relacionados.

- La información está relacionada con el tiempo.

- La información existe independientemente de la ubicación física de los datos. Sin embargo, el acceso a la información puede ser dependiente.

- La calidad de la información depende no solo del contenido de los datos, sino también de la estructura utilizada para presentarla y las herramientas analíticas aplicadas.

- El éxito de la información se mide mejor en términos de la experiencia del usuario al utilizarla.

- Cuando se habla de activos de información, estos son activos secundarios, que representan los principales activos que desea proteger.

Información digital estática y dinámica

La información estática es aquella que no se mueve ni cambia en el corto plazo.

Ejemplos de información estática incluye:

- Registros y archivos maestros.
- Información de configuración para sistemas y aplicaciones.
- Información histórica, incluidos todos los registros de auditoría almacenados, todos los registros históricos de trabajo y todos los registros de mensajes históricos.

La información dinámica cambia, se mueve a corto plazo y puede que tenga una vida útil corta. Ejemplos de información dinámica incluyen:

- Mensajes de formato libre en tiempo real, como los utilizados en el correo electrónico.
- Mensajes de aplicación estructurados en tiempo real, como consultas de base de datos.
- Información de operaciones en tiempo real.

- Gestión de sistemas y servicios de intercambio de información en tiempo real.
- Información junto con otros registros históricos.

La protección de información tanto estática como dinámica requiere servicios de seguridad tales como:

- Protección de la confidencialidad.
- Protección de la integridad.
- Protección de la disponibilidad.

Además, la protección de información dinámica requiere servicios de seguridad tales como:

- Autenticidad de la fuente.
- No repudio.

Políticas de ciberseguridad

Para llevar a cabo la metodología SABSA en la institución, es importante saber qué tipo de ciberseguridad y como se debe aplicar para proteger la operación de varias maneras, definir reglas de alto nivel para lograr esta seguridad y las actividades que serán autorizadas o no para alcanzar los objetivos de ciberseguridad.

La política de ciberseguridad estará determinada por los requisitos operacionales de la institución para la gestión de los sistemas y de la información digital, a partir de una evaluación de los posibles riesgos operacionales.

Arquitectura de la política de ciberseguridad

En la política de ciberseguridad existirán varios niveles diferentes, es útil concebir una arquitectura de la política jerárquicamente en capas.

Hay declaraciones de política que son aplicables a todas las disciplinas relacionadas dentro de la entidad pero es mejor no repetir las mismas declaraciones bajo diferentes encabezados de políticas, sino ensamblarlas en una política integrada de nivel superior. Esta política de alto nivel estará dirigida a todos los usuarios en la Fuerza.

Como parte de la arquitectura de seguridad lógica necesitará determinar cuál es la arquitectura de política adecuada para la institución y las reglas que necesitará para esto.

Servicios de ciberseguridad

Los servicios de ciberseguridad son servicios lógicos, especificados independientemente de qué mecanismo físico podría ser utilizado para entregarlos, se conducen desde la capa superior, los objetivos de control y las estrategias de ciberseguridad.

En el modelo de ciberseguridad en capas de servicios se incluyen:

- Servicios de prevención.
- Servicios de contención.
- Servicios de detección y notificación.
- Servicios de almacenamiento y seguimiento de eventos.
- Servicios de recuperación y restauración.
- Servicios de garantía.

A continuación se presenta una lista base de los servicios de ciberseguridad en cada uno de las capas de servicios, ver la Tabla 14. En esta, cada servicio de seguridad esta descrito pero se deberá decidir cuál de estos se necesita en la arquitectura de ciberseguridad de la institución para cumplir con los requisitos y políticas que ha derivado.

Tabla 14 Servicios de ciberseguridad por estrategia defensiva

Estrategia defensiva	**Servicios de ciberseguridad**
Prevención	Servicios de ciberseguridad de la entidad: • Nombre único de la entidad • Registro de la entidad • Certificación de la clave pública de la entidad • Certificación de credenciales de la entidad • Servicio de directorio • Autorización de la entidad • Autenticación de la entidad • Autenticación de usuario • Autenticación del dispositivo Servicios de ciberseguridad de comunicaciones: • Autenticación de sesión • Autenticación del origen del mensaje • Protección de la integridad del mensaje • Confidencialidad del contenido del mensaje • Administración de seguridad (gestión de privilegios) • Soporte al usuario • Servicios de seguridad física • Servicios de seguridad ambiental • No repudio • Protección de reproducción de mensajes • Confidencialidad del flujo de tráfico Servicios de ciberseguridad de aplicaciones y sistemas: • Autorización de la entidad • Control lógico de acceso • Logs de auditoría • Protección de integridad de datos almacenados • Confidencialidad de los datos almacenados • Protección de la integridad del software • Gestión de licencias de software • Protección de la configuración del sistema • Replicación de datos y respaldo • Replicación y respaldo de software • Tiempo de confianza • Interfaz de usuario para seguridad Servicios de gestión de ciberseguridad: • Gestión de la política de seguridad • Formación y sensibilización en seguridad • Gestión de operaciones de seguridad • Aprovisionamiento de seguridad

Estrategia defensiva	Servicios de ciberseguridad
	• Monitoreo de seguridad • Medición de seguridad y métricas • Dispositivos de seguridad física • Dispositivos de seguridad ambiental
Contención	Autorización de la entidad Confidencialidad de los datos almacenados Protección de la integridad del software Seguridad física Seguridad ambiental Formación y sensibilización en ciberseguridad
Detección y notificación	Protección de la integridad del mensaje Protección de integridad de datos almacenados Monitoreo de ciberseguridad Detección de intrusión Gestión de alarmas de ciberseguridad Formación y sensibilización en ciberseguridad Medición de seguridad y métricas
Correlación y seguimiento de eventos	Logs de auditoría Gestión de operaciones de ciberseguridad Monitoreo de ciberseguridad Medición de seguridad y métricas
Recuperación y restauración	Respuesta al incidente Replicación de datos y respaldo Replicación y respaldo de software Recuperación de desastres Gestión de crisis
Garantía	Logs de auditoría Auditoria de ciberseguridad Monitoreo de ciberseguridad Medición de ciberseguridad y métricas

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Integración del servicio de ciberseguridad

Un aspecto crítico de la arquitectura de seguridad lógica es el ajuste de estos diversos servicios de ciberseguridad en la Fuerza. La Ilustración 18 muestra algunos de los principales servicios de ciberseguridad y cómo interactúan lógicamente uno con otro.

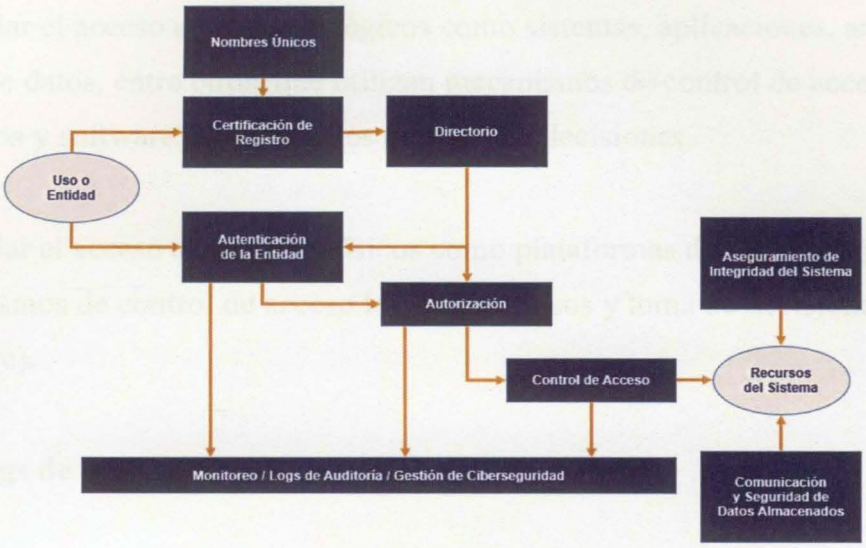

Ilustración 18 Integración de los principales servicios de ciberseguridad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Servicios de ciberseguridad de aplicaciones y sistemas

El grupo de servicios base de ciberseguridad de la Tabla 14 ayudara a la Fuerza a proteger las aplicaciones y los sistemas contra ciberataques o abusos informáticos, en su mayoría estos servicios están de alguna manera preocupados por prevenir o revelar accesos no autorizados o acciones no autorizadas por parte de cibercriminales.

Control de acceso

Los servicios de control de acceso pueden regir dominios físicos y lógicos, y el control de los mecanismos puede ser de naturaleza física o lógica.

Hay tres tipos de control de acceso:

- Controlar el acceso a dominios físicos tales como sitios e instalaciones utilizando mecanismos como puertas, cerraduras, resguardos, entre otros.

- Controlar el acceso a dominios lógicos como sistemas, aplicaciones, archivos, registros, bases de datos, entre otros, que utilizan mecanismos de control de acceso lógico, como permisos y software con funciones de toma de decisiones.
- Controlar el acceso a dominios físicos como plataformas de hardware y redes de uso de mecanismos de control de acceso lógico (permisos y toma de decisiones de funciones de software).

Logs de auditoría

En los últimos años, la auditoría de información ha aumentado en importancia como resultado de su impacto en la prevención o detección de violaciones que afectan la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos de la organización. Dado los riesgos de seguridad a los que se enfrentan los sistemas de información, estas auditorías son un componente importante para la ciberseguridad y depende en gran medida de la expresividad de los log de eventos para garantizar la calidad de los resultados. (Baryolo et al., 2012).

Los logs de auditoría proporcionan evidencia histórica de las actividades en los sistemas de la Fuerza para fines de monitoreo o examen forense, la protección de la integridad del seguimiento de auditoría en sí misma se convierte en un problema en algunas circunstancias, ya que la manipulación de estas puede cubrir actividades no autorizadas.

Estos servicios necesitan no solo mecanismos para la captura y almacenamiento de la información de los eventos, sino también mecanismos para proteger la integridad de esa información almacenada.

Protección de integridad de datos almacenados

Del mismo modo que los datos de mensajes que transitan por la red institucional, pueden estar sujetos a alteración, eliminación o resecuenciación no autorizadas por un cibercriminal, los datos pueden sufrir el mismo destino entre el momento en que se almacenan y el tiempo que se recupera para su uso. El uso de mecanismos de control de acceso físico y lógico también ayudara a prevenir el acceso no autorizado que conduciría a tal modificación de los datos almacenados.

Confidencialidad de datos almacenados

Este servicio evita la divulgación no autorizada de datos almacenados de la Fuerza. Varios mecanismos están disponibles como el cifrado, espacios bien protegidos y control de acceso lógico.

Protección de integridad de software

La ciberamenaza más importante proviene del software malicioso en la forma de virus, gusanos, virus de macro, caballos de troya, etc., esta clase de software no autorizado también puede insertarse en un sistema informático de la institución manualmente por un cibercriminal que ya ha penetrado a un alto nivel de privilegio e instala objetos de este tipo para uso futuro.

Los mecanismos utilizados para implementar los servicios de defensa contra ciberataques maliciosos incluyen herramientas de detección de virus, mecanismos de detección de cambios, como sumas de comprobación y entornos de cuarentena para probar el software recién importado antes de su lanzamiento.

Cabe señalar que no se puede contrarrestar a un cien por ciento que el software sea atacado en sistemas reales, la única defensa real es tratar de atrapar la mayor cantidad

posible de agentes infecciosos antes de que ellos hagan daño y estar listo para limpiar cuando algunos de esos agentes penetren el perímetro de seguridad.

Protección de la configuración del sistema

La configuración del sistema incluye tanto el software ejecutable incluido los scripts, como los datos de configuración que muchos de los archivos ejecutables necesitan para realizar su función, todos estos archivos y la estructura del directorio en el que están almacenados deben estar protegidos de los cibercriminales.

Este servicio generalmente se entrega mediante la aplicación de varios mecanismos de ciberseguridad ejemplo:

- Escaneo antivirus.
- Uso de sumas de comprobación para verificar la integridad de los archivos y directorios.
- Uso de herramientas de escaneo que comparan la configuración real con una configuración almacenada de archivo de política.

Replicación de datos y respaldo

Para habilitar la recuperación de los sistemas de la institución después de un incidente de desastre, se debe hacer una copia de seguridad de los datos.

El servicio de replicación, copia de seguridad y restauración debe cubrir:

- Proceso de copia de seguridad regular.
- Administración de medios de respaldo: etiquetado, indexación, almacenamiento seguro externo, recuperación, etc.
- Proceso de restauración de datos.
- Copia de seguridad y recuperación de pruebas del sistema.

Replicación y respaldo de software

Si bien se debe hacer una copia de seguridad de los datos institucionales con regularidad para tener disponible la última versión, el software debe realizar una copia de seguridad sobre la base de una copia maestra de la última versión. El software no se debería copiar desde el sistema, ya que esto puede incorporar alteraciones en las copias de seguridad, este servicio proporciona una biblioteca de copia maestras de seguridad desde la cual se puede reinstalar el software en caso de requerir la recuperación.

Interfaz de usuario para la ciberseguridad

La interfaz de usuario debe ser fácil de usar y no presentar obstáculos significativos para las operaciones legítimas. Los elementos principales de una interfaz de usuario de ciberseguridad diseñada pueden ser ejemplo:

- Autenticación fuerte y fácil de usar.
- Inicio de sesión único a todas las aplicaciones.
- Pantallas de inicio de sesión basadas en GUI y mensajes operativos.
- Fácil navegación a través de menús jerárquicos e hipertexto.

Servicios de gestión de ciberseguridad

Los servicios de administración de ciberseguridad se dividen en dos grupos: servicios de administración de ciberseguridad de procedimientos y servicios técnicos de gestión de ciberseguridad.

Ilustración 19 Arquitectura lógica de los servicios de administración de seguridad

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

En el caso de los servicios de administración de ciberseguridad existe una arquitectura lógica básica que describe cómo funcionan. La Ilustración 19 muestra esto.

Gestión de políticas de ciberseguridad

Este grupo de servicios corresponde a dos tipos: de procedimiento y técnico, la creación y el acuerdo de políticas y estándares es claramente un proceso legal para la Fuerza.

Gestión de operaciones de ciberseguridad

Este es un conjunto de servicios que involucran servicios de procedimiento y servicios técnicos. El modelo de arquitectura lógico muestra cómo se entregan los servicios de ciberseguridad.

Aprovisionamiento de ciberseguridad

Estos servicios se ocupan de configurar los objetos de seguridad administrados.

Administración de ciberseguridad (gestión de privilegios)

La administración de privilegios de acceso es un caso especial de aprovisionamiento de la ciberseguridad. Una vez más La arquitectura lógica subyacente es como se muestra en la Ilustración 19.

Monitoreo de ciberseguridad

La supervisión de la ciberseguridad es otro subconjunto de los servicios de administración integrados en la arquitectura lógica. Los agentes de administración de ciberseguridad reportarán información del estado al centro de gestión de la ciberseguridad.

Medición de la ciberseguridad y métricas

En el centro de gestión de la ciberseguridad, los datos por el servicio de monitoreo deben ser recopilados y analizados para notificar sobre la información de gestión, incluida la medición del rendimiento en forma de métricas acordadas. Algunos de los elementos de rendimiento del entorno que podrían medirse incluyen:

- Tiempos de respuesta de los servicios de ciberseguridad.
- Preservación de la política de ciberseguridad en todos los dominios.
- Confirmación de que el proceso de autorización y autenticación está funcionando correctamente.
- Confirmación de que los servicios de no repudio y autenticación están funcionando correctamente.

- Relación entre el comportamiento real del sistema observado y la seguridad estándar.
- Líneas de base para fines de diagnóstico y planificación.

El desarrollo de métricas de ciberseguridad adecuadas es importante para la evolución de la arquitectura de ciberseguridad. El resultado final de esta actividad para la institución será saber con confianza si la ciberseguridad de los sistemas de gestión están funcionando y qué tan bien.

Gestión de alarmas de ciberseguridad

Las alarmas de ciberseguridad son manejadas por servicios en el centro de gestión de ciberseguridad. Se alimentan de los servicios de respuesta a incidentes.

Detección de intrusión

El ciberespacio ha facilitado el flujo de la información, al mismo tiempo ha promovido muchos peligros. Los ciberatacantes buscan objetivos vulnerables tales como sistemas no actualizados, sistemas infectados con troyanos y redes ejecutando servicios inseguros. Las alarmas son necesarias para notificar a los administradores y a los miembros del equipo de ciberseguridad de la Fuerza que ha ocurrido una entrada ilegal para que así estos puedan responder en tiempo real a la amenaza. Se han diseñado los sistemas de detección de intrusos como tales sistemas de notificación.

Un sistema de detección de intrusos protege a un sistema contra ciberataques, malos usos y compromisos. De igual manera, puede monitorear la actividad de la red, auditar las configuraciones de la red y sistemas por vulnerabilidades, analizar la integridad de los datos y más. Dependiendo de los métodos de detección que seleccione utilizar. (Red Hat Enterprise, Inc, 2003).

Si se produce un ciberataque en el Ejército Nacional, debe detectarse lo antes posible y notificarse para que los servicios de respuesta a incidentes puedan tomar las medidas apropiadas.

Los indicadores de incidentes de intrusión pueden incluir:

- Varias instancias del mismo usuario.
- Intentos fallidos de inicio de sesión y acceso a recursos no autorizados.
- Condiciones inusuales de carga de la red.
- Componentes que fallan pruebas de integridad.
- Direcciones de origen desconocido.
- Detección de ciertas firmas de ataques por un software especializado de monitoreo de intrusiones.
- Los agentes se implementan para monitorear plataformas de host y componentes de red.

La arquitectura lógica global para un sistema de detección de intrusos se muestra en la Ilustración 20.

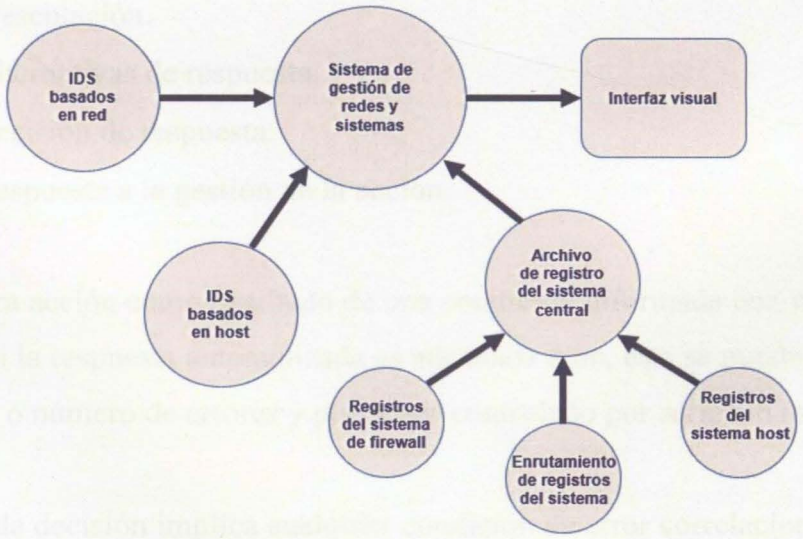

Ilustración 20 Arquitectura lógica para la detección de intrusiones

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Respuesta al incidente

En el evento de que la seguridad de un sistema haya sido comprometida, se requiere una respuesta a incidentes. Es la responsabilidad del equipo de seguridad responder rápida y efectivamente a los problemas. (Red Hat Enterprise, Inc, 2003).

Los servicios de respuesta a incidentes entregan acciones a incidentes de ciberseguridad detectados en la Fuerza, un incidente o grupo de incidentes requerirá un proceso de decisión: ¿qué se debe hacer a continuación?, la decisión sobre qué acción tomar puede ser automatizada en algunos casos y en otros casos requerirá intervención humana.

Los pasos lógicos requeridos para una respuesta apropiada al incidente incluyen:

- Recopilación de datos.
- Normalización de datos y de confrontación.
- Análisis de los datos.
- Evaluación de incidentes y conclusiones.
- Presentación.
- Alternativas de respuesta.
- Decisión de respuesta.
- Respuesta a la gestión de la acción.

La primera acción como resultado de una condición informada una vez analizada, es determinar si la respuesta automatizada es adecuada o no, esta se puede tomar en base al tipo de error o número de errores y puede ser controlado por scripts o motores lógicos.

La segunda decisión implica cualquier condición de error correlacionado, en la mayoría de los casos de falla del sistema se vuelve progresivo y puede requerir una acción rápida para contener el daño.

Un buen enfoque es desarrollar los peores escenarios y el análisis de requerimientos para que una configuración mínima sostenible sea conocida y pueda implementarse rápidamente. Esto incluiría la segmentación del dominio físico, la intervención humana, los firewall en el dominio crítico, enlaces de comunicaciones alternativos y otros recursos requeridos.

La arquitectura lógica global para la respuesta y la gestión de incidentes se muestra en la Ilustración 21.

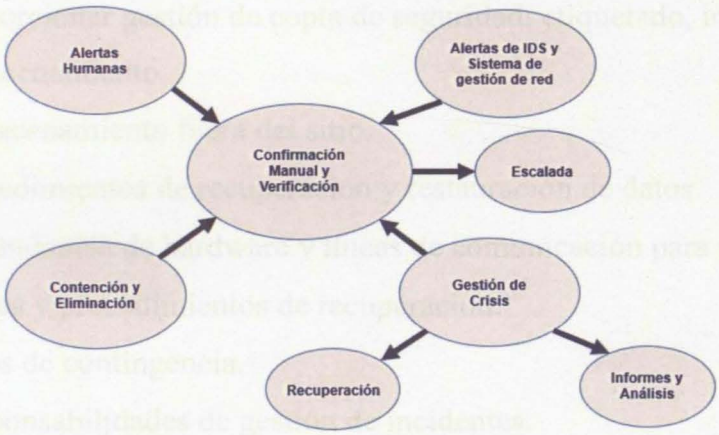

Ilustración 21 Arquitectura lógica para respuesta a incidentes

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Soporte al usuario

Muchos problemas operativos experimentados por los usuarios de sistemas y aplicaciones de la institución están relacionados con la ciberseguridad, los impactos potenciales de los problemas no resueltos son la pérdida de tiempo de producción y los servicios de ciberseguridad en desacato entre la comunidad de usuarios. Debe haber un soporte adecuado para el usuario a través de la función de mesa de ayuda de ciberseguridad para gestionar estos problemas y garantizar su oportuna resolución.

Recuperación de desastres

La recuperación ante desastres se basa esencialmente en medidas organizativas o en medidas técnicas que tienen un alcance más amplio que la ciberseguridad. A menudo se considera como parte de la gestión de la continuidad.

Los mecanismos que apoyan los servicios de recuperación de desastres incluyen:

- Tomar copias de seguridad apropiadas de datos y software.
- Proporcionar gestión de copia de seguridad: etiquetado, indexación, almacenamiento.
- Almacenamiento fuera del sitio.
- Procedimientos de recuperación y restauración de datos.
- Redundancia de hardware y líneas de comunicación para operaciones resilientes.
- Planes y procedimientos de recuperación.
- Sitios de contingencia.
- Responsabilidades de gestión de incidentes.
- Planes de activación.

Gestión de crisis

La gestión de crisis es un servicio organizativo y basado en procesos que se necesita para manejar incidentes. Es una extensión y escalamiento de los servicios de gestión de incidentes descritos anteriormente.

Auditoria del sistema

Los servicios de auditoría de ciberseguridad proporcionarán la recopilación y el análisis independiente de los registros del sistema de la Fuerza, están generalmente organizados por un equipo de auditoría de ciberseguridad especializado. Las técnicas y mecanismos

utilizados incluyen tanto la recopilación y el análisis de registros manuales como el uso de herramientas automatizadas de auditoría del sistema que comparan las configuraciones reales del sistema con las configuraciones esperadas.

Ciberseguridad física

Los servicios de ciberseguridad física incluyen los siguientes:

- Diseño e implementación, incluyendo instalaciones y perímetros del sitio.
- Protección de perímetros de zonas controladas.
- Autorización de personal para acceso físico a áreas controladas.
- Autenticación de personal en puntos de acceso físicos.
- Manejo de usuarios externos.
- Manejo de contratistas.
- Manejo de la actividad de mantenimiento.

Seguridad de personal

Los servicios de seguridad del personal incluyen lo siguiente:

- Contratación de políticas sobre antecedentes laborales, antecedentes penales, calificaciones.
- Verificaciones de antecedentes y verificación de referencias.
- Formación y sensibilización para todo el personal.
- Procesos disciplinarios.

13.2.2. Arquitectura de seguridad física

La arquitectura de ciberseguridad física para SABSA, describe la presentación de material duro de la organización, en el nivel lógico se habla de servicios, pero en el nivel físico se identifican los equipos involucrados, estando interesados ahora en el tamaño, la capacidad, el rendimiento, el número y ubicación de los dispositivos físicos que entregan los servicios lógicos.

Cifrado de archivos

Las técnicas criptográficas se pueden utilizar para mejorar la protección de la integridad de los archivos de la institución, mediante la computación de sumas de comprobación criptográficas en cada archivo o cada registro, si se realizan cambios no autorizados, esto puede ser detectado, aunque esto puede no ayudar a recuperar los datos originales. Como con todos los mecanismos criptográficos, gestionar y almacenar de forma segura las claves de autenticación es el principal desafío, estas claves deben colocarse en un lugar físicamente seguro, lo que implica algún tipo de manipulación del dispositivo de hardware resistente.

Ciberseguridad de la base de datos

La recuperación de la base de datos se gestiona a través de una serie de mecanismos de ciberseguridad:

- Copias de seguridad completas sobre una base semanal.
- Copia de seguridad de la base de datos para crear puntos de control.
- Copias de seguridad incrementales diarias.
- Registro de imágenes (antes): toma una imagen (copia) del registro antes de una transacción y almacenándolo en una tabla de diario.

- Registro de imágenes (después): toma una imagen (copia) del registro después de una transacción y almacenar en una tabla de diario.
- Después de restaurar la base de datos a un punto de control, se proporciona un retroceso desde el punto de control guardado a una posición comercial anterior, ejecutando las transacciones en el diario de imagen anterior en orden cronológico inverso contra la base de datos de puntos de control hasta el punto que se desea alcanzar.
- Después de restaurar la base de datos a un punto de control, se proporciona un avance desde el archivo guardado hasta el punto de control a una futura posición comercial mediante la ejecución de las transacciones en la imagen posterior diario en orden cronológico contra la base de datos de puntos de control hasta el punto deseado es alcanzado.

Reglas de ciberseguridad, prácticas y procedimientos

Reglas de ciberseguridad

Una regla será un filtro específico contra el cual los subsistemas de seguridad toman decisiones automatizadas, por ejemplo, las reglas se utilizan en los siguientes tipos de subsistema de ciberseguridad:

- Reglas de firewall: para determinar qué tipos de tráfico están o no permitidos.
- Reglas de la base de datos: para determinar qué tipos de acceso y qué tipos de acciones se permiten o no.
- Reglas del sistema de archivos: para tomar decisiones sobre el acceso a los datos.

La diferencia clave entre las reglas de ciberseguridad y las políticas de seguridad es que mientras que las políticas pueden requerir interpretación, las reglas de ciberseguridad son absolutas e inequívocas.

Prácticas y procedimientos de ciberseguridad

Las prácticas de ciberseguridad son descripciones genéricas de cómo lograr ciertos objetivos en la administración de seguridad de la institución. Las prácticas de ciberseguridad son más específicas que las políticas de seguridad e implican un contenido de comportamiento definido para ellos, pero no son tan específicos como los procedimientos de ciberseguridad.

Los procedimientos de ciberseguridad es donde se documentan paso a paso las instrucciones sobre cómo deben realizarse las tareas específicas, un procedimiento es específico para una plataforma o producto en particular, y se ocupa de los detalles de cómo funciona ese ambiente técnico específico.

Otro término que se utiliza en este contexto general es "directrices", estas son prácticas similares, pero tienden a estar más en el estilo de dar buenos consejos a las personas sobre cómo comportarse para cumplir con la política y para exhibir buenas prácticas. Las directrices requieren una buena interpretación.

Mecanismos de ciberseguridad

Un mecanismo de ciberseguridad es un medio físico mediante el cual se implementa un servicio de seguridad lógico, los mecanismos de la base de datos y del sistema de archivos podrían usarse con fines de ciberseguridad.

Mecanismos criptográficos y sus usos

La criptografía tiene roles muy específicos que desempeñar en la obtención de la información. Existen cuatro servicios de seguridad fundamentales que pueden implementarse en la Fuerza mediante criptografía:

- Confidencialidad: evitar la divulgación no autorizada de información.
- Integridad: proteger el contenido de la información para que no se modifique de ninguna manera sin esto ser detectado (no puede evitar las alteraciones mediante el uso de la criptografía, pero puede asegurar que serán detectados).
- Autenticidad: probar que la información se originó de una fuente confiable auténtica.
- No repudio: evitar que una parte deshonesta luego niegue (repudie) la autenticidad de la información proporcionada por esa parte.

La eficacia de los mecanismos criptográficos está relacionada principalmente con la cantidad de bits en la clave criptográfica y por tanto, el número de valores clave posibles. Esta afirmación asume que no hay debilidades analíticas específicas en el algoritmo y que el criptoanalista debe confiar en la búsqueda en todo el espacio clave para encontrar el valor que se está utilizando.

Mecanismos de cifrado

Los mecanismos de cifrado garantizan que se hace un uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad, integridad, autenticidad y el no repudio de la información sensible manejada por una empresa, tanto almacenada como en tránsito. Por ejemplo: datos de carácter personal, información sensible o información confidencial, backups en la nube o en proveedores externos, datos en móviles o dispositivos extraíbles, contratos, etc. (Instituto Nacional de Ciberseguridad de España, 2017).

Un mecanismo de cifrado transforma los datos originales sin procesar (llamados texto sin formato) en un cifrado la forma de los datos (llamado texto cifrado). Si se utiliza un algoritmo de cifrado de buena calidad, la transformación es compleja y opaca, de modo que no es factible que un oponente analice el texto cifrado (un proceso llamado análisis criptográfico) para descubrir el texto plano original. En la mayoría de los casos la transformación es controlada por una clave de cifrado este es un dato adicional que influye

en la transformación, para un texto simple dado, si cambia la clave obtendrá un texto cifrado diferente. El mapeo del resultado del texto cifrado a la clave es igualmente opaco de manera que el oponente no puede determinar el valor de la clave por criptoanálisis.

Otros mecanismos de cifrado

- Certificados de clave pública.
- Mecanismos de firma digital.
- Mecanismos de intercambio de autenticación.
- Mecanismos de gestión de claves criptográficas.

Ciberseguridad de infraestructura de red

Esta sección describe los mecanismos de ciberseguridad más importantes que se pueden utilizar para proporcionar ciberseguridad en la institución dentro de la plataforma e infraestructura de red.

Ciber-resiliencia

Tomando como referencia lo dicho por Lucas Paus de ESET (2018), la resiliencia es la capacidad de un sistema para volver a su forma original, o lo que es lo mismo; recuperarse y volver a su normal funcionamiento luego de sufrir un incidente.

La idea detrás del desarrollo de la resiliencia, además de ayudar a la institución a saber lidiar con una situación para la cual no está preparada, pasa por reconocer la complejidad de un escenario y prepararse mediante la elaboración de un plan de contingencias y defensas en distintos niveles de seguridad. De esta manera, se podrá mitigar de la mejor manera posible el impacto de futuros ciberataques. (Lucas Paus - ESET , 2018).

La infraestructura de la red física en la Fuerza, se debe construir en configuraciones resilientes para incorporar un grado de tolerancia a fallos, la cantidad de estas (y por lo tanto el costo de proporcionarlo) dependerá de los requisitos para la capacidad de recuperación y continuidad de las operaciones.

Los principios fundamentales del diseño resilientes son:

- Evitar puntos únicos de falla asegurando que siempre haya un mecanismo alternativo para entregar una función o servicio dado.
- Redundancia de componentes físicos fuertes, de manera que si uno falla, otro está disponible para toma su lugar.
- Procedimientos de copia de seguridad y restauración para todos los componentes físicos, como el software y datos.
- Los procedimientos de recuperación se elaborarán por adelantado para todos los escenarios de falla previsibles.
- Recuperación y reconfiguración automatizadas cuando sea posible.
- Extenso registro de eventos, monitoreo e informes para ayudar a prevenir posibles fallas antes de que ocurran y para ayudar a la recuperación proporcionando evidencia de la naturaleza del fracaso.

Al aplicar estos principios al diseño de topologías de red, una serie de enfoques específicos se utilizan comúnmente:

- Múltiples cables y canales de comunicaciones, a menudo con diversos enrutamientos físicos.
- Separación de las rutas de cable de las instalaciones para evitar que todos los cables múltiples sufran el mismo fallo físico.
- Intercambios telefónicos alternativos para enrutar líneas de telecomunicaciones de terceros desde un sitio determinado.

- Operadores de telecomunicaciones alternativos.
- Redireccionamiento automático dinámico y reconfiguración para crear una red de recuperación automática basado en una red multirruta de conexiones.
- Pruebas y monitoreo regulares de estas diversas características de resistencia para asegurarse de que estén funcionando correctamente.
- Duplicar marcos donde las líneas de telecomunicaciones externas están terminados y conectados a la infraestructura de las instalaciones.

Los mismos principios también se aplican para proporcionar facilidades de plataforma host altamente resilientes para aplicaciones:

- Instalaciones de procesamiento dual en centros de datos separados, a menudo separados geográficamente por varios kilómetros.
- Sistemas informáticos tolerantes a fallos con sistemas operativos especiales o middleware que organiza automáticamente la duplicación de datos o el procesamiento distribuido.
- Configuraciones RAID para el almacenamiento de datos.

Topología de la red

Comprende cajas reales, enrutadores, firewalls, plataformas de servidores, plataformas de clientes, etc., y conexiones de red reales, tanto de LAN como de WAN. Una vez se ha capturado con precisión los dominios lógicos, es relativamente sencillo diseñar la implementación física de los mismos. Sin embargo, es difícil pasar por alto el paso del dominio lógico sin conseguir la topología física correcta.

Las principales características para una topología de red segura en la Fuerza son:

- El dominio de producción está contenido detrás de los firewalls internos en el centro de datos, la arquitectura de firewall debe comprender una combinación de hosts endurecidos para resistir ciberataques de doble origen y enrutadores de detección.

- El acceso público de internet y los servicios web se realizarán a través de un enrutador de detección que solo conduce a la LAN externa en la que se encuentra el servidor web.

- Los firewalls internos en todas las conexiones WAN corporativas aíslan este dominio de todos los demás dominios.

- El host VPN (otro host endurecidos para resistir ciberataques de doble enlace) proporciona una segunda ruta con doble búfer a internet y soporta el tráfico de usuarios de la institución que requieren acceso desde otro sitio.

- Los clientes de VPN se usan para usuarios de la institución que requieren acceso desde otro sitio, para construir la implementación física de la red privada que utiliza protocolos de internet, comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información digital de la Fuerza.

- Los servicios asociados y los servidores de servicios externos se deben encontrar en subredes protegidas separadas también fuera del dominio de producción principal.

- Nadie debería tener acceso directo a los principales servidores de aplicaciones en el centro de datos, excepto para el personal de operaciones del centro de datos. Todo el acceso de los usuarios es a través de firewall internos y a través de WAN corporativa, todo el acceso a la intranet es a través de servidores intermedios, nunca directamente a las aplicaciones en sí mismas.

13.2.3. Arquitectura de seguridad de componentes

La arquitectura de ciberseguridad de los componentes es la visión de la vida del comerciante: las herramientas especializadas y componentes del producto de la arquitectura de ciberseguridad.

Normas internas de ciberseguridad

Además de los diversos estándares internacionales, nacionales y de la industria que promueven la operatividad, se necesitará propios estándares de ciberseguridad internos para promover la coherencia y las buenas prácticas a través de la institución.

Los estándares de ciberseguridad interna mínimos incluirán lo siguiente:

- Estándares de ciberseguridad para cada tipo de plataforma en uso de la institución, indicando los estándares para configurar y operar esas plataformas.

- Estándares criptográficos, que definen los algoritmos y protocolos que se utilizarán para ciertas aplicaciones, generalmente alineadas con estándares externos.

- Normas de gestión de contraseñas, que tratan la longitud de la contraseña, la sintaxis de la contraseña, frecuencia de cambio, etc.

- Normas de seguridad física para diversos tipos de instalaciones.

- Normas de documentos para todo tipo de documentos relacionados con la ciberseguridad.

- Normas de interfaz de comunicaciones seguras para conectar aplicaciones a la infraestructura institucional.

- Estándares de interfaz de usuario para proporcionar un inicio de sesión consistente.

Productos y herramientas de ciberseguridad

La Tabla 15 tabula algunos de los tipos más comunes de herramientas y productos de ciberseguridad y proporciona una visión general de las características más comunes de esos componentes para aplicar a la institución.

Tabla 15 Herramientas y productos de ciberseguridad

Tipo de componente	Características comunes / Mecanismos
Herramientas antipiratería	Prevención de la copia y distribución ilegal de software
Dispositivos antirrobo	Prevención del robo de elementos de equipos como PC
Escáneres antivirus	Escanear en busca de virus conocidos y otro software malicioso, y reparar cualquier archivo dañado (aunque la reparación no puede ser perfecto y por lo tanto puede no ser la forma correcta de proceder)
Dispositivos biométricos	Proporcionando autenticación personal basada en la medición de una característica corporal, como huella dactilar, patrón de retina y facial
Software de protección de arranque	Prevenir el arranque de una PC desde un disquete para obtener acceso no autorizado al disco duro
Planificación de la continuidad del negocio y herramientas de planificación de recuperación de desastres	Apoyando la recogida y gestión de la planificación
Herramientas de informática forense	Recuperar datos borrados y juntar un historial de actividad
Filtrado de contenidos por correo electrónico	Detección y filtrado de contenido inaceptable.
Filtrado de contenidos para la navegación	Detección y filtrado de contenido inaceptable.
Hardware criptográfico	Proporcionando procesamiento criptográfico de alto rendimiento, almacenamiento de claves de seguridad, fuente de tiempo segura, número aleatorio Generación para la gestión de llaves, cerramientos a prueba de manipulaciones
Kits de herramientas de software criptográfico	Tiempo de ejecución para cifrado de datos, autenticación, digital. Procesamiento de firmas y certificados
Sistemas de gestión de respaldo de datos	Copia y gestión de almacenamiento, y restauración a una posición comercial previa
Productos de directorio	Proporcionar servicios de directorio
Caja fuerte de documentos	Protección de documentos contra robo y daños por incendio

Tipo de componente	Características comunes / Mecanismos
Herramientas de gestión de seguridad organizacional	Administrar una amplia gama de servicios de seguridad en múltiples plataformas
Soluciones informáticas tolerantes a fallos	Plataformas informáticas resistentes que sobrevivirán al fallo de los componentes.
Productos de cifrado de archivos	Cifrado de archivos para transmisión o para almacenamiento.
Firewalls	Filtrado del tráfico de red según origen, destino y contenido para permitir solamente el tráfico autorizado
Sistema de detección de intrusos	Buscando actividad no autorizada de intrusos tanto en la red y en plataformas de host
Productos de seguridad LAN	Proporcionar funcionalidad de seguridad en redes de área local
Plataformas operativas	Control de acceso lógico y protección de integridad
Tokens de autenticación personal y dispositivos	Autenticación multifactor de los usuarios.
Alarmas de seguridad física	Alarmas contra intrusos y alarmas contra incendios en edificios y salas de computadoras
Software PKI	Gestión de certificados digitales y los servicios criptográficos que admite.
Herramientas de evaluación de riesgos	Paquete de software para capturar y procesar datos de riesgo
Soluciones de control de acceso basadas en roles	Administración centralizada de control de acceso basada en roles y autenticación de usuarios
Productos de middleware seguros	Proporciona comunicaciones seguras de nodo a nodo y una API para que las aplicaciones llamen a servicios de seguridad
Herramientas de auditoría de seguridad	Herramientas de inspección automatizadas para verificar la configuración de una plataforma o aplicación operativa
Productos de software de seguridad	Productos de software complementarios para proporcionar niveles adicionales de control de acceso a sistemas operativos estándar
Soluciones de servicio de autenticación de inicio de sesión único	Servidores de autenticación centralizados que integran aplicaciones distribuidas y proporcionan un front-end de autenticación con inicio de sesión único
Tarjetas inteligentes	Una computadora autónoma en una tarjeta de plástico con sus propias funciones de autenticación y control de acceso a bordo
Herramientas de gestión de licencias de software	Administrar la distribución de software con licencia para garantizar el cumplimiento de la licencia
Fuente de poder ininterrumpida	Protección contra fallas de energía eléctrica
Productos VPN	Redes privadas virtuales creadas con IPsec o SSL
Herramientas de escaneo de vulnerabilidades	Buscando agujeros en la red o configuraciones de host
Productos de seguridad inalámbrica	Prevención de espionaje y autenticación de nodos

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

13.2.4. Arquitectura de seguridad operacional

Para Sherwood (2005), las operaciones se mapean en la tercera y cuarta etapas del ciclo de vida del SABSA (implementar, administrar y medir, que tratan de cómo se desarrolla y aplica el arquitectura de ciberseguridad operacional, que es la vista del administrador quien se preocupa por mantener la ciberseguridad de los procesos y sistemas completamente operativos durante toda su vida útil.

La arquitectura de ciberseguridad operacional describe los procesos, procedimientos, métodos y acciones mediante los cuales se operan los sistemas de una manera segura.

Gestión de la política de ciberseguridad

La política de ciberseguridad será la representación lógica de los requisitos de la arquitectura de seguridad y control de la institución, por lo tanto puede verse como algo que una vez determinada es una impulsora clave del programa operativo de gestión de la ciberseguridad en su conjunto.

Una visión cultural de la política de ciberseguridad

La política de ciberseguridad debe ser una cultura dentro de la institución. Describirá la forma en que los usuarios se comportan cuando hacen su trabajo, debe ser una mentalidad que ha sido aceptada en todos los niveles de la Fuerza y sus resultados pueden ser vistos en todas partes en la forma en que se llevan a cabo los procesos.

Los requisitos de ciberseguridad traducidos a una estructura lógica que puede aplicarse de manera consistente monitoreada y medida, deben ser únicos y comunicarán las intenciones para administrar el riesgo y hacer cumplir la ciberseguridad en la institución.

Estructuración del contenido de una política de ciberseguridad

El driver crítico para tomar las decisiones sobre la estructura y el contenido de la política de ciberseguridad deberá ser:

¿Cuál es el propósito de esta política de ciberseguridad?

- Lo que probablemente se desea de una política es un medio para influir en la mentalidad y por lo tanto en el comportamiento de ciertas personas en la institución, definir los usuarios a quienes se dirige esta política de ciberseguridad es clave.

¿A qué comportamiento se está tratando de influir?

- Si al definir el grupo al que va dirigida la política resulta difícil, entonces se debe hacer una lista de estos considerando para cada uno qué tipo de política de ciberseguridad se necesitara para influir en este grupo, algunos usuarios podrían estar en más de uno grupo y deberán conocer más de una política.

Política y arquitectura jerárquica

Se necesitarán políticas dirigidas a diferentes grupos de usuarios, una política de ciberseguridad de la institución de nivel superior estará dirigida a todos. Se emitirá con la autoridad superior de la institución y debe llevar su firma, esta política es un mensaje de los altos mandos a todos en la institución.

Debajo de esta política de ciberseguridad superior, habrá otras políticas más detalladas que están destinadas a subgrupos específicos de usuarios, aunque algunas de estas podrán ser aplicables a todos (ejemplo: política de uso aceptable). Estas políticas secundarias reforzarán la política de ciberseguridad institucional.

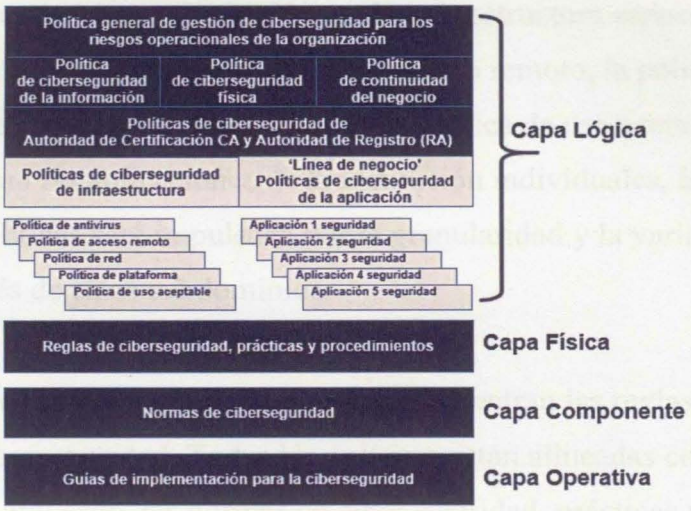

Ilustración 22 Una arquitectura de política jerárquica sugerida

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

La política de nivel superior (política general de gestión de ciberseguridad para los riesgos operacionales de la institución) sugiere reunir todos los temas comunes de la gestión del riesgo operacional en todas las disciplinas.

En la siguiente capa habrá políticas para diversificar el riesgo operacional en sus disciplinas constitutivas. Los tres dominios: política de ciberseguridad de la información, política de continuidad del negocio y política de ciberseguridad física.

El tercer nivel para políticas en la Ilustración 22 muestra las políticas de seguridad de CA y RA, estas se refieren a las autoridades de certificación y de registro que se esperaría en la arquitectura de ciberseguridad de la organización construida alrededor del concepto de infraestructura de clave pública y certificados digitales. En un entorno de este tipo, potencialmente habrá varios dominios en los que las entidades están registrados y emitidos con certificados digitales, las autoridades de certificación y de registro que controlan estos dominios: tienen políticas que establecen los requisitos dentro de los dominios.

En el cuarto nivel está el lugar para políticas de infraestructura específicas, incluidos ejemplos como la política antivirus, la política de acceso remoto, la política de seguridad de la red, la seguridad de las políticas de plataforma y política de uso aceptable. También a este nivel se encuentran las aplicaciones de la institución individuales, la decisión sobre cómo dividir estas políticas será impulsada por la granularidad y la variabilidad de riesgo organizacional a través de estos subdominios.

En el quinto nivel de la jerarquía de políticas se encuentran las reglas, prácticas y procedimientos de ciberseguridad. Todas las políticas están alineadas con la arquitectura de seguridad lógica. Sin embargo, las normas de ciberseguridad, prácticas y procedimientos están alineados con la arquitectura de seguridad física.

En el sexto nivel de la jerarquía de políticas, la ciberseguridad deberá estar alineada a través de estándares internos y externos, internacionales, nacionales y operacionales.

Finalmente, en la base de la jerarquía hay una capa donde puede colocar documentos que proporcionan pautas de implementación, dando consejos sobre cómo usar o implementar ciertas herramientas o productos.

Política de ciberseguridad corporativa

Son las políticas a más alto nivel que debe tener la institución, en este punto el Comandante debe establecer una administración clara y demostrar su apoyo y compromiso con la ciberseguridad a través del tema de una política en toda la Fuerza.

Las políticas corporativas deben abordar los siguientes puntos:

- La política a este nivel debe originarse del nivel más alto de la gerencia. Preferiblemente debe ser firmado personalmente por el alto mando de la institución.

- Para obtener dicho protección de alto nivel, se deberá invertir tiempo en desarrollar la política, principalmente en un proceso de consulta amplia en toda la institución para garantizar que representa una visión de consenso y no son solo las opiniones personales de un individuo.
- La política debe referirse a la gestión de riesgos de la institución como el principal promotor.
- La necesidad de ciberseguridad y gestión de riesgos debe estar relacionada con los objetivos generales de la institución.
- La política debe proporcionar un mandato fuerte, instruir en todos los niveles y a los usuarios en general formar comportamientos.
- La política debe delegar formalmente la responsabilidad con frases como ejemplo: "los directores son responsables de..." y "todo el personal es responsable para…"
- Mencionar los temas de propiedad y custodia.
- Podría mencionar específicamente el cumplimiento de leyes, regulaciones y contratos.
- Debe referirse a un proceso de notificación de presuntos incidentes de ciberseguridad.
- Debe mencionar la necesidad de educación, capacitación y la provisión de un centro de experiencia para brindar asesoría interna y soporte en temas de ciberseguridad.
- Debe referirse a otros documentos donde se pueden encontrar más detalles.

Principios de política

Hay una serie de principios que pueden ayudar a formular políticas de ciberseguridad en la institución, estos no son presentados como algo a lo que debe adherirse a la letra, de hecho, algunos de estos principios pueden ser contrarios a sus intenciones en algunas circunstancias. Deben verse simplemente como un recurso en el que puede inspirarse.

- Principio de privilegios mínimos: los usuarios y los procesos del sistema deberán recibir la menor cantidad posible de autoridad y accesos mínimos a los recursos necesarios para realizar una tarea determinada.

- Principio de responsabilidad: todos los eventos significativos del sistema y del proceso deben ser rastreables.

- Dependencia mínima del principio de secreto: los controles aún deben ser efectivos incluso si un ciberatacante sabe de su existencia y conoce su modo de operación.

- Principio de automatización del control: se deben utilizar controles automáticos, en lugar de controles que dependen de la vigilancia humana y el comportamiento humano.

- Principio de ciber-resiliencia: los sistemas deben diseñarse y administrarse de manera que, en caso de imperfección compromete el menor daño posible y los inconvenientes causados.

- Principio de defensa en profundidad: los controles se deben colocar en capas de manera que si una capa de control falla, hay otro tipo diferente de control en la siguiente capa que evitará la violación de la seguridad.

- Principio de excepción aprobada: las excepciones de política siempre deben tener la aprobación de la administración.

- Principio de anulación de emergencia segura: los controles solo deben anularse de forma predeterminada y de forma segura. Los sistemas son más vulnerables cuando se eliminan los controles normales, por ejemplo por mantenimiento de emergencia u otras razones similares. Siempre debe haber procedimientos y controles para minimizar el nivel de riesgo en estas circunstancias.

- Principio de auditoría: debe ser posible que un experto independiente verifique que el sistema se ajusta a la política de ciberseguridad, una condición necesaria, pero no totalmente suficiente para esto es que el sistema debe ser capaz de registrar eventos relacionados con la ciberseguridad en un dispositivo a prueba de manipulaciones en el registro de auditoría.

Clasificación de la información

Una forma de abordar la política de ciberseguridad y su implementación es clasificar la información en una de varias clasificaciones, cada una de las cuales tiene una política de ciberseguridad asociada. Así, una vez clasificada la información de la institución debe ser manejada bajo los términos de la política de ciberseguridad asociada.

El concepto de clasificación de la información se ha desarrollado durante muchos siglos en organizaciones militares y gubernamentales, es habitual definir varios niveles de clasificación, como ultrasecreto, secreto, confidencial y restringido, dejando todo lo demás sin clasificar de forma predeterminada, cada documento (u objeto) se clasifica en uno de estos niveles. Cada objeto también está marcado de forma que pueda decidirse sobre cómo debe manejarse, de acuerdo con la política de ciberseguridad pertinente.

Las personas (sujetos) que podrían acceder a los documentos (objetos) reciben una autorización en uno de estos niveles, alguien que está autorizado a nivel secreto puede leer cualquier documento clasificado como secreto, pero no está permitido leer documentos clasificados como de ultrasecreto, los niveles de autorización del sujeto y las clasificaciones de objetos son un elemento fundamental de los sistemas de seguridad multinivel (MLS).

La idea luego deberá ser transportada a la integridad de los datos, diferentes niveles de protección de integridad pueden ser definidos, como "sensible para misión operacional", "sensible para función misional" y por defecto, todo lo demás es "no sensible".

Si bien todos estos modelos son muy buenos en teoría, en la práctica son difíciles de operar y utilizar, incluso en el entorno militar estos modelos plantean muchas dificultades prácticas, y deben aplicarse con sumo cuidado para garantizar que los sistemas de la Fuerza ofrezcan una funcionalidad útil para la comunidad de usuarios.

Clasificación del sistema

Una forma mucho más útil de abordar la clasificación como un medio para administrar la política de ciberseguridad podría ser para clasificar los sistemas o aplicaciones según el nivel de riesgo organizacional (alto/medio/bajo) revelado a través de una evaluación de riesgos, la razón para hacer esto es establecer una política de ciberseguridad para cada nivel de riesgo y asociar cada sistema con un procedimiento de control específico: un conjunto estándar de controles que se debe aplicar para proteger el sistema de aplicación de acuerdo con el nivel de riesgo especificado en la política de ciberseguridad asociada.

Se puede diversificar esto a otro nivel teniendo el nivel de riesgo establecido para los atributos (como confidencial, integridad protegida y disponibilidad) porque el régimen de control estándar para cada uno será diferente. Así, un sistema puede ser clasificado como de alto riesgo para disponibilidad, riesgo medio para integridad protegida y bajo riesgo para confidencialidad.

Los beneficios de este enfoque son:

- Proporciona a la institución un método para garantizar un enfoque coherente y estandarizado para hacer cumplir políticas de ciberseguridad en múltiples sistemas y aplicaciones en una organización grande y compleja como el Ejército Nacional donde hay diversos sistemas de aplicación.
- Asegura que el nivel de seguridad y control en cada sistema de aplicación se adapte al riesgo organizacional percibido para ese sistema y está en línea con la política de ciberseguridad apropiada a ese nivel de riesgo.

- Es completamente transparente para la comunidad de usuarios que no tienen que involucrarse en cualquier decisión sobre cómo manejar un documento específico, los administradores del sistema aplican el régimen de control de la política de ciberseguridad en el nivel del sistema, no en el nivel del usuario.
- Hace que el trabajo de auditoría de ciberseguridad de los sistemas sea más simple, ya que elimina el juicio subjetivo e introduce un conjunto objetivo de criterios para la auditoría.

El equipo de auditoría ahora puede verificar:

- ¿Se ha realizado la evaluación de riesgos de la institución para el sistema de aplicación correctamente?
- ¿Las categorías de riesgo de la institución para el sistema de aplicación han sido fijadas correctamente?
- ¿El régimen de control del sistema de aplicación cumple con la ciberseguridad, la política y los controles estándar están asociados con las categorías de riesgos asignados al sistema?
- ¿Si se encuentran brechas entre los estándares de control y la aplicación real del sistema, hay una buena razón? ¿Existen otras circunstancias atenuantes? ¿Qué acciones correctivas se requieren?

Políticas de ciberseguridad del sistema de aplicación

Si la institución adopta el enfoque según el cual cada sistema de aplicación es evaluado en función de unos pocos atributos organizacionales (como confidencial, protegido por integridad y disponibilidad) entonces necesitará una política de ciberseguridad del sistema de aplicación para cada categoría de riesgo y atributo, como se ve en la Ilustración 23.

Este pequeño número de políticas de aplicación se puede aplicar a un gran número de sistemas de aplicación, haciendo que el proceso de establecimiento de políticas y gestión de

políticas sea eficiente y también garantizando prácticas de gestión de riesgos consistentes en todas las aplicaciones.

	Riesgo bajo	Riesgo Medio	Riesgo Alto
Confidencial	Política 1	Política 2	Política 3
Integridad	Política 4	Política 5	Política 6
Disponibilidad	Política 7	Política 8	Política 9

Ilustración 23 Matriz de políticas de seguridad de los sistemas de aplicación

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Otra posibilidad es tener un conjunto de políticas de ciberseguridad para cada nivel de riesgo con cada línea institucional. Esto proporciona eficiencia al limitar el número total de políticas en uso. La Ilustración 24 muestra este enfoque.

	Riesgo bajo	Riesgo Medio	Riesgo Alto
Línea de negocio A	Política 1	Política 2	Política 3
Línea de negocio B	Política 4	Política 5	Política 6
Línea de negocio C	Política 7	Política 8	Política 9
Línea de negocio D	Política 10	Política 11	Política 12
Línea de negocio E	Política 13	Política 14	Política 15

Ilustración 24 Matriz de política de seguridad de línea de negocio

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

La política de ciberseguridad del sistema de aplicación se refiere a:

- Autorización (el proceso de otorgar un privilegio).
- Autenticación (el proceso de verificación de identidad).

- Control de acceso (el proceso de toma de decisiones de acceso basado en la verificación de autorizaciones y autenticando la identidad).
- Auditoría (el proceso de escribir, almacenar y revisar registros de todos los intentos de acceso, decisiones y resultados).
- Administración (privilegios de administración y todas las actividades asociadas).
- Seguridad de comunicaciones de aplicación a aplicación.

Políticas de ciberseguridad de la plataforma

Una plataforma es una caja de hardware combinada y su sistema operativo puede ser utilizado para alojar una o múltiples aplicaciones. Las plataformas incluyen supercomputadoras; servidores, PC, portátiles y cualquier otro tipo de computadora.

Un factor distintivo importante con respecto a la política de ciberseguridad es el sistema operativo, pero también puede haber aspectos clave del hardware (como su portabilidad y el entorno en que podría ser utilizado) que también impulsará la política de la Fuerza.

A partir de las diferentes combinaciones de hardware y el sistema operativo se debe desarrollar una política de ciberseguridad (y también estándares de seguridad asociados) para cada uno de estos tipos de plataformas.

Se debe tener en cuenta el nivel de riesgo de la aplicación, en el caso de múltiples aplicaciones en la misma plataforma, habrá que preguntarse ¿Cuál será la política de ciberseguridad de la plataforma de alto riesgo? es decir, ¿Será apropiada para la aplicación de mayor riesgo?, cuanta más granularidad se introduce, más complejo y menos eficiente se convierte el proceso de gestionar las políticas.

Los principales principios estratégicos para conducir las políticas de ciberseguridad de la plataforma serán:

- Reducir las vulnerabilidades en las plataformas de procesamiento de información e infraestructura.
- Segregar y aislar plataformas, y entornos de producción de aquellos utilizados para desarrollo y pruebas.
- Proporcionar y mantener entornos de ejecución altamente confiables para personas altamente sensibles.
- Proporcionar entornos de almacenamiento seguros para datos almacenados no volátiles altamente sensibles.

Políticas de ciberseguridad de red

La institución necesitará desarrollar una política de ciberseguridad que rija a todo el dominio de red y se aplique a todas las partes de ella. También puede ser necesario desarrollar una serie de redes políticas de subdominio, dependiendo el grado de separación que requieres entre estos subdominios.

Cuando haya implementado redes privadas virtuales (VPN), éstas deberán regirse por una política. Los firewalls también necesitan una política de seguridad que se convierta en reglas en la capa física capa para configurar el firewall.

Los problemas que las políticas de ciberseguridad de la red de la institución deberán abordar los principios estratégicos de seguridad de la red se conocen como servicios de seguridad en la capa de transferencia de información (Red).

Otras políticas de seguridad de infraestructura

Hay otros aspectos de la infraestructura de las TIC que necesitarán políticas de ciberseguridad específicas dentro de las cuales se pueden incluir:

Políticas generales de seguridad de infraestructura:

- Antivirus y otras políticas de malware.
- Política de acceso remoto.
- Política de uso aceptable.
- Política de autenticación del usuario y de seguridad del servicio de directorio
- Política de seguridad de middleware.
- Política de seguridad de gestión de datos.
- Política de los servicios de gestión de la seguridad.

Organización de la ciberseguridad y responsabilidades

Uno de los temas importantes que debe abordar la Fuerza es con respecto a quién o quienes dentro de la institución son responsables de la ciberseguridad. Entendiendo que todo individuo que de una u otra manera interactúa con el ciberespacio y hacen uso de las aplicaciones y sistemas informáticos interconectados son responsables de ello.

Sin embargo, hay una jerarquía de responsabilidades de manera específica, lo que implica que hay una estructura organizativa dedicada a la gestión de la ciberseguridad, incluida la formulación de políticas de ciberseguridad.

La responsabilidad en la materia, debe comenzar desde lo más alto de la estructura organizativa, es decir, desde el Comandante del Ejército Nacional; en este nivel hay una responsabilidad ante los entes superiores a este como el Comando General de las Fuerzas Militares, el Ministerio de Defensa y la Presidencia de la República, para asegurar que su misión se gestione adecuadamente. Esta cae bajo el paraguas general del gobierno corporativo e incluye el establecimiento de riesgos de alto nivel lo que se traduce en políticas de gestión.

En el siguiente nivel están los Comandantes de las Jefaturas de la Fuerza, para el caso específico de la ciberseguridad y ciberdefensa se comparte la responsabilidad entre la

Jefatura de Estado Mayor de Planeación y Políticas y la Jefatura de Estado Mayor de Operaciones del Ejército, es allí, donde se planean y ejecutan las para la gestión del riesgo cibernético en la institución. Para que esto sea posible, este equipo debe crear un marco organizativo específico para gestionar todos los aspectos de la ciberseguridad corporativa en general y en particular.

Las diversas unidades que participan en la gestión de la ciberseguridad de la información, indican el liderazgo:

Los Altos Mandos deberán:

- Aprobar e instruir la política de gobierno corporativa general.
- Establecer metas y expectativas para la gestión de riesgos.
- Aprobar los principales presupuestos para iniciativas y programas de ciberseguridad.

El Grupo de Ciberseguridad será responsable de:

- Revisar y aprobar la política de ciberseguridad y ciberdefensa, las políticas subordinadas según lo desarrollado y propuesto por el Comandante del Ejército.
- Apoyar iniciativas para desarrollar los programas de ciberseguridad.
- Planear todas las actividades relacionadas con la ciberseguridad.
- Monitoreo de las principales ciberamenazas que enfrenta la institución.
- Aprobación de metodologías y procesos específicos para la gestión de la ciberseguridad en toda la institución.
- Promover la visibilidad del apoyo de la institución para las actividades de ciberseguridad.
- Seguimiento y revisión de incidentes de ciberseguridad significativos.

- Proporcionar un canal de comunicaciones para escuchar vistas, ideas y aportaciones de todos aquellos con responsabilidades operativas para algún aspecto de la ciberseguridad.
- Proporcionar un canal de difusión para comunicar nuevas políticas, procesos y metodologías para todos aquellos con responsabilidades operativas para algún aspecto de la ciberseguridad.
- Encontrar la resolución de problemas operativos o escalarlos si se trata de una resolución inmediata.

Desarrollo de la cultura de ciberseguridad

El primer componente clave de una cultura es una declaración de política de ciberseguridad corporativa firmada en el nivel más alto nivel de la institución. Todos deben ver esta política como el eje de la postura de ciberseguridad en la Fuerza.

El reporte regular y constante de incidentes de ciberseguridad es una parte importante del desarrollo cultural. Así, el número y tipo de los incidentes se pueden utilizar como una métrica del éxito.

Otro aspecto del desarrollo de la cultura de ciberseguridad es el programa de educación y capacitación las cuales deben llevarse a cabo, de acuerdo con las necesidades específicas de la institución. Éstas incluyen:

- Capacitación de inducción para todos los empleados nuevos para garantizar que estén plenamente conscientes de la política de ciberseguridad y que entiendan cómo aplicarla a sus actividades diarias.
- Capacitación técnica específica para cualquier persona cuyo trabajo incluya una actividad técnica relevante para mantener la postura de ciberseguridad.
- Cursos cortos sobre diversos aspectos de la ciberseguridad, incluidos nuevos temas a medida que surgen, como nuevas amenazas, nuevas soluciones, nuevos productos y nuevas tecnologías.

Gestión del riesgo operacional

Es importante que la institución haga una revisión de los objetivos de la gestión del riesgo operacional, tales como, comprender el perfil de riesgo de la organización en detalle y tomar decisiones bien informadas sobre la mitigación de riesgos y la toma de riesgos.

La complejidad de la gestión del riesgo operacional

Modelado estadístico

El cálculo de un valor en riesgo (VAR, por sus siglas en inglés) para un evento de pérdida particular generalmente se basa en alguna fórmula que tiene la estructura fundamental, así:

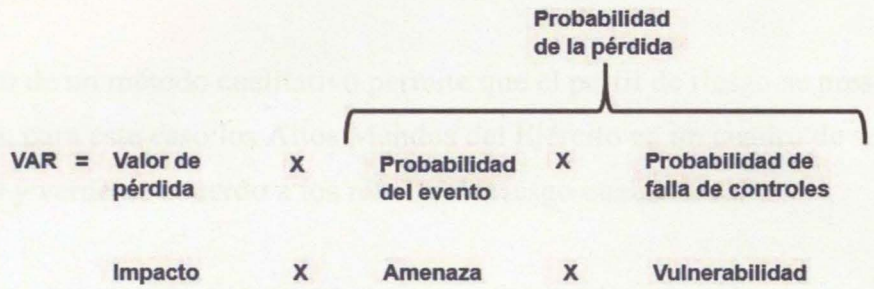

Ilustración 25 El cálculo del valor de riesgo (VAR)

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

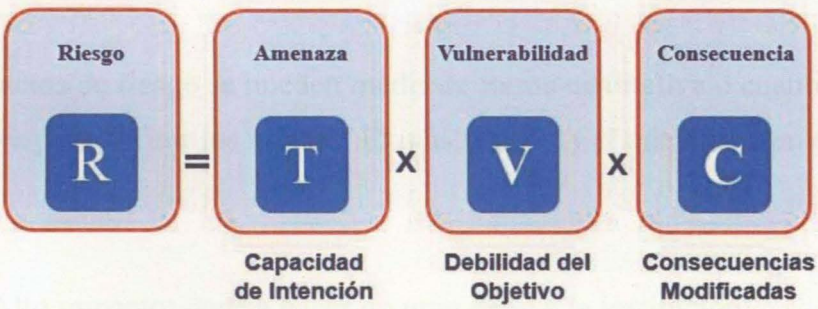

Ilustración 26 Modelo para cuantificar el riesgo de ciberseguridad

Fuente: Recuperado de (Infocyte, 2019)

Aproximaciones a la evaluación de riesgos

Métodos cuantitativos

El riesgo operacional representa una gran área de riesgo para la institución, sin embargo al tiempo presente es difícil de vincular al análisis numérico cuantitativo. El problema principal es la falta de datos disponibles, confiables y consistentes para realizar el análisis estadístico. La clave de la gestión del riesgo operacional es poder analizar los datos históricos de pérdidas y hacer predicciones acerca del futuro. Sobre la base de este análisis, planearía, implementaría, administraría y operaría una gama de controles diseñados para cumplir con estas predicciones.

Métodos cualitativos

El uso de un método cualitativo permite que el perfil de riesgo se presente a la alta gerencia, para este caso los Altos Mandos del Ejército en un cuadro de semáforo en rojo, amarillo y verde de acuerdo a los niveles de riesgo cualitativos.

Evaluación de la criticidad e impacto en la institución

Un aspecto de la medición del riesgo es evaluar qué tan crítico puede ser el resultado de un evento de riesgo para la institución.

Los impactos de riesgo se pueden medir de forma cualitativa o cuantitativa. El enfoque cualitativo es para definir los niveles. El más simple, y el que se usa en el método SABSA es:

- Alto impacto: podría hacer un gran daño a la institución.
- Impacto medio: podría hacer un daño significativo a la institución.
- Bajo impacto: solo daños mínimos a la institución.

Los métodos cuantitativos para medir el impacto en la organización tienden a centrarse en la equivalencia de valor financiero ¿Cuál es el costo de un evento en particular en dinero?, en los tipos más estratégicos de impacto, donde está en juego la reputación como es el caso del Ejército Nacional, esto puede ser difícil de lograr con precisión.

En la Ilustración 27 hay un diagrama de flujo que representa un proceso típico de evaluación de impacto organizacional, en este caso basado en haber construido un perfil de atributos de negocio SABSA.

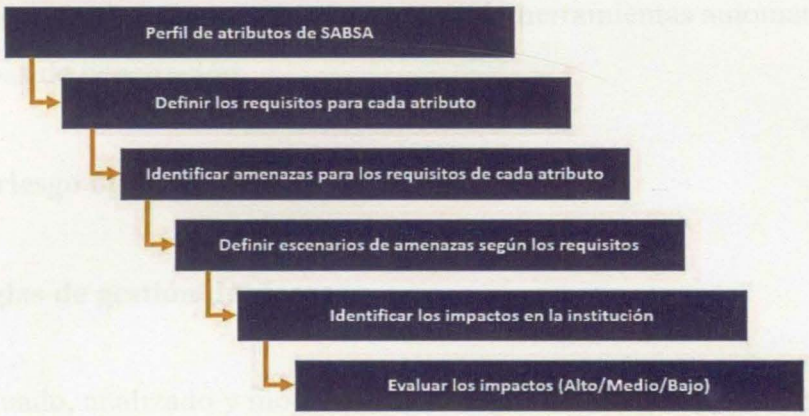

Ilustración 27 Proceso de evaluación de impacto organizacional.

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Evaluación de probabilidad

Existen dos probabilidades de que un evento cause un impacto en la institución:

- La probabilidad de que ocurra el evento (el nivel de la ciberamenaza).
- La probabilidad de que cuando ocurra el evento los controles fallarán (el nivel de vulnerabilidad).

La evaluación de la ciberamenaza puede ser difícil de realizar sobre una base estadística, ya que los datos históricos a menudo no están disponibles, la historia no es necesariamente un buen predictor del futuro, y las ciberamenazas cambian constantemente.

También existen métodos técnicos específicos para evaluar la vulnerabilidad en los sistemas de información de la institución. Éstos incluyen:

- Pruebas del sistema.
- Auditoria del sistema.
- Exploración de vulnerabilidades utilizando herramientas automatizadas.
- Pruebas de penetración.

Gestión del riesgo operacional

Estrategias de gestión de riesgos

Una vez evaluado, analizado y modelado los riesgos de la Fuerza, las estrategias de manejo para comprenderlos incluyen:

- Reducir o mitigar el riesgo aumentando el nivel de control.
- Transferir el riesgo a otra parte (ejemplo: un seguro).
- Evitar el riesgo al evitar las actividades operacionales con riesgos, reduciendo así las oportunidades.
- Retrasar el riesgo hasta otro momento, lo que retrasa los costos, pero también retrasa las oportunidades.
- Compensar el riesgo supliendo otros beneficios asociados con un análisis costo / beneficio para justificar riesgos.
- Distribuir el riesgo para obtener ventajas utilizando la distribución estadística del riesgo eventos.

- Aceptar el riesgo (siempre hay un nivel residual de riesgo que debe ser aceptado).
- Rechazar el riesgo, no es un riesgo real.

El registro de riesgos

El propósito es registrar los detalles de todos los riesgos que se han identificado, junto con su análisis y planes sobre cómo se deben tratar esos riesgos, el registro de riesgos es un importante componente del marco general de gestión de riesgos, incluirá todos los riesgos, no solo los riesgos operacionales.

Un ejemplo de un registro de riesgos, se muestra en la Tabla 16, donde cada entrada de riesgo en la tabla tiene un identificador único para evitar confusiones en los riesgos de referencia cruzada con otros documentos.

Tabla 16 Ejemplo tabla para el registro de riesgos

ID de riesgo	Nombre de riesgo	Tipo de riesgo	Descripción de la amenaza	Descripción y calificación del impacto institucional (H / M / L)	Vulnerabilidades y probabilidad general (H / M / L)	Categoría de riesgo Clasificación (A / B / C / D)	Propietario	Fecha identificada	Última actualización	Acciones planificadas	Informe de estado actual	Fecha de cierre

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Mitigación de riesgos

Tipos de control

La mitigación de riesgos es el proceso de introducción de controles para reducir la frecuencia o severidad de un impacto operacional.

Esto se puede hacer de diferentes maneras, dependiendo del tipo de riesgo a controlar:

- Control disuasivo: reduce una ciberamenaza.
- Control preventivo: reduce una vulnerabilidad.
- Control correctivo: reduce un impacto.
- Control de detección: detecta un problema y activa otros controles.

La forma en que estos diferentes tipos de control interactúan con los componentes de riesgo se muestra en Ilustración 27.

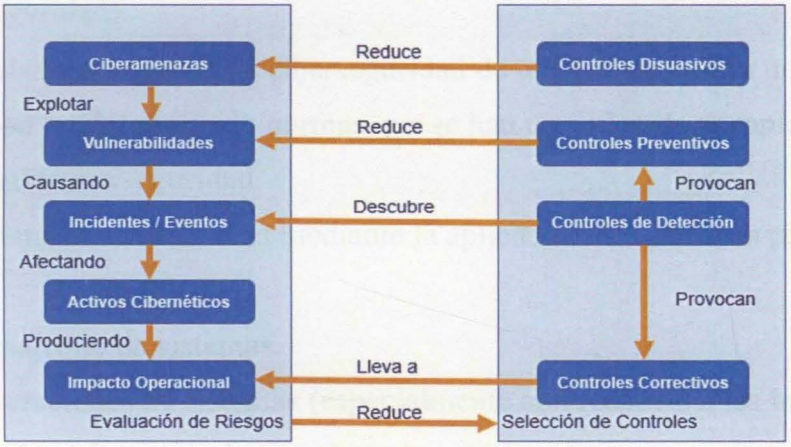

Ilustración 28 Los tipos de control y cómo funcionan

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Gestión de la Garantía

La Fuerza no solo necesita planificar y ejecutar un programa de ciberseguridad adecuado, sino también debe tener un medio por el cual pueda verificar que esto es así, para garantizar que todo está bien a este respecto.

Aseguramiento de la continuidad operacional

El punto de vista del auditor se preocupa por garantizar que la arquitectura de ciberseguridad es completa, consistente, robusta y apta para el propósito en todos los sentidos.

Hay varios tipos de actividades de inspección que se utilizan para proporcionar la ciberseguridad:

- Auditorías y revisiones de ciberseguridad de una unidad organizativa contra un código adecuado de práctica (como Norma ISO 27032: Gestión de la Ciberseguridad).
- Auditorías y revisiones de ciberseguridad de un sistema contra un conjunto de seguridad predeterminado normas que se han considerado apropiadas según la política de ciberseguridad.
- Aseguramiento del sistema mediante la aplicación de controles para:

    - Desarrollo de sistemas.
    - Operaciones de sistemas (especialmente con respecto a las instalaciones de producción en un sistema de centro de datos).
    - Protección de la integridad de los sistemas frente a ciberataques con software malintencionado desde cualquier ubicación.
    - Sistemas más utilizados por los usuarios de la institución.

Auditorias de ciberseguridad institucional

El programa de auditoria

El proceso de auditoría y revisión de la ciberseguridad de los procesos de la institución, deben ser un importante programa estratégico de actividad.

Tal programa necesitará abordar los siguientes puntos:

- Establecimiento de las guías y la auditoría de ciberseguridad.
- Definición de los enfoques generales y estrategia para la auditoría de ciberseguridad.
- Niveles de seguridad requeridos como resultado de una auditoría de ciberseguridad.
- Establecimiento de trabajos de pre-auditoría.
- Definición de objetivos de ciberseguridad (cuánta seguridad se necesita).
- Establecimiento de la línea de base de auditoría.
- Diseñar el programa de trabajo de auditoría.
- Evaluación y análisis del sistema utilizando herramientas automatizadas y entrevistas con el personal clave.
- Pruebas de penetración (búsqueda de debilidades).
- Evaluación del entorno de desarrollo de sistemas y software.
- Evaluación del entorno operacional.
- Informes de auditoría de ciberseguridad.
- Responder a los informes de auditoría y seguimiento.

Hay varios marcos estándar externos disponibles para que se pueden considerar para la adopción en la Fuerza. Quizás los más importantes de estos son primero el marco CobiT, la ISO / IEC 17799 y la ISO / IEC 27032/ BS 7799. Estas se asegurarán de abordar una amplia gama de problemas de auditoría importantes dentro de un marco común internacionalmente aceptado. Aquí unos ejemplos:

CobiT como marco de auditoría

Como marco de gobierno de las tecnologías de información proporciona una serie de herramientas para que el nivel directivo de la organización pueda relacionar los objetivos

de control con los aspectos técnicos y los riesgos en el área de la seguridad de la información. (Carlos Encalada Loja, Diego Cordero Guzmán, 2016).

CobiT no se trata solo de la seguridad de los sistemas de información, tiene un alcance mucho más amplio, tratando con todos los aspectos de la gobernanza de los sistemas de información, para algunas organizaciones esto será un enfoque apropiado para la auditoría de TIC.

ISO / IEC 17799: 2000 como marco de auditoría

Es un marco común reconocido internacionalmente para la planificación y ejecución del Sistema de Gestión de Seguridad de la Información (SGSI). También puede cumplir la función de un marco de auditoría para evaluar la idoneidad del SGSI corporativo existente.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. (International Organization for Standarization, ISO, 2000).

ISO 27032 como marco de auditoría

La norma ISO 27032 está totalmente orientada a intentar garantizar un entorno seguro a través de directrices de seguridad, ofrece unas líneas generales de orientación para fortalecer el estado de la ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados. (The International Organization for Standardization, 2012).

- Seguridad en la redes.
- Seguridad en internet.
- Seguridad de la información.
- Seguridad de las aplicaciones.

Auditorias de ciberseguridad del sistema

Auditoria de ciberseguridad

La auditoría de ciberseguridad es el proceso de verificar que el sistema cumple con todas las políticas de ciberseguridad, procedimientos operativos y estándares de ciberseguridad impuestos en la Fuerza que se aplican a su operación.

Dentro de la definición dada anteriormente, hay tres tipos de actividad de auditoría de ciberseguridad que se pueden seguir:

- Monitoreo diario de eventos y seguimiento para buscar violaciones de políticas, procedimientos y normas. Esto se logra mejor mediante el uso de herramientas automatizadas de escaneo de registros que crear informes de excepción para ser seguidos manualmente.
- Inspecciones periódicas de rutina de los parámetros del sistema para garantizar el cumplimiento continuo de normas de ciberseguridad. Esto se logra mejor mediante el uso de herramientas automatizadas que analizan todo el sistema de archivos y directorios, comparando los ajustes de parámetros con los ajustes preferidos (que son generalmente almacenados en un archivo de políticas) y creando informes de excepciones para el seguimiento manual.
- Revisiones periódicas de las operaciones del sistema para garantizar el cumplimiento de las políticas de ciberseguridad, procedimientos y normas. Expertos en auditoría, posiblemente asistidos por listas de verificación de problemas para ser investigados, lograr esto a través de la recopilación de información manual y la presentación de informes.

La estrategia de auditoría de ciberseguridad de la institución deberá incluir preferiblemente los tres enfoques anteriores ya que todos contribuyen de manera diferente al proceso general de aseguramiento.

La estrategia también deberá abordar los siguientes puntos:

- Definición: ¿qué quiere decir con el término auditoría de ciberseguridad?
- Experiencia: ¿quién llevará a cabo las auditorías de ciberseguridad y qué capacitación y curso profesional necesitarán?
- Herramientas y técnicas: ¿cuáles son las herramientas estándar que se utilizarán para ejecutar su auditoria de ciberseguridad?
- Planificación del trabajo de auditoría: ¿cuál es el alcance de una auditoría de ciberseguridad y los recursos necesarios?
- Ejecución: ¿cuál es la metodología que se utilizará para la auditoría de ciberseguridad?
- Informes: ¿cuál es el estilo y el contenido de los informes de auditoría de ciberseguridad, los consumidores esperados, los objetivos y qué valor agregará el informe?

Estrategia de aseguramiento del sistema

Integridad del software y estrategia antimalware

El objetivo de esta estrategia para la institución, es prevenir la contaminación por ejecutables maliciosos, detectar la contaminación lo antes posible, contenerla y eliminarla.

El software malicioso puede provenir de varias fuentes:

- Software malintencionado de autorreplicación que proviene de un ciberdelincuente, entre ellos están: virus, caballos de troya, gusanos, entre otros, son todos ejemplos de este tipo de vehículo de ciberataque.
- Código móvil malicioso en forma de applets de java, activeX, varios tipos de dispositivos móviles script, consultas de bases de datos remotas.

- Código insertado maliciosamente en un programa o sistema por un miembro del equipo de desarrollo o el equipo de operación de sistemas, o por un ciberdelincuente externo que haya obtuvo acceso no autorizado a un sistema.

Las posibles técnicas para abordar estos problemas incluyen:

- Escaneo de archivos y directorios almacenados en busca de códigos maliciosos conocidos.
- Escaneo de archivos y directorios almacenados en busca de cambios inesperados.
- Monitoreo en tiempo real del entorno de ejecución para rutas de ejecución no autorizadas.
- Filtrar y escanear materiales digitales importados en el perímetro de la institución, incluido el escaneo de dispositivos removibles y otros elementos multimedia, el filtrado en tiempo real llevado a cabo en un firewall u otros dispositivos de seguridad.
- Establecer reglas de control en los navegadores web para evitar la ejecución de ciertos tipos de objetos de códigos móviles, mediante el uso de objetos firmados digitalmente de fuentes de confianza.
- Software de autenticación de objetos en la instalación.
- Autenticación de objetos de software en el arranque.
- Implementación de prácticas seguras de codificación como parte de los estándares de desarrollo para desarrollo de software.
- Auditoría de código del software desarrollado internamente para verificar el código troyano antes de su lanzamiento en producción en vivo (esto es difícil, costoso y debe considerarse solo para sistemas de aseguramiento extremadamente altos).

Los controles estratégicos deben incluir:

- Una política institucional que requiere el uso de software autorizado y con licencia, incluyendo el uso de código abierto y software de dominio público, que la organización puede optar por utilizar, pero dicho software debe ser adquirido, probado y distribuido oficialmente.
- Una política institucional dirigida a todos los usuarios de la institución para que conozcan el software malicioso y sus patrones de comportamiento.
- Un estándar institucional para la configuración de clientes de correo electrónico y navegadores web para reducir las vulnerabilidades de la infección a niveles aceptables.
- Un programa de concientización continúo para asegurar que los empleados se comporten de manera sensata y en particular, saber sospechar de ciertos tipos de archivos adjuntos de correo electrónico y descargas web.
- La implementación y el uso regular del software de detección antivirus de un proveedor de confianza para estos productos, con actualizaciones periódicas frecuentes. Esto debe ser usado para escanear todos los archivos entrantes en medios removibles, en archivos adjuntos de correo electrónico, a través de transferencias FTP y cualquier otro medio de importación de archivos.
- La reinstalación de cualquier software dañado utilizando los archivos de instalación originales (o posiblemente una buena copia de seguridad conocida de estos).
- El uso de medidas de limpieza adecuadas para la copia de seguridad y restauración de software y datos (de copias operativas recientes).
- Un proceso de gestión de incidentes para hacer frente a la contaminación de software malicioso.

Uso aceptable

Se refiere al uso de sistemas de información de la Fuerza para propósitos aceptables. Los propósitos inaceptables son aquellos que son ilegales, no autorizados y pueden causar ofensa a personas tanto dentro como fuera de la institución.

El uso inaceptable podría incluir actividades tales como:

- Navegar sitios web pornográficos desde los host institucionales, y posiblemente descargar y almacenar este tipo de material.
- Navegar por los sitios de juego y usar el tiempo corporativo para apostar.
- Acoso sexual de colegas a través del sistema de correo electrónico institucional, mediante el envío de materiales sugestivos o sexualmente explícitos no deseados.
- Acosar a los usuarios a través del sistema de correo electrónico institucional mediante el envío racial o religioso materiales abusivos que ofenden a los destinatarios.
- Perder el tiempo corporativo al navegar por sitios web que no tienen relevancia para las funciones que ejerce en el trabajo.
- Incurrir en costos de comunicaciones inaceptables al acceder a sitios web no autorizados o números de teléfono de tarifa premium.
- Utilizar los sistemas de información institucional para la gestión de intereses privados.
- Usar las instalaciones de los sistemas informáticos de la institución para hackear otros, tanto dentro y fuera de ella.

Los controles estratégicos deben incluir:

- Una política de uso aceptable para garantizar que todos los usuarios estén al tanto de la posición institucional y saber qué constituye un uso aceptable y un uso inaceptable.
- La implementación de software de filtrado de contenido para garantizar que los elementos más ofensivos y los elementos ilegales pueden ser detectados.
- Un proceso disciplinario como elemento disuasivo para los usuarios que violan la política de uso aceptable.

Pruebas de penetración

Las pruebas de penetración están diseñadas para comprobar un sistema y validar las vulnerabilidades que puedan ser explotadas por ciberatacantes para obtener privilegios de acceso no autorizados en la institución. Requiere una investigación constante de nuevas vulnerabilidades y desarrollo de nuevas herramientas para estas pruebas.

Las pruebas de penetración pueden cubrir varios niveles diferentes de acceso al sistema, que incluyen:

- Penetración interna de la red: intentar atacar la red desde el interior de la institución.
- Análisis estático de registros generados por computadora y conjuntos de reglas de firewall.
- Auditoría en el host, asegurando que las políticas y estándares de ciberseguridad han sido rigurosamente aplicadas.
- Evaluación de vulnerabilidad, escaneo automatizado de redes y sistemas para conocidos vulnerabilidades (nuevas emergen continuamente).
- Penetración de red externa: intentar atacar la red desde ubicaciones externas, incluso desde internet.
- Prueba de aplicaciones: intentar perturbar aplicaciones mediante la manipulación de entradas de datos, buscando funcionalidad no deseada.
- Análisis del código fuente: busca prácticas de codificación deficientes o rutinas sospechosas.
- Pruebas de penetración de telefonía móvil e inalámbrica para sistemas que emplean estas tecnologías.
- Auditoría y prueba de penetración a sistemas institucionales de voz y datos.
- Pruebas del servidor de acceso remoto, para buscar vulnerabilidades que podrían ser explotadas por un oponente para penetrar en la red.

- Ingeniería social: para probar si el personal puede revelar contraseñas o permitir que personal no autorizado ingrese a las áreas de control de la institución.

Al armar la estrategia de prueba de penetración se debe considerar los siguientes puntos:

- Utilizar expertos: debe realizarse por personal capacitado.
- Si se van a realizar con un proveedor de servicios, verificar que sea experto con amplia experiencia y múltiples herramientas de prueba.
- Si se utiliza un tercero, validar más de una empresa para suministrar estos servicios y rotarlos, tienen diferentes herramientas y expertos, así lo que un equipo pasa por alto puede ser encontrado por el otro.
- Organizar un programa regular de pruebas para sistemas y aplicaciones existentes, las nuevas vulnerabilidades emergen todo el tiempo.
- Si las pruebas se realizan en un entorno de prueba separado en lugar de en vivo entorno, se debe replicar el entorno en vivo lo más cerca posible. Si el entorno cambia entonces un exploit que falló ahora puede ser exitoso, así un sistema de prueba que era impenetrable, puede que no garantice las mismas propiedades para el sistema en vivo.

El proceso de prevención operacional

Un aspecto crítico de las operaciones de ciberseguridad en curso es la coordinación de un proceso de prevención que reúne muchos hilos diferentes de actividad operativa. La Ilustración 29 muestra algunos de los principales componentes de este proceso.

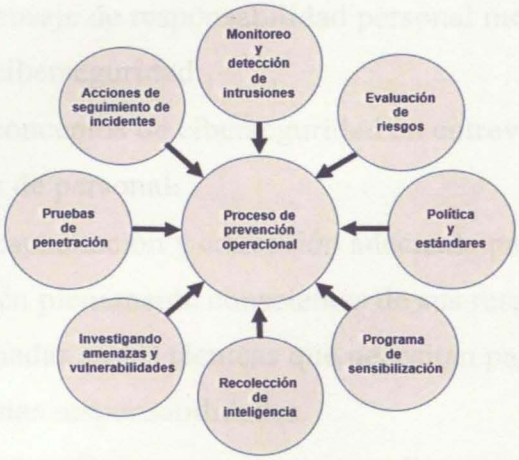

Ilustración 29 Componentes principales del proceso de prevención operativa

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Manejando el personal

Responsabilidades de ciberseguridad

El reto principal para llevar a cabo una transformación digital exitosa, sin comprometer la seguridad de los procesos institucionales, solo es posible si se asume la ciberseguridad como responsabilidad de todos. (Gianluca D'Antonio, Portafolio, 2017).

Uno de los objetivos principales de cualquier programa de ciberseguridad es garantizar que todos entienden que esta parte de la responsabilidad es de todos.

A continuación se pueden observar un número de medidas operativas que ayudarán a la Fuerza a alcanzar este objetivo:

- Asegurar que la responsabilidad de ciberseguridad se mencione adecuadamente en cada descripción del trabajo y que todos los contratos incluyan acuerdos de confidencialidad.

- Reforzar el mensaje de responsabilidad personal mediante referencia directa en la política de ciberseguridad.
- Presentar los conceptos de ciberseguridad en entrevistas, reuniones y capacitaciones de personal.
- Proporcionar capacitación y educación adecuada para garantizar que todos los empleados estén plenamente conscientes de sus responsabilidades personales y también entrenadas en las técnicas que necesitan para aplicar en su trabajo para cumplir con estas responsabilidades.
- Proporcionar procedimientos operativos obligatorios para reportar incidentes de ciberseguridad de todo tipo y asegurar que todos los empleados estén conscientes y conozcan los mecanismos por los cuales se presentan los informes.

Gestionando operaciones y soporte

Manejo de incidentes

En cualquier entorno operativo institucional, puede haber incidentes que deben ser manejados en el curso de eventos. Los tipos de incidentes pueden incluir:

- Fallos del sistema y pérdida de servicio.
- Denegación de servicio.
- Incumplimientos de la confidencialidad.
- Cambios no autorizados.

Los procedimientos de manejo de incidentes deben cubrir:

- Recepción de la alarma que llama la atención sobre un incidente.
- Identificación y análisis de la causa del incidente.
- Evaluación de impacto y priorización del incidente (triage).

- Revisión de opciones para acciones correctivas.
- Planificación e implementación de recursos, tanto para eliminar la causa como para recuperar los efectos del incidente y también para prevenir su repetición.
- Recopilación y conservación de logs de auditoría y pruebas forenses similares para análisis y uso en posibles procedimientos legales.
- Comunicación con las partes afectadas por el incidente.
- Reportar el incidente y las respuestas a una autoridad apropiada.

El área de ciberseguridad debe estar al tanto de incidentes que no son conocidos, sino que son el resultado de nuevas ciberamenazas, que puede ser muy difícil de identificar. Por lo tanto, se requieren procedimientos especiales para:

- Identificación y clasificación de un incidente de ciberseguridad.
- Informar y escalar el incidente de ciberseguridad.
- Investigación del incidente de ciberseguridad.
- Manejo de información relevante a un incidente de ciberseguridad; por ejemplo, si el incidente es el uso inapropiado o ilegal de recursos informáticos sería inapropiado para la ayuda de escritorio o sistemas de gestión de incidentes para mostrar y registrar abiertamente los detalles confidenciales de quien estaba involucrado.

Protección contra software malicioso

El software malicioso incluye una amplia variedad de virus, troyanos, gusanos y similares. El núcleo de una estrategia institucional para proteger los sistemas contra software malicioso es:

- Buena conciencia y buen comportamiento entre la comunidad de usuarios.

- Control apropiado del acceso a sistemas basados en la necesidad de la institución.
- Un estricto régimen de control de cambios.
- Escaneo automatizado de todas las importaciones de datos y software a través de correo electrónico, acceso web, archivo transferencia, etc.

Copia de seguridad y recuperación de datos

Los datos operativos están cambiando constantemente y por lo tanto, es esencial realizar copias de respaldo frecuentes, donde el objetivo es poder recuperar los datos de la institución (siguiendo algún tipo de falla o desastre) a una posición anterior que sea aceptable para los términos del acuerdo al nivel de servicio.

Dependiendo de las necesidades de la institución, la estrategia de copia de seguridad puede basarse en el método semanal convencional, copias de seguridad de datos completos con copias de seguridad incrementales diarias.

Cualquiera que sea el tipo de mecanismo de copia de seguridad en uso, debe probarse con regularidad para garantizar que esté funcionando correctamente y que realmente se están creando copias de seguridad, el mecanismo de restauración del uso de las copias de seguridad también debe ser probado.

Manejo de medios

Todos los medios de salida extraíbles generados por algún sistema informático, incluyen:

- Medios magnéticos: discos, USB, cintas, etc.
- Medios ópticos: DVD, CD y otros medios de dispositivos ópticos, etc.
- Salida de papel impreso y otros medios impresos especializados, etc.

El manejo seguro de dichos medios requiere procedimientos operativos controlados, que incluyen:

- Borrado seguro y permanente de todos los datos de medios magnéticos u ópticos que no están requeridos por la institución.
- Autorización para la eliminación de cualquier elemento multimedia de las instalaciones de la institución, sea o no con fines de eliminación.
- Un registro de auditoría completo de todos los elementos de los medios: su creación, su uso, su almacenamiento y su eliminación.
- Instalaciones de almacenamiento seguro para todos los elementos multimedia, incluido el almacenamiento externo para copias de seguridad y medios de comunicación.
- Procedimientos y estándares de manejo seguro de medios, incluidos aquellos para:
  - Estándares de calidad y adquisición de medios.
  - Denominación, etiquetado e indexación.
  - Procedimientos de almacenamiento y recuperación seguros.
  - Transporte seguro desde y hacia lugares autorizados.
  - Eliminación segura y destrucción.

Intercambio de información

Los intercambios que requiera la institución para el fin que lo necesite, deben ser controlados a través de una serie de medidas operativas, incluyendo:

- Evaluación de riesgos para revelar las ciberamenazas, impactos y vulnerabilidades asociadas con intercambios de información.

- Procedimientos y normas para proteger la información en tránsito, de acuerdo con los requisitos derivados de la evaluación de riesgos, incluidos los procedimientos específicos para el envío y recibiendo la información.
- Acuerdos formales y contratos entre las partes que intercambian información para definir claramente los roles y responsabilidades de cada parte.

Los mecanismos para intercambiar información pueden variar ampliamente, cada mecanismo requiere su propia evaluación de ciberamenazas y vulnerabilidades.

Los mecanismos más frecuentes para los que se requieren normas y procedimientos incluyen:

- Transporte físico de elementos multimedia como discos, cintas y documentos en papel.
- Comercio electrónico basado en la web.
- Transferencia de archivos.
- Correo electrónico y archivos adjuntos.
- Telefonía.
- Videoconferencia.
- Conferencias web.
- La mensajería instantánea (IM) basada en IRC y las constantemente existentes versiones multimedia de este tipo de servicio.

Gestión de registro de eventos y auditoría

Se utilizará para registrar cualquier evento del sistema que pueda tener importancia para la administración de los servicios institucionales. El registro de eventos crea un log de auditoría de lo que ha sucedido, debe ser almacenado por un período de tiempo acordado para facilitar el análisis histórico y la investigación.

Entre estos eventos importantes se incluyen aquellos que tienen algún significado para la administración de ciberseguridad. Estos incluirán:

- Excepciones: eventos que son inusuales y más allá del patrón normalmente esperado.
- Intentos fallidos de inicio de sesión.
- Inicios de sesión exitosos y cierres de sesión.
- Acceso a cualquier recurso de información especialmente sensible que haya sido marcado para acceso el registro de eventos.
- Uso de recursos privilegiados tales como administrador o identidades de raíz.
- Errores o fallas en cualquier componente lógico o físico del sistema.
- Alertas de seguridad de software antivirus, firewalls, sistemas de detección de intrusos u otros equipos de seguridad.

Los registros de eventos deben contener datos suficientes para que sean útiles. Campos típicos en un evento de registro incluirá como mínimo:

- Datos y hora del evento.
- Identificadores de usuario asociados con el evento.
- Ubicación lógica o física, o ambas.
- Tipo de evento (puede codificarse para ahorrar espacio de almacenamiento de registro).
- Cualquier otra información de contexto necesaria para explicar la naturaleza completa del evento.

Cualquiera que sea el tipo de registro de auditoría apropiado, normalmente se almacenará en orden cronológico y tendrá que tener herramientas adecuadas para administrar y buscar la información del evento.

Estas herramientas deben incluir una serie de capacidades:

- Buscar ciertos tipos de eventos o ciertos identificadores.
- Buscar ciertas combinaciones y patrones de eventos, usando una base de datos normal o funciones de consulta del motor de búsqueda (AND, OR, NOT, XOR) para combinar búsquedas condicionales para combinaciones de campos en los registros.
- Análisis estadístico de patrones de eventos, frecuencias y severidad.
- Archivar, indexar y recuperar registros de eventos.

Investigaciones forenses

De acuerdo al artículo publicado por la agencia6 (2019), "La seguridad cibernética y el análisis forense digital son fundamentales para crear una defensa, análisis e investigación eficaces del delito cibernético. La práctica del análisis forense digital incluye la recopilación, el examen, el análisis y la notificación de incidentes relacionados con computadoras, redes y dispositivos móviles". (Javier Blanco, 2019).

La investigación forense se deberá centrar en la recopilación y preservación de evidencia, generalmente para que dicha evidencia puede presentarse ante un ente judicial, pero también podría ser en apoyo de un proceso disciplinario, esto identifica inmediatamente una serie de objetivos importantes para las investigaciones forenses:

- Mantener la continuidad de la cadena de evidencia.
- Preservar la integridad de la evidencia, evitando que sea contaminada durante o después del proceso de recolección.
- Asegurarse de que las pruebas sean admisibles de acuerdo con las reglas de las leyes relevantes.
- Preservar su calidad e integridad.

Los principales elementos del proceso de investigación forense necesarios para lograr estos objetivos son:

- Planificación de la investigación:
    - Establecer los objetivos y el alcance.
    - Establecer los principios.
    - Defender los protocolos.
- Aprovechando la evidencia:
    - Herramientas necesarias.
    - Realización del proceso de incautación.
- Análisis de la evidencia:
    - Procesos de análisis lógico.
- Establecer la historia de la evidencia digital capturada:
    - Detectar y superar las herramientas y técnicas de ocultación de datos utilizadas por los datos propietarios para disfrazar evidencia incriminatoria.
    - Manejo de material forense encriptado.
- Informes:
    - Informes escritos.
    - Declaraciones de testigos expertos y comparecencias judiciales.

Seguimiento y gestión de problemas

La gestión de problemas difiere de la gestión de incidentes en que su objetivo principal es detectar causas subyacentes de un incidente y eliminar o evitar esas causas a largo plazo.

La gestión de problemas y la gestión de incidentes pueden estar en conflicto entre sí. El objetivo de gestionar un incidente es restaurar el servicio lo antes posible, mientras que la gestión de problemas requiere la investigación de las causas, lo que puede retrasar la recuperación del servicio.

La gestión de problemas se puede dividir en dos clases principales:

- Gestión reactiva de problemas: gestionar problemas ya identificados y resolverlos dentro de los tiempos de servicio acordados para minimizar el impacto de los mismos.
- Gestión proactiva de problemas: análisis de incidencias para prevenir recurrencias y llevar a mejoras en el servicio. Los informes de servicio e informes de incidencias son fundamentales para el proceso proactivo de gestión de problemas.

El proceso de gestión de problemas incluye:

- Investigación y diagnóstico.
- Evaluación de impacto para priorizar las tareas de gestión de problemas.
- Provisión de soluciones para mantener los niveles de servicio a corto plazo mientras el problema es investigado y resuelto.
- Resolución de problemas.
- Comunicar información a quienes necesitan conocer el resultado de la resolución del problema.

- Seguimiento del estado de problemas pendientes y verificación del progreso contra objetivos de nivel de servicio.
- Escalamiento de problemas mayores a niveles apropiados de autoridad.
- El registro de problemas se cierra para garantizar que se capturan todos los detalles.
- Manejo de incidentes mayores.
- Revisiones de problemas.
- Incidencia y prevención de problemas.

Gestión de control de acceso

Política de control de acceso

Los principales aspectos relevantes en la política de control institucional de acceso deberán ser:

- Clasificación de la información.
- Clasificación del sistema.
- Gestión de identidades.
- Reglas de control de acceso obligatorias.
- Consistencia de las reglas de control de acceso en múltiples sistemas y redes que forman diferentes dominios de políticas.
- Cumplimiento de la legislación y disposiciones contractuales.
- Principios de política.
- Control de acceso basado en roles para simplificar la administración y mejorar el control centralizado.
- Fuerza de los mecanismos de autenticación de usuario a utilizar.
- El proceso de autorización, el modelo de propiedad, custodia y uso.

Gestión de cumplimiento

Cumplimiento en el ámbito de la gestión de la ciberseguridad

Los elementos principales de una estrategia de cumplimiento de leyes y normas específicas de la ciberseguridad y su gestión son:

- Asegurarse de identificar de manera integral todas las leyes y regulaciones relevantes y comprender su aplicabilidad en las operaciones de la institución. La identificación también debe extenderse a los contratos con terceros para garantizar que se está cumpliendo con todas las obligaciones contractuales que ha contraído.
- Implementar procedimientos apropiados para proteger los derechos de propiedad intelectual. Esto incluirá especialmente la protección de los derechos de autor de documentos y software, la copia y distribución no autorizada.
- Retener y salvaguardar los registros de la organización que deben archivarse para ciertos períodos cumpliendo con los requisitos legales y reglamentarios.
- Proteger la privacidad de la información personal según la protección de datos.
- Asegurar que la recopilación de evidencia cumpla con las rigurosas reglas de evidencia y que las pruebas serán admisibles cuando se presenten en un tribunal de justicia.
- Proporcionar seguridad de que se cumplen todas las políticas internas de ciberseguridad y normas.

Operaciones específicas de ciberseguridad

Gestión del mecanismo de ciberseguridad

La gestión de los mecanismos de ciberseguridad requiere una serie de procesos operativos, procedimientos y herramientas.

Los mecanismos a gestionar incluyen los siguientes:

- Gestión de claves criptográficas.
- Mantenimiento de listas de control de acceso y perfiles de privilegios de usuario.
- Gestionar el proceso de copia de seguridad y restauración de datos.
- Gestión de medios incluyendo etiquetado, indexación, transporte, almacenamiento (fuera del sitio), recuperación, reciclaje de medios y control de por vida.
- Mantenimiento y distribución de firmas de virus.
- Mantenimiento de reglas de firewall.
- Gestión de archivos de eventos y archivo.

Gestión de usuarios

Una gran proporción de la administración y las operaciones de ciberseguridad se centran en torno a gestión de identidad y privilegios de usuario:

- Registro de nuevos usuarios.
- Autorización de privilegios de usuario.
- Implementación de los privilegios autorizados.
- Adición, modificación, eliminación de registros de usuario y credenciales en la seguridad del sistema bases de datos.
- Seguimiento y gestión de problemas.
- Gestión de contraseñas, actualización y cambio.
- Sistema de gestión de cuentas de alto privilegio para aplicaciones, sistemas, operadores, gerentes y auditores.

Servicios de ciberseguridad gestionados

Existe una tendencia actual hacia la externalización de ciertos servicios de ciberseguridad operacional.

Los tipos de servicio que son potenciales para este enfoque son:

- Firewalls y VPN gestionados.
- Servicio de autenticación gestionado.
- Gestión operaciones SOC.
- Gestión de la detección y prevención de intrusiones.
- Gestión de detección de virus.
- Filtrado de contenido gestionado.
- Pruebas de intrusión.

Gestión de la continuidad del negocio

Las organizaciones de hoy son cada vez más conscientes de su vulnerabilidad a los ataques cibernéticos que pueden paralizar una empresa o destruir permanentemente sus sistemas de TI. (Ciberseguridad.com, 2019).

El plan de continuidad del negocio para la Fuerza tiene que incluir una estrategia de resiliencia cibernética que puede ayudar a soportar incidentes cibernéticos disruptivos. Este plan generalmente incluye formas de defenderse contra esos riesgos, proteger aplicaciones y datos críticos y recuperarse de una violación o fallo de una manera controlada y medible.

Proceso de negocio basado en el enfoque de BCM

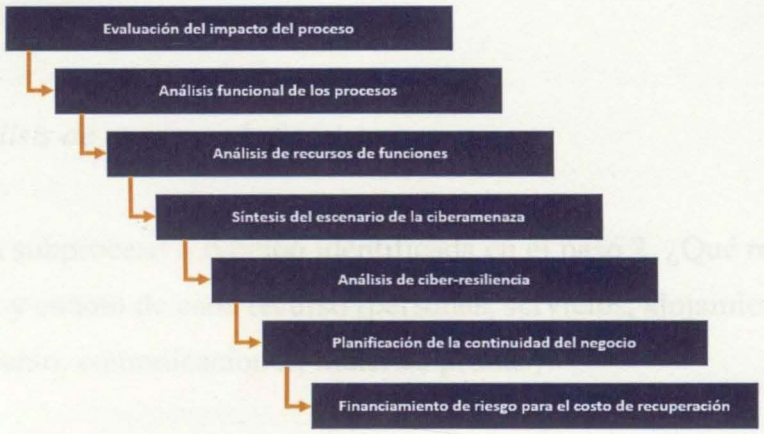

Ilustración 30 El proceso de gestión de la continuidad del negocio

Fuente: Recuperado de (John Sherwood, Andrew Clark, David Lynas, 2005)

Paso 1: Evaluación del impacto del proceso de negocio

- Identificar y mapear los procesos de la institución.
- Evaluar el impacto en el negocio de la pérdida de cada proceso de la institución.
- Clasificar los procesos de la institución como:

  - Crítico: la pérdida destruirá el proceso.
  - Grave: la pérdida causará un daño persistente y grave en el proceso.
  - Significativo (banda opcional): la pérdida causará daños importantes.
  - Otros: el daño causado por la pérdida puede ser absorbida.

Paso 2: Análisis funcional de procesos de la institución.

- Seleccionar los procesos clasificados como critico o grave.

- Analizar todos los subprocesos en pasos funcionales únicos para descubrir todo el proceso y componentes funcionales necesarios para mantener este proceso de alto nivel en continuo.

Paso 3: Análisis de recursos de funciones

- Para cada subproceso o función identificada en el paso 2, ¿Qué recursos se necesitan y cuánto de cada recurso (personas, servicios, alojamiento, equipamiento, comunicaciones, materias primas)?

Paso 4: Síntesis del escenario de la ciberamenaza

- Para cada recurso identificado en el paso 3, ¿Qué escenarios de alto nivel de ciberamenazas ponen ese recurso en riesgo?

Paso 5: Análisis de ciber-resiliencia

- Para cada combinación de recurso / escenario, se proporcionan los recursos actuales con suficiente resiliencia para el negocio en general para soportar el escenario, ¿hay algunos puntos únicos de fracaso?

Paso 6: Planificación de la continuidad del negocio

- Qué protección adicional de recursos se necesita para proporcionar el nivel requerido de recursos ¿ciber-resiliencia para que el negocio en general pueda soportar los escenarios de ciberamenazas?, como:

    - Medidas preventivas para evitar que las ciberamenazas se materialicen.
    - Medidas de contención para limitar el daño.

- Redundancia de recursos para evitar puntos únicos de falla y para proporcionar capacidad de respaldo.
- Planes de gestión de incidencias.
- Planes de recuperación para reanudar los procesos después de un incidente.
- Planes de gestión de crisis.
- Formación y sensibilización.

Paso 7: Financiamiento de riesgo para el costo de recuperación

- Seguros y servicios relacionados.

14. Conclusiones

Con la realización de este proyecto se proporcionó un marco para desarrollar y documentar la arquitectura de seguridad de la metodología SABSA la cual está enfocada en la ciberseguridad de la información digital, permitiendo entregar una seguridad completa y de alto nivel a la institución para proteger los activos principales del negocio; donde se logró determinar la importancia de dar a conocer a los Altos Mandos los beneficios del programa de arquitectura de ciberseguridad que se quisiera implementar en todos los niveles de la Fuerza, encaminados a la mejora de los procesos, la continuidad operativa y la estabilidad institucional; contribuyendo a la protección contra ciberataques y garantizando el correcto funcionamiento de los sistemas interconectados de la institución.

Así mismo, se precisó una parte importante de la ejecución de la metodología, la que se lleva a cabo a través de las técnicas por capas, las cuales proveen un enfoque importante para el desarrollo de la arquitectura de seguridad de SABSA para el Ejército Nacional, adoptando una estrategia de servicios de ciberseguridad multicapa, donde estos servicios de ciberseguridad se colocan dentro de estas capas, para proporcionar la combinación más adecuada para la prevención, contención, detección y notificación; recopilación de eventos y seguimiento de eventos; recuperación, restauración y garantía.

Con la referenciación de las normas y leyes en la materia, se mostró la importancia de contar con estas y la existencia de numerosos organismos que las regulan, a las cuales la institución debe acogerse para incorporar la arquitectura de ciberseguridad SABSA, cada una con un enfoque específico y en muchos casos superposición en sus áreas de estandarización. Sin embargo, no hay una regla específica que indique cuál es el estándar más apropiado para elegir y la variedad de opciones posibles puede ser confusa, pero al final se reduce a cuáles se adoptan ampliamente en la comunidad con la que la Fuerza necesita interacción.

Por otro lado y dando respuesta al objetivo específico número dos de este trabajo, se analizó y determinó la arquitectura actual del Ejército Nacional mostrando sus dificultades, oportunidades, fortalezas y amenazas a través de la matriz DOFA, analizando la necesidad de contar con una arquitectura de ciberseguridad idónea y articulándola a las necesidades propias de la institución, vislumbrando las brechas y vulnerabilidades a ser cubiertas si se llegara a la implementación de la metodología. Donde la clasificación de la información es una forma de simplificar la administración de políticas de ciberseguridad, lo cual es comúnmente utilizado en organizaciones militares y entornos gubernamentales, como es el caso del Ejército Nacional.

De igual forma, se dio a conocer la importancia de las políticas de ciberseguridad, concepto que va mucho más allá de un conjunto de declaraciones impuestas por un grupo de personas, pues éstas representan la cultura de la institución y describen cómo las personas abordan su trabajo y cómo se comportan con respecto a los asuntos de seguridad. De esto dependerá en gran parte el éxito de la estrategia, concepto, diseño, implementación, gestión y medición de la arquitectura de seguridad, donde la responsabilidad recae en todos los niveles de la organización.

Finalmente, para definir los planes a seguir y llegar a la arquitectura de ciberseguridad objetivo dando respuesta a la pregunta de investigación, la institución debe llevar a cabo una metodología de arquitectura correcta que le permita no sólo hacer un aseguramiento de la información digital de manera superficial, sino utilizar de manera efectiva y eficiente las herramientas que una metodología como la SABSA le brinda, aprovechando aquellas fortalezas y oportunidades con las que se cuenta actualmente para ajustar un sistema integral que le permita transformar las debilidades y amenazas en nuevas fortalezas y oportunidades, lo que puede aportar para el aseguramiento de los procesos a través de la ciberseguridad.

15. Bibliografía

Andy Wood, Ying He, Leandros A Maglaras, Helge Janicke. (2009). *A Security Architectural Pattern for Risk Management of Industry Control Systems within Critical National Infrastructure*. Obtenido de https://pdfs.semanticscholar.org/d788/c19222afa47ec4e8a346721c7da615a025d1.pdf

Baryolo, O. G., Sentí, V. E., Camejo, R. R. B., & Rodríguez, I. G. (2012). Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones. *ACIMED*.

Carlos Encalada Loja, Diego Cordero Guzmán. (2016). *GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE COBIT 5.* Revista Científica y Tecnológica UPSE.

Ciberseguridad.com. (2019). *Ciberseguridad continuidad del negocio.* Obtenido de https://ciberseguridad.com/normativa/espana/medidas/continuidad-negocio/#%C2%BFQue_es_un_Plan_de_Continuidad_de_Negocio

Ciberseguridad L, Estrategia De Negocio C, Gabriela P, Rey G. (2016). *LA CIBERSEGURIDAD COMO ESTRATEGIA DE NEGOCIO LA CIBERSEGURIDAD COMO ESTRATEGIA DE NEGOCIO CIBERSEGURIDAD CONTRA CIBERCRIMEN.* Netmedia Research.

Comando General Fuerzas Militares de Colombia. (2012). *Oficio No. 05289 "Creación de*

unidades de ciberdefensa en las FF.MM". Bogotá, D.C.

Comando General de las Fuerzas Militares. (2019). *Directiva Estructural de Ciberdefensa CCOCI 2019.* Bogotá, D.C.

Congreso de la República . (2009). *MINTIC.* Obtenido de Ley 1273 "Protección de la información y de los datos": https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

Congreso de la República. (2012). *LEY ESTATUTARIA 1581* . Obtenido de Secretaria Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo de Europa . (2001). *Convenio sobre la ciberdelincuencia.* Budapest.

Deobold B. Van Dalen y William J. Meyer. (2006). *La investigación descriptiva.*

Departamento Administrativo de la Función Pública (DAFP). (2011). *Guía para la Administración del Riesgo.* Obtenido de https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba#:~:text=La%20actualizaci%C3%B3n%20de%20la%20Cartilla,Racionalizaci%C3%B3n%20de%20Tr%C3%A1mites%20del%20Departamento.

Departamento de Comunicaciones CEDE6 del Ejército Nacional. (2017). *Directiva Permanente 00201/2017 "Lineamientos de Ciberseguridad y Ciberdefensa para el Ejército Nacional".* Bogotá D.C.

Departamento Nacional de Planeación. (2011). *CONPES 3701 Lineamientos de política para la ciberseguridad y ciberdefensa.* Bogotá D.C.

Departamento Nacional de Planeación. (2016). *CONPES 3854 Política nacional de seguridad digital.* Obtenido de DNP: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Ejército Nacional de Colombia. (2020). *Misión y Visión.* Obtenido de https://www.ejercito.mil.co/conozcanos/mision_vision_362168

Ejército Nacional de Colombia. (2016). *Documento estructural.*

ESET. (2014). *¿Por qué es necesario el firewall en entornos corporativos?* Obtenido de welivesecurity by ESET: https://www.welivesecurity.com/la-es/2014/07/29/por-que-necesario-firewall-entornos-corporativos/

Gregg Kreizman, Bruce Robertson. (2006). *Incorporating Security Into the Enterprise Architecture Process.* Gartner, Inc.

Grupo de Apoyo Operacional de Comunicaciones y Ciberdefensa. (2020). *Misión.* Bogotá D.C.

Help Net Security. (2015). *Engaging business units in security governance: Why everyone should be concerned.* Obtenido de https://www.helpnetsecurity.com/2020/08/05/engaging-business-units-in-security-governance/

Infocyte. (2019). *Nuevos programas para reducir el riesgo cibernético.* Obtenido de https://www.infocyte.com/es/blog/2019/01/04/managing-cybersecurity-risk-and-a-framework-for-making-investments/

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC. (2006). *NTC-ISO/IEC 27001.*

Instituto Nacional de Ciberseguridad de España – INCIBE. (2015). *¿Acceso remoto a la oficina? es posible con VPN.* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/acceso-remoto-oficina-posible-vpn

Instituto Nacional de Ciberseguridad de España. (2017). *Uso de técnicas criptográficas.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

Instituto SABSA CIC. (2020). *SABSA Arquitectura de seguridad empresarial/Resumen ejecutivo de SABSA*. Obtenido de https://sabsa.org/sabsa-executive-summary/

International Organization for Standarization, ISO. (2000). *Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799.*

International Organization for Standardization (ISO). (2013). *ISO/IEC 27001. Information security management.*

International Organization for Standardization (ISO). (2012). *ISO/IEC 27032:2012* . Obtenido de Information Technology — Security Techniques — Guidelines for Cybersecurity: https://www.iso.org/standard/44375.html

International Organization for Standardization (ISO) . (2005). *ISO/IEC 27001 Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos*.

International Organization for Standarization. (2018). *ISO 27000*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf.

ISACA Information Systems Audit and Control Association. (2015)

Javier Blanco. (2019). *Agenci6.com.* Obtenido de Combatir el cibercrimen: la ciberseguridad y el análisis forense digital son el nuevo equipo por excelencia: https://agencia6.com/index.php/2019/08/25/combatir-el-cibercrimen-la-ciberseguridad-y-el-analisis-forense-digital-son-el-nuevo-equipo-por-excelencia/

Jeimy Cano. (2008). *Arquitecturas de Seguridad Informática: Entre la administración y el gobierno de la Seguridad de la Información.*

John Sherwood, Andrew Clark, David Lynas. (2005). *Enterprise Security Architecture.* Boca Raton, Londres, Nueva York: Tylor & Francis Group.

J.P.Morgan. (2014). Gestión del Riesgo Operacional. Chase Bank.

Killmeyer, Jan. (2006). Information Security Architecture: An Integrated Approach to Security in the Organization. Boca Raton Nueva York: Taylor & Francis Group.

Lucas Paus - ESET . (2018). Aspectos a tener en cuenta para mejorar la capacidad de resiliencia ante un ciberataque. Obtenido de welivesecurity by ESET: https://www.welivesecurity.com/la-es/2018/05/04/aspectos-a-tener-en-cuenta-para-mejorar-la-capacidad-de-resiliencia-ante-un-ciberataque/

Ministerio de Defensa Nacional. (2014). *Directiva Permanente Ministerial DIR2014-18 "Políticas de Seguridad de la Información para el Sector Defensa".* Bogotá, D.C.

Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. (2014). *Agenda Estratégica de Innovación: Ciberseguridad.* Obtenido de MINTIC: https://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

National Institute of Standards and Technology NIST. (2013). Obtenido de Security and Privacy Controls for Federal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Organización de Estados Americanos OEA. (2004). *DECISIÓN 587 Lineamientos de la Política de Seguridad Externa Común Andina.* Obtenido de Sistema de información sobre Comercio Exterior SICE: http://www.sice.oas.org/Trade/Junac/decisiones/DEC587s.asp

Organización de Estados Americanos OEA. (2012). *AG/RES. 2004 (XXXIV-O/04) ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA* . Obtenido de https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf

Organización de Naciones Unidas. (2009). *Resolución A/RES/64/25.2010 "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional".* Obtenido de https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/25&Lang=S

Organización Internacional de Normalización (ISO). (2018). *ISO 31000:2018 Gestión del Riesgo.* Obtenido de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Open Security Architecture. (2020). *OSA*. Obtenido de Open Security Architecture: http://www.opensecurityarchitecture.org/cms/

Red Hat Enterprise, Inc. (2003). Manual de Seguridad. Obtenido de http://web.mit.edu/rhel-doc/3/rhel-sg-es-3/ch-detection.html.

Red Hat Enterprise, Inc. (2003). *Manual de Seguridad.* Obtenido de http://web.mit.edu/rhel-doc/3/rhel-sg-es-3/ch-response.html

SANS. (2004). *Information Systems Security Architecture A Novel Approach to Layered Protection, Worm Propagation and Countermeasures.*

The Open Group. (2018). *Open Group Standard The Open Group. In The TOGAF® Standard, Version 9.2.*