DEFINICION DEL PLAN DIRECTOR DE SEGURIDAD PARA EL GRUPO ASD

Presentado por:
RICARDO ALBERTO DUITAMA LEAL

UNIVERSIDAD OBERTA DE CATALUNYA
MASTER INTERINSTITUCIONAL EN SEGURIDAD DE LA INFORMACION Y LAS TELECOMUNICACIONES
BARCELONA, ESPAÑA
2013

DEFINICION DEL PLAN DIRECTOR DE SEGURIDAD PARA GRUPO ASD

Presentado por:
RICARDO ALBERTO DUITAMA LEAL

Tutor Asignado:
Antonio José Segovia Henares

UNIVERSIDAD OBERTA DE CATALUNYA
MASTER INTERINSTITUCIONAL EN SEGURIDAD DE LA INFORMACION Y LAS TELECOMUNICACIONES
BARCELONA, ESPAÑA
2013

TABLA DE CONTENIDO

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE TABLAS

Pág.

GLOSARIO DE TERMINOS

Aceptación de riesgo: Una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Administración de riesgos: Involucra la cultura, procesos y estructuras de la organización que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.

Amenaza: Evento inesperado con el potencial para causar daños. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.

Análisis de riesgo: Un uso sistemático de la información disponible para determinar cuan frecuentemente puede ocurrir eventos especificados y la magnitud de sus consecuencias.

Confidencialidad: Pilar de seguridad que garantiza que la información solo es conocida por quien está autorizado para conocerla.

Consecuencia: El producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia.

Control de riesgos: El componente de la administración de riesgos, que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

Disponibilidad: Pilar de seguridad que consiste en garantizar que la información puede ser accedida por quien la requiere y cuando lo requiere.

Evaluación de riesgos: El proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivos u otro criterio.

Frecuencia: Una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado.

Gestión de riesgos: Es el proceso de identificación, evaluación y toma de acciones para reducir los riesgos a un nivel aceptable.

Identificación de riesgos: El proceso de determinar qué puede suceder, por qué y cómo.

Integridad: Pilar de seguridad de la información que garantiza que la información es completa y veraz.

No Repudiación: Pilar de seguridad que consiste en no poder negar la autoría de una transacción.

Probabilidad: La posibilidad de presentación de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados. La probabilidad se expresa como un número entre 0 y 1, donde 0 indica un evento o resultado imposible y 1 indica un evento o resultado cierto.

Proceso de administración de riesgos: La aplicación sistemática de políticas, procedimientos y prácticas de administración, a las tareas de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.

Riesgo residual: El nivel restante de riesgo luego de tomar medidas de tratamiento del riesgo.

Riesgo: La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se le mide en términos de consecuencias y probabilidades.

Tratamiento de riesgos: Selección e implementación de opciones apropiadas para tratar el riesgo.

Vulnerabilidad: Es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente.

0. INTRODUCCION

El presente Trabajo Final de Máster (TFM) tiene como finalidad la definición de un Plan Director de Seguridad para GRUPO ASD, el cual permitirá definir las bases de mejora continua a nivel de seguridad de la información permitiendo conocer el estado actual y definir las acciones necesarias para mitigar los riesgos que se presentan en los activos de información de la organización.

Este proyecto se dividirá en las siguientes cinco fases que permitirán identificar:

- Alcance del TFM y caracterización de la empresa: El objetivo es caracterizar la organización y definir el o los procesos sobre los cuales se desarrollara el presente proyecto.

- Identificación de Activos de Información: Una vez identificados el o los procesos a evaluar, se procederá a identificar cuáles son los activos de información que los soportan.

- Análisis de Riesgos: El análisis de riesgos permitirá identificar la situación actual de la organización y definir los controles para mantener un nivel de riesgo aceptable en la organización

- Definición del Plan Director de Seguridad: Este plan definirá la estrategia de toda la organización a corto, mediano y largo plazo.

- Presentación de informes: Una vez realizado un diagnóstico del estado actual de seguridad y de definir el Plan Director de Seguridad, se procede a presentar los resultados a la alta dirección y a los diferentes sponsors para garantizar así el apoyo en todo los niveles de la organización.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

El principal objetivo del presente proyecto es definir el Plan Director de seguridad para GRUPO ASD, el cual estará alineado bajo los estándares ISO 27001 e ISO 27002 y la metodología de análisis de riesgos MARGERIT.

1.2 OBJETIVOS ESPECIFICOS

Dentro de los objetivos que se pretende alcanzar con este proyecto están:

- Identificación de Activos Críticos para el proceso y subprocesos a evaluar.
- Realizar un proceso de análisis de riesgos bajo una metodología de riesgos identificando los riesgos y amenazas en cada uno de los activos de información.
- Realizar un análisis de Brecha para evaluar la situación actual de seguridad de la GRUPO ASD respecto a un estándar de buenas practica como lo es ISO 27002.
- Definición del Pan director para la organización teniendo como referencia el análisis de riesgo efectuado sobre los activos de información.
- Optimizar las inversiones en seguridad de la información al ejecutar planes de acción que apoyen la consecución de los objetivos de la organización.
- Mejorar los niveles de Seguridad de la Información al fomentar la adopción de una cultura de seguridad de la información a todos los niveles.

2. CONTEXTUALIZACION Y DOCUMENTACION

2.1 SELECCIÓN DE LA EMPRESA

El presente proyecto se pretende desarrollar en el GRUPO ASD, la cual es la entidad de más alto nivel de planeamiento y dirección estratégica para las instituciones castrenses de Colombia. Bajo su égida y faro están el Ejército Nacional, la Armada y la Fuerza Aérea.

De sus dependencias emanan las directrices y las políticas de mando para los soldados de tierra, de mar y de aire, en estricto y cabal cumplimiento de la misión prevista en el artículo 217 de nuestra Constitución Nacional.

“Las FM tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional”, reza en uno de sus apartes nuestra Carta Magna al hacer referencia específica al rol de las instituciones armadas colombianas.

Por motivos de seguridad no se mencionara la organización para garantizar la confidencialidad de la misma.

2.1.1 Principios, Valores, Misión y Visión de la Organización.

Misión.

Defender la soberanía, la independencia, la integridad del territorio nacional y la vigencia del orden constitucional, contribuir a la seguridad de la población y sus recursos, así como la ejecución de las funciones del Estado y los deberes de los individuos.

Visión.

La fuerza militar moderna, con estándares de alta profesionalidad, altos niveles de formación asegurados en sus valores a dar en la voluntad de lucha de las organizaciones terroristas, comprometida con el alcance de la paz y el desarrollo de la nación.

Principios.

Verdades inalterables que refuercen la base ética profunda de los hombres y mujeres que conforman las FM, cuya inviolabilidad es un compromiso para todos nosotros, y que nos guíe en la ejecución de la Política de Seguridad Democrática, encabezada por el Ministro de Defensa Nacional en el desarrollo de sus políticas sectoriales. Ellos son:

- Integridad en la observancia de la Constitución y la ley Depende de nosotros para defenderlos, para su conservación, para hacer que se respeten y cumplan estrictamente sus preceptos.

- Total respeto a la persona humana: Actuaciones guiadas con un examen profundo de las personas, tanto al interior como al exterior de la Institución, no el comportamiento del personal de las Fuerzas Militares atentar contra la calidad de la gente, la dignidad y la autoestima.

- Buscar la cooperación interinstitucional y la integración: Optimizar y servicios suplemento, prácticas de información y articular esfuerzos para garantizar la efectividad y oportunidad en los resultados.

- Transparencia y eficacia en todos sus actos: Profesionalismo, honestidad y dedicación en las misiones y tareas asignadas, para mejorar las acciones y la obtención de resultados efectivos, permite llevar a través de conceptos gerenciales y mandos modernos, la ganadora de la guerra y facilitar la solución del conflicto armado.

- Unión y el cambio: Unión y el cambio debe existir en toda la organización, para trabajar de manera conjunta en la consolidación y sostenibilidad de la seguridad en Colombia, y para adaptarse de manera eficiente a los cambios ambientales continuos y complejos.

Valores.

Actúan como el conjunto de creencias construidas en forma colectiva, otorgando estabilidad, sobre todo en la transformación diferente y los procesos de cambio, sino que son los primeros de todos los axiomas que acompañan al ejercicio de los principios. Los valores corporativos que sustentan la organización y las actividades que las FM realizan son:

- La honestidad de actuar con rectitud, sinceridad, transparencia y legalidad.

- Solidaridad para responder con acciones humanitarias ante situaciones que pongan en peligro la vida de los colombianos, la paz, el orden y la seguridad, fomentando la cooperación cívica.

- Justicia para dar a cada uno lo que le corresponde a él / ella, de acuerdo con sus méritos y / actos.

- La responsabilidad de asumir y aceptar las consecuencias de nuestros actos libres y conscientes.

- La lealtad es la plena manifestación de la fidelidad a la verdad, hacia uno mismo, la familia, la institución y la patria.

- El compromiso de conocer y cumplir con profesionalismo y sentido de pertenencia los deberes y obligaciones.

- Coraje al actuar con audacia intrepidez y sabiduría en cada situación necesaria para defender el bienestar de la nación.

- Honor virtud que caracteriza a la persona y que le hace a uno acorde con su / esencia de su ser y de los principios que él / ella ha prometido defender, respetar y aceptar.

- Respetar a tratar a los demás con respeto y consideración y aceptar su dignidad, creencias, tradiciones, costumbres y derechos.

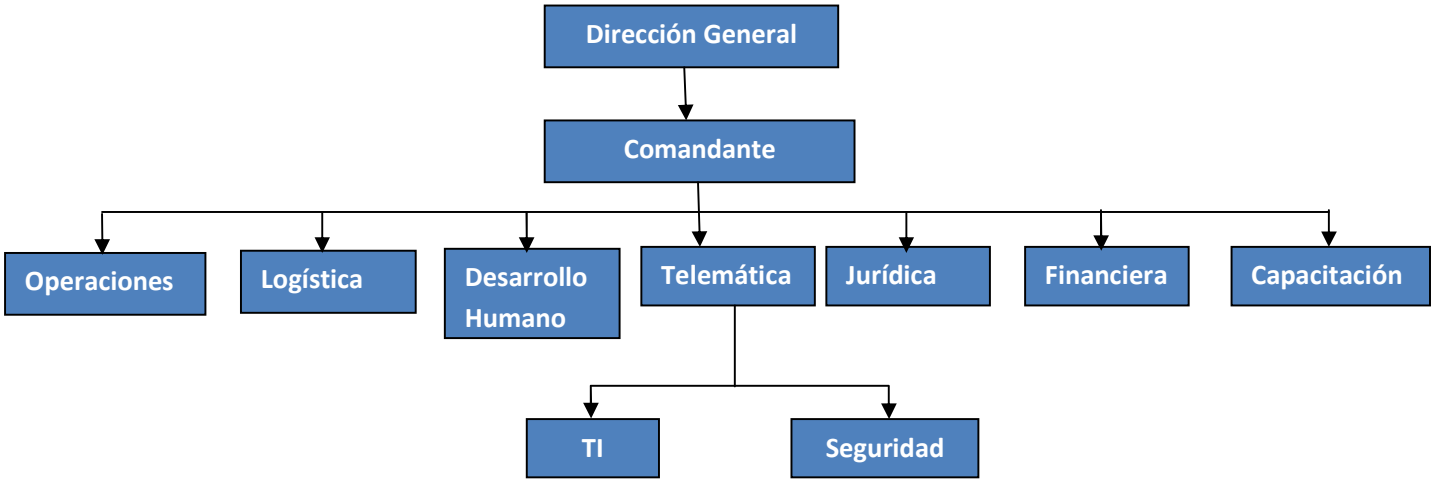
- Servicio de satisfacer las necesidades de la comunidad en los objetivos que la Constitución y la ley nos han confiado.

- Disciplina Cumplir con las normas establecidas y aceptar la autoridad.

2.1.2 Organigrama.

A continuación se muestra un Diagrama del Esquema donde se encuentra enmarcado el proyecto:

Figura 1. Organigrama General

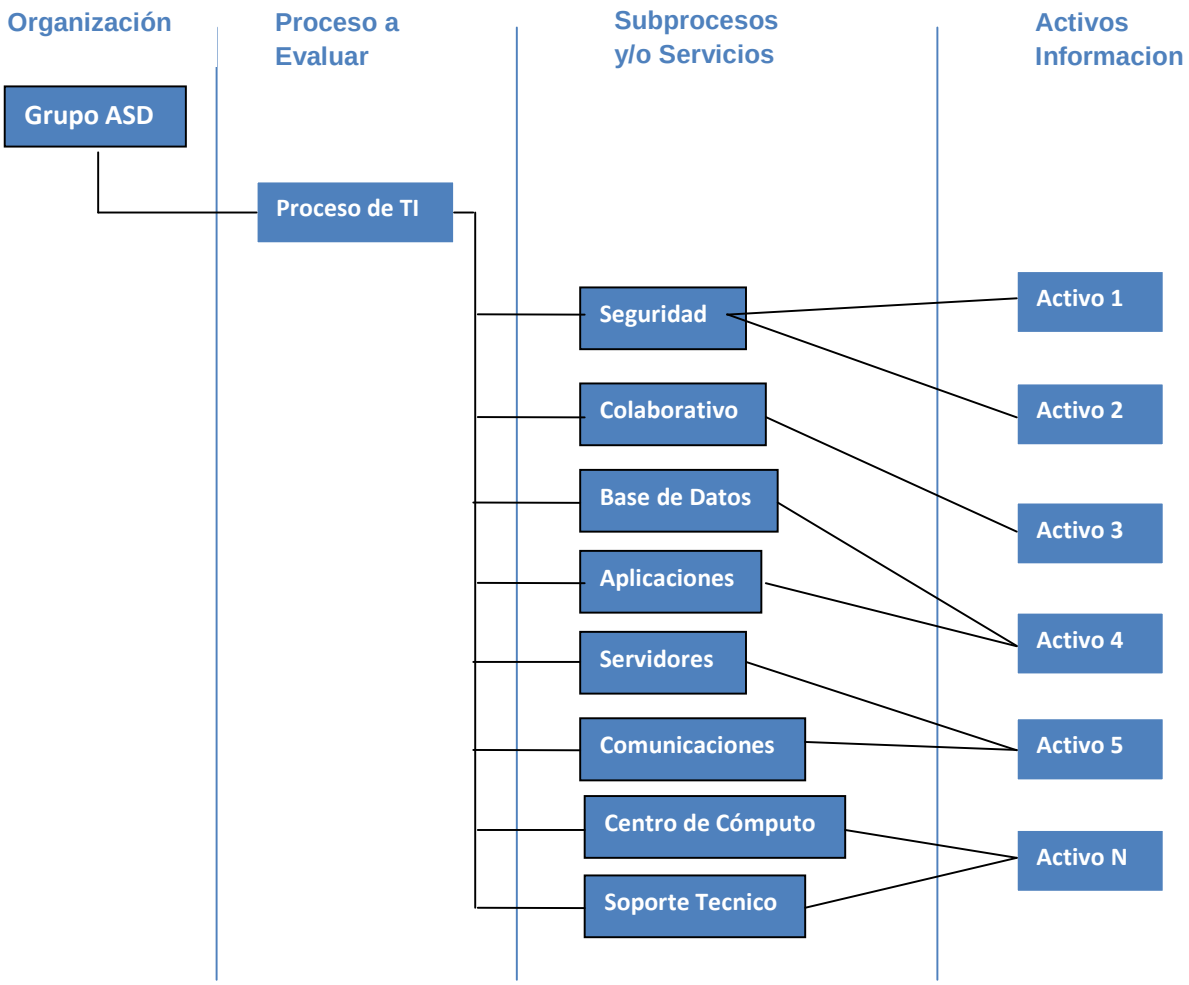


El Proyecto se desarrollara en el Área de TI donde se enmarcan todos los activos y servicios que dan soporte al funcionamiento de la organización.

2.2 ENFOQUE DEL PROYECTO

Este proyecto pretender definir el Plan director para los procesos más importantes del área de Tecnología de la información (TI) del GRUPO ASD. Es por ello que a continuación se definen los servicios sobre los cuales se soporta este proceso:

Figura 2. Definición Alcance Análisis de Riesgos y SGSI



Es importante aclarar que sobre el proceso de TI se hará el ejercicio de análisis de riesgos y definición del plan director de seguridad basado en el estándar ISO 27002.

Sobre cada subproceso se definirán los activos de información que los soporta para realizar el análisis correspondiente.

2.3 DOCUMENTACION NORMATIVA RIESGOS.

Para este Trabajo Final de Master (TFM) se aprobó el uso de AS/NZS 4360:2004 como metodología estándar de evaluación de Riesgos. A continuación se describen los elementos más relevantes de estas metodologías de análisis de riesgos.

2.3.1 AS/NZS 4360:2004

Introducción.

La Gestión del Riesgo es una de las actividades contenidas en el modelo de control COSO, y se entiende que es una de las mejores prácticas que actualmente se llevan a cabo en todo tipo de organizaciones a lo largo y ancho del mundo entero. Su finalidad es que las organizaciones gestionen los riesgos tanto de su ambiente exterior o interior, con el fin de que de una parte, mitiguen todos aquellos eventos que puedan impactar negativamente el logro de sus objetivos y/o que potencialicen aquellos eventos que puedan impactar positivamente el logro de los mismos.

La gestión del riesgo permite mejorar el gobierno corporativo de las organizaciones en donde se aplica, al pasar de una gestión riesgosa a una gestión con un eficiente manejo del riesgo en sus operaciones.

Objetivos.

- Mejor identificación de oportunidades y amenazas
- Tener una base rigurosa para la toma de decisiones y la planificación
- Gestión proactiva y no reactiva
- Mejorar la conformidad con la legislación pertinente
- Mejorar la gestión de incidentes y la reducción de las pérdidas y el costo del riesgo

Fases.

La valoración de riesgos es el primer proceso de la metodología de administración de riesgos. Una entidad usa la valoración de riesgos para determinar la extensión de amenazas potenciales y riesgos asociados con sistemas de TI. La salida de este proceso ayuda a identificar apropiados controles para reducir o eliminar riesgos durante el proceso de mitigación.

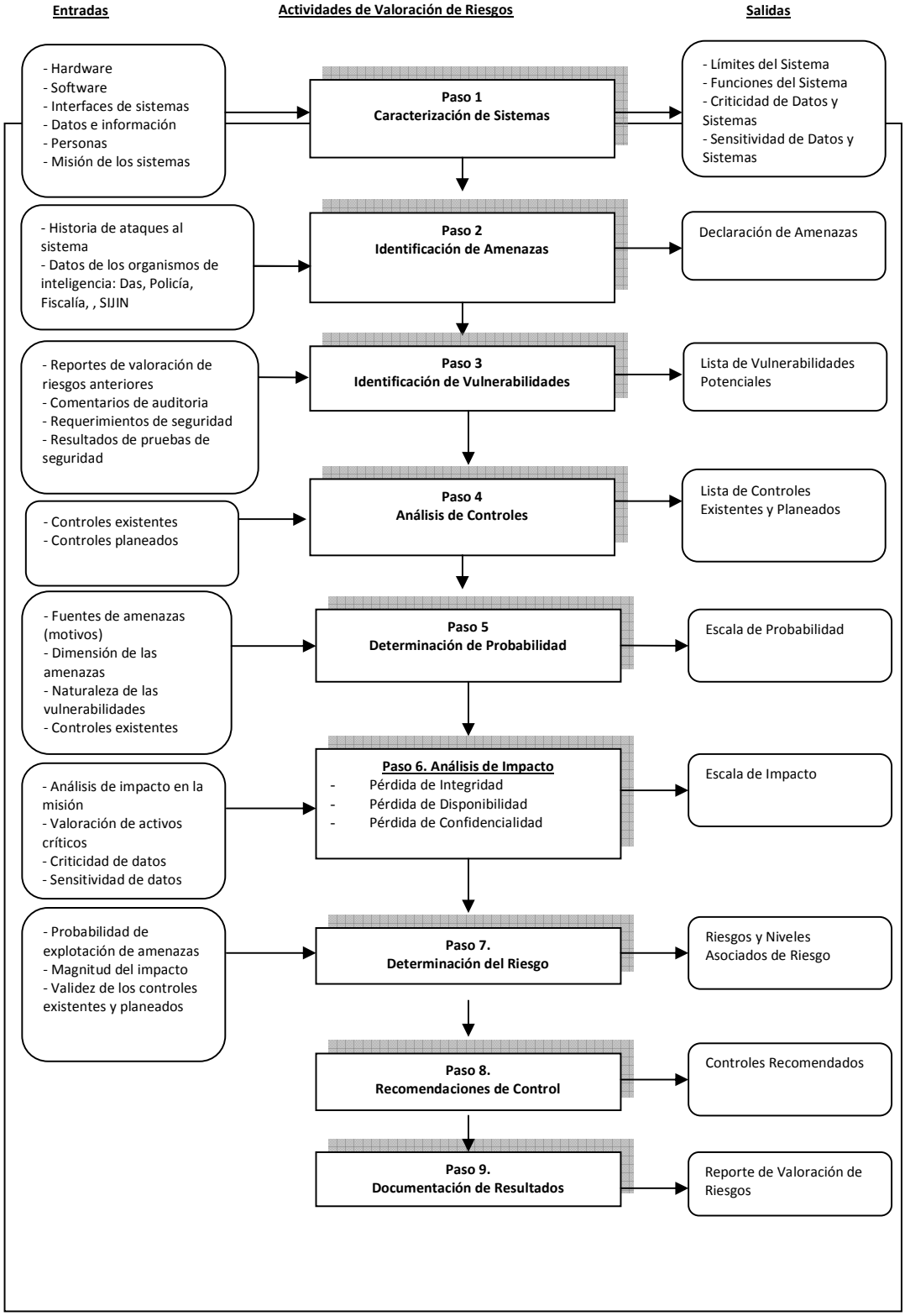
Para determinar la probabilidad de un evento adverso futuro, las amenazas de los sistemas de TI deben ser analizadas en conjunto con las vulnerabilidades potenciales y los controles existentes en los mismos. El impacto se refiere a la magnitud del daño que podría ser causado porque las amenazas exploten una vulnerabilidad. El nivel de impacto es determinado por el impacto potencial en el logro de la misión y el valor relativo de los activos de TI que resultaren afectados (por ejemplo, la criticidad y sensitividad de componentes de sistemas de TI y datos). La metodología de valoración de riesgos está compuesta por nueve (9) pasos primarios, que se definen a continuación:

Paso 1 - Caracterización de sistemas
Paso 2 - Identificación de amenazas
Paso 3 - Identificación de vulnerabilidades
Paso 4 - Análisis de controles
Paso 5 - Determinación de probabilidades
Paso 6 - Análisis de impacto

Paso 7 - Determinación de riesgos
Paso 8 - Recomendaciones de control
Paso 9 - Documentación de resultados

Los elementos principales del proceso de administración de riesgos, como se muestra en la figura 3:

Figura 3. Metodología análisis de riesgos



- **Caracterización de Sistemas:** En la valoración de riesgos para un sistema de TI, el primer paso es definir el alcance del esfuerzo. En este paso, se identifican los límites del sistema de TI, la información y los recursos que componen dicho sistema. La caracterización de un sistema de TI establece el alcance del esfuerzo de valoración de riesgos, establece los límites de la autorización operacional (acreditación) y provee información relacionada con el hardware, software, conectividad, personal de soporte y áreas responsables, esenciales para la definición de los riesgos.

- **Identificación de Amenazas:** Una amenaza es la posibilidad que una situación o evento inesperado explote exitosamente una vulnerabilidad en particular. Una vulnerabilidad es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente. Una fuente de amenaza no representa un riesgo cuando no existe una vulnerabilidad que pueda ser explotada.

    - Una fuente de amenaza se define como cualquier circunstancia o evento con el potencial para causar daños a un sistema de TI. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.
    - Amenazas humanas: Eventos activados o causados por las personas, tales como actos no intencionados (errores en la entrada de datos) o malintencionados (ataques a la red, activación de software malicioso, acceso no autorizado a información confidencial).
    - Amenazas naturales: Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas eléctricas y otros eventos similares.
    - Amenazas ambientales: Faltas prolongadas de energía eléctrica, polución, químicos, dispersión de líquidos.

- **Identificación de Vulnerabilidades:** El análisis de las amenazas de un sistema de TI incluye el análisis de las vulnerabilidades asociadas al ambiente del sistema. La meta de este paso es desarrollar una lista de vulnerabilidades del sistema (defectos o debilidades) que podrían ser explotadas por fuentes de amenazas potenciales.

- **Análisis de Controles:** La meta de este paso es analizar los controles que se encuentran implementados o cuya implementación está planeada por la entidad para minimizar o eliminar la probabilidad de que las amenazas exploten las vulnerabilidades del sistema.

- **Determinación de Probabilidad:** Se hace el análisis para cada amenaza de cual es la probabilidad de ocurrencia de la misma.

    La probabilidad de que una vulnerabilidad pueda ser explotada por una fuente de amenaza se puede describir como Alta, Mayor, posible, no esperada y remota.

- **Análisis de Impacto:** En esta actividad se establece el impacto adverso para el negocio resultante de que una amenaza explote exitosamente una vulnerabilidad. El impacto adverso de un evento de seguridad se puede describir en términos de la degradación de una o varias de las metas de seguridad: Integridad, Disponibilidad y Confidencialidad.

- **Determinación de Riesgos:** El propósito de este paso es valorar el nivel de riesgo de un sistema de TI. La determinación del riesgo para una amenaza/vulnerabilidad en particular se expresa en función de:

    - La probabilidad que una fuente de amenaza intente explotar una vulnerabilidad
    - La magnitud del impacto resultante de la explotación exitosa de una vulnerabilidad

- Lo apropiado de los controles existentes o planeados para reducir o eliminar los riesgos.

- **Recomendaciones de Control:** Una vez identificado el nivel de riesgo del sistema de TI y de los datos se formulan una serie de recomendaciones orientadas a la implementación de medidas de control para mitigar los riesgos a niveles aceptables.

  Las recomendaciones de control son los resultados del proceso de valoración de riesgos y proveen una entrada al proceso de mitigación de riesgos, durante el cual los controles técnicos y procedimientos recomendados se evalúan, priorizan e implementan. Es posible que no todos los controles recomendados se implementen. Esto depende del resultado del análisis costo/beneficio, el cual debe demostrar que la implementación se justifica porque hay una reducción en el nivel de riesgo. Adicionalmente es necesario evaluar cuidadosamente el impacto operacional causado por la introducción de las recomendaciones durante el proceso de mitigación.

- **Documentación de resultados:** Una vez se valoran los riesgos y se emiten las recomendaciones de control, los resultados se documentan en un informe oficial.

  Un informe de valoración de riesgos es un reporte gerencial de ayuda para la Alta Dirección, los responsables de la misión, la toma de decisiones, el cálculo de presupuestos y la gestión de cambios administrativos y operacionales.

- **Mitigación de Riesgos:** La mitigación de riesgos comprende la priorización, evaluación e implementación de controles que reduzcan los riesgos de acuerdo con las recomendaciones emanadas del proceso de valoración de riesgos. Considerando que eliminar todos los riesgos es algo imposible de llevar a cabo, es responsabilidad de la Alta Dirección y de los administradores funcionales y del negocio utilizar el enfoque del menor costo e implementar los controles más apropiados para reducir la exposición a riesgos a un nivel aceptable, con un mínimo impacto adverso sobre los recursos y la misión de la entidad.

  - Opciones de Mitigación de Riesgos: La mitigación de riesgos es una metodología sistemática utilizada por la Alta Dirección para reducir los riesgos que afecten la misión del negocio. La reducción de riesgos se puede alcanzar siguiente alguna o varias de las siguientes opciones:
  - Asumir el riesgo: Consiste en aceptar el riesgo y continuar operando o implementar controles para bajar el nivel de exposición.
  - Anular el riesgo: Es eliminar las causas del riesgo y por ende sus consecuencias (desinstalar un sistema por ejemplo)
  - Mitigar el riesgo: Consiste en implementar controles que reduzcan los impactos negativos de la explotación exitosa de las vulnerabilidades (implementar controles preventivos y detectivos).
  - Transferir riesgos: Es acudir a medidas contingentes para compensar las pérdidas, el ejemplo clásico es la compra de pólizas de seguros.

  Las metas y objetivos de la entidad se deben tener en cuenta en la selección de opciones de mitigación de riesgos. La mitigación de riesgos requiere que la entidad implemente tecnologías de diferentes proveedores de seguridad junto con controles no técnicos y medidas administrativas.

2.4 CODIGO DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACION.

EL TFM se basara en la implementación de la ISO 27001 como modelo de gestión del Sistema de Seguridad de la Información e ISO 27002 como guía de controles de seguridad a ser implementados.

2.4.1 ISO 27001

Introducción.

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

Para el presente proyecto la ISO 27001 se tomara como referencia para definir el Plan Director de Seguridad de la Información, bajo el foque PHVA, tomando elementos que puedan estructurarlo de forma adecuada.

Cuatro fases del sistema de gestión de seguridad de la información

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

- La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

- La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.

- La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.

- La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

Documentos de ISO 27001.

La norma ISO 27001 requiere los siguientes documentos:

- Alcance del SGSI;
- Política del SGSI;
- Procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas;
- Todos los demás documentos, según los controles aplicables;
- Metodología de evaluación de riesgos;
- Informe de evaluación de riesgos;
- Declaración de aplicabilidad;
- Plan de tratamiento del riesgo;
- Registros.

La cantidad y exactitud de la documentación depende del tamaño y de las exigencias de seguridad de la organización; esto significa que una docena de documentos serán suficientes para una pequeña organización, mientras que las organizaciones grandes y complejas tendrán varios cientos de documentos en su SGSI.

La Fase de planificación.

Esta fase está formada por los siguientes pasos:

- determinación del alcance del SGSI;
- redacción de una Política de SGSI;
- identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
- identificación de activos, vulnerabilidades y amenazas;
- evaluación de la magnitud de los riesgos;
- identificación y evaluación de opciones para el tratamiento de riesgos;

- selección de controles para el tratamiento de riesgos;
- obtención de la aprobación de la gerencia para los riesgos residuales;
- obtención de la aprobación de la gerencia para la implementación del SGSI;
- redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

La Fase de implementación

Esta fase incluye las siguientes actividades:

- redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes;
- implementación de un plan de tratamiento del riesgo;
- implementación de los controles de seguridad correspondientes;
- determinación de cómo medir la eficacia de los controles;
- realización de programas de concienciación y capacitación de empleados;
- gestión del funcionamiento normal del SGSI;
- gestión de los recursos del SGSI;
- implementación de procedimientos para detectar y gestionar incidentes de seguridad.

La Fase de verificación

Esta fase incluye lo siguiente:

- implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
- revisiones periódicas de la eficacia del SGSI;
- medición la eficacia de los controles;
- revisión periódica de la evaluación de riesgos;
- auditorías internas planificadas;
- revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;

- actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
- mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.
-

La fase de mantenimiento y mejora

Esta fase incluye lo siguiente:

- Implementación en el SGSI de las mejoras identificadas;
- Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
- Comunicación de actividades y mejoras a todos los grupos de interés;
- Asegurar que las mejoras cumplan los objetivos previstos.

2.4.2 ISO 27002

Introducción.

Desde el 1 de Julio de 2000, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

En España ya se encuentra traducida desde el 2009: UNE ISO/IEC 2700. Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

Directrices

ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes secciones principales:

- Introducción: Conceptos generales de seguridad de la información y SGSI.

- Campo de aplicación: Se especifica el objetivo de la norma.
- Términos y definiciones: Breve descripción de los términos más usados en la norma.
- Estructura del estándar: Descripción de la estructura de la norma.
- Evaluación y tratamiento del riesgo: Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Política de Seguridad: Documento de política de seguridad y su gestión.
- Aspectos Organizativos: Organización interna; organización externa.
- Gestión de Activos: Responsabilidad sobre los activos; clasificación de la información.
- Recursos Humanos: Anterior al empleo; durante el empleo; finalización o cambio de empleo.
- Física y Ambiental: Áreas seguras; seguridad de los equipos.
- Comunicaciones y Operaciones: Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.
- Control Accesos: Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.
- Adquisición, desarrollo y mantenimiento de sistemas: Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.
- Gestión de incidentes: Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.
- Gestión Continuidad de negocio: Aspectos de la seguridad de la información en la gestión de continuidad del negocio.
- Cumplimiento legal: Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación.

El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

3. PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACION

3.1 INTRODUCCION

El GRUPO ASD ha elaborado una estrategia de protección de los activos de información de la organización (Plan Director de Seguridad de la Información-PDSI), que tiene como objetivos preservar la integridad, confidencialidad y disponibilidad de la Información.

El plan director de seguridad permitirá establecer un marco de seguridad donde se establecerá el nivel de riesgo asumido, plan de tratamiento de riesgo los cuales nos permitirán establecer la situación actual y donde se quiere llegar respecto a la seguridad de la información.

Se definirán los mecanismos para gestionar el ciclo de vida de la seguridad de la información con el objetivo de garantizar que los riesgos estén en niveles aceptables dentro de Grupo ASD. Inicialmente se definirá la Política General de Seguridad de la Información y se establecerá el esquema de implementación del plan de tratamiento de riesgos, normativas y procedimientos operativos, medidas técnicas para el tratamiento de riesgo, desarrollo de procedimientos operativos, y las actividades de capacitación e cultura organizacional en temas de seguridad, monitoreo de controles, elaboración y coordinación de planes de continuidad y la revisión del SGSI (Sistema de Gestión de Seguridad de la Información).

Con este ejercicio se introduce de manera intrínseca la seguridad como una elemento dentro de la operación del GRUPO ASD.

La elaboración del Plan de Seguridad se ha constituido siguiendo los principales marcos de referencia en materia de seguridad (ISO 27001, ISO 27002, MARGERIT, AZ/NZS 4360, etc.).

3.2 OBJETIVO GENERAL

Definición de un Plan Director de Seguridad de información que de los lineamientos generales que debe seguir el GRUPO ASD para mantener un esquema de seguridad adecuado dentro de la organización en los sistemas y tecnologías de información que soportan los diferentes subprocesos y/o servicios del área de TI..

3.3 OBJETIVOS ESPECIFICOS

- Identificar el nivel de seguridad existente en los sistemas, servicios, aplicaciones e infraestructura que ofrece el área de TI.
- Definir directrices en temas de seguridad de la información para el área de TI.
- Definir y planificar los planes de acción a realizar (a corto, mediano y largo plazo) teniendo como referencia la diferencia existente entre el nivel de seguridad actual y el nivel de seguridad objetivo.
- Conocer y planificar las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado.

- Implementación y Seguimiento del Plan Director de Seguridad de la Informacion. Se hará seguimiento a los planes de acción a través de métricas y se Implementara una cultura corporativa en temas de seguridad de la información dentro del GRUPO ASD.

3.4 ESQUEMA DEL PLAN DIRECTOR

A continuación se da una breve descripción de cómo se definirá el Plan Director de Seguridad de la Información:

Figura 4. Esquema Plan director de Seguridad

El Plan director de Seguridad de la Información para GRUPO ASD tendrá como base 4 Pilares los cuales permitirán realizar una análisis de la situación actual, identificar la brecha que hay respecto a la situación deseada a nivel de seguridad; se define el Marco de seguridad que se aplicara al interior de la organización; se establecerá los Planes de acción necesarios para dar cumplimiento al PDSI y por último se hará seguimiento a todo el plan definiendo métricas de seguimiento e incluyendo como punto importante la implementación de una cultura de seguridad de la información en toda la entidad.

A continuación se describen cada uno de los pilares que componen el Plan Director de Seguridad de la Información:

- Situación Actual: Se realiza un análisis del estado actual de seguridad de la organización. Para ello se realiza un análisis de riesgo para evaluar el nivel actual de seguridad de la organización, luego se definen a dónde quiere llegar la organización y se determinan las actividades necesarias para cerrar esa brecha.

- Marco de Seguridad: Redefinir los aspectos organizativos y crear un marco normativo suficiente para regular la seguridad de la organización.

- Plan: Elaborar los planes de Acción necesarios para gestionar los riesgos detectados. De estos planes pueden desprenderse proyectos que deberán ser gestionados para cumplir con el PDS.

- Implementación y Seguimiento: Facilitar las métricas del nivel de seguridad de forma que se pueda realizar un seguimiento del mismo, conocer la efectividad del plan trazado y reaccionar ante desviaciones que impacten en el negocio.

3.5 FASES PLAN DIRECTOR DE SEGURIDAD

Para la implementación del actual Plan Director de Seguridad de la Información se han definido las siguientes Fases las cuales serán descritas a continuación.

3.5.1 Identificación de los Requerimientos Normativos.

Para el Presenta plan director se tendrán en cuenta los requerimientos y lineamientos definidos en la ISO/IEC 13335-1 el cual define los lineamientos generales para la gestión de seguridad IT.

Otros de los requerimientos necesarios en el presente plan director es el uso de los estándares ISO 27001 (Requerimientos normativos para la implementación de un SGSI) e ISO 27002 (Controles de seguridad a implementar).

Para el ejercicio de análisis de riesgos se hará uso de MARGERIT y AZ/NZS 4360 para poder identificar los niveles de riesgos dentro de los activos de información del proceso de TI del GRUPO ASD.

3.5.2 Definición del estado Actual de seguridad.

El objetivo de esta fase es identificar la situación actual de seguridad de la organización con la finalidad de establecer la brecha que hay entre la situación actual y la deseada en temas de seguridad de la información.

Para llevar a cabo este análisis se realizaran las siguientes actividades:

- Identificación y valoración de los activos: Durante esta tarea se identifican (por medio de entrevistas y/o accediendo a información de configuración de dispositivos, servidores, aplicaciones, servicios, etc.) los activos necesarios para que los Subprocesos, servicios y/o aplicaciones del área de TI funcionen de forma adecuada.
- Se clasificaran los activos en un mapa (que es una red estructurada en niveles, donde el nivel superior representa los procesos de negocio que se encuentran del alcance, en un nivel inferior estarán aquellos subprocesos, servicios y/o aplicaciones relevantes; en los niveles inferiores se encontrara la infraestructura física, pasando por el software de base y de aplicación).
- Diagnóstico de vulnerabilidades: Se identifican las amenazas presentes sobre los activos en base a los ficheros históricos de incidencias, documentación aportada y entrevistas.
- Asignación de impactos: Se evalúa el daño que produce cada amenaza en el caso de que se materialice una vulnerabilidad sobre un activo. Se mide en términos de disminución de su nivel de seguridad o del valor del activo.

- Análisis de los riesgos: Se definen los mecanismos de seguridad más adecuados a las necesidades de la organización desde el punto de vista de la capacidad tecnológica y de los procedimientos organizativos necesarios.
- Se analiza el riesgo en los activos en función de la probabilidad y del impacto. Se determina el riesgo intrínseco (el calculado sin implantar medidas de seguridad), el efectivo (una vez tenidas en cuenta las medidas de seguridad) y el umbral (el que la organización está dispuesta a asumir).
- Definición de Controles de Seguridad: Luego se procede a definir aquellos controles que deben implementarse o que se ya se encuentran implementados, y que permitirán disminuir los niveles de riesgos a niveles aceptables. En este punto se definirá el nivel de riesgo residual y la efectividad de los controles a implantar.
- Declaración de Aplicabilidad y Análisis de Brecha ISO 27002: La declaración de Aplicabilidad (SOA) permitirá orientar los esfuerzos del PDSI para definir cuales controles serán implementados y cuáles no; los que se indiquen que no van a ser implementados deben ser justificados.
- El análisis de Brecha permitirá obtener información precisa sobre el nivel de cumplimiento de la norma ISO 27002 en los diferentes niveles (global, por dominios, objetivos y controles)

3.5.3 Marco de Seguridad.

El marco de seguridad es el conjunto d e políticas, normas y procedimientos internos que deben existir para definir y estandarizar los principios, criterios y controles de seguridad necesarios en la organización, basándose en el riesgo que la dirección está dispuesta a asumir o en otros requisitos como la legislación vigente.

Este marco sigue una estructura ISO/IEC 27002 y es jerárquico. La base es la política de seguridad que recoge el compromiso de la alta dirección de GRUPO ASD. Esta se articula en normas que se basan a su vez en procedimientos específicos para su implantación. Una de las normas básicas es la definición de roles y la organización de la seguridad que garantizan y soportan el cumplimiento del resto de las normas

Figura 5. Marco de Seguridad

Como se puede observar los controles a implementar se estructuran en el Nivel estratégico, táctico y operativo

Nivel Estratégico.

Los planes estratégicos están alineados con los objetivos estratégicos del negocio y de la tecnología de información. Estos planes se ejecutan a largo plazo (de tres a cinco años o más) para guiar las actividades de seguridad de la información.

El proceso de desarrollar un plan estratégico hace énfasis en que se piense en un entorno organizacional y técnico de pocos años.

Aquí se presentan los Objetivos de alto nivel para proporcionar proyectos que permitan alcanzar los objetivos de negocio. Estos planes deben ser revisados de forma anual o cuando se produzcan cambios importantes en el negocio, tal como una fusión, adquisición, establecimiento de relaciones y/o subcontratación, cambios importantes en los negocios, presentaciones de nuevos competidores, y así sucesivamente. Los cambios tecnológicos serán frecuentes durante un período de cinco años, por lo que el plan debe ser ajustado.

El plan de alto nivel proporciona una guía de la organización para garantizar que las decisiones de nivel inferior son consistentes con las intenciones de la dirección para el futuro de la organización.

Por ejemplo, los objetivos estratégicos pueden consistir en:

- Establecer políticas y procedimientos de seguridad
- Implementar servidores, estaciones de trabajo y dispositivos de red a reducir el tiempo de inactividad
- Asegúrese de que todos los usuarios entienden las responsabilidades de seguridad y recompensar el desempeño excelente
- Establecer una organización de seguridad para administrar la seguridad de toda la entidad
- Asegúrese de que los riesgos son efectivamente comprendidos y controlados.

Nivel Táctico.

Planificación Táctica. Los planes tácticos ofrecer amplias iniciativas para apoyar la consecución de los objetivos especificados en el plan estratégico. Estas iniciativas puede incluir implementaciones como el desarrollo de una política electrónica para el proceso de desarrollo y distribución, la implementación de un control de cambio robusto para el entorno de servidores reduciendo la probabilidad de vulnerabilidades residentes en los servidores, la implementación de un "hot site" para la recuperación de desastres o implementar una solución de gestión de identidades. Estos planes son más específicos y puede consistir en varios proyectos para completar el esfuerzo. Los planes tácticos son más cortos en longitud, tal como de 6 a 18 meses para conseguir un Objetivo específico de seguridad en la organización.

Nivel Operativo.

Los planes se especifican con metas, fechas, y esquemas de revisión de resultados para proporcionar comunicación y orientación, asegurando que los proyectos individuales se han

completado. Por ejemplo, establecer un proceso de desarrollo de políticas y comunicación puede implicar múltiples proyectos con muchas actividades:

- Ejecutar una evaluación de riesgos.
- Desarrollar políticas de seguridad y un proceso de aprobación
- Desarrollar la infraestructura técnica para implementar las políticas y el seguimiento de cumplimento
- Entrenar a los usuarios finales sobre las políticas
- Vigilar el cumplimiento

Dependiendo del tamaño y el alcance de los esfuerzos, estas iniciativas pueden ser actividades de un plan individual, o pueden ser múltiples planes gestionados a través de varios proyectos. La duración de estos esfuerzos es de corto plazo para proporcionar funcionalidad discreta en la realización del esfuerzo. Tradicionalmente los métodos de "Cascada" en la ejecución de los proyectos gastan una gran cantidad de tiempo detallando las medidas concretas necesarias para completar el proyecto.

Algunas organizaciones de hoy están más centradas en el logro de resultados de algunos proyectos a corto plazo, o, al menos provisional, para demostrar el valor de la inversión a lo largo del proyecto general. Tal demostración de valor mantiene interés de las organizaciones y visibilidad al esfuerzo, lo que aumenta las posibilidades de sostener la financiación a largo tiempo. La dirección ejecutiva puede impacientarse sin darse cuenta de estos beneficios rápidamente.

3.5.4. Plan del proyecto

El Plan de acción define la estrategia a corto, medio y largo plazo (habitualmente 1, 2 ó 3 años) para reducir y mantener los niveles de seguridad requeridos. Facilita a la dirección la información necesaria para decidir qué proyectos abordar y su justificación necesaria según el riesgo que disminuyen. Además del calendario de proyectos, también se entregó la información de requisitos particularizados para GRUPO ASD y el coste estimado de todos ellos para facilitar la elaboración de futuras RFP’s, si la organización lo considera necesario.

El reto conseguido fue dar información de valor para poder priorizar las acciones y tener claro por qué y cómo se deben abordar determinados proyectos con un coste identificado. Los factores clave para el éxito del proyecto han sido la capacidad de Cepsa para alinear el plan director de seguridad con el plan de sistemas, la importancia que ha tenido la involucración de la dirección, la jefatura del proyecto y las facilidades de acceso a la información.

Dentro de los Proyectos a realizar por parte del GRUPO ASD están las siguientes:

Estratégicos:

- Análisis y Gestión de Riesgos.
- Diseño e implementación de un SGSI
- Organización Área de Seguridad

Tácticos:

- Clasificación de la Información
- Inventario de Activos
- Cultura y concientización en Seguridad de la Información

- Procedimiento control de cambios
- Plan de Contingencias (Plan de Continuidad del Negocio y DRP)
- Gestión de incidentes de seguridad

Operativos:

- Análisis Seguridad Red y Seguridad Perimetral
- Implementación controles de Seguridad en Centro de Datos
- Monitorización y auditoría
- Gestión de Usuarios
- Parcheado y Actualización de Sistemas
- Seguridad frente a intrusiones
- Desarrollo Seguro de Aplicaciones

3.5.5 Implementación y Seguimiento

El objetivo de esta fase es poder hacer seguimiento a cada uno de los planes de acción definidos para dar cumplimiento a lo definido en el Plan Director de Seguridad de la Información.

Dentro de las actividades a realizar podemos mencionar:

- Seguimiento a Proyectos: Una vez definidos e implementados los proyectos, debe hacerse un seguimiento de la ejecución de los mimos para garantizar que se cumplan con los objetivos de los mismos. El seguimiento de proyectos también permitirá hacer un avance sobre el nivel de cumplimiento que se está efectuando en el Plan Director de Seguridad de la Información.
- Concienciación de los usuarios sobre la seguridad: El objetivo es que junto con la implementación de controles de seguridad y planes de acción se generen campañas de entrenamiento y concientización para garantizar una cultura de seguridad que garantice que el tema de seguridad esta difundido en toda la organización.

- Métricas de Seguridad: Facilitar las métricas del nivel de seguridad de forma que se pueda realizar un seguimiento del mismo, conocer la efectividad del plan trazado y reaccionar ante desviaciones que impacten en el negocio.

4. CONTEXTO DE VALORACION DE RIESGOS

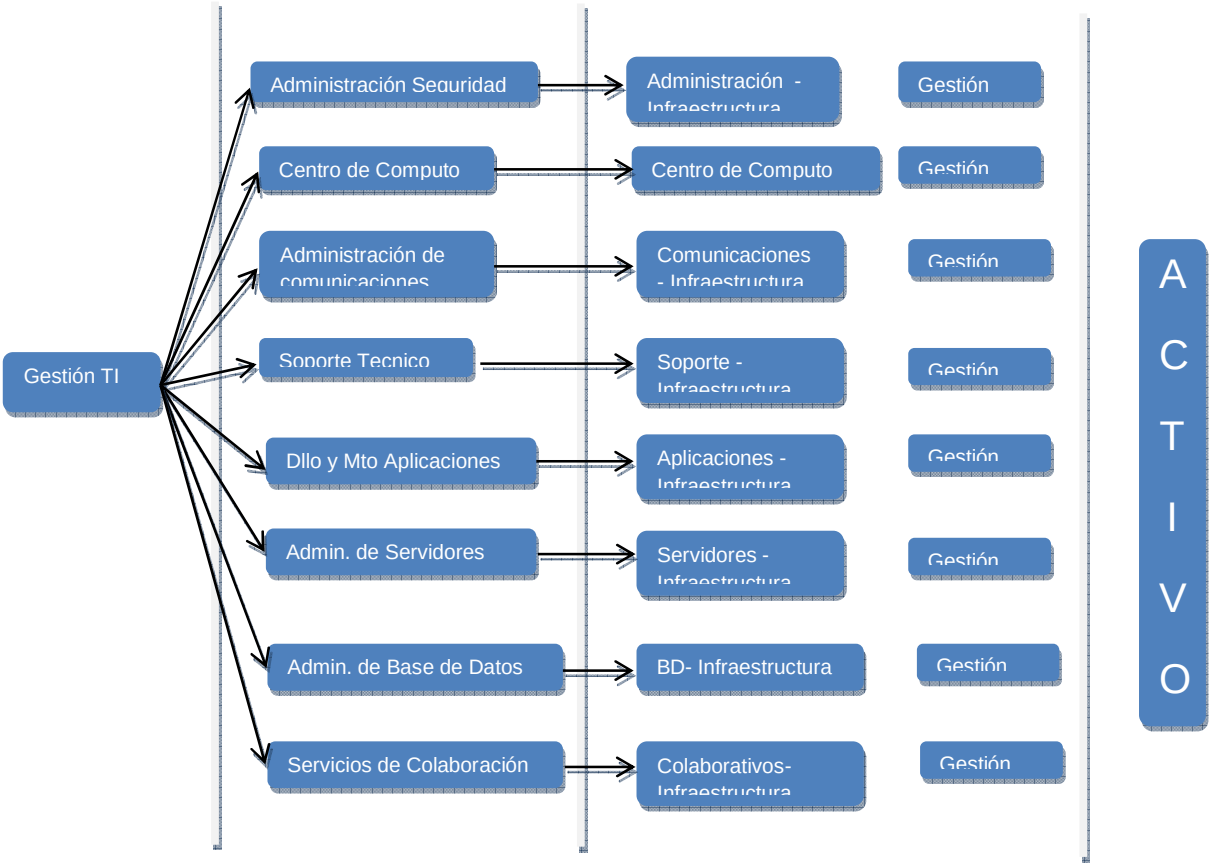
En consonancia con la metodología de Gestión de Riesgos definida en el presente proyecto, lo primero que se debe realizar al iniciar un proceso de Valoración de Riesgos es establecer las reglas de juego en cuanto a:

- Estructura del informe de valoración de riesgos.
- Identificación de Activos.
- Escalas para calificar los requerimientos de seguridad de los activos o recursos de información (disponibilidad, integridad, confidencialidad).
- Escala a utilizar para la calificación de la probabilidad que una amenaza ocurra.
- Lista de impactos de la institución a ser analizados.
- Escala a utilizar para calificar el nivel de impacto que puede generar la ocurrencia de una amenaza
- Escala de medición del riesgo inherente
- Escala de medición del riesgo residual

4.1 ESTRUCTURA INFORME VALORACION RIESGOS

Para el presente análisis de riesgos se divide el Proceso de Tecnología de la Información en sus componentes, lo cual permitirá entender de forma más clara su distribución. Para presentar los resultados de la valoración de riesgos, se organizó una estructura de cuatro niveles: Proceso, servicios, módulos y activos, tal como se observa en la siguiente figura:

Figura 6. Estructura Análisis Riesgos



Cada uno de los servicios identificados fue dividido en dos tipos de módulos: El módulo de infraestructura y el módulo de gestión.

Al final de la rama de infraestructura se ubican los recursos tecnológicos correspondientes. Por la rama de gestión se evalúa la existencia y aplicación de buenas prácticas relacionadas con: Planeación, Organización, Entrenamiento, Documentación, Respaldo y Recuperación, Contratos y Control de cambios concordantes con el respectivo módulo.

La identificación de vulnerabilidades, amenazas y controles se realiza a nivel de activo o recurso de información, lo que facilita la determinación de impactos a nivel de módulo, servicio o proceso.

4.2 IDENTIFICACION DE ACTIVOS

Debido a que el área de TI se soporta en diferentes servicios, se procedió a identificar los activos por módulos y servicios con lo cual se garantiza un mejor entendimiento de la distribución de los mismos.

Los activos identificados se categorizaran en Instalaciones, Hardware, software, aplicación, datos, red, servicios y personal (Para visualizar los activos Identificados ver el archivo Analisis_Riesgos_ASD.xlsx en la ficha Identificacion_Activos)

4.3 ESCALAS PARA CALIFICAR LOS REQUERIMIENTOS DE SEGURIDAD

En conjunto con los responsables de seguridad, se definieron las escalas para calificar los siguientes requerimientos de seguridad de la información:

- Integridad
- Confidencialidad
- Disponibilidad

La configuración de estas escalas así como la calificación dada por el personal de ASD quedó registrada en el archivo de Excel Analisis_Riesgos_ASD.xlsx, nombre que se seguirá utilizando a lo largo del presente documento.

4.3.1 Requerimientos de seguridad - Integridad

Para calificar los requerimientos de integridad (exactitud de la información) se definió la siguiente escala:

Tabla 1. Requerimientos de integridad

REQUERIMIENTOS DE INTEGRIDAD	
Calificación	**Explicación**
Baja	Si tras el daño se puede reemplazar fácilmente y ofrecer la misma calidad de información.
Normal	Si tras el daño se puede reemplazar y ofrecer una calidad semejante de información con una molestia razonable.
Alta	Si la calidad necesaria de la información se puede reconstruir de forma difícil y costosa.
Crítica	Si no puede volver a obtenerse una calidad semejante a la información original.

4.3.2 Requerimientos de seguridad - Confidencialidad

Para calificar los requerimientos de confidencialidad (garantizar que la información solo es conocida por quien está autorizado para conocerla) se definió la siguiente escala:

Tabla 2: Requerimientos de confidencialidad

REQUERIMIENTOS DE CONFIDENCIALIDAD	
Calificación	**Explicación**
Pública	Cualquier información no clasificada se considera como pública. La información no catalogada y por tanto pública, será aquella cuya divulgación no afecte al Grupo ASD en términos de pérdida de imagen y/o económica.
Uso Interno	Información que sin ser reservada ni restringida, debe mantenerse dentro de la Empresa y no debe estar disponible externamente, excepto para terceros involucrados en el tema. En el caso de terceros, deberán comprometerse a no divulgar dicha información.
Restringida	Información sensible, interna a áreas o proyectos a los que deben tener acceso controlado otros grupos pero no todo el Grupo ASD debido a que se pueda poner en riesgo la seguridad e intereses de la compañía, de sus clientes o asociados y empleados.
Crítica	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales.

4.3.3 Requerimientos de seguridad - Disponibilidad

Para calificar los requerimientos de disponibilidad (garantía que la información puede ser accedida por quien la requiere y cuando lo requiere.) se definió la siguiente escala:

Tabla 3. Requerimientos de Disponibilidad

REQUERIMIENTOS DE DISPONIBILIDAD	
Calificación	**Explicación**
De 0 a 2 horas	Se puede estar sin el activo en funcionamiento máximo 2 horas al cabo de la cual se comienzan a materializar riesgos financieros y operativos.
Entre 2 y 3:59 horas	Se puede estar sin el activo en funcionamiento máximo 4 horas al cabo del cual se comienzan a materializar riesgos financieros y operativos.
Entre 4 a 7:59 horas	Se puede estar sin el activo en funcionamiento máximo 8 horas al cabo de los cuales se comienzan a materializar riesgos financieros y operativos.
Entre 8 y 47:59 horas	Se puede estar sin el activo en funcionamiento máximo 48 horas al cabo de la cual se comienzan a materializar riesgos financieros y operativos.
Más de 48 horas	Se puede estar sin el activo en funcionamiento máximo 1 mes al cabo del cual se comienzan a materializar riesgos financieros y operativos.

4.4 AMENAZAS

Las amenazas son eventos inesperados con el potencial para causar daños. Las amenazas explotan las vulnerabilidades presentes en las tecnologías, las personas o los procesos. Las amenazas se conocen como causas de riesgos, esto es, si la amenaza no explota una vulnerabilidad el riesgo no acontece.

Las amenazas se presentan agrupadas en las siguientes categorías:

- Los desastres naturales
- Los actos malintencionados
- Las fallas de hardware y software

- Los errores humanos
- Fallas en la gestión y operación del servicio

Como resultado del análisis de riesgos efectuado en el grupo ASD, se identificaron como principales amenazas las siguientes:

Tabla 4. Amenazas.

Categoría	Amenaza	Descripción
Errores Humanos	Errores humanos	Ingreso de información errada Errores de aplicación Tareas incompletas / no ejecutadas Perdida de información
	Dependencia de funcionarios críticos	Concentración de información o permisos en uno o algunos funcionarios, que se convierten en elementos intocables
	Ingreso de información errada	El usuario introduce información que no es correcta (integra)
	Tareas incompletas / no ejecutadas	Error humano por medio del cual se omiten tareas o se hacen de forma incompleta
	Ejecución de comandos equivocados	Ejecución de comandos incorrectos por desconocimiento o por error humano
	Sobrecarga laboral	Exceso de trabajo de funcionarios que puede conducirlos a cometer errores
Fallas de Hardware y Software	Fallas de HW, SW o comunicaciones	Fallas de Hardware Fallas de Software Fallas en comunicaciones Fallas de energía Desempeño deficiente Obsolescencia Tecnológica
	Fallas de HW	Malfuncionamiento a nivel de hardware
	Fallas de SW	Malfuncionamiento a nivel de software
	Fallas de comunicaciones	Malfuncionamiento a nivel de hardware de comunicaciones
	Fallas de energía	Interrupción del suministro de energía eléctrica
Actos Malintencionados	Actos Malintencionados	Acceso no autorizado Suplantación de usuarios Ataque (intrusión) al sistema Sabotaje Robo de información Alteración de la información
	Ingeniería social	Actividades que mediante el engaño a personas se obtiene información que permite acceso a información o servicios.
	Código malicioso o virus	Contaminación de equipos por medio de programas maliciosos.
	Terrorismo	Actos terroristas, bomba, atentado
	Acceso lógico no autorizado	Acceso a recursos para los cuales no tiene atribuciones de acceso
	Suplantación de usuarios	Un usuario utiliza la cuenta de otro para obtener acceso de forma abusiva, Utilización de sesiones abiertas para suplantar al dueño de la misma
	Ataques al sistema	Proceso organizado para tener acceso abusivo sobre un sistema
	Alteración de la información	Obtener acceso de forma no autorizada y modificar datos o información
	Interceptación de información	Hombre en el medio - interceptar las comunicaciones entre dos partes y robar información

	Acceso físico no autorizado	Acceder de forma física a activos de información
	Hurto	Robo de activos de información como computadores portátiles
	Robo de información	Hurtar información
Desastres Naturales	Desastres Naturales	Terremoto Inundación Tsunami Huracán Erupciones volcánicas Avalancha
	Contaminación	Polución del aire o el ambiente
	Temperatura o humedad extremas	Temperaturas extremas que pueden ocasionar fallas de equipos
	Terremoto	Desastre natural
	Incendio	Amenazas relacionadas con fuego
Fallas en la gestión y operación del servicio	Obsolescencia tecnológica	La infraestructura de TI no soporta los requerimientos de capacidad
	Servicio no alineado con las necesidades del negocio	Inexistencia de planes de tecnología de largo plazo alineados con los objetivos del negocio

4.5 RIESGOS

Riesgo es el impacto negativo derivado de la explotación de una vulnerabilidad por una amenaza. A manera de ejemplo:

Vulnerabilidad presente: Se comparten contraseñas con privilegios de administración
Amenaza: Suplantación de usuarios
Riesgos: Fuga de información
Fraude y malversación de fondos

Como resultado del análisis efectuado en el área de TI del Grupo ASD, se identificaron como principales riesgos de la institución, los siguientes:

Tabla 5. Riesgos (Impactos)

Riesgo
Fraude y malversación de fondos
Toma de decisiones erradas
Sanciones
Baja en la moral de la tropa
Deterioro de la imagen pública.
Incumplimiento de tipo legal o contractual
Indisponibilidad colateral de otros servicios
Bajos índices de transparencia
Pérdida en la efectividad
Retraso en la toma de decisiones
Perjuicio a la relaciones de la Entidad con otros organismos

Pérdida de productividad de los empleados
Interrupción del servicio o del negocio
Fuga de información

Para determinar la importancia de los riesgos o impactos es necesario establecer la probabilidad (frecuencia de ocurrencia) y el nivel de impacto (daño) de cada ocurrencia de amenaza. A continuación se presentan las escalas utilizadas para calificar probabilidades y niveles de impacto.

4.6 ESCALA PARA LA MEDICION DE LA PROBABILIDAD

Para establecer la probabilidad (frecuencia de ocurrencia) de los eventos negativos o amenazas que se pudieran presentar en los sistemas del Grupo ASD se utilizó la siguiente escala:

Tabla 6. Escala de probabilidad

ESCALA DE PROBABILIDAD		
Calificación	**Explicación**	**Número de incidentes en el último año**
B	**Baja:** El evento es teóricamente posible pero nunca ha ocurrido en el EN	0
M-	**Medio baja:** El evento se presentó 1 vez	1
M	**Medio:** El evento se presentó 2 veces	2
M+	**Media alta:** El evento se presentó 3 veces.	3
A	**Alta:** El evento se presentó más de 3 veces.	Más de 3

Como se puede observar, la probabilidad se establece con base en la historia reciente de incidentes negativos sucedidos en la institución

4.7 ESCALA PARA LA MEDICION DEL NIVEL DE IMPACTO (CONSECUENCIAS)

Para establecer el impacto (pérdida en la que incurre la institución) cada vez que se presenta un evento negativo en los sistemas de ASD se utilizó la siguiente escala:

Tabla 7. Escala de impactos

Escala de impactos						
1.Calificación	**2. Aspecto legal y de Incumplimiento**	**3. Aspecto de Tiempo improductivo diario (horas)**	**4. Máximo tiempo sin servicio Disponibilidad**	**5. Esfuerzo de reconstrucción (horas) Integridad**	**6. Fuga de información Confidencialidad**	**7. Imagen**
B	Llamado de atención interno	Hasta 1	Más de 48	Menor a 8	Informativa	Difusión dependencia afectada
M-	Destitución	Entre 1 y 2:59	Entre 8 y 47:59 horas	Entre 8 y 11:59		
M	Sanción económica	Entre 3 y 4:59	Entre 4 y 7:59 horas	Entre 12 y 23:59	Información Personal	
M+	Cárcel	Entre 5 y 7:59	Entre 2 y 3:59 horas	Entre 24 y 71:59	Información Administrativa o técnica	Difusión a nivel Nacional
A	Cárcel mas sanción económica	Más de 8	Entre 0 y 1:59 horas	Más de 72	Información operacional	Difusión a nivel Internacional

Una vez seleccionado el impacto, se considera el aspecto de mayor relevancia para la institución y de esta forma se orientó al entrevistado, sobre los criterios para calificarlo según la afectación:

- Aspectos legales y de incumplimiento, el entrevistado, debe seleccionar la calificación del impacto de la columna 1: **"B"**, **"M-"**, **"M"**, **"M+"** o **"A"** de acuerdo al nivel de severidad que se estime puede presentarse a nivel de incumplimiento descrito en la columna 2.
- Productividad de los funcionarios, el entrevistado debe seleccionar la calificación del impacto de la columna 1: **"B"**, **"M-"**, **"M"**, **"M+"** o **"A"** de acuerdo al nivel de severidad que se estime puede presentarse a nivel de productividad descrito en la columna 3
- Disponibilidad del servicio, el entrevistado debe seleccionar la calificación del impacto de la columna 1: **"B"**, **"M-"**, **"M"**, **"M+"** o **"A"** de acuerdo al nivel de severidad que se estime puede presentarse a nivel de disponibilidad del servicio descrito en la columna 4
- Integridad, el entrevistado debe seleccionar la calificación del impacto de la columna 1: **"B"**, **"M-"**, **"M"**, **"M+"** o **"A"** de acuerdo al nivel de esfuerzo requerido para reconstruir información descrito en la columna 5.
- Confidencialidad, el entrevistado debe seleccionar la calificación del impacto de la columna 1: **"B"**, **"M-"**, **"M"**, **"M+"** o **"A"** de acuerdo al nivel de severidad que se estime puede presentarse a nivel de confidencialidad descrito en la columna 6
- Imagen de la institución, el entrevistado debe seleccionar la calificación del impacto de la columna 1: **"B"**, **"M-"**, **"M"**, **"M+"** o **"A"** de acuerdo al nivel de severidad que se estime puede presentarse a nivel de imagen institucional descrito 7.

4.8 ESCALA PARA EL CÁLCULO DEL RIESGO INHERENTE

El riesgo inherente es el nivel de exposición presente en ausencia de controles, esto es, en la determinación del riesgo inherente no se toman en cuenta los controles existentes en la organización.

Para calcular el valor del riesgo inherente (severidad) se combinan las calificaciones de probabilidad y nivel de impacto de acuerdo con la siguiente tabla:

Tabla 8: Cálculo del nivel de riesgo inherente (severidad)

PROBABILIDAD	**A**	**M**	**M**	**M+**	**A**	**A**
	M+	**B**	**M-**	**M**	**M+**	**A**
	M	**B**	**M-**	**M**	**M+**	**M+**
	M-	**B**	**B**	**M-**	**M**	**M+**
	B	**B**	**B**	**M-**	**M**	**M**
		B	**M-**	**M**	**M+**	**A**
		IMPACTO				

La interpretación de la escala de nivel de riesgo inherente (severidad) es la siguiente:

Tabla 9. Interpretación del Nivel de Riesgo Inherente (Severidad)

Alta	Riesgo extremo, se requiere acción inmediata. Planes de Tratamiento requeridos, implementados y reportados a los altos mandos
Medio Alto	Riesgo alto requiere atención de la alta Dirección. Planes de Tratamiento requeridos, implementados y reportados a los Líderes funcionales.
Media	Riesgo moderado, requiere atención del área involucrada, definición de procedimientos y controles de mitigación.
Medio bajo	Riesgo aceptable – Administrado con procedimientos normales de control
BAJA	Riesgo bajo, se administra con procedimientos rutinarios.

En la siguiente tabla se mencionan dos ejemplos para ayudar a interpretar la calificación del riesgo inherente:

Tabla 10. Ejemplo del cálculo de riesgo inherente

Activo	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo Inherente
Servidor de BD	Corte de suministro de energía eléctrica	Interrupción del servicio	M+ (ha ocurrido 3 veces en los últimos 2 años)	Alto (máximo tiempo de interrupción tolerable de 2 horas)	Alto. Requiere atención inmediata
Centro de cómputo	Terremoto – Desastre Natural	Interrupción del servicio	B (No ha ocurrido)	Alto (Se interrumpen servicios de máximo 2 horas de tolerancia)	M (Medio), Deben especificarse responsabilidades administrativas: La Dirección debe tomar acción sobre los controles necesarios para mitigar el impacto de un posible desastre natural.

4.9 ESCALA PARA EL CÁLCULO DEL RIESGO RESIDUAL

Anteriormente se ha establecido el riesgo inherente (nivel de riesgo sin considerar los controles existentes), ahora, es necesario establecer el nivel de efectividad del conjunto de controles existentes para determinar el nivel de riesgo residual.

La efectividad del conjunto de controles se establece en dos pasos:

- Determinación de la efectividad individual de cada control
- Determinación de la efectividad del conjunto de controles

4.9.1 Determinación de la efectividad de cada control individual

Esta calificación se fundamente en el análisis de los atributos del control, para la cual se utiliza la siguiente tabla:

Tabla 11: Atributos para calificar la efectividad de un control

Categoría	Tipo	Explicación	Ejemplos de controles	Puntaje
Oportunidad	Preventivo	Evitan que la amenaza se materialice	Acceso por contraseñas	10
			Cifrado de mensajes	
			Autenticación fuerte	
	Detectivo	Alertan sobre violaciones o intentos de violación de la política de seguridad	Pistas de auditoría	5
			Sistemas de detección de intrusos – IDS	
			Dígitos de chequeo	
	Correctivo	Se utilizan para restaurar recursos de computación perdidos o dañados	Restauración de sistemas y datos	3
			Plan de recuperación de desastres	
			Sistemas automáticos de extinción de incendios	
Grado de automatización	Automático	El control se ejecuta sin intervención humana	Control de acceso biométrico	5
			Acceso por contraseñas	
	Manual	Es requerida la intervención humana para la ejecución del control	Inspección física de paquetes, bolsos, etc.	3
			Entrevistas de selección	
			Procedimientos de aprobación	
Obligatoriedad	Mandatorio	El control se ejecuta siempre	Acceso por contraseñas	5
			Verificación de antecedentes	
	Discrecional	La ejecución del control es potestativa de una persona o grupo de personas	Aseguramiento de plataformas (actualización de parches, desactivación de puertos y servicios)	3
			Revisión de logs de acceso	
Relevancia	No aplica	Es la importancia del control para cada amenaza en particular. Esto es, un control es indispensable para una amenaza pero puede ser secundario para contrarrestar otra.	Acceso por contraseñas es relevante para prevenir acceso lógico no autorizado pero es secundario para fuga de información.	10
			Cifrado es relevante para fuga de información pero secundario para prevenir acceso lógico no autorizado	

Notas:

- La asignación de puntajes obedece al análisis que realice el responsable de dicha actividad.
- Un control puede obtener un máximo de 30 puntos.
- Dentro de cada categoría los atributos son excluyentes: Un control no puede ser preventivo, detectivo y correctivo simultáneamente.

4.9.2 Determinación de la efectividad del conjunto de controles

La escala de efectividad de los controles se debe entender de la siguiente manera:

Tabla 12: Escala interpretar la efectividad de los controles

ESCALA	INTERPRETACIÓN
81 – 100%	Los controles existentes son altamente efectivos. Las buenas prácticas indican que su aplicación previene o detecta y corrige la mayoría de ocurrencias de la amenaza analizada.
61 – 80%	Los controles son efectivos en la mayoría de las situaciones, pero se requieren controles adicionales para fortalecer la protección del activo o recurso analizado.
41 – 60%	Los controles existentes brindan un nivel de protección medio. Son insuficientes. Se requieren controles adicionales en el mediano plazo para elevar los niveles de protección.
21 – 40%	Los controles existentes pueden contrarrestar situaciones particulares pero son insuficientes. Se requieren medidas de control adicionales en el corto plazo.
0 – 20%	Los controles son inefectivos. Se requieren fuertes medidas de control de manera urgente para fortalecer los niveles de protección sobre el activo o recurso analizado.

El riesgo residual es el nivel real de exposición de la institución gracias a la protección brindada por los controles existentes. Esto es, el riesgo inherente es contrarrestado (mitigado) por los controles. El valor del riesgo residual debe ser siempre menor o igual al valor del riesgo inherente.

El resultado del riesgo residual se obtiene de la combinación del riesgo Inherente y la efectividad de los controles existentes, con base en la siguiente regla:

Tabla 13. Escala para determinar el riesgo residual

Riesgo Inherente	A	A	M+	M	M-	B
	M+	M+	M	M	M-	B
	M	M	M	M	M-	B
	M-	M-	M-	B	B	B
	B	B	B	B	B	B
		0-20%	21-40%	41-60%	61-80%	81-100%
		EFECTIVIDAD DE LOS CONTROLES				

4.10 VALORACION DE LOS ACTIVOS

Para la valoración de los activos del presente proyecto se realizara teniendo en cuenta las tres principales dimensiones de seguridad (Confidencialidad, integridad y disponibilidad).

Se evaluara cada activo respecto a estas dimensiones y así poder establecer el valor para la organización; para ello se hará uso de la siguiente escala de valoración de activos:

Tabla 14. Tabla Valoración de Activos

Valoración de activos			
Descripción	**Abreviatura**	**Rango**	**Valor Estimado Calculo (Pesos)**
Critico	C	64-80	80
Muy alto	MA	48-63	64
Alto	A	32-47	48
Medio	M	16-31	32
Bajo	B	1-15	16

El Informe de Valoración de activos pude visualizarse en el archivo Analisis_Riesgos_ASD.xlsx Ficha Valoracion_Activos.

4.11 VALORACION DE RIESGO

El Informe de Valoración de activos pude visualizarse en el archivo Analisis_Riesgos_ASD.xlsx Ficha Analisis_Riesgos. Se puede visualizar como se analizo por activo de Informacion las amenazas que presenta y los riesgos; seguidamente se puede encontrar el cálculo del Riesgo Inherente, controles Implementados y el valor del riesgo residual.

4.12 TRATAMIENTO DE RIESGOS

Una vez valorados los diferentes activos de información en el ejercicio de análisis de riesgos y de identificar el riesgo Inherente y Riesgo Residual, la dirección toma como decisión dar tratamiento a los Riesgos que se encuentren valorados en las escalas de Alto (A), Medio Alto (M+) y Medio (M).

Los Riesgos que se encuentren en una escala inferior se aceptaran y se verificaran puntualmente para identificar posibles riesgos que deban ser tratados.

5. AUDITORIA DE CUMPLIMIENTO DE LA ISO: IEC 27002:2005

5.1 INTRODUCCION

A continuación se realizara una evaluación del nivel de cumplimiento respecto a los controles definidos por la norma ISO/IEC 27002:2005. Este análisis permitirá establecer aquellos controles que serán implementados por parte de la organización, aquellos que no y así determinar proyectos que mejoren la seguridad de la organización

5.2 METODOLOGIA

El estándar ISO/IEC 27002:2005, agrupa un total de 133 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 11 áreas y 39 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

Para la presente auditoria se diseño un archivo en Excel (Anexo 2.Matriz Análisis GAP v2.xlsx) en el cual se encontrara el análisis GAP respecto a la norma ISO/IEC 27002:2005

5.3 EVALUACION DE MADUREZ

En esta sección se es evalúa la madurez de la seguridad en lo que respecta a los 11 dominios de control y los 133 controles planteados por la ISO/IEC 27002:2005. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización.

Los dominios que deben analizarse son:

- Política de seguridad
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento

El estudio debe realizar una revisión de los 133 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los dominios-. Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

Tabla 15. Niveles de Madurez CMM

EFECTIVIDAD	CALIFICACION	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	0	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	1	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	2	L2	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	3	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	4	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	5	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

5.4 RESULTADOS OBTENIDOS

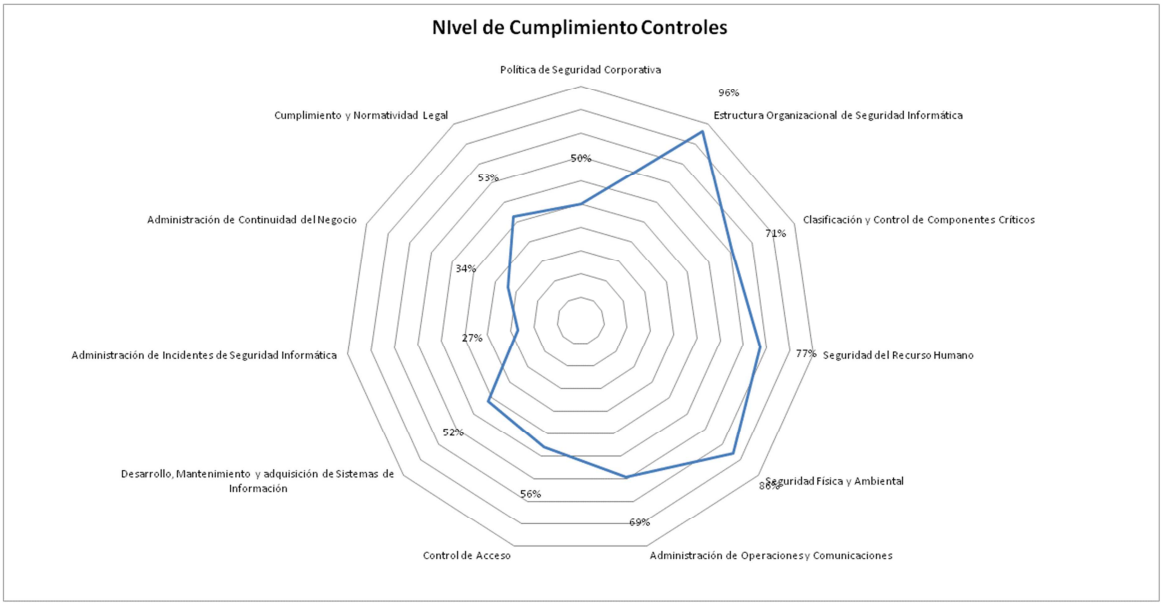
El análisis de cada uno de los 133 controles se puede observar en el Anexo 2 Matriz Análisis GAP v2.xlxs. En este anexo se dividieron en 11 fichas el cual contiene cada uno de los controles. Se evaluó el estado actual del control y se dio una recomendación, adicionalmente se evaluó el grado de madurez de cada uno respecto al Modelo de Madurez de Capacidad (CMM).

A continuación se describe los controles implementados y el porcentaje de cumplimiento por cada dominio:

Tabla 16. Porcentaje de Cumplimiento Controles

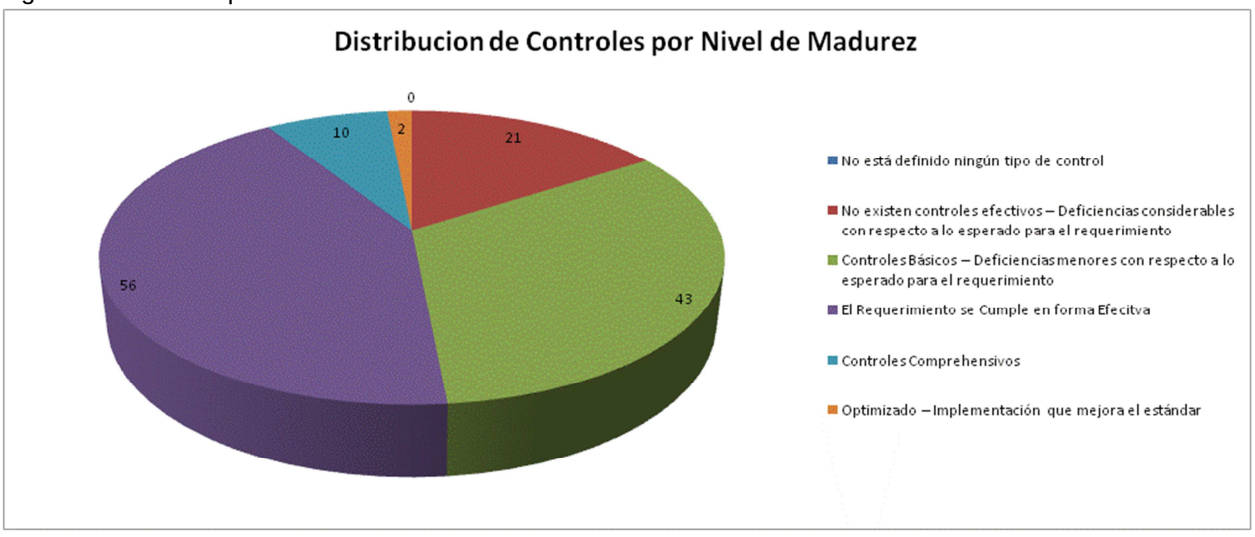
Dominio	Aprobados	NO Aprobados	Porcentaje Cumplimiento
Política de Seguridad Corporativa	2	0	50%
Estructura Organizacional de Seguridad Informática	11	0	96%
Clasificación y Control de Componentes Críticos	5	0	71%
Seguridad del Recurso Humano	9	0	77%
Seguridad Física y Ambiental	13	0	86%
Administración de Operaciones y Comunicaciones	29	2	69%
Control de Acceso	25	0	56%
Desarrollo, Mantenimiento y adquisición de Sistemas de Información	16	0	52%
Administración de Incidentes de Seguridad Informática	5	0	27%
Administración de Continuidad del Negocio	5	0	34%
Cumplimiento y Normatividad Legal	10	0	53%

Figura 7. Nivel de cumplimiento por dominios



Si se evalúa por nivel de madurez, observamos que la mayora de controles se encuentran implementados de forma efectiva (L3) seguido de controles básicos (L2). Esto indica que hay un nivel aceptable de implementación de los controles planteados en la ISO 27002.

Figura 8. Controles por niveles de madurez



6. PROPUESTAS DE PROYECTOS

El tratamiento del riesgo, es el segundo proceso de la gestión de riesgos, comprende la priorización, evaluación e implementación de controles que reduzcan los riesgos de identificados en el proceso de valoración de riesgos.

Puesto que la eliminación de todos los riesgos es algo imposible de llevar a cabo, es responsabilidad de la Gerencia Ejecutiva y de los administradores funcionales y del negocio utilizar el enfoque del menor costo e implementar los controles más apropiados para reducir la exposición a riesgos a un nivel aceptable, con un mínimo impacto adverso sobre los recursos y la misión de la organización, para lo cual a continuación se presenta un plan de acción recomendado.

6.1 PLAN DE ACCION

Es el conjunto de actividades que recomendamos se deben emprender para reducir los riesgos significativos y que contribuyen a la implementación del SGSI. El plan se ha clasificado de acuerdo a la prioridad con la cual los controles ayudan a reducir el nivel de riesgo inherente.

- Alta: Son controles que contribuyen de una forma más efectiva para evitar que las vulnerabilidades sean explotadas. La protección tiene un cubrimiento sobre múltiples vulnerabilidades.

- Media: Son controles complementarios que ayudan a elevar la efectividad de los controles y optimizar el nivel de protección.

- Baja: Son controles que ayudan a evitar vulnerabilidades para situaciones particulares.

6.1.1 Prioridad alta

Plan Estratégico de tecnología de Información

- Objetivo: Los servicios de tecnología de información deben estar alineados con las necesidades del negocio (misionales), para lo cual es importante que Grupo ASD establezca el plan estratégico de TI y definir las necesidades de control para proteger la información. El plan Estratégico de TI deben considerar los aspectos más relevantes a nivel de Instalaciones, Aplicaciones y recursos para optimizar

- Tiempo de Implementación: 2 Años

- Responsables: Dirección de TI.

- Costo: Por establecer de acuerdo a las actividades a realizar y las implementaciones necesarias.

Control de cambios

- Objetivo: Es una buena práctica para asegurar que los cambios que se realicen en la infraestructura de tecnología, se lleven a cabo en un ambiente controlado, con plena integración de las partes involucradas, pruebas funcionales, actividades de preparación y aprobación por parte de los responsables técnicos y funcionales.

  El proceso de control de cambios debe considerar al menos los siguientes aspectos:
  - Registro de solicitud de cambio
  - Revisión de solicitud de cambio
  - Autorización de solicitud de cambio
  - Planeación del cambio
  - Coordinar la implementación del cambio
  - Revisar y registrar cierre del cambio

  El proceso de control de cambios es una buena práctica para la gestión de servicios de tecnología, sin embargo lo ideal es que Grupo ASD adopte otros procesos de gestión tales como:
  - Gestión de configuración
  - Gestión de incidentes
  - Gestión de problemas
  - Gestión de acceso

- Tiempo Implementación: 1 Meses.

- Responsables: Área de Seguridad de la Información.

- Costo: El costo se definió por las horas requeridas por parte de los recursos del área de seguridad de la información el cual se estima en 160 Hora por un valor de 3.000.000 millones de pesos.

Firewall interno / segmentación de redes

- Objetivo: Grupo ASD tiene todos los dispositivos de su red LAN sobre la misma red, permitiendo que cualquier equipo pueda alcanzar dispositivos de relevancia crítica como pueden ser servidores de procesamiento central o equipos que contengan información “secreta”.

- El área de TI debe implementar zonas de seguridad y configurar segmentos de red que agrupen dispositivos por sus niveles de seguridad y la implementación de un firewall interno o listas de acceso que controlen el tráfico entre las diferentes redes. Mayor información se puede encontrar en el anexo “Valoración de la red ideal”.

- Tiempo Implementación: 1 Meses.

- Responsables: Área de TI (Administrador de redes).

- Costo: Se implementara un Cisco ASA 5505-SEC-BUN-k8 el cual incluye licenciamiento por un valor de $2.363.971 Pesos (dos millones trescientos sesenta y tres mil novecientos setenta y un pesos). Los costos asociados por la implementación del firewall y de la segmentación de redes se estima en 4.000.000 con una duración de 4 meses trabajando medio tiempo.

Sitio alterno

- Objetivo: Para garantizar la prestación de los servicios de tecnología de la información se debe contar con un plan estructurado de continuidad ante desastres. Para grupo ASD se recomienda la implementación de un plan de recuperación de desastres o DRP (por sus siglas en ingles Disaster Recovery Plan) que permita de forma organizada realizar las actividades de recuperación.

  Para desarrollar el DRP del CE se debe considerar al menos las siguientes fases propuestas por el DRI (Disaster Recovery Institute):

  - Iniciación y manejo del proyecto
  - Evaluación de Riesgos
  - Análisis de Impacto al Negocio (BIA)
  - Selección de Estrategias de Continuidad
  - Respuesta a Emergencias
  - Desarrollo de los Planes de Continuidad
  - Ejercicios y Mantenimiento de los Planes de Continuidad
  - Sensibilización y Programas de Entrenamiento

- Tiempo Implementación: 6 Meses.

- Responsables: Área de TI (Administrador de redes y Servidores).

- Costo: El sitio Alterno se implementara con el proveedor Claro, quién prestara las instalaciones de su Datacenter para montar este Esquema. Mensualmente se cobrara un valor de 5.000.000 (cinco millones de pesos) por el arrendamiento de servidores y canales de comunicación para tener operativo el Sitio Alterno para las aplicaciones sensibles de la organización.

Organización del Área de Seguridad de la Información

- Objetivo: El grupo ASD debe adoptar una estructura organizacional de Seguridad de la información que le permita gestionar de forma apropiada el nivel de seguridad. Esta estructura debe abarcar roles que permitan gestionar los temas técnicos, temas orientados a la gestión de la seguridad, análisis de riesgos, Continuidad del negocio, etc.

- Tiempo Implementación: 1 Mes.

- Responsables: Oficial Seguridad de la Información.

- Costo: Los costos asociados a este control estarán asociados a dos conceptos:

  1. Costos de la definición del área de seguridad de la información que se estimara de acuerdo a las horas requeridas para esta definición (20 Horas – 1 millón de pesos).

  2. Costos de la definición de los roles para el área de seguridad de la información (Depende de la asignación salarial que realice el área de talento humano a los perfiles que integraran el área de seguridad de la información).

Implementación de SGSI

- Objetivo: La implementación y operación de un Sistema de Gestión de Seguridad de la Información (SGSI) le permite a ASD contar con un proceso metodológico para gestionar la Seguridad de la Información con el objetivo de una optimización continuada de los niveles de seguridad.

- Tiempo Implementación: 6 Meses.

- Responsables: Oficial Seguridad de la Información.

- Costo: Los costos asociados se cargaran a las actividades que tengan que realizar cada uno de los roles definidos para el área de seguridad de la información quienes deben tener asignado la responsabilidad de implementar y mantener el SGSI. Se estima que la implementación del SGSI tendrá un costo de 80.000.000 (ochenta millones de pesos) y se gestionara como un proyecto interno en la organización.

Clasificación de la información

- Objetivo: La clasificación de la información le permite al grupo ASD establecer los requerimientos de seguridad de los activos de información y de esta forma definir los controles respectivos de acuerdo al nivel de clasificación. El proceso de clasificación de información debe ser coordinado y orientado metodológicamente por el Área de Seguridad de la información y llevado a cabo por las áreas funcionales que son las propietarias de la información y quienes deben establecer el nivel de clasificación y sus necesidades de protección.

- Tiempo Implementación: 6 Meses.

- Responsables: Oficial Seguridad de la Información.

- Costo: Los costos asociados se cargaran a las actividades que tengan que realizar cada uno de los recursos asignados para apoyar la labor de clasificación de la información. Se estima un costo de 4.000.000 (4 millones de pesos).

Endurecimiento

- Objetivo: Los equipos de procesamiento central deben ser objeto de un proceso de aseguramiento con el cual se configure de forma segura los servicios y programas. Es importante adoptar como buena práctica la realización de endurecimiento siempre que se instale un nuevo equipo o programa.

- Tiempo Implementación: 4 Meses.

- Responsables: Oficial Seguridad de la Información.

- Costo: Para el proceso de aseguramiento se contratara una empresa consultora externa la cual ha definido un valor aproximado de 1.000.000 por servidor, asegurando el sistema operativo y/o aplicaciones (Web server, Base de Datos, etc.).

Ambientes independientes de: producción, desarrollo y pruebas

- Objetivo: Grupo ASD no tiene ambiente de pruebas para realizar las actividades de verificación de funcionamiento de los programas en mantenimiento y el ambiente de desarrollo no cuentas con la segregación de funciones que garantice que los programas en producción son debidamente controlados.

- El área de TI debe implementar ambientes independientes y con restricción de permisos para garantizar que los programas y datos de producción no sean modificados por el grupo de desarrollo de sistemas.

- Tiempo Implementación: 4 Meses.

- Responsables: Área de TI.

- Costo: Se adquirirán 2 Appliance Dell PowerEdge T110 II para montar los ambientes de Desarrollo y Pruebas. El valor de estos equipos es de 3.949.003 por servidor (Valor total 7.898.006 pesos).

Protección de datos de desarrollo

- Objetivo: Las bases de datos utilizadas en el ambiente de desarrollo contienen una réplica de la información de las bases de producción. El grupo ASD debe implementar un proceso de transformación o enmascaramiento de la información de forma que los valores de la información de los ambientes de desarrollo y pruebas no contengan información real de la Base de Datos de producción.

- Tiempo Implementación: 4 Meses.

- Responsables: Área de TI.

- Costo: Dentro de las responsabilidades del área de desarrollo debe asignarse la responsabilidad de implementar un procedimiento para enmascarar la información y así poderla usar en los ambientes de pruebas.

Cuentas locales con privilegios de administración

- Objetivo: Partiendo del principio “menor privilegio” en el cual los usuarios solo deben tener acceso a las funciones necesarias para la realización de sus actividades, el grupo ASD debe retirar las cuentas locales con privilegios de administración. Los usuarios deben tener cuentas del Dominio Corporativo con los roles respectivos a sus funciones. Las actividades de instalación de programas deben ser realizadas de forma controlada por el grupo de soporte técnico.

- Tiempo Implementación: 1 Meses.

- Responsables: Área de TI.

- Costo: Se estima que el administrador el realizar esta actividad en 1 meses a un costo de 1.500.000 (un millón quinientos mil pesos).

Implementación de solución de Gestión de Identidad.

- Objetivo: Para el acceso a las aplicaciones y servicios de tecnología recomendamos que Grupo ASD implemente una solución de Gestión de Identidades que permita de forma centralizada gestionar las cuentas y permisos de las cuentas y que adicionalmente facilita el manejo cuentas y contraseñas a los usuarios finales.

- Tiempo Implementación: 1 Meses.

- Responsables: Área de TI.

- Costo: Se adquirirá el Oracle Identity Manager como aplicación para gestionar las identidades en ASD. La solución tiene un costo de adquisición de 20.000.000 (Veinte millones de pesos) y se pagara anualmente un valor de licenciamiento de 4.000.000 (cuatro millones de pesos).

Cuentas de acceso

- Objetivo: Actualmente el acceso a las aplicaciones se realiza a través de cuentas de Base de Datos sin embargo estas cuentas no tienen control de complejidad permitiendo que los usuarios asignen cuentas fáciles de adivinar aumentando el riesgo de suplantación de usuarios.

- Tiempo Implementación: 1 Meses.

- Responsables: Área de TI.

- Costo: Se implementara un servicio de LDAP para gestionar las cuentas de usuarios y poder aplicar políticas de contraseñas fuertes. No hay costo de licenciamiento ya que se usara la aplicación OpenLDAP.

Controles varios – Centro de Cómputo

- Objetivo: En el Centro de Cómputo se identificó la ausencia de algunos controles importantes para la protección general del centro de cómputo, los cuales se relacionan a continuación:
    - Suministro de energía aire acondicionado: ASD debe implementar una solución que garantice el suministro de energía al Aire Acondicionado del Centro de Cómputo que permita garantizar esquemas adecuados a los equipos de cómputos que se encuentran funcionando allí.
    - Sensores de humo: Para mayor cubrimiento de las condiciones ambientales se recomienda la instalación de sensores de humo en el techo, piso falso y ductos de aire acondicionado.
    - Salida de emergencia: Se recomienda la habilitación de una salida de emergencia independiente a la puerta de acceso normal.

- Tiempo Implementación: 1 Meses.

- Responsables: Área de TI.

- Costo: La implementación de un Esquema de Aire Acondicionado, Sensores de humo y la construcción de la salida de emergencia por un valor de 30.000.000 (treinta millones de pesos).

Rack de piso

- Objetivo: El CE debe proteger los rack donde se encuentran los switches de piso para evitar que personal no autorizado tenga acceso. Los gabinetes deben estar asegurados con llave y deseable que estén monitoreados por cámaras de CCTV.

- Tiempo Implementación: 1 Meses.

- Responsables: Área de TI.

- Costo: La implementación de un Esquema de Aire Acondicionado, Sensores de humo y la construcción de la salida de emergencia por un valor de 70.000.000 (setenta millones de pesos).

6.1.2 Prioridad Media

Puntos únicos de falla

- Objetivos: Se identificaron algunos puntos únicos de falla que no cuentan con esquema de redundancia, para los cuales se recomienda que Grupo ASD evalúe la implementación de una solución de alta disponibilidad.

    - Switch Core de Seguridad
    - Switch Core de LAN

- Tiempo Implementación: 6 Meses.

- Responsables: Área de TI.

- Costo: El valor del Switch de Core (Catalyst 6500 4-Port 10 GigaBit) es de 31.228.900 millones y el switch de Core LAN (Cisco Catalyst 3750X-48P-L) es de 14.792.375 millones. Los costos de Implementación se asociaran a las actividades que realiza el administrador de red.

Logs de auditoría

- Objetivos: Para efectos de monitoreo y seguimiento se recomienda que los logs del sistema se habiliten a nivel de sistema operativo, aplicaciones y que se implemente un proceso de revisión periódico y que se documente los resultados y acciones iniciadas.

- Tiempo Implementación: 6 Meses.

- Responsables: Área de TI.

- Costo: Se incurrirá en la implementación de un servidor SYSLOG para centralizar los Logs que se generen. Este tipo de software tiene un licenciamiento Freeware. Las actividades de configuración serán realizadas como actividades de los diferentes administradores.

Cuentas genéricas

- Objetivos: Las cuentas para administración de los servicios de tecnología y de seguridad de la información deben ser individuales y no deben ser compartidas.

- Tiempo Implementación: 2 Meses.

- Responsables: Área de TI.

- Costo: El costo de esta actividad se estima en 1.500.000 (un millón quinientos mil pesos).

Conexiones remotas

- Objetivo: Grupo ASD debe definir un proyecto para implementación de controles de protección de red en las Unidades con las cuales tiene enlaces WAN. Las unidades deben tener un nivel de protección similar al que existe en el sitio de procesamiento central donde se controle que los equipos que están accediendo al sitio central posean el mismo nivel de seguridad que los equipos de la red LAN, tales como:

    - Firewall perimetral
    - Cifrado de datos
    - Antivirus actualizado
    - Parches actualizados
    - Cuentas no privilegiadas para usuarios normales
    - Protección de memorias usb

- Tiempo Implementación: 8 Meses.

- Responsables: Área de TI.

- Costo: Muchos de los mecanismos ya se encuentran implementados y debe realizarse un proceso de verificación de cada uno por parte del área de tecnología de la información.

Documentación de procedimientos

- Objetivo: La Dirección de Telemática debe documentar los procedimientos de operación y mantenerlos actualizados. De igual forma los procedimientos deben tener un propietario y deben ser controlados de acuerdo al nivel de clasificación del documento.

- Tiempo Implementación: 12 Meses.

- Responsables: Área de TI.

- Costo: Para la documentación de los procedimientos se recurría al área de calidad para poder contar con un recurso de esa área.

6.1.3 Prioridad Baja

Servidor de archivos

- Objetivo: El servidor de archivos es un repositorio central de la información de los usuarios, el cual permite respaldar la información de los usuarios. Recomendamos que ASD implemente el servicio de Servidor de archivos, le asigne un espacio a cada usuario y defina las políticas de copia de respaldo de forma que permita recuperar la información en caso de daños en los discos duros de los equipos.

- Tiempo Implementación: 12 Meses.

- Responsables: Área de TI.

- Costo: Se adquirirán 1 Appliance Dell PowerEdge T110 II para montar el servidor de archivos con un valor de 3.949.003 por servidor.

Herramientas de gestión

- Objetivo: Recomendamos que Grupo ASD implemente herramientas centralizadas de gestión para los servidores, de forma que permita monitorear el funcionamiento e identificar alertas preventivas para evitar suspensión del servicio. De igual forma estas herramientas permiten generar informes de desempeño.

- Tiempo Implementación: 12 Meses.

- Responsables: Área de TI.

- Costo: Se adquirirán 1 Appliance Dell PowerEdge T110 II para montar el servidor de archivos por 3.949.003 por servidor.

Consola de gestión de red

- Objetivo: La consola de gestión de red “What´sup” debe ser ingresada al dominio para que le apliquen las características de seguridad de los equipos del Comando de CE.

- Tiempo Implementación: 12 Meses.

- Responsables: Área de TI.

- Costo: Se adquirirán 1 Appliance Dell PowerEdge T110 II para montar el servidor de archivos 3.949.003 por servidor.

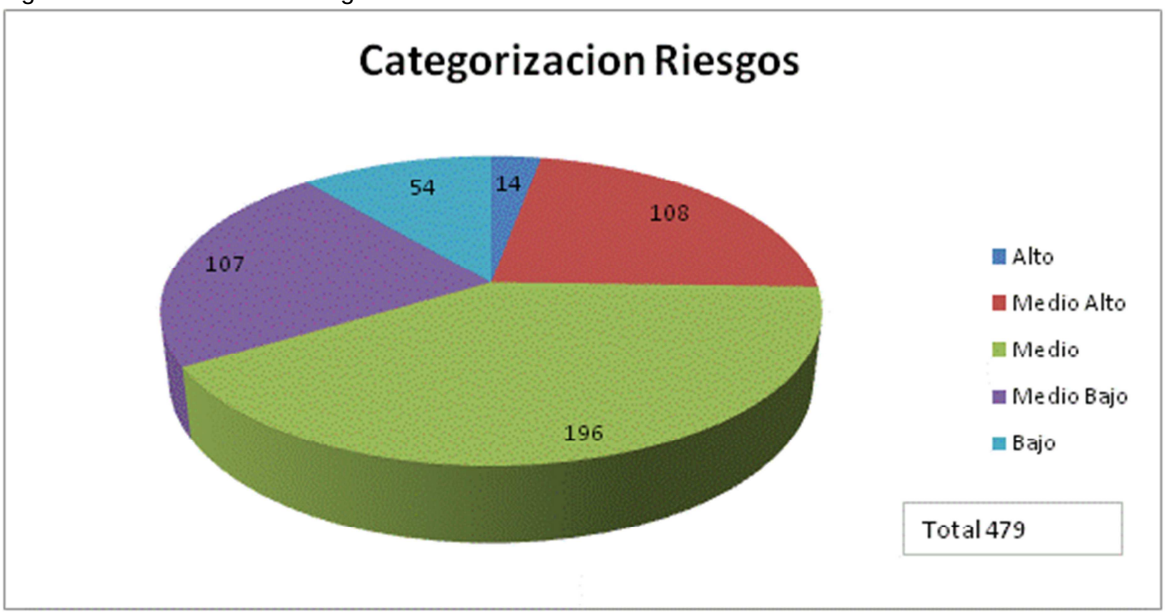
6.2 ANALISIS DE IMPACTO

Una vez finalizada la fase de definición de proyectos e identificando los controles a ser implementados, se hace necesario realizar un análisis del impacto que van a tener estos proyectos en el esquema de gestión de riesgos y en la política de cumplimiento respecto a la ISO 27002.

En primera medida se analizaran el impacto respecto a los riesgos Identificados. Durante el ejercicio de Análisis de riesgo de identificaron 50 activos des información que soportan la operación del área de TI.

Del total de activos reportados, se identificaron 479 riesgos Inherentes (nivel de riesgo sin tener en cuenta la implementación de controles de seguridad) categorizados de la siguiente forma:

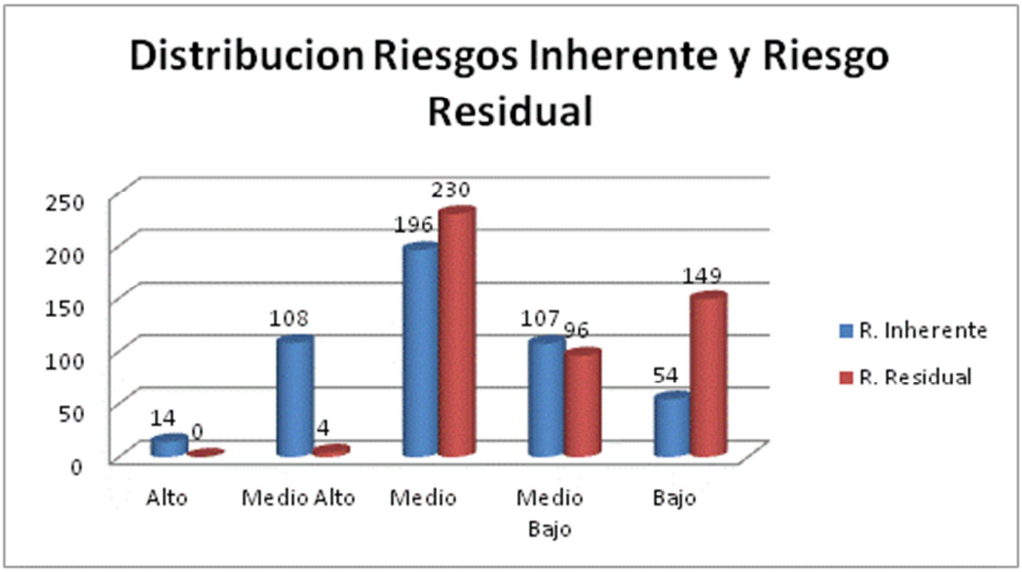
Figura 9. Distribución de Riesgos Por Niveles



La mayor cantidad de riesgos se concentran en las categorías de Medio, medio alto, Medio bajo, Bajo y Alto.

De acuerdo a las consideraciones definidas por la organización, se estableció definir un nivel de riesgo aceptable para las categorías Alto, Medio Alto y Medio, con lo cual al implementar los controles y proyectos definidos se tiene la siguiente distribución:

Figura 10. Distribución de Riesgo Inherente y riesgo Residual



Podemos observar como una vez se implementen los controles propuestos y se ejecuten los proyectos definidos, los niveles de riesgos tienden a varias considerablemente. Para la categoría de riesgos Altos se pasa de 14 riesgos identificados a 0; para los Medio Altos se pasa de 108 a 4; para los riesgos Medios se pasa de 196 a 230; aquí observamos un aumento el cual esta justificado porque mucho de los riesgos de la categoría de alto y medio altos debieron reducirse y caen en esta categoría.

Los riesgos de la categoría Medio Bajo hay una reducción al pasar de 107 a 96; los riesgos Bajos pasaron de 54 a 149. De forma similar el aumento se dio porque los controles implementados redujeron considerablemente los riesgos de las categorías superiores.

El otro enfoque para evaluar el impacto de los proyectos y controles de seguridad a implementar se da en los niveles de madurez en cada uno de los dominios definidos del estándar ISO 27002. A continuación se presenta el porcentaje de cumplimiento o nivel de madurez por dominio actual y el que se espera obtener una vez se han implementado los controles y proyectos de seguridad:

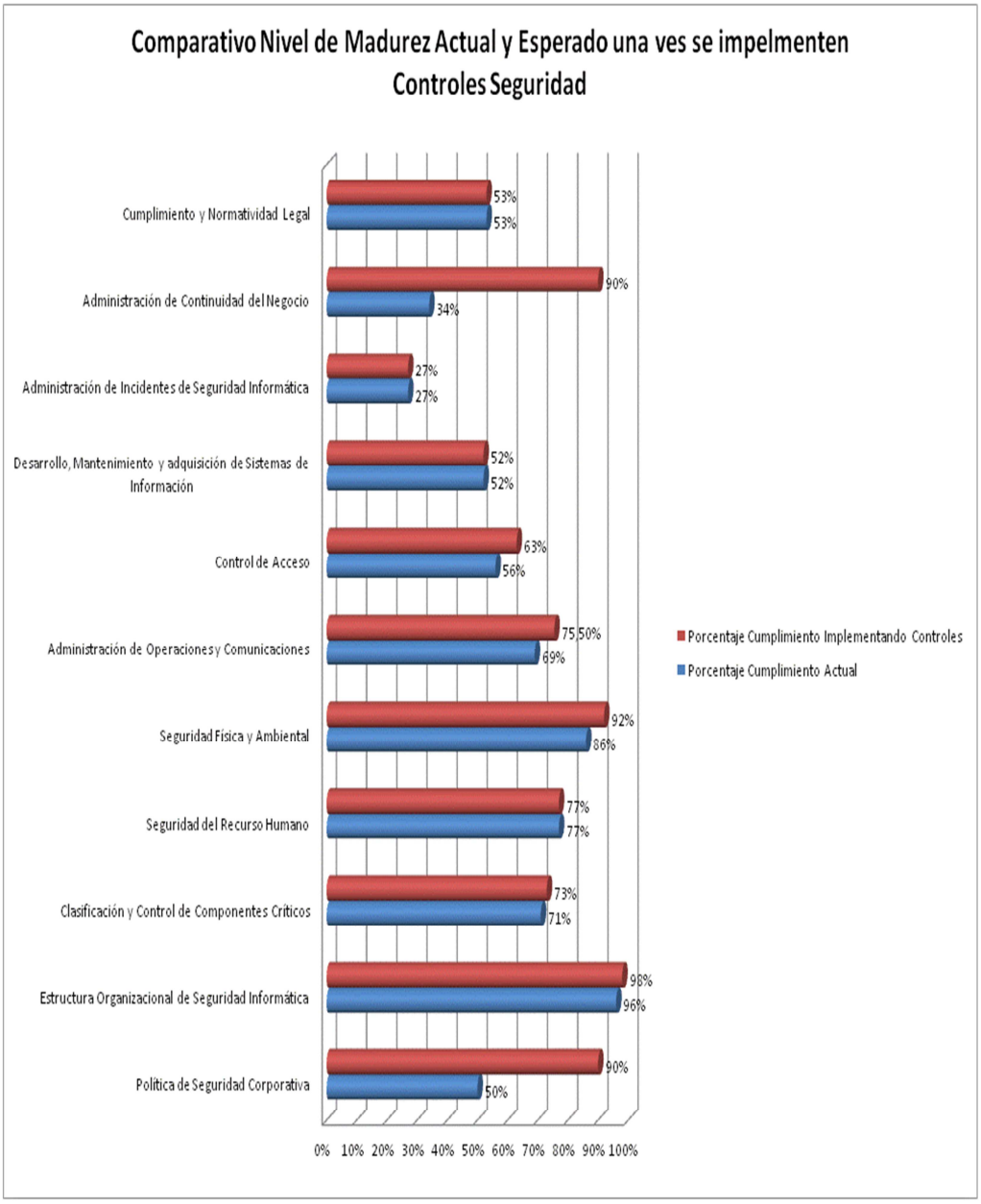
Tabla 17. Nivel cumplimiento con controles implementados

Dominio	Aprobados	NO Aprobados	Porcentaje Cumplimiento	Cumplimiento con Controles Implementados
Política de Seguridad Corporativa	2	0	50%	90%
Estructura Organizacional de Seguridad Informática	11	0	96%	98%
Clasificación y Control de Componentes Críticos	5	0	71%	73%
Seguridad del Recurso Humano	9	0	77%	77%
Seguridad Física y Ambiental	13	0	86%	92%
Administración de Operaciones y Comunicaciones	29	2	69%	75,50%
Control de Acceso	25	0	56%	63%

Desarrollo, Mantenimiento y adquisición de Sistemas de Información	16	0	52%	52%
Administración de Incidentes de Seguridad Informática	5	0	27%	27%
Administración de Continuidad del Negocio	5	0	34%	90%
Cumplimiento y Normatividad Legal	10	0	53%	53%

A continuación se muestra la misma distribución pero de forma grafica para que sea mucho más entendible:

Figura 11. Comparativo Niveles Madurez



Podemos ver como se mejoran los niveles de madurez en los siguientes dominios:

- Administración y continuidad del negocio
- control de acceso
- administración de operaciones y comunicaciones
- Seguridad física y ambiental
- clasificación y control de componentes críticos
- estructura organizacional de seguridad informática
- políticas de seguridad corporativa.

Esto indica que los proyectos se encuentran bien enfocados y dan cubrimiento a la mayoría de dominios de la ISO 27002.

INFOGRAFIA

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P800292251293651550991&langPae=es&detalleLista=PAE_1276529683497133
http://www.iso27000.es/iso27000.html#section3b
http://www.iso27001standard.com/es/que-es-la-norma-iso-27001
http://iso27002.wiki.zoho.com/00-Cl%C3%A1usulas-ISO-27002.html
http://www.iso27000.es/download/doc_iso27000_all.pdf
http://auditoriauc20102mivi.wikispaces.com/file/view/NTCAS436020101700422184.pdf
http://www.cancer.gov.co/contenido/contenido.aspx?catID=-1&conID=793
http://www.innotecsystem.com/plandirectorseguridad.htm
http://blog.s21sec.com/2007/12/por-qu-un-plan-director-de-seguridad.html
http://www.sia.es/img/Plan_director_Cepsa-Sia.pdf
http://www.rediris.es/difusion/eventos/foros-seguridad/fs2010/pres/viii-foroseguridadRI2.pdf
http://www.socinfo.info/seminarios/datos/navarra.pdf
http://www.virtual.unal.edu.co/cursos/sedes/manizales/4010014/Contenidos/Capitulo4/Pages/4.17/417Control_operacional.htm

BIBLIOGRAFIA

DANIEL CRUZ ALLENDE. Análisis de riesgos, Universidad Oberta de Catalunya, PID_00177810 Barcelona España

ANEXOS

Anexo 1. Analisis_Riesgos_ASD_v2.xlsx

Anexo 2. Matriz Análisis GAP v2.xlsx