IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DEL MINISTERIO DE DEFENSA NACIONAL EN EL PROCESO DE TALENTO HUMANO

JAIRO ANDRES MORENO CIRO

INSTITUCION UNIVERSITARIA POLITECNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS

BOGOTA

2016

IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DEL MINISTERIO DE DEFENSA NACIONAL EN EL PROCESO DE TALENTO HUMANO

JAIRO ANDRES MORENO CIRO

Asesor Principal

Ing. Martha Lucia Sánchez Niño

Ministerio de Defensa Nacional – Oficina Asesora de Sistemas

Asesor Académico

Msc. Wilmar Jaimes Fernández

Politécnico Grancolombiano

INSTITUCION UNIVERSITARIA POLITECNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS

BOGOTA

2016

CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1. INTRODUCCION

A través de los años las tecnologías de la información y comunicación han ido en una constante evolución, lo cual ha traído grandes beneficios para la humanidad y desafortunadamente el crecimiento de medios delictivos en el robo de información, por esta razón se ha visto la necesidad de adoptar nuevas medidas, políticas y controles que permitan proteger al estado de nuevas amenazas [1,2].

Durante los años 2000 a 2011 ocurrieron varios tipos de incidentes generados por ataques o intrusión de software maliciosos en el mundo [1], donde Colombia no es la excepción, para gobiernos como el de Estonia un ataque ocurrido en el 2007 se consideró como el más grave de la historia, en el cual los ministerios, el parlamento, partidos políticos, dos de sus más grandes bancos y presidencia se vieron afectados. Este ataque armo una crisis en la cual requirió la intervención de grandes organizaciones entre estas la OTAN, quien un año después puso en marcha el centro de experiencia para la cooperación en ciberdefensa (CCD) [1].

Cabe retomar que Colombia ha sido también centro de ataques, en el 2011 sufrimos un ataque por el grupo Hacktivista autodenominado Anonymous, el cual ataco varios portales dejándolos inutilizables por varias horas [1].

Donde el Ministerio de Tecnologías de la información y las Comunicaciones en el 2011, crea la forma de implementar instancias más apropiadas con el fin de gestionar y regular incidentes o emergencias cibernéticas, de manera que se puedan mitigar las amenazas que atenten contra la ciberseguridad y ciberdefensa nacional. En la cual se establece una comisión intersectorial formada por el ColCERT (Grupo de Respuestas a Emergencias Cibernéticas de Colombia), CCP (Centro Cibernético Policial) y CCOC (Comando Conjunto Cibernético) [1].

Viendo la necesidad de protección de la información se crean planes de acción, liderados por el Ministerio de Tecnologías de la información y las Comunicaciones, en cuanto a todo lo relacionado con seguridad informática y de la información, que busca reconocer la Seguridad de la información como un factor necesario y relevante para la apropiación del manual de Gobierno en Línea (GEL) [3,4], en la educación y orientación de los PILARES FUNDAMENTALES DE LA SEGURIDAD DE LA INFORMACION, Confidencialidad (La información solo debe ser accesible para solo personas con el nivel

de privilegios para hacerlo.), Integridad (La información no puede ser manipulada sin autorización.) y Disponibilidad (La información Debe estar Disponible en el momento que sea solicitada.) [3].

Todo este conjunto de protocolos y lineamientos definidos en el manual de gobierno en línea [2,3], en el desarrollo del proyecto dentro del Ministerio de Defensa Nacional, busca la expansión de la certificación en el proceso de Talento Humano en el estándar NTC-ISO IEC 27001:2013 con el objeto de gestionar de forma correcta la seguridad de la información, El proyecto iniciara con un mecanismo de sensibilización a los usuarios de talento humano de la manera adecuada en gestión de seguridad de la información.

El desarrollo del proyecto dentro del Ministerio de Defensa Nacional, busca la certificación del Grupo Talento Humano en el estándar NTC-ISO IEC 27001:2013 con el objeto de gestionar de forma correcta la seguridad de la información. El proyecto iniciara con un mecanismo de sensibilización a los usuarios del Grupo Talento Humano, con el fin de que tomen cultura sobre la seguridad de la información.

2. JUSTIFICACIÓN

La información, a lo largo de la era tecnológica, ha sido un blanco de ataque y para resguardarla se ha visto la necesidad de establecer un plan de acción con el fin de su protección, por esto se implementan modelos de seguridad de la información ligados a buenas prácticas, de manera que el proceso de implementación del SGSI se pueda realizar de forma eficiente y mejore la seguridad de nuestra información.

Teniendo en cuenta que la Oficina Asesora de Sistemas del Ministerio de Defensa Nacional, durante el periodo 2015 obtuvo la certificación del sistema de gestión de la seguridad de la información para TICS basado en la norma NTC-ISO IEC 27001:2013 se requiere ampliar la cobertura de la certificación al proceso de talento humano ya que son procesos transversales a la entidad de acuerdo a los lineamientos y políticas del Ministerio de Defensa Nacional.

En el sistema de gestión de la seguridad de la información se clasifica y se cargan los activos a la plataforma de gestión de activos, procediendo a clasificar los riesgos que puedan ser valorados, revisar la probabilidad de ocurrencia e impacto y determinar los

niveles de riesgo de estos. Con el fin de generar una matriz, para después aplicar un plan de tratamiento de la seguridad de la información.

La metodología de implementación del Sistema de Gestión de Seguridad de la Información, manifestara la forma correcta de implementación dentro de una entidad pública como el Ministerio de Defensa Nacional, con lo cual la universidad podrá sumar esta metodología para el uso investigativo.

Dentro del proceso de formación del estudiante, tendrá profundización en los temas referentes a seguridad de la información en su carrera como Ingeniero de Telecomunicaciones.

3. OBJETIVO GENERAL

Documentar la metodología de implementación del sistema de gestión de seguridad de la información del Ministerio de Defensa Nacional, en el proceso de talento humano, cubriendo los requerimientos de la norma NTC-ISO/IEC 27001:2013 con énfasis en tratamiento de riesgos.

4. OBJETIVOS ESPECÍFICOS

1. Realizar el levantamiento de información en el Grupo de Talento Humano para el cargue de los activos en la plataforma, para su posterior monitoreo.
2. Aplicar los procesos de valoración de riesgos de la seguridad de la información, para identificar los asociados con la perdida de confidencialidad, integridad y disponibilidad dentro del sistema de gestión.
3. Clasificar la información de acuerdo al nivel de clasificación de la información del Ministerio de Defensa Nacional.
4. Identificar los Riesgos en el Grupo Talento Humano.
5. Definir y aplicar planes de tratamiento de riesgos de la seguridad de la información.
6. Promover el nivel de cultura en seguridad de la información logrando un manejo más adecuado de la información.

5. MARCO REFERENCIAL- IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD EN LA INFORMACION – MINISTERIO DE DEFENSA NACIONAL - TALENTO HUMANO

Para la implementación de un sistema de gestión de seguridad de la información se tiene que tener anteriormente conocimientos en temas relacionados al mismo, de manera que hay que iniciar desde donde se fundamenta hasta el punto donde este se implementa.

5.1 SEGURIDAD DE LA INFORMACION

Para la implementación de un sistema de seguridad de la información tenemos que tener algunos ítems en cuenta, uno de estos y el más importante es la seguridad de la información que esta cimentada en los tres PILARES FUNDAMENTALES DE LA SEGURIDAD DE LA INFORMACION, Confidencialidad (La información solo debe ser accesible para solo personas con el nivel de privilegios para hacerlo.), Integridad (La información no puede ser manipulada sin autorización.) y Disponibilidad (La información Debe estar Disponible en el momento que sea solicitada para la persona con acceso a esta.) [3].

Donde lo que principalmente busca es la protección de la información ya que en estos momentos es uno de los bienes más preciados y más buscados por personas mal intencionadas.

5.2 CYBERSEGURIDAD

La cyberseguridad es la ausencia de ataques o amenazas a nuestras infraestructuras, donde el principal objetivo de un tercero mal intencionado es el robo de la información. Lo que busca es que a partir de herramientas o políticas detener o frenar ataques de robos de información y de los daños que puedan causar vulnerabilidades dentro de nuestros sistemas tecnológicos [5].

5.3 SISTEMA DE GESTION DE SEGURIDAD EN LA INFORMACION

Para poder iniciar con un proceso adecuado dentro de la implementación de un sistema de seguridad de la información, tenemos que llegar al trasfondo del por qué se ha llegado a implementar y que soluciona con el acogimiento de este sistema.

En este momento tenemos una gran cantidad de amenazas las cuales atentan contra nuestra información. Estas materializándose pueden ser ambientales informáticos y/o legales a la hora de no actuar como es debido con la sensibilidad de los activos que se manejen y el Core de negocio de la organización.

Dentro de las normas las cuales nos vamos a guiar y vamos a estar cimentados serán la familia 27000

Esta es un estándar de las buenas prácticas que proporciona un marco de gestión de la seguridad de la información.

5.4 ISO/IEC 27000

Esta es un conjunto estándar de buenas prácticas que proporciona un marco de gestión para la seguridad de la información, donde es aplicable en cualquier tipo de entidad sea Pública o Privada.

De donde su conjunto de normas más importantes para la gestión de la seguridad de la información son:

ISO/IEC 27001 REQUERIMIENTOS PARA IMPLEMENTAR UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION.

ISO/IEC 27002 CODIGO DE PRACTICAS PARA CONTROLES DE SEGURIDAD DE LA INFORMACION.

ISO/IEC 27003 GUIA PARA LA IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD DE LA INFORMACION.

ISO/IEC 27004 GUIA PARA EVALUAR LA EFICACIA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

ISO/IEC 27005 GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

ISO/IEC 27006 PROCESO DE ACREDITACION DE ENTIDADES DE CERTIFICACION Y EL REGISTRO DEL SISTEMA DE GESTION EN SEGURIDAD DE LA INFORMACION

5.4.1 ISO/IEC 27001 REQUERIMIENTOS PARA IMPLEMENTAR UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Esta norma proporciona un modelo de seguridad en seguridad de la información con el fin de implementar un sistema en nuestra organización, de manera que podamos

proteger nuestra información, monitorizar, mantener y mejorar constantemente nuestros indicadores en seguridad.

Esta norma se basa en el ciclo PHVA donde este se divide de esta manera.

- P (Planear)=Establecer el Sistema de gestión de seguridad de la información.
- H (Hacer)= Implementar y operar el SGSI.
- V (Verificar)=Monitorear y Seguir el SGSI.
- A (Actuar)=Mantener y Mejorar el SGSI.

Este estándar permite acceder a la certificación esto significa que la organización ha ampliado sus parámetros en seguridad de la información y ha aplicado los controles necesarios [6].

5.4.2 ISO/IEC 27002 CODIGO DE PRACTICAS PARA CONTROLES DE SEGURIDAD DE LA INFORMACION

En esta norma se describen los dominios de control y mecanismos, donde se encuentran controles para reducir la probabilidad de ocurrencia o mitigar el impacto de un riesgo en alguna organización

5.4.3 ISO/IEC 27005 GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Esta norma indica directrices, controles o recomendaciones para hacer una tratarlos de manera apropiada para la implementación correcta de nuestro sistema. Buena gestión del riesgo, de manera que podamos identificarlos valorarlos y tratarlos.

5.4.4 ISO/IEC 31000 GESTION DEL RIESGO

Esta norma da directrices y principios para identificar los diferentes tipos de riesgos existentes dentro de una organización sea pública, privada, chica o grande.

Esto con el fin de ayudar a mejorar la cultura en todo el tema relacionado a riesgos, como identificarles, como tratarles y como evitar que un riesgo se materialice provocando pérdidas innecesarias dentro de una organización.

5.5 TALENTO HUMANO

Esta área de trabajo dentro de una organización es la más importante ya que es la que principalmente se encarga del proceso de selección para la persona que quiera aplicar al empleo.

Se tienen 3 modalidades las cuales son:

- Antes de asumir el empleo
- Durante la ejecución del empleo
- Salida del empleador de la organización

De esta manera se gestiona talento humano, donde entre los ítems presentados anteriormente se desarrollan una variedad de actividades para cada uno de los ítems contemplados para el bienestar o seguimiento del empleado.

5.6 LEYES APLICABLES AL SGSI

5.6.1 LEY ESTATUTARIA 1581 DE 2012

Por la cual se dictan disposiciones generales para la protección de datos personales.

5.6.2 DECRETO 1377 DEL 2013

Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

5.6.3 LEY ESTATUTARIA 1266 DE 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

5.6.4 LEY 1273 DEL 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

6. METODOLOGIA DE IMPLEMENTACION SGSI

La metodología de Implementación del Sistema de Gestión en Seguridad de la Información tiene unos pasos a seguir, de tal manera que tiene un orden dentro de la implementación, los cuales seguimos de la siguiente manera:

1. Planificación del Proyecto
2. Presentación General del Sistema de Gestión en Seguridad de la Información
3. Levantamiento de Información e identificación de activos de información.
4. Valoración de Activos de Información
5. Clasificación de la información
6. Aprobación de Activos de Información
7. Identificación de Riesgos en Seguridad de la Información
8. Tratamiento de los Riesgos en Seguridad de la Información
9. Identificación de la Normatividad

Entre todos los puntos tratados las actas son un tema de tratar en todos los pasos, de manera que esto va a ser nuestro sustento de que se realizaron cada una de las actividades en el tiempo propuesto y se realizaron con cada uno de los líderes o coordinadores

6.1. PLANIFICACION DEL PROYECTO

Para iniciar con la implementación del proyecto, se inicia con una planificación mes a mes de las actividades que se van a realizar, se determina que tiempo asignar a cada actividad a partir de su complejidad, el objetivo a tratar durante la implementación con su alcance respectico y los funcionarios los cuales tendrían roles de custodios o propietarios de la información para iniciar las actividades acordadas durante la planificación.

6.1.1. ACTAS Y FORMATOS DE ASISTENCIA

Para todo procedimiento que se realice bajo la norma ISO 27001 se tiene que llevar un control de las actividades que se lleven a cabo incluyendo las mesas de trabajo que se realicen con cada uno de los líderes que se asignen dentro de Talento Humano, esto con el fin de llevar un control de las actividades realizadas y compromisos de lo que se realizara en cada fase del proyecto hasta su culminación para el momento que se realice la auditoria de la implementación dentro del Ministerio de Defensa Nacional. [8]

6.1.2. PRESENTACION GENERAL SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION

Se realiza una presentación donde van contemplados los temas que se van a tratar dentro de la implementación del SGSI.

Esto con el fin de informar de cada una de las actividades que se van a llevar a cabo en Talento Humano.

Las cuales son:

Levantamiento de información de activos SGSI.

Identificación de activos de información.

Valoración de activos de información.

Clasificación activos de información.

Identificación de Riesgos de la Información.

Planes de Tratamiento de Riesgos

6.2. LEVANTAMIENTO DE INFORMACION E IDENTIFICACION DE ACTIVOS DE INFORMACION

Se realiza una presentación personalizada donde se les da una asesoría acompañada, se les explica cómo se hace la identificación de los activos de información. Para la cual comenzando se les habla de activos primarios, activos de soporte, como identificarlos y como subirlos en la plataforma de gestión de activos de la información donde se hace un inventario de todos los activos levantados durante el levantamiento de información. De esta manera dentro de la plataforma iniciamos el proceso de clasificación de la información con sus respectivos atributos [6].

6.2.1 ACTIVOS DE PRIMARIO

Los activos primarios son todo tipo de información impresa, electrónica y servicios Centrales los cuales sean vitales para la organización.

Activos de información**:** Es todo aquel elemento que procese, almacena o trasmite información.

Ejemplo:

Hojas de vida

Memorandos

Actas

Etc.

6.2.2 ACTIVOS DE SOPORTE

Los activos de soporte son todo los cuales dependen de los activos primarios, los cuales se clasifican en:

Software

Hardware

Recurso Humano

Servicios

Sitios (Lugar físico de almacenamiento de la información)

6.2.3 ROLES

Los roles son la clasificación de los funcionarios dentro de la organización, es decir a partir de su área se les asigna un rol como líder de la siguiente manera:

Área de trabajo: Seguridad y Salud en el Trabajo

Líder: Líder área Seguridad y Salud en el Trabajo

Esto para los custodios de la información pero en el caso que sea propietario de la información, es decir la persona que sea el líder o coordinador de todo el proceso se le asignar un rol de propietario de la información.

Líder Talento Humano, Coordinador Talento Humano o de la manera más adecuada que se quiera clasificar según el criterio de la metodología [6,7].

6.3 CLASIFICACION DE ACTIVOS DE INFORMACION

Iniciando la clasificación de la información hay que tener muy en cuenta en como los identificamos, si como Activos de información o activos de soporte, para iniciar con la clasificación de los atributos hay que tener muy en cuenta 2 factores [6,7].

Si son Activos Primarios

Si son Activos de Soporte

Si son activos primarios de información se les diligencia como atributos:

Tipo de activo

Lugar físico de estancia del activo

Lugar Electrónico de estancia del activo

Custodio (Rol) Persona encargada de ejecutar las acciones en los activos de información

Propietario (Rol) Persona encargada de tomar decisiones sobre los activos de un proceso dentro de la organización

Área de trabajo

Datos Personales

Tipos de información (Publica Semiprivada y Privada)

Dependencia entre activos (Activos de soporte o primarios)

Si son activos de soporte se les diligencia como atributos:

Tipo de activo

Lugar físico de estancia del activo

Lugar Electrónico de estancia del activo

Custodio (Rol) Persona encargada de ejecutar las acciones en los activos de información

Propietario (Rol) Persona encargada de tomar decisiones sobre los activos de un proceso dentro de la organización

Área de Trabajo

6.4 VALORACION DE ACTIVOS DE INFORMACION

Para realizar la valoración de activos de la información se realiza otra presentación personalizada con cada uno de los miembros para definir de qué manera se va a valorar los activos a partir de una breve encuesta donde se les realizan preguntas a partir de una matriz de valoración establecida por el Ministerio de Defensa Nacional, donde se encuentra el área de impacto y el valor para la organización de cada uno de los activos que se valoran.

La valoración únicamente se les realiza a los activos Primarios de información, de esta manera se agiliza el proceso de valoración sin entrar en contexto de valoración a los

activos de soporte ya que no representan una alta importancia o que puedan incurrir en algún riesgos alto para la organización.

Ilustración 1 Valoración de Activos

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

Fuente: Proceso de valoración de activos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7].

6.4.1 AREA DE IMPACTO

Para el área de impacto tenemos varios tipos de impactos dentro de una organización.

Como lo son:

IMAGEN

FINANCIERO

ESTABILIDAD

HUMANO

Donde cada uno de estos tiene un nivel de clasificación diferente a partir de la gravedad del activo afectado. Es decir a partir del activo calificado dependiendo su valor para la organización.

De manera que la forma más grave como ejemplo es que un activo pueda afectar la imagen internacionalmente de la organización, o en su forma menos grave que ese activo no afecte la imagen de nada dentro de la organización [7].

6.4.2 VALOR DEL ACTIVO DENTRO DE LA ORGANIZACIÓN

Dentro de una organización existen diferentes tipos de activos de información unos con más importancia o valor que otros, de esta manera podemos clasificar los activos a partir de su importancia dentro de la organización, un activo puede ser de lo menos significante hasta uno de los activos más importantes de la organización y dependiendo su valor pueden afectar a la organización de muchas maneras a partir del impacto.

6.5 CLASIFICACION DE LA INFORMACION

Dentro de la clasificación de la información del MDN se utiliza una clasificación privada diseñada según el core de negocio y las necesidades que pudieran surgir a un futuro de tal manera que se toma en cuenta el impacto de la información a clasificar y el valor para el MDN [7].

Esto con el fin de indicar la necesidad, prioridades y el nivel de protección de la información. Para el Ministerio de Defensa Nacional por el nivel de información que se maneja la clasificación de la información diseñada por ellos es de tan alta sensibilidad que no se puede dar a conocer abiertamente al público.

La clasificación de la información se puede dar de esta manera como ejemplo:

Tabla 1 Clasificación de la información

Publico	Información abierta al público y que se puede ser accesible por terceros
Privado	Información privada de acceso para solo entes de la organización.
Confidencial	Información con clasificación confidencial de forma que solo lo pueden ver altos ejecutivos o custodios de esa información
Secreto	Información con clasificación secreta de acceso para algunos altos ejecutivos y el presidente de la organización

Tabla elaborada a partir de la Guía para la Administración del Riesgo [8].

6.6 APROBACION DE ACTIVOS DE INFORMACION

Para la aprobación de activos de activos de información se hace una serie de mesas de trabajo con los líderes de cada área y la Coordinadora del Grupo Talento Humano, con el fin que de cada junta Líder – Coordinadora se aprueben los activos y se corrijan de manera que podamos tener el inventario de activos al día y autorizados por la Coordinadora del grupo o la propietaria de los activos de información del Proceso o Grupo. [7]

6.7 IDENTIFICACION DE RIESGOS EN SEGURIDAD DE LA INFORMACION

Se define riesgo la posibilidad de que un evento se materialice y que tenga impacto en los objetivos de la organización.

Este riesgo se compone de:

Tabla 2 Composición del Riesgo

Causa	Factor o Circunstancia
Evento	Suceso o acontecimiento imprevisto con cierta importancia
Efecto	Consecuencia de ocurrencia de un riesgo

Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7].

Donde el primer análisis del riesgo se denomina inherente, el cual es el riesgo sin controles aplicados, donde es el riesgo en su estado más puro.

6.7.1 CLASES DE RIESGO

Los riesgos se podría decir que son un tema del día a día en las organizaciones de manera que los riesgos se clasifican en:

Tabla 3 Clases de Riesgo

Riesgo Estratégico	Este se asocia a la estructura de la entidad, la administración de este riesgo se enfoca en misión y cumplimiento de la organización en temas relacionados con objetivos estratégicos.
Riego de Imagen	Estos están relacionados en temas de confianza por parte de la ciudadana hacia la institución u organización.

Riesgos Operativos	Los riesgos operativos están relacionados con el funcionamiento y operatividad de los procesos dentro de la organización.
Riesgos Financieros	Para los riesgos financieros son todos lo relacionados con todo el manejo de recursos de la entidad.
Riesgos de Cumplimiento	Cumplimientos de todas las normatividades legales, Contractuales, de ética pública y compromiso con la comunidad
Riesgos Tecnológicos	Capacidad de la entidad para satisfacer sus necesidades tecnológicas actuales y futuras
Riesgos de Seguridad de la Información	Protección de la información de la entidad en cuanto a los 3 pilares de seguridad de la información

Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7].

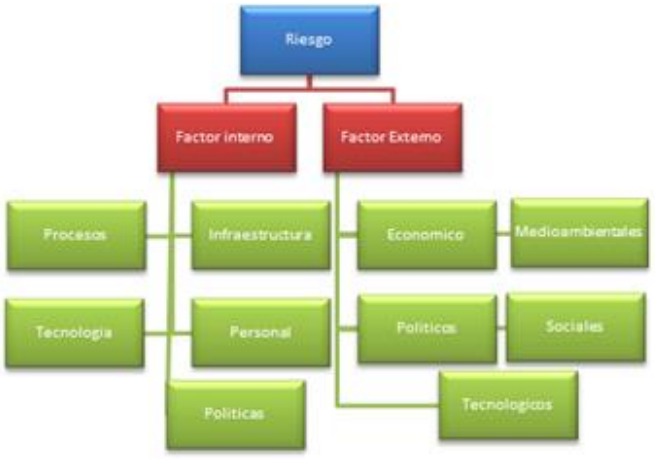
Riesgo en seguridad de la información

Es la probabilidad de que un evento relacionado con Confidencialidad, Integridad y Disponibilidad se materialice convirtiéndose en un riesgo en Seguridad de la información.

6.7.2 CONTEXTO ORGANIZACIONAL

Son las condiciones internas o externas que puedan afectar un proceso dentro de la organización y están divididos de la siguiente manera:

Ilustración 2 Contexto Organizacional



Nota :Imagen elaborada a partir de la Guía para la Administración del Riesgo [8].

Donde los riesgos externos se monitorean y los riesgos internos se administran ya que los factores internos se pueden controlar y los externos no.

Ilustración 3 Factores Externos e Internos

EJEMPLO DE FACTORES INTERNOS Y EXTERNOS DE RIESGO	
FACTORES EXTERNOS	FACTORES INTERNOS
Económicos: disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempleo, competencia	**Infraestructura:** disponibilidad de activos, capacidad de los activos, acceso al capital
Medioambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible	**Personal:** capacidad del personal, salud, seguridad
Políticos: cambios de gobierno, legislación, políticas públicas, regulación	**Procesos:** capacidad, diseño, ejecución, proveedores, entradas, salidas, conocimiento
Sociales: demografía, responsabilidad social, terrorismo	**Tecnología:** integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento
Tecnológicos: interrupciones, comercio electrónico, datos externos, tecnología emergente	

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública. 2011 [8].

6.7.3 IDENTIFICACION DEL RIESGO

Tabla 4 Tipos de Riesgo en Seguridad de la Información

Acceso o divulgación no autorizada lo cual genera uso indebido de la información.	Confidencialidad
Pérdida de la Integridad : 1. Dificultad en la lectura de la información. 2. Contención errónea o modificada de la información.	Integridad
Pérdida de la Disponibilidad 1. Pérdida de la disponibilidad parcial o total dificultando que una operación se pueda cumplir	Disponibilidad

Nota: Tomada de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7].

Donde los riesgos están compuestos por:

Tabla 5 Composición del Riesgo

Causa	Vulnerabilidades y Amenazas
Evento	Escenarios
Efecto	Consecuencia del riesgo que afecta a los activos primarios

Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7].

Tabla 6 Identificación del Riesgo en el Activo

Nombre del activo	Hoja de vida
Nombre del riesgo	Pérdida de Confidencialidad por divulgación de la información
Causas	Inadecuada protección de datos personales. Divulgación no autorizada de la información.
Evento	Divulgación de la información física debido a fallas en el seguimiento y revisión de los acuerdos de confidencialidad con terceros
Efecto del riesgo	Robo de la información por tercero

Fuente: Tomada de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7].

Tabla de probabilidad e impacto

Según la metodología del Ministerio de Defensa Nacional la medición de la probabilidad se debe hacer con la siguiente tabla, en el caso de una organización diferente pueden usar estándares de esta tabla.

Ilustración 4 Tabla de Probabilidad del Riesgo

NIVEL	PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
5	Casi con certeza	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en el último año.
3	Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de 1 vez en los últimos 5 años.
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.

Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7].

Para el criterio de impacto se debe medir de la siguiente manera.

Ilustración 5 Tabla de Impacto General del Riesgo

NIVEL	IMPACTO	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o **efectos mínimos** sobre la entidad, en los siguientes aspectos: **IMAGEN:** Afectaría a un Grupo de Funcionarios. **LEGAL:** Multas. **OPERATIVO:** Se presentarían ajustes a una actividad concreta. **OBJETIVOS:** Impacto insignificante sobre los objetivos.
2	Menor	Si el hecho llegara a presentarse, tendría **bajo impacto** o efecto sobre la entidad, en los siguientes aspectos: **IMAGEN:** Afectaría a Todos los Funcionarios. **LEGAL:** Demandas. **OPERATIVO:** Se presentarían cambios en procedimientos. **OBJETIVOS:** Efectos menores que se remedian fácilmente.
3	Moderado	Si el hecho llegara a presentarse, tendría **medianas consecuencias** o efectos sobre la entidad, en los siguientes aspectos: **IMAGEN:** Afectaría a los Usuarios de la Ciudad. **LEGAL:** Investigación Disciplinaria. **OPERATIVO:** Se presentarían cambios en la interacción de los Procesos. **OBJETIVOS:** Algunos objetivos afectados.
4	Mayor	Si el hecho llegara a presentarse, tendría **altas consecuencias** o efectos sobre la entidad, en los siguientes aspectos: **IMAGEN:** Afectaría a los Usuarios de la Región. **LEGAL:** Investigación Fiscal. **OPERATIVO:** Se presentarían intermitencia en el Servicio. **OBJETIVOS:** Algunos objetivos importante no se pueden lograr.
5	Catastrófico	Si el hecho llegara a presentarse, tendría **desastrosas consecuencias** o efectos sobre la entidad, en los siguientes aspectos: **IMAGEN:** Afectaría a los Usuarios del País. **LEGAL:** Intervención - Sanción. **OPERATIVO:** Paro Total del proceso. **OBJETIVOS:** La mayoría de los objetivos no se pueden lograr.

Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7,8].

6.8 TRATAMIENTO DE LOS RIESGOS EN SEGURIDAD DE LA INFORMACION

6.8.1 VALORACION DEL RIESGO

Para poder iniciar con el tratamiento de los riesgos en seguridad de la información hay que tener en cuenta 4 puntos los cuales son:

- La identificación de los controles existentes
- Verificación de la efectividad de los controles
- Establecer las prioridades del tratamiento
- Clasificación de los controles

Clasificación de Controles

Existen tres tipos de controles los preventivos los cuales reducen la probabilidad de materialización del riesgo eliminando las causas del riesgo (Vulnerabilidades) y los controles correctivos y detectivos los cuales reducen el impacto del riesgo (Amenazas) , estos controles se pueden identificar en el Anexo A de la ISO 27001:2013 o más específicamente en la 27002:2013.

Tabla 7 Ejemplos de Control

A.9.2.6	Retiro o ajuste de los derechos de acceso	Correctivo	Reduce impacto
A.9.2.5	Revisión de los derechos de acceso de usuarios	Detectivo	Reduce Impacto
A.8.3.2	Disposición de los medios de soporte	Preventivo	Reduce Probabilidad

Nota: Elaborada a partir de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7].

A partir de los controles tenemos que valorarlos para determinar que tantos cuadrantes nos vamos a mover dentro de la matriz de riesgos, la valoración de los controles estada dada por la siguiente tabla [8].

Ilustración 6 Valoración de Controles

¿Cómo se valoran los Controles?

CONTROLES		Cumple Criterio SI/NO		PUNTAJES
PARAMETROS	CRITERIOS	Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			20
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta			20
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			20
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			20
	La frecuencia de ejecución del control y seguimiento es adecuada.			20
	TOTAL			100

Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas

A partir de la tabla que se presenta a continuación valoramos cuantos cuadrantes en probabilidad y en impacto vamos a reducir:

Tabla 8 Valoración de Controles por Cuadrantes

0-74	0 Cuadrantes
75-97	Un Cuadrante
97-100	Dos Cuadrantes

Nota: Tomada de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7]

Inicialmente damos una calificación de la probabilidad y del impacto del riesgo en nuestro activo de información asociado al riesgo, a partir de la probabilidad y el impacto vamos a tener las siguientes calificaciones del riesgo las cuales van desde bajo a extremo y que

su nivel de riesgo está dada por probabilidad e impacto donde es evidenciada en la siguiente tabla.

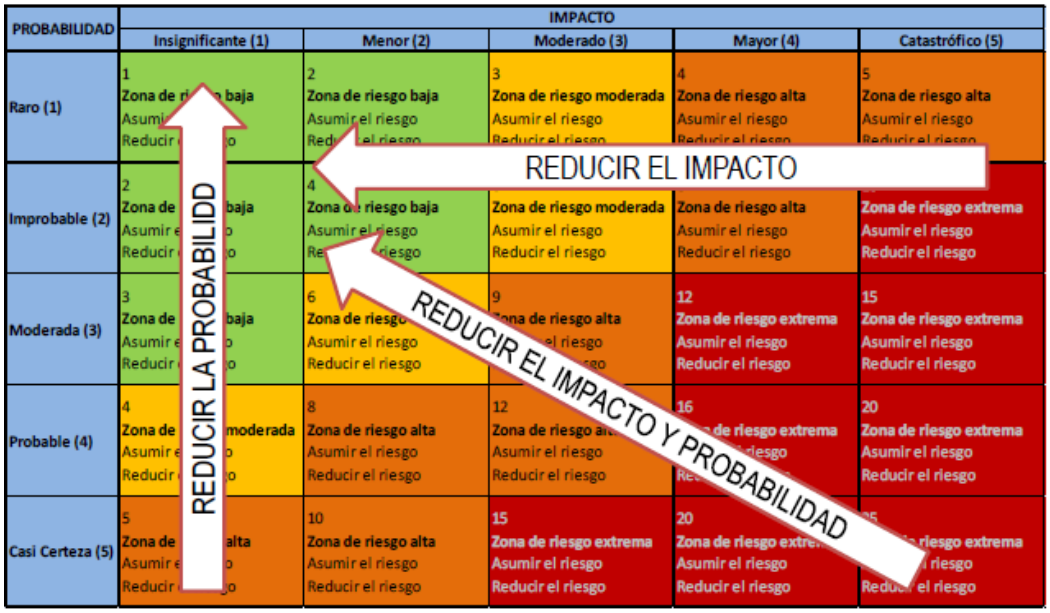
Tabla 9 Nivel del Riesgo

		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Raro	Bajo	Bajo	Moderado	Alta	Alta
	Improbable	Bajo	Bajo	Moderado	Alta	Extrema
	Moderado	Bajo	Moderado	Alta	Extrema	Extrema
	Probable	Moderada	Alta	Alta	Extrema	Extrema
	Casi con certeza	Alta	Alta	Extrema	Extrema	Extrema

Nota: Tomada de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7].

De manera que cuando iniciamos a aplicar los controles en seguridad de la información para los riesgos empezamos a reducir en cuadrantes a partir de la calificación que nos indique la valoración de los controles.

Tabla 10 Reducción de Cuadrantes según el Control



Fuente: Identificación de Riesgos. Ministerio de Defensa Nacional – Oficina Asesora de Sistemas [7]

A partir del nivel del riesgo inicial decidimos que tratamiento iniciar si asumimos, compartimos, evitamos o transferimos dependiendo el nivel del riesgo que nos quede calificado.

Donde los tratamientos son:

Tabla 11 Tratamiento Según el Nivel Riesgo

Asumimos	Se asume el riesgo y no hay necesidad de aplicar más controles para reducir su criticidad **Esto para zona de riesgo Baja.**
Compartir o trasferir el riesgo	Reduce el efecto compartiendo las pérdidas del riesgo con otras entidades o compartiendo la información. **Esto Para zona de riesgo Alta o Extrema.**
Evitamos	Cese de las actividades para prevenir la materialización del Riesgo **Esto para zonas de riesgo Alta y Extrema.**
Reducimos	Se decide aplicar controles en seguridad de la información para reducir el nivel de riesgo asociado. **Esto para las zonas de riesgo Moderada, Alta o Extrema.**

Nota: Tomada de Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública. 2011 [8].

En el momento de aplicar controles a un riesgo en seguridad de la información pasa a ser un riesgo residual, el cual es el riesgo con controles establecidos, una vez sabiendo esto en el momento de saber cuántos cuadrantes debemos desplazarnos en probabilidad y/o

en impacto vamos a reducir el nivel de riesgo según la matriz riesgos establecida anteriormente.

Ejemplo

Tabla 12 Riesgo Inherente

Riesgo Inherente						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Raro	Bajo	Bajo	Moderado	Alta	Alta
	Improbable	Bajo	Bajo	Moderado	Alta	Extrema
	Moderado	Bajo	Moderado	Alta	Extrema	Extrema
	Probable	Moderada	Alta	Alta	Extrema	Extrema
	Casi con certeza	Alta	Alta	Extrema	Extrema	Extrema

Nota: Tomada de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7].

Si nuestro riesgo valorado se encuentra en extrema una vez iniciado el proceso como riesgo inherente, nos tenemos que remitir a decidir cómo lo vamos a tratar.

En el caso más común el riesgo se Reduce**,** entonces necesitamos como primer objetivo un control o varios controles que nos mueva 2 casillas hacia la izquierda y 2 hacia arriba es decir necesitamos utilizar un control preventivo y correctivo que sean eficientes para poder llevar el riesgo a un nivel menor, para esto se inicia un proceso de asignación de controles para el riesgo determinado, de manera que podamos llegar a la meta de reducir el riesgo a bajo.

La reducción del Riesgo no tiene que ser inmediata, el tiempo calificara si los controles son efectivos para mitigar el riesgo y determinar si es necesario aplicar más controles en un futuro, o si iniciar un plan de mejora de los controles para volverlos más robustos .

Tabla 13 Riesgo Residual

Riesgo Residual						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Raro	Bajo	Bajo	Moderado	Alta	Alta
	Improbable	Bajo	Bajo	Moderado	Alta	Extrema
	Moderado	Bajo	Moderado	Alta	Extrema	Extrema
	Probable	Moderada	Alta	Alta	Extrema	Extrema
	Casi con certeza	Alta	Alta	Extrema	Extrema	Extrema

Nota: elaborada a partir de identificación de riesgos. Ministerio de defensa Nacional - Oficina Asesora de Sistemas [7].

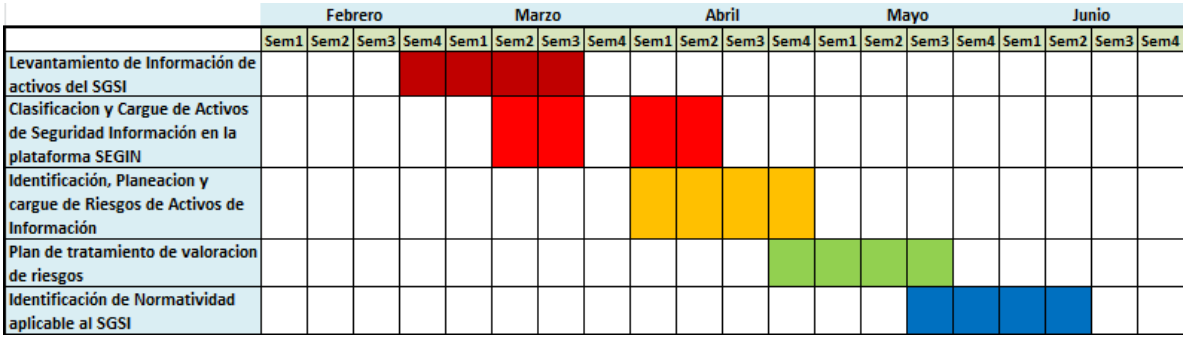
6.9 IDENTIFICACION DE NORMATIVIDAD

Realizar la identificación dentro del proceso de talento humano es un procedimiento largo y es fundamental tener en cuenta cuales son los procesos en los que se centra Talento Humano.

Dentro de Talento Humano se manejan los procedimientos de 3 formas antes de la contratación, durante la contratación del funcionario y en la salida del funcionario de la organización, de esta manera iniciaremos a clasificar las normatividades que van de la mano con el proceso de Talento Humano y del Sistema de Gestión en Seguridad de la Información.

La forma de identificar las normatividades ligadas al SGSI en Talento Humano se desarrolla creando un formato de normatividades donde los funcionarios durante una semana van a ligar las normatividades que estén ligadas al proceso, todo con relación a los decretos leyes normativas circulares entre otras, las cuales sirven o ya bien sea de consulta para hacer algún tipo de contratación, cuando un funcionario pide vacaciones o cuando un funcionario sale por renuncia o por pensión entre otros diferentes casos los cuales sucedan durante la administración de Talento Humano [7].

7. CRONOGRAMA



8. CONCLUSIONES

Dentro del camino en la implementación del sistema de gestión en seguridad de la información, podemos encontrar que dentro de los procesos realizados se puede ir hallando o encontrando medidas para prevenir perdida de la confidencialidad, integridad o disponibilidad de la información. Demostrando que la información nunca va a poder ser totalmente segura pero se pueden llegar a implementar medidas o controles los cuales pueden llevar a nuestra información a ser más segura, pero no afirmando que no siga siendo vulnerable ante distintas formas de amenazas o vulnerabilidades presentadas por factores interno o externos. Estamos en torno a un mundo donde la era tecnológica no tiene manera de detenerse más si de tomar controles para ayudar a gestionar nuestros medios tecnológicos y de información, a su misma vez tenemos medios externos de los cuales no podemos tomar ningún control de ellos los cuales nos generan amenazas o vulnerabilidades y lo único que podemos hacer es monitorizar lo que sucede día a día.

La certificación en la ISO 27001 ayuda a tener un control más adecuado de nuestros activos de información ya sean primarios o de soporte, ayuda a valorarlos de manera que sepamos qué nivel de importancia tiene ese activo para la organización, que nivel de impacto y qué valor tiene este sobre la organización para poder proceder a clasificar la

información y asegurar que se aplica un nivel de protección adecuado, la información se debe clasificar para indicar necesidades, prioridades y el nivel de protección.

Los riesgos los cuales tenemos que identificar para asegurar nuestra información es uno de los factores críticos para iniciar un tratamiento con controles, de esta manera nos adelantamos al riesgo aplicando controles para prevenir su materialización, evitando perdida de confidencialidad, integridad o disponibilidad, de forma que podamos asegurar nuestra información de diferentes tipos de amenazas o vulnerabilidades presentadas por factores internos o externos.

9. REFERENCIAS BIBLIOGRAFICAS

[1] Ministerio de Tecnologías de la información y las Comunicaciones. . (2011, 07, 23). Conpes 3701 de 2011 Disponible: http://www.mintic.gov.co/portal/604/w3-article-3510.html

[2] Ministerio de Tecnologías de la información y las Comunicaciones.(2014, 03). AGENDA ESTRATÉGICA DE INNOVACIÓN: CIBERSEGURIDAD Disponible: http://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

[3] Ministerio de Tecnologías de la información y las Comunicaciones. (2011, 12, 07). Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea 2.0 Disponible: http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf

[4] Gobierno en línea (2008, 12, 26) INFORME FINAL –MODELO DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA SANSI – SGSI -MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA Disponible: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

[5] Departamento de Comunicación del Ejército de Tierra. (2010, 03) RETOS, RIESGOS Y AMENAZAS AL INICIO DEL SIGLO XXI Disponible: http://www.ejercito.mde.es/Galerias/multimedia/revista-ejercito/2010/Revista_Ejercito_837.pdf

[6] International Organization for Standardization (2013, 11 , 25). ISO/IEC 27001:2013 Disponible: http://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

[7] Ministerio de Defensa Nacional

[8] Departamento Administrativo de la Función Pública. (2011, 09) Guía para la Administración del Riesgo Disponible: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592