“PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA DEL SECTOR INDUSTRIAL BASADO EN ISO/IEC 27001” CASO DE ESTUDIO: COTECMAR (CORPORACIÓN DE CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO DE LA INDUSTRIA NAVAL, MARÍTIMA Y FLUVIAL)

MICHELLE URRUCHURTU GOMEZ

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS D.T Y C
2013

“PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA DEL SECTOR INDUSTRIAL BASADO EN ISO/IEC 27001” CASO DE ESTUDIO: COTECMAR (CORPORACIÓN DE CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO DE LA INDUSTRIA NAVAL, MARÍTIMA Y FLUVIAL)

MICHELLE URRUCHURTU GOMEZ

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE

INGENIERO DE SISTEMAS

DIRECTOR
ISAAC ZUÑIGA SILGADO
ING. DE SISTEMAS

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS D.T Y C
2013

Cartagena de Indias D.T. H. y C. 09 de Octubre del 2013

Señores:
Comité Evaluador de Proyectos de Grados.
Programa de Ingeniería de Sistemas.
Universidad Tecnológica de Bolívar
Ciudad.

Respetados Señores:

Yo Michelle Urruchurtu Gómez Identificada con Nro. De Cédula 1.047.386.494 de Cartagena. En mi carácter de estudiante del programa de Ingeniería de Sistemas y cumpliendo con todos los requisitos exigidos por el Reglamento de estudios de Pregrado de la Universidad Tecnológica de Bolívar, someto a consideración el trabajo de Grado titulado: "Plan Estratégico de Seguridad de Información en una empresa del sector Industrial Basado En ISO/IEC 27001" Caso De Estudio: Cotecmar (Corporación De Ciencia Y Tecnología Para El Desarrollo De La Industria Naval, Marítima Y Fluvial)

Cordialmente,

Michelle Urruchurtu Gómez
CC. 1.047.386,494 de Cartagena

Cartagena de Indias D.T. H. y C. 28 de Octubre del 2013

Señores:
Comité Evaluador de Proyectos de Grados.
Programa de Ingeniería de Sistemas.
Universidad Tecnológica de Bolívar
Ciudad.

Respetados Señores:

A través de la presente certifico que he asesorado el trabajo de grado titulado: "Plan Estratégico de Seguridad de Información en una empresa del sector Industrial Basado En ISO/IEC 27001" Caso De Estudio: Cotecmar (Corporación De Ciencia Y Tecnología Para El Desarrollo De La Industria Naval, Marítima Y Fluvial) realizado por la estudiante Michelle Urruchurtu Gómez portador de la Cédula de identidad Nro. 1.047.386.494 de Cartagena, informo que dicho trabajo reúne los requisitos exigidos para ser sometido a la evaluación y presentación ante el jurado que se designe.

Cordialmente,

Isaac Zúñiga Silgado SE, MBA
Director del Proyecto

Cartagena de indias D.T.H y C 10 de Diciembre del 2013

Yo, **Michelle Urruchurtu Gómez**, **identificada con cedula 1047386494 de Cartagena**, manifiesto en este documento mi voluntad de ceder a la Universidad Tecnológica de Bolívar los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982 sobre Derechos de Autor, del trabajo final denominado **Plan Estratégico de la Seguridad de la Información basada en la ISO 27001** producto de mi actividad académica para optar el título de **Ingeniera de Sistemas** de la Universidad Tecnológica de Bolívar. La Universidad Tecnológica de Bolívar, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y extensión. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento que hace parte integral del trabajo antes mencionado y entrego al Sistema de Bibliotecas de la Universidad Tecnológica de Bolívar.

Nota de aceptación

Firma del Presidente del jurado

Firma del Jurado

Firma del Jurado

Cartagena de Indias D.T. H. y C. 09 de Octubre del 2013

AGRADECIMIENTOS

Agradezco a Dios por protegerme y bendecirme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida.

A mi familia por apoyarme y brindarme la confianza.

A mi esposo por enseñarme a no desfallecer ni rendirme ante nada y siempre perseverar a través de sus sabios consejos

A la Universidad Tecnológica de Bolívar por darme la oportunidad de estudiar y ser un profesional.

A mi director de tesis, Isaac Zúñiga por su guía y asesoramiento ha logrado en mí que pueda terminar mis estudios.

A Personas que durante toda mi carrera profesional han aportado con un granito de arena a mi formación.

DEDICATORIA

A Dios, a mi familia, a mi Hermana Irina Urruchurtu por confiar en mí.

A mi esposo Juan Fajardo por ser mi apoyo incondicional.

Michelle Urruchurtu

CONTENIDO

RESUMEN

Con el propósito de ayudar a las organizaciones a contribuir en la sensibilización permanente de mantener segura su información de amenazas que puedan perjudicar a la empresa. Se ha realizado una investigación mediante el diseño de un plan estratégico de seguridad de información, el cual muestra la importancia, el valor y vulnerabilidades de la información para formar un criterio del porqué es necesario mantenerla segura.

Para la elaboración del proyecto este se dividió en tres etapas fundamentales: la primera es la recolección de información, en la cual, mediante la información proporcionada por el personal de Sistemas y visitas de campo a las instalaciones de la empresa, se levantó los datos más relevantes que denoten vulnerabilidad definidos en los dominios de la ISO 27001 ; la segunda etapa es el análisis de la información recolectada en la que se enumeran los riesgos a los que está expuesta la empresa, para luego evaluar y priorizar los riesgos identificados; y en la tercera etapa se dan a conocer las recomendaciones para reducir los riesgos y sus respectivos impactos.

Luego, se presentan las normas y estándares internacionales más relevantes en el tema con sus respectivos lineamientos.

Finalmente, se dan a conocer las conclusiones y recomendaciones que guían la implementación de las estrategias y el desarrollo del plan de acción a seguir de acuerdo con las inseguridades encontradas durante la realización de este proyecto.

ABSTRACT

With the aim of helping organizations to contribute to the ongoing awareness of keeping information secure threats that may harm the company. Research has been carried out by designing a strategic plan for information security, which will show importance, value and vulnerabilities of information to form a judgment on why it should be kept safe.

For the development of this project is divided into three basic stages to be performed: the first is the collection of information, which, through information provided by the systems staff and field visits to the premises of the company, will raise the data denoting vulnerability relevant domains defined in ISO 27001, the second step is the analysis of the information collected on listing the risks to which the company is exposed, and then assess and prioritize the risks identified, the third stage the recommendations to reduce risks and their respective covenants.

Then, we present rules and relevant international standards on the subject with their respective guidelines.

Finally, we present the conclusions and recommendations that guide the implementation of development strategies and action plan to be followed according to the uncertainties encountered during the implementation of this project.

INTRODUCCIÓN

La información es el principal activo de muchas organizaciones y precisa ser protegida adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio.

Actualmente, las empresas confían en la tecnología para generar y conservar una gran cantidad de información. Sin embargo, más tecnología y más exposición pueden resultar en un mayor nivel de riesgo de ser objeto de todo tipo de ataques no autorizados a sus sistemas de TI, los que pueden violar la seguridad de las organizaciones.

La seguridad de la información es de vital importancia en momentos en que las organizaciones deciden que sus bienes deberían estar protegidos ante amenazas y cuando establecen medidas para proteger la confidencialidad e integridad de dicha información.

La mayoría de las empresas desconocen la magnitud del problema con el que se enfrentan considerando la seguridad como algo secundario y generalmente no se invierte el capital humano ni económico necesario para prevenir principalmente el daño y/o pérdida de la información.

Por tal motivo, muchos son los riesgos que afectan la seguridad de las empresas y por lo general el capital con el que se cuenta para protegerlas no es el suficiente debemos tener identificadas y controladas las vulnerabilidades y para obtener dicha protección, las organizaciones deben ir más allá de pensar en tomar esas medidas.

Por lo anterior, este trabajo de grado tiene como objetivo principal el desarrollo de un Plan Estratégico de Seguridad de la Información tomando como Caso de estudio la empresa Cotecmar – Sector Industrial, para ayudar a definir qué deberían hacer para asegurar la seguridad de la información con metodologías estructuradas de sistemas de gestión o de mejores prácticas, tales como la norma ISO 27001, Nist 800-30, COBIT.

1. PLANTEAMIENTO DEL PROBLEMA

Cotecmar no cuenta con un Plan Estratégico de Seguridad de la Información que permitan estar protegidos ante amenazas, riesgos de ser objeto de todo tipo de ataques no autorizados a sus sistemas de TI, para prevenir principalmente el daño y/o pérdida de la información.

2. OBJETIVOS

Formular el Plan Estratégico de Seguridad de la Información basado en el cumplimiento del estándar ISO 27001 con el fin de salvaguardar la integridad, disponibilidad y confidencialidad de la información en Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR

3. OBJETIVOS ESPECÍFICOS

I. Elaborar un estado del arte de los servicios prestados ((hardware, Software, aplicaciones, seguridad, redes y telecomunicaciones) por la Oficina de Tecnologías de la Información y las Comunicaciones en la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR, basados en el estándar ISO 27001 e identificar infraestructura actual que los soporta.

II. Ejecutar un proceso de gestión de riesgo de la seguridad de la información basada en la metodología NIST SP 800-30 en la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial-COTECMAR para detectar las vulnerabilidades, riesgos y amenazas a las que se encuentra expuesta.

III. Identificar brechas de seguridad de la información con base al análisis de riesgo y a los objetivos de direccionamiento estratégico de la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial -COTECMAR

IV. Plasmar las iniciativas o proyectos a corto, mediano y largo plazo requerido para el cierre de las brechas identificadas en el estado del arte y las valoraciones de riesgos.

JUSTIFICACIÓN

Este proyecto será relevante, ya que las organizaciones en la actualidad se interesan por tener un buen control en cuanto a la seguridad de la información que se opera en la misma, puesto que se considera un factor crítico de éxito para cualquier empresa madura en el uso y la adopción de los Sistemas de Información y las Tecnologías de la Información y las Comunicaciones, basándose en distintos estándares internacionales que permiten identificar las falencias y elaborar iniciativas que logren darle solución.

Se hace necesario elaborar un plan estratégico de seguridad de la información que incida en la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR de tal forma que permita identificar las brechas que existen en la seguridad de la información, así mismo las formas de gestionar los procesos que pueden considerarse como factores de riesgos en el área, por otra parte da una percepción clara de lo que se ha proyectado en un pequeño, mediano y largo plazo. Basándose en el direccionamiento estratégico de la Corporación, donde se da una noción general de lo que se espera en distintos escenarios (periodos de tiempo) y de igual forma se espera que surjan distintas estratégicas para resarcir dichos eventos.

Esta iniciativa es muy beneficiosa y factible, ya que además de lograr salvaguardar la integridad, disponibilidad y confidencialidad de la información, también ayuda al crecimiento de la Corporación en lo referente a la ciencias y tecnologías, más específicamente en la parte de seguridad de la información, de igual forma dará solución a la problemática que ha sido motivo de estudio este proyecto, para alcanzar los propósitos planteados se espera contar ayuda del personas encargado del área y todas las personas que tienen relación directa con la temática. Para ello se cuenta con una infraestructura TIC’S (Tecnología de la

Información y las Comunicaciones) ajustable a cualquier plan que involucre su mejora o progreso en la organización de alguna de sus funciones.

Podemos ver que día a día los avances tecnológicos están en su mayor auge por lo tanto la Corporación debe tomar medidas preventivas, donde además de plantear e implementar, también deberá proteger su infraestructura en general. Debe existir una serie de controles para contrarrestar todas las amenazas.

1. SEGURIDAD DE LA INFORMACIÓN

La información es un activo que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido adecuadamente.

La Seguridad de la Información es la protección de la información de un rango amplio de amenaza para poder asegurar la continuidad del negocio; es garantizar que existe y se mantiene un marco de referencia con el fin de asegurar que las estrategias de seguridad de la Información están alineadas con los objetivos del negocio.

La seguridad de la Información estaba basada en 3 elementos fundamentales:

- **Personas**: Ejecutar y soporta lo procesos de seguridad de la Información
- **Procesos**: Definen la operativa que soporta los procedimientos de seguridad y la normatividad.
- **Tecnología:** Son un conjunto de herramientas informáticas que facilitan los procesos.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del organismo.

La seguridad de la información es necesaria porque hoy en día las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso,

pirateo computarizado o negación. Y es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

1.1. Requerimientos de Seguridad

Se empieza con identificar los requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad, Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la empresa.

A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos funcionales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

1.2. Políticas de Seguridad de Información

La seguridad de la información está basada en combinar, las políticas de seguridad Lógica, Física y Ambiental, con los procedimientos y controles en el desarrollo y mantenimiento de las aplicaciones, los procedimientos y controles de los sistemas de respaldo y una estructura organizacional para efectos de tener un sistema informático confiable y que cumpla con los criterios básicos como son:

- **Confidencialidad:** Propiedad por la cual la información no esté disponible ni sea divulgada a individuos, organismos o procesos no autorizados. (ISO27001:2005, 2005) (ISO27001: 2005, Cláusula 3.8)

- **Integridad:** Propiedad de proteger la precisión y la totalidad de los activos.. (ISO27001: 2005, Cláusula 3.8)
- **Disponibilidad**: Propiedad de estar accesible y ser utilizable a demanda por parte de un organismo autorizado (ISO 27001: 2005. cláusula 3.2)

La seguridad se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial.

1.3. Términos y definiciones

- ***AoAs***

  Áreas de análisis que son la infraestructura, las aplicaciones, operaciones y la gente.

- ***Actividad***

  Conjunto de tareas necesarias para la obtención de un resultado

- ***Activo***

  Cualquier elemento de software, hardware, datos, administrativo, físico, comunicaciones, o recurso de personal dentro de un sistema de información. Recursos del sistemas de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

- ***Antivirus (AV)***

  Software o tecnología de hardware que protege al entorno informático frente a cualquier software peligroso.

- ***Aplicaciones***

  Software informático que proporciona funcionalidad al usuario final. Requiere la existencia de un sistema operativo en el que ejecutarse.

- ***Amenazas***

  Causa potencial de un incidente que puede resultar en un daño a un sistema o a una organización. [ISO 27002]

- ***Análisis de Riesgo***

  Es la complejidad de determinar el impacto de un evento no deseado y, principalmente, la falta de datos suficiente para poder determinar de manera exacta las funciones de distribución de probabilidad para las amenazas más comunes.

- ***Brechas de Seguridad***

  Son todas las oportunidades de amenaza contra la infraestructura, en la cual puede ocurrir una fuga de información que perjudique la empresa.

- ***Buenas Practicas***

  Es un proceso o una metodología que representa la forma más efectiva de conseguir un objetivo específico.

- ***Concienciación***

  Conjunto de medidas para que las personas relacionadas con la organización (personal, contratistas, clientes, proveedores, etc.) conozcan los riesgos de seguridad y los controles que pueden y deben aplicar para colaborar en su mitigación.

- ***Confidencialidad***

  Propiedad de que la información no está disponible ni es divulgada a personas, procesos o dispositivos no autorizados. [ISO 27002].

- ***Consistencia***

  Es asegurar que el sistema se comporte como se supone que debe hacerlo con los usuarios autorizados. Si el software o el hardware de repente comienzan a comportarse de un modo radicalmente diferente al esperado, puede ser un desastre.

- ***Controles***

  Cualquier acción o proceso que se utiliza para mitigar el riesgo

- ***Control de Acceso***

  Limitar el acceso autorizado solo a entidades autenticadas.

- ***Direccionamiento Estratégico***

  Es el análisis prospectivo de la Corporación, que está proyectado en distinto escenarios (periodos de tiempo) y plantea distintas estrategias con las que se puede suplir las necesidades de la empresa.

- ***Disponibilidad***

  Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o

aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran.

- ***Dominio***

  Clasificación de los procesos de las unidades de tecnología de información

- ***Eficiencia***

  Propiedad de que un requerimiento de negocio se alcanza realizando un consumo óptimo de los recursos disponibles para ello.

- ***Escenario de riesgos***

  Descripción del efecto de un conjunto determinado de amenazas entre un determinado conjunto de activos, recursos.

- ***Estándar ISO/IEC 270001***

  Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

- ***Estrategia***

  Una estrategia es el conjunto de acciones que se implementarán en un contexto determinado con el objetivo de lograr el fin propuesto.

- ***Factores de Riesgo***

  Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad.

- ***Gestión de Riesgo***

  Es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

(ISO27001)

- ***Gobierno***

  Proporcionar control y dirección a las actividades
- ***Gobierno de la Seguridad de la Información***

  Determinar los riesgos que le atañen y su forma de reducir y/o mitigar impactos adversos a un nivel aceptable mediante el establecimiento de un programa amplio y conciso en seguridad de la información y el uso efectivo de recursos cuya guía principal sean los objetivos del negocio, es decir, un programa que asegure una dirección estratégica enfocada a los objetivos de una organización y la protección de su información.
- ***Índice de Defensa en profundidad (DiDi)***

  Medida de las defensas de Seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.
- ***Información***

  Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- ***Integridad***

  Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
- ***Impacto***

  El impacto es la estimación del grado de daño o de la pérdida que podría ocurrir en una organización. Las consecuencias se refieren al daño total, no únicamente a los impactos a corto plazo o inmediatos. Cuando más severas las consecuencias de una amenaza, mayor es el riesgo relacionado al sistema y, por lo tanto, la organización.

- ***Métricas de Seguridad, Monitoreo***

  Medición de actividades de seguridad
- ***Mitigación***

  Son las medidas de intervención dirigidas a reducir el riesgo de la información basado en las políticas de seguridad. Hay que tener en cuenta que dicho riesgo es imposible reducir totalmente.
- ***NIST***

  (Instituto Nacional de Normas y Tecnología) Es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
- ***NIST 800-30 (National Institute of Standards and Technology)***

  Metodología para el análisis y gestión de riesgos de seguridad de la información.
- ***Normativa de seguridad***

  Conjunto de documentos que desarrollan la política de seguridad.
- ***Normas***

  Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.
- ***Método***

  "Método es el camino o medio para llegar a un fin, el modo de hacer algo ordenadamente, el modo de obrar y de proceder para alcanzar un objetivo determinado" - Mendieta Alatorre
- ***Metodología***

  Estudio de los métodos.
- ***Objetivos de Control***

  Consisten en políticas, procedimientos, prácticas y estructuras organizacionales

- ***Perfil de Riesgos para la Empresa (BRP)***

  Medida del riesgo al que está expuesto una empresa según el entorno empresarial y el sector en que compite.

- ***Plan de Acción***

  Es un tipo de plan que prioriza las iniciativas más importantes para cumplir con ciertos objetivos y metas. Se constituye como una especie de guía que brinda un marco o una estructura a la hora de llevar a cabo un proyecto.

  Plan de Seguridad

  Conjunto de proyectos de seguridad priorizados y presupuestados que permiten materializar las decisiones de gestión de riesgos.

- ***Políticas***

  Son los planes, prácticas, criterios elegidos para alcanzar un objetivo de terminado.

- ***Política de Seguridad***

  Es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

- ***Procedimiento***

  Forma especificada para llevar a cabo una actividad o proceso"- ISO

- ***Proceso***

  Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados"- ISO

- **Probabilidad**

  Es una valoración de la frecuencia o de la ocurrencia de una amenaza sobre un sistema de información. La información histórica sobre muchas amenazas es generalmente utilizada, sin embargo, con respecto a las amenazas humanas, la experiencia en esta área es importante. Generalmente cuanto mayor es la probabilidad de una amenaza que ocurre, mayor es el riesgo.

- ***Riesgo***

  Posibilidad que una amenaza particular afecte a un sistema de información explotando una vulnerabilidad particular. El riesgo permite conocer de forma cuantitativa o cualitativa los daños causados a los elementos del sistema de información, si no son aplicadas acciones preventivas y correctivas rápidamente.

- ***Seguridad***

  Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a un sistema o a la organización.

- **Seguridad Informática**

  Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

- ***Seguridad de la Información***

  Aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma.

- ***Seguridad Física***

  Este tipo de seguridad se asocia a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.

- ***Seguridad Lógica***

  Es la protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía.

- ***Servidor de Seguridad (Cortafuego)***

  Dispositivo de hardware o software que ofrece protección a los equipos frente al acceso no autorizado a través de la red.

- ***Sistema de Información***

  Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- ***SGSI***

  (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

- ***Tecnología de la Información***

  Se refiere al hardware y software operado por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- ***Vulnerabilidad***

  Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas. (ISO27001)

- ***Zona Desmilitarizada (DMZ)***

  Parte de la red separada de la red interna mediante un cortafuego y conectada a Internet a través de otro cortafuego.

2. EVALUACIÓN DE RIESGO

2.1. Evaluación del riesgo

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Los dos puntos considerados son:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.

Los resultados de la evaluación del riesgo ayudaron a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

Los pasos para realizar una valoración de riesgos se detallan a continuación:

a) Identificar los riesgos
b) Análisis de riesgos

La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo.

2.2. Tratamiento de riesgos

El tratamiento de riesgos es la segunda parte de la gestión de riesgos, inmediatamente después del proceso de evaluación de riesgos. El objetivo de esta parte es definir cómo controlarlos.

Durante el tratamiento de riesgos, generalmente se escogen los controles de la norma ISO 27001 para disminuir los riesgos; y al hacerlo, es muy importante evaluar entre disminuir los riesgos y el costo de los controles, porque puede terminar invirtiendo demasiado en un determinado control mientras que podría haber encontrado una alternativa más económica.

1. Manejo de riesgos

Los problemas de seguridad se multiplican con gran facilidad, por lo que las empresas deben perfeccionar los sistemas y los procesos para evitar amenazas o abordarlas cuando se produzcan. Para garantizar que la información de nuestra organización posea las características de seguridad ya mencionadas como son la confidencialidad, integridad y disponibilidad se debe poner en práctica un plan de seguridad de la Información.

2. Identificar Riesgos

En este paso se identifican los factores que introducen una amenaza en la planificación del entorno de tecnologías de la información, existen formas de identificarlos como:

Cuestionarios de análisis de riesgos: La herramienta clave en la identificación de riesgos son los cuestionarios los mismos que están diseñados para guiar al

administrador de riesgos para descubrir amenazas a través de una serie de preguntas y en algunas instancias.
Este cuestionario está diseñado para servir como repositorio de la información acumulada de documentos, entrevistas, etc. Su propósito es guiar a la identificar exposiciones de riesgos a través del proceso en un modelo lógico y consistente.

Lista de Chequeo: Una segunda ayuda importante en la identificación de riesgos y una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo las cuales son simplemente una lista de exposiciones a riesgos.

3. Ponderación de los Factores de Riesgo

Ponderar el factor de riesgo es darle un valor de importancia en términos porcentuales al mismo bajos los criterios de especialistas en el área de tecnologías de la información que pueden identificar su impacto en la organización, teniendo en cuenta las posibilidades de que se puedan convertir en realidad.

4. Valoración del Riesgo

La valoración del riesgo envuelve la medición del potencial de las pérdidas y la probabilidad de la pérdida categorizando el orden de las prioridades.

3. METODOLOGIAS

Para la puesta en marcha de la gestión de la seguridad de la información existen diversas normas y estándares aprobados mundialmente, las cuales permiten llevar a cabo el proceso de seguridad de la información de manera estructurada, organizada y documentada, basada en diferentes controles y políticas que se establecen.

Por este motivo el presente capitulo hace referencia en forma reducida las normas y/o estándares internacionales que guarden relación con la seguridad de la información y que sirvieron de apoyo para la realización del caso de estudio.

Estas normas y estándares además de ser tomadas como referencia para reflejar las mejores prácticas en gobierno de tecnología de la Información, también han brindado la orientación precisa para apoyar la investigación, ya que lo que se procura tener una infraestructura en la que se cumplan con la confiabilidad, disponibilidad y la integridad de la información de la Corporación.

Entre las diferentes normas y estándares se encuentra:

- **ISO/IEC 27001**
- **NIST SP 800-30**
- **CORAS**
- **OCTAVE**
- **MAGERIT**

3.1. Norma ISO/IEC 27001

Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

A continuación se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.*Figura 3-1*

Figura 3-1 *Evolución ISO 27001*

.

3.2. Objetivos de la ISO 27001

- Enmarcar la Seguridad dentro de la cultura y gestión de la organización.
- Garantizar la confidencialidad, disponibilidad e integración de la información de la organización. De esta manera ésta puede cumplir sus objetivos, tanto de negocios como contractuales y legales.

3.3. Beneficios ISO 27001

Los beneficios de la Norma ISO 27001 son: (ISO27001)

a) Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
b) Reducción del riesgo de pérdida, robo o corrupción de información.
c) Los clientes tienen acceso a la información a través medidas de seguridad.
d) Los riesgos y sus controles son continuamente revisados.
e) Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
f) Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
g) Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
h) Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
i) Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
j) Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
k) Confianza y reglas claras para las personas de la organización.
l) Reducción de costes y mejora de los procesos y servicio.
m) Aumento de la motivación y satisfacción del personal.
n) Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías

3.4. Áreas o Dominios contemplados

La norma se desarrolla en 11 áreas o dominios que recogen los 133 controles a seguir.

a. Política de seguridad
b. Organización de la información de seguridad
c. Administración de recursos
d. Seguridad de los recursos humanos
e. Seguridad física y del entorno
f. Administración de las comunicaciones y operaciones
g. Control de accesos
h. Adquisición de sistemas de información, desarrollo y
i. mantenimiento
j. Administración de los incidentes de seguridad
k. Administración de la continuidad de negocio
l. Marco legal y buenas prácticas

Figura 3-2 *Dominios ISO 27001*

3.5. Definición de Control

El concepto de “control” dentro de la norma agrupa todo el conjunto de acciones, documentos, procedimientos y medidas técnicas adoptadas para garantizar que cada amenaza, identificada y valorada con un cierto riesgo, sea minimizada.

Se definen 133 controles dentro de las 11 áreas o dominios que podrían agruparse e identificarse en procesos:

- Organizativos
- Implementación de tecnologías de la seguridad.
- Establecimiento de relaciones contractuales
- Gestión de Incidencias
- Gestión de Recursos Humanos
- Cumplimiento con la normativa vigente

3.6. Dominio de la ISO27001

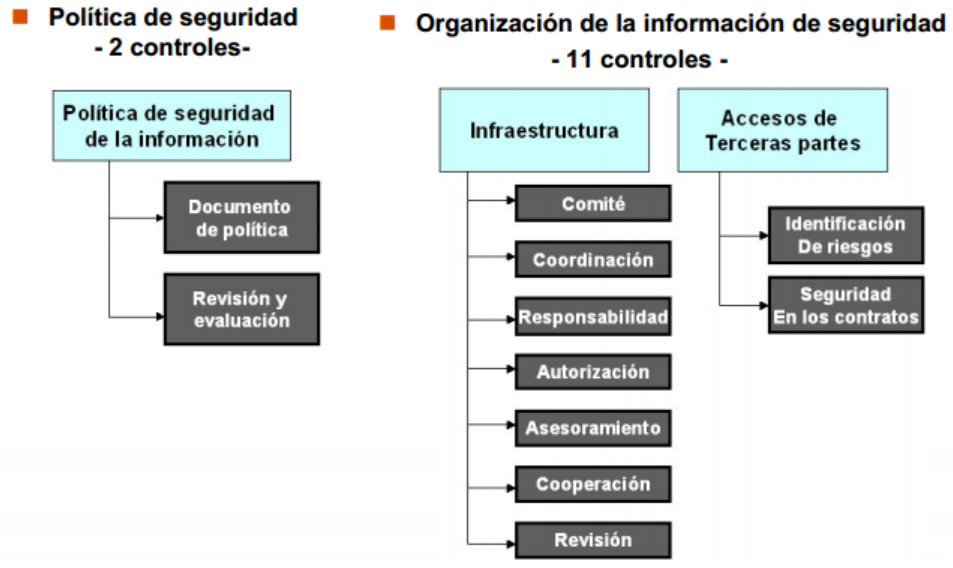


Figura 3-3 Dominios de ISO27001

Fuente: ISO27001.es

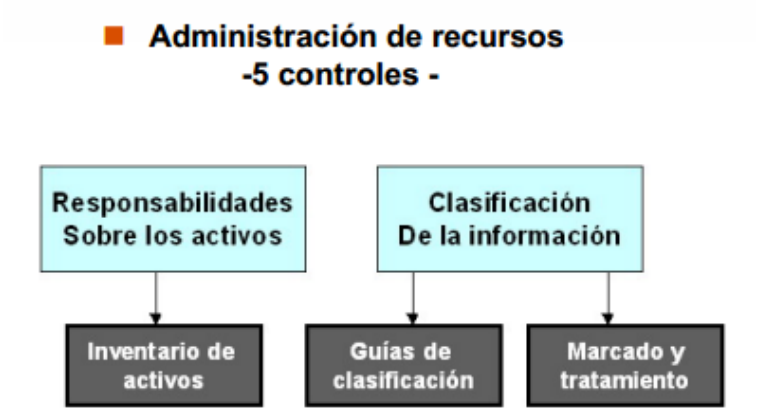


Figura 3-4Dominios de ISO27001

Fuente: ISO27001.es

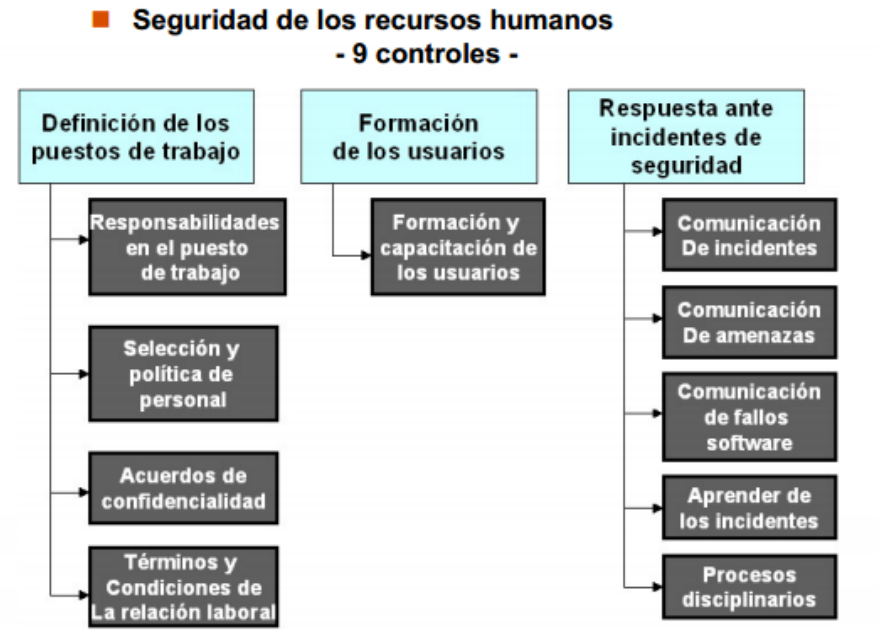


Figura 3-5 Dominios de ISO27001

Fuente: ISO27001.es

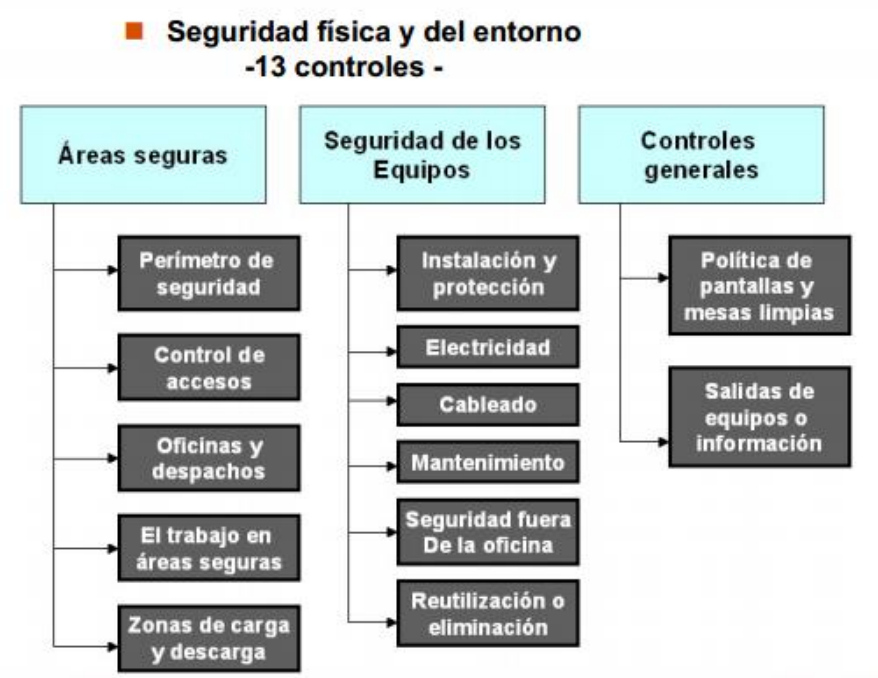


Figura 3-6Dominios de ISO27001

Figura 3-7Dominios de ISO27001

Fuente: ISO27001.es

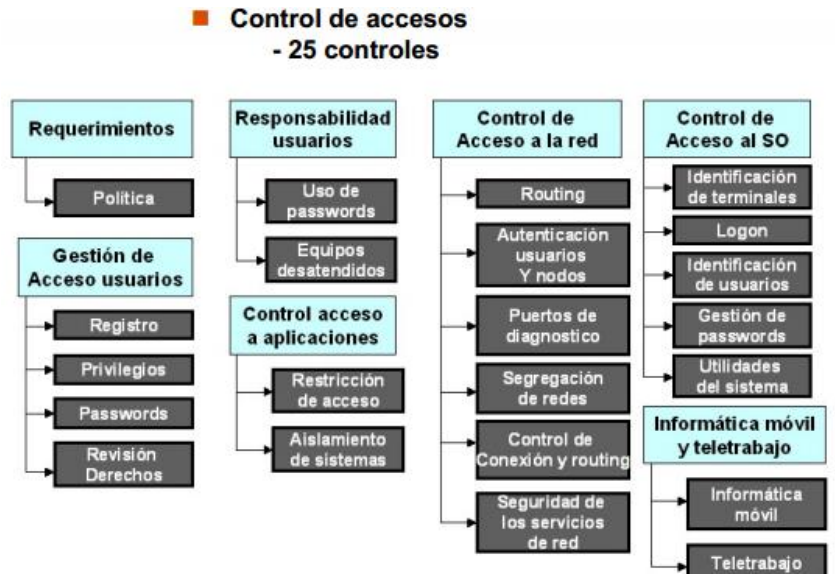


Figura 3-8 *Dominios de ISO27001*

Fuente: ISO27001.es

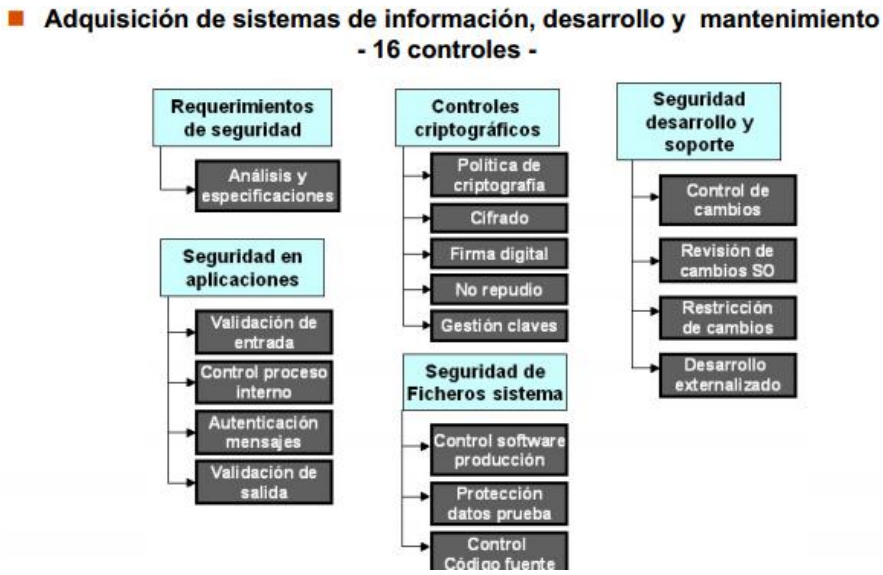


Figura 3-9 Dominios de ISO27001

Fuente: ISO27001.es

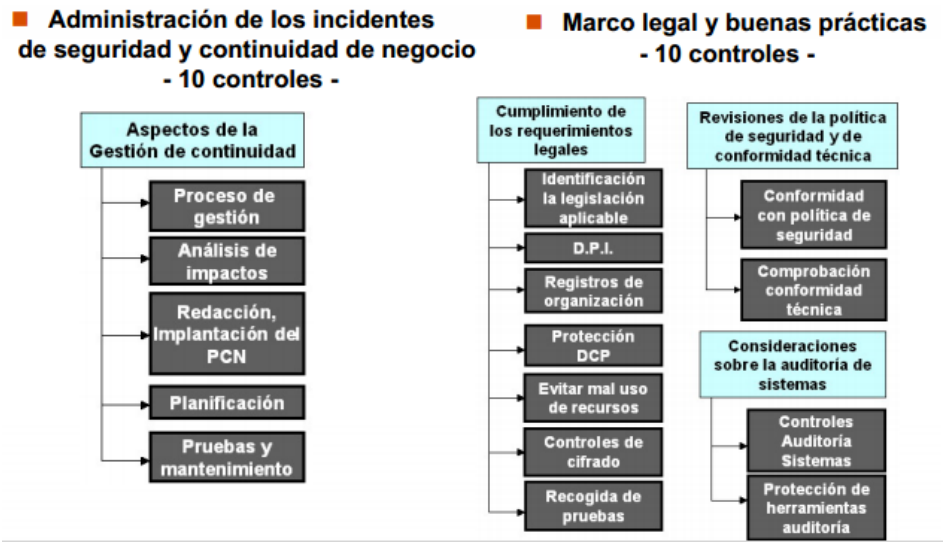


Figura 3-10 Dominios de ISO27001

Fuente: ISO27001.es

3.7. Otras Metodologías

Existen otras metodologías para el análisis de riesgos de la seguridad de la Información, los cuales son:

a) **NIST SP 800-30** (Nist)

National Institute of Standards and Technology ha dedicado una serie de publicaciones especiales, la SP 800 a la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, alineada y complementaria con el resto de documentos de la serie.

La Metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo:

Paso 1. Caracterización del Sistema

Caracteriza el sistema, incluyendo hardware (servidores, puertos), software (aplicaciones, sistemas operativos, protocolos), interfaces del sistema (enlace de comunicaciones), datos, y usuarios, es decir todo los activos TIC.

Pasa 2. Identificación de Amenazas

Identifica las fuentes de amenaza potenciales y compila un listado de fuentes de amenaza potenciales que son aplicables al sistema TI a ser evaluado.

Paso 3. Identificación de Vulnerabilidad

Desarrolla una lista de vulnerabilidades del sistema (fallas o debilidades) que pudieran ser explotadas por las potenciales fuentes de amenaza.

Paso 4. Análisis de Controles

Analiza los controles que ha sido implementados o están planificados para minimizar o eliminar la probabilidad de que se explote una amenaza sobre una vulnerabilidad del sistema.

Paso 5. Determinación de Probabilidad

Determina la probabilidad de que una vulnerabilidad potencial puede ser explotada dentro del ambiente de amenazas asociado.

Paso 6. Análisis del Impacto

Determinar el impacto adverso resultante de una explotación exitosa de una amenaza sobre una vulnerabilidad.

Paso 7. Determinación del Riesgo

Evalúa el nivel de riesgo para el sistema TI. Se realiza un matriz para la determinación del riesgo.

Paso 8. Recomendaciones del Control

Se proveen los controles que podrían mitigar o eliminar los riesgos identificados, y que sean apropiados para las operaciones de la organización.

Paso 9. Documentación de Resultados

Una vez que se ha completado la evaluación de riesgo los resultados se documentan en un reporte oficial.

El proceso de análisis de riesgos definido en la metodología NIST SP 800-30 puede resumirse en la siguiente *Figura 3-11 [NIST800-30.02]*:

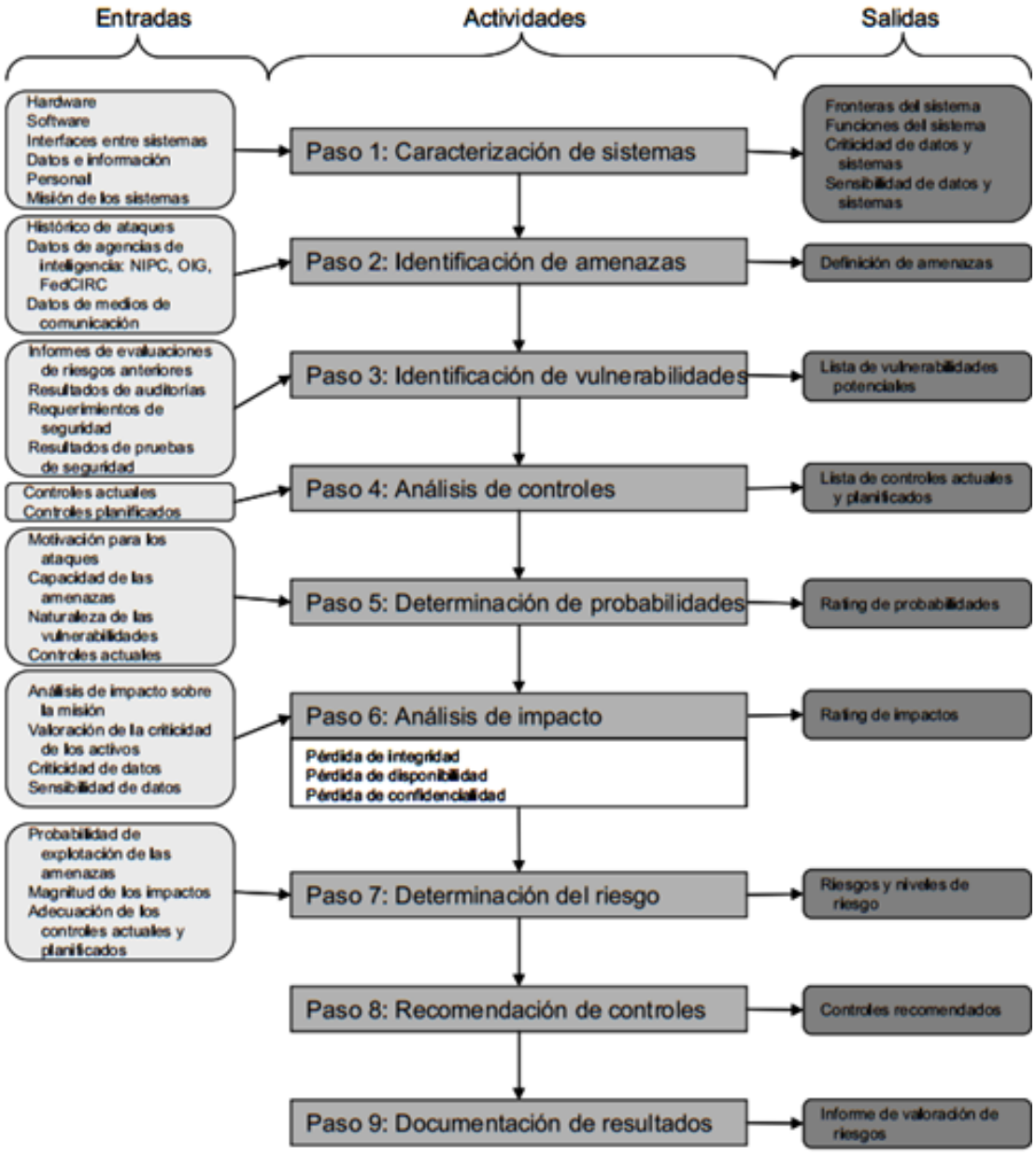


Figura 3-11 [NIST800-30.02]

b) METODOLOGÍA MAGERIT

Es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas" elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

Se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

MAGERIT, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

La Metodología MAGERIT está compuesta por 7 pasos para el análisis de riesgo

Figura 3-12 *Metodología Magerit*

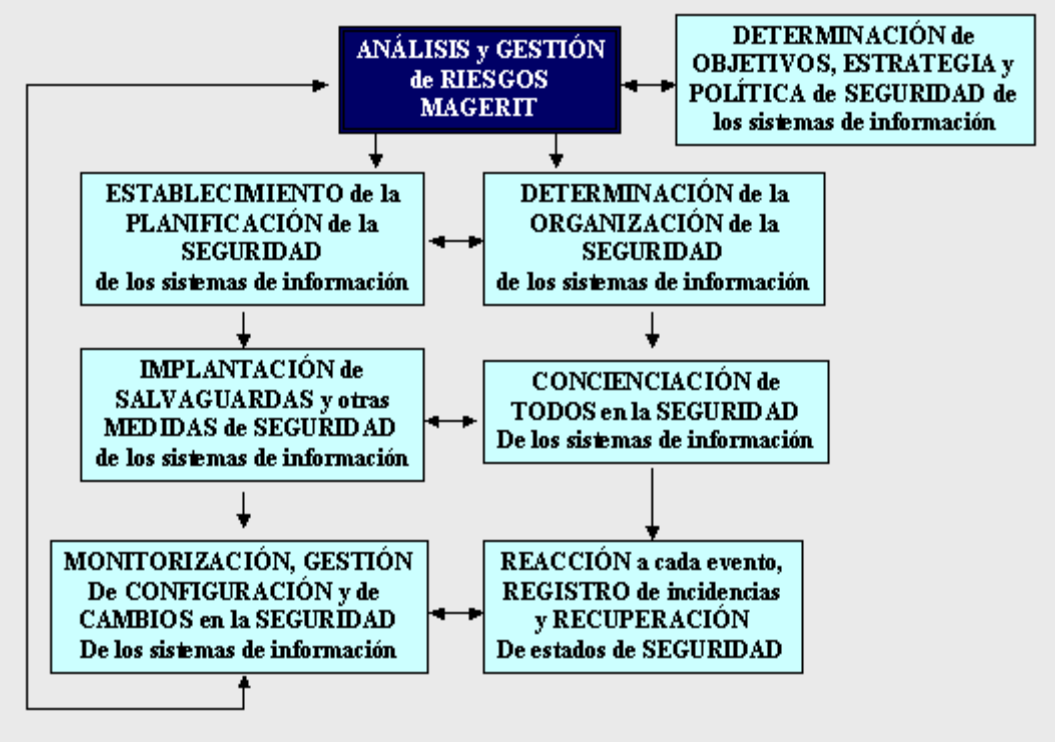


Figura 3-12 Metodología Magerit

c) METODOLOGÍA CORAS (Construct a platform for Risk Analysis of Security critical system)

Desarrollado a partir de 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Se desarrolló en el marco del Proyecto CORAS (IST-2000-25031) financiado por la Unión Europea.

El método CORAS proporciona:

- Una metodología de análisis de riesgos basado en la elaboración de modelos, que consta de siete pasos, basados fundamentalmente en entrevistas con los expertos.
- Un lenguaje gráfico basado en UML (UnifiedModellingLanguage) para la definición de los modelos (activos, amenazas, riesgos y salvaguardas), y guías para su utilización a lo largo del proceso. El lenguaje se ha definido como un perfil UML.
- Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos, que permite su gestión y reutilización.
- Representación textual basada en XML (extensible Mark-up Language) del lenguaje gráfico.
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

Los siete pasos del método CORAS pueden representarse gráficamente de la siguiente forma:

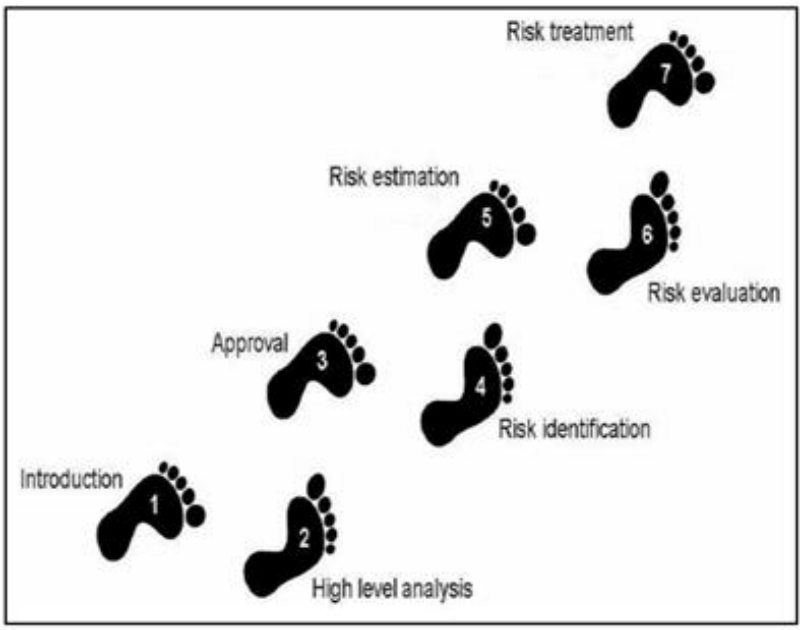


Figura 3-13 Pasos Metodología Coras

Paso 1, *Presentación: Reunión inicial, para presentar los objetivos y el alcance del análisis y recabar información inicial.*

Paso 2, *Análisis de alto nivel: Entrevistas para verificar la comprensión de la información obtenida y la documentación analizada. Se identifican amenazas, vulnerabilidades, escenarios e incidentes.*

Paso 3, *Aprobación: Descripción detallada de los objetivos, alcance y consideraciones, para su aprobación por parte del destinatario del análisis de riesgos.*

Paso 4*, Identificación de riesgos: Identificación detallada de amenazas, vulnerabilidades, escenarios e incidentes.*

Paso 5, *Estimación de riesgo: Estimación de probabilidades e impactos de los incidentes identificados en el paso anterior.*

Paso 6, *Evaluación de riesgo: Emisión del informe de riesgos, para su ajuste fino y correcciones.*

Paso 7, *Tratamiento del riesgo: Identificación de las salvaguardas necesarias, y realización de análisis coste/beneficio*

d) METODOLOGÍA OCTAVE

OCTAVE (Operación Critica de Amenazas y Evaluación de Vulnerabilidades) fue desarrollada por Carnegie Mellon Software Engineering Institute(SEI). El núcleo de OCTAVE son criterios que la organización puede usar para desarrollar su propia metodología. Aunque el método OCTAVE fue desarrollado para largas organizaciones, un método conocido como OCTAVE-S fue también desarrollado para pequeñas organizaciones. Al igual que el método OCTAVE, este es de disponibilidad gratuita.

La premisa básica OCTAVE de estructurada mediante entrevistas en varios niveles de la organización para identificar lo valioso y así determinar los riesgos de estos objetivos específicos:

- Desmitificar la falsa creencia: La Seguridad Informática es un asunto meramente técnico
- Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.
- Octave divide los activos en dos tipos que son:
- Sistemas, (Hardware. Software y Datos)
- Personas

La metodología OCTAVE está compuesta en tres fases:

1) Visión de organización: Donde se definen los siguientes elementos: activos, vulnerabilidades de organización, amenazas, exigencias de seguridad y normas existentes.
2) Visión tecnológica: se clasifican en dos componentes o elementos: componentes claves y vulnerabilidades técnicas.
3) Planificación de las medidas y reducción de los riesgos: se clasifican en los siguientes elementos: evaluación de los riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de los riesgos.

Las fases del proceso OCTAVE pueden resumirse en la ***Figura 3-14***

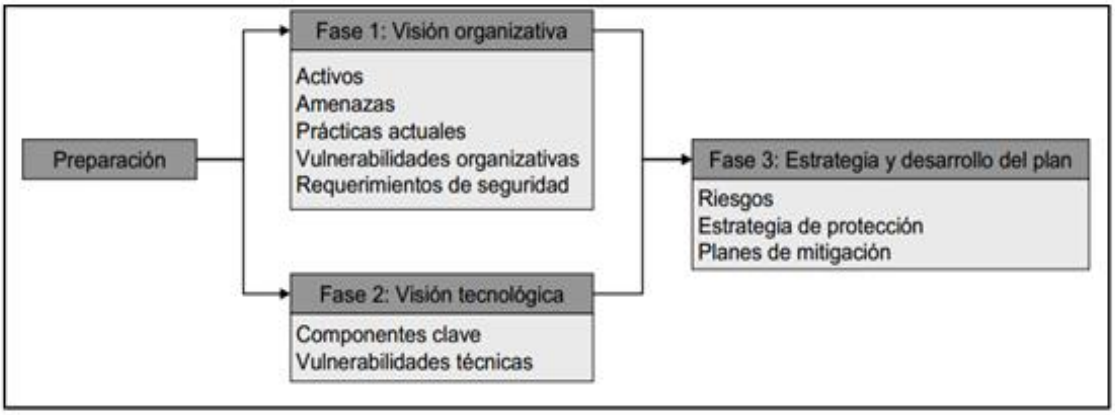


Figura 3-14 Fases del Proceso OCTAVE

4. HERRAMIENTAS DE DIAGNOSTICO PARA ANÁLISIS DE RIESGO

Para analizar el estado de seguridad a nivel técnico se utilizó varias herramientas para el análisis de riesgo y las Vulnerabilidades, las cuales fueron:

4.1. Microsoft Security Assessment Tool (MSAT)

La Herramienta de Evaluación de la Seguridad de Microsoft (por su sigla en inglés MSAT, Microsoft Security Assessment Tool) es una herramienta que ha sido diseñada para ayudar a organizaciones como la suya a evaluar las debilidades de su entorno de TI actual, relevar una lista de temas prioritarios y brindarle una guía que lo ayudará especialmente a minimizar los riesgos. La MSAT constituye una forma fácil y rentable de fortalecer la seguridad de su entorno informático y de su negocio. Comience el proceso con una reseña del estado actual de su seguridad y luego utilice la MSAT para controlar en forma continua la capacidad de su infraestructura para responder a las amenazas a su seguridad.

En Microsoft, la seguridad de las redes de nuestros clientes, los servidores de negocios, las computadoras de usuarios finales, los dispositivos móviles y el acceso a los datos constituyen la prioridad principal. Estamos comprometidos con brindar herramientas de seguridad como la MSAT para ayudarlo a mejorar el estado de seguridad de su negocio.

La MSAT ha sido diseñada para ayudarla a identificar y abordar los riesgos a la seguridad de su entorno TI. La herramienta emplea un enfoque holístico para medir la postura de su seguridad y cubrir temas que incluyen a la gente, los procesos y la tecnología.

La MSAT brinda:

- Una toma de conciencia continua, integral y de fácil uso.
- Un marco de defensa en profundidad con un análisis comparativo de la industria.
- Un informe detallado, continúo comparando el punto de referencia con su progreso.
- Recomendaciones comprobadas y actividades prioritarias para mejorar su seguridad.
- Microsoft estructurado y orientación de la industria.

La MSAT contiene más de 200 preguntas acerca de la infraestructura, las aplicaciones, las operaciones y la gente. Las preguntas, sus respuestas asociadas, y las recomendaciones en cuestión están basadas en las mejores prácticas aceptadas, normas tales como las ISO 17799 y NIST-800.30, las recomendaciones y la orientación prescriptiva del Grupo de Informática de Confianza de Microsoft (Microsoft Trustworthy Computing Group) y otras fuentes externas de seguridad.

La evaluación se ha diseñada para identificar el riesgo comercial a su organización y las medidas de seguridad desplegadas para mitigar dicho peligro. Centrándose en temas comunes, las preguntas han sido desarrolladas para brindar una evaluación de los riesgos de alto grado en la seguridad a la tecnología, procesos y la gente que dan soporte a su negocio.

Comenzando con una serie de preguntas acerca del modelo del negocio de su empresa, la herramienta crea un **Perfil de Riesgo Comercial (Business Risk Profile - BRP)**, midiendo los riesgos de su compañía en base al modelo de la industria y el negocio definido para el BRP. Una segunda serie de preguntas han sido preparadas para compilar una lista de medidas de seguridad que su

compañía ha desarrollado a lo largo del tiempo. En forma conjunta, estas medidas de seguridad forman capas de defensa, brindando una mayor protección contra los riesgos de seguridad y otras vulnerabilidades específicas. Cada capa contribuye una estrategia combinada para una defensa en profundidad. La suma de las mismas constituye el **Índice de Defensa en Profundidad (Defense-in-Depth Index - DiDI)**. El BRP y el DiDI son entonces comparados para medir la distribución del riesgo entre las áreas de análisis (AoAs)

La siguiente tabla ofrece una lista de las áreas que son incluidas en la evaluación de los riesgos a la seguridad.

Infraestructura	**Su Importancia para la Seguridad**
Defensa del Perímetro	La defensa del perímetro trata de la defensa de los límites de la red, allí donde su red interna se conecta al mundo exterior. Esta constituye su primera línea de defensa contra los intrusos.
Autentificación	Los procedimientos de autentificación rigurosos para los usuarios, administradores, y usuarios remotos ayudan a prevenir a que extraños ganen acceso autorizado a la red por medio de ataques locales o remotos.
Gestión y Control	La gestión, control y registros adecuados resultan críticos para el mantenimiento y el análisis de los entornos TI. Estas herramientas son más importantes luego de

Infraestructura	Su Importancia para la Seguridad
	que el ataque haya ocurrido y un análisis de incidentes sea solicitado.
Terminales	La seguridad de las terminales individuales son un factor crítico en la defensa de cualquier entorno, especialmente cuando el acceso remoto es permitido. Las terminales tienen protecciones para resistir ataques comunes.
Aplicaciones	**Su Importancia para la Seguridad**
Implementación y uso	Cuando las aplicaciones críticas comerciales son desplegadas, la producción, la seguridad y la disponibilidad de dichas aplicaciones y los servidores alojados deben ser protegidos. El mantenimiento continuo es esencial para ayudar a asegurar el bloqueo a virus y que las nuevas vulnerabilidades no sean introducidas al entorno.
Diseño de la Aplicación	El diseño que no cuente con los mecanismos adecuados de seguridad como la autentificación, la autorización y la validación de los datos puede permitir a los atacantes explotar las vulnerabilidades de la seguridad y, por lo tanto, ganar acceso a

Aplicaciones	Su Importancia para la Seguridad
	información delicada. Las metodologías de desarrollo de aplicaciones seguras son clave para asegurar las aplicaciones desarrolladas contractadas y abordan los modelos de amenaza a la seguridad que pueden dejar una organización abierta a estas explotaciones de vulnerabilidades. La integridad y la confidencialidad de los datos constituyen la mayor preocupación de cualquier negocio. La pérdida o robo de datos puede impactar en las rentas de la organización y en su reputación en forma negativa. Resulta importante entender como las aplicaciones manejan los datos críticos del negocio y como los datos son protegidos.
Operaciones	**Su Importancia para la Seguridad**
Entorno	La seguridad de una organización depende de los procedimientos, los procesos y las orientaciones operativas que son aplicadas al entorno. Contribuyen a la seguridad de una organización al incluir mucho más que

Operaciones	Su Importancia para la Seguridad
	meras defensas tecnológicas. La documentación precisa del entorno y la orientación resulta crítica para la habilidad del equipo en cuestión para gobernar, brindar soporte y mantener la seguridad del entorno.
Política de Seguridad	La política de seguridad corporativa se refiere al conjunto de políticas y orientaciones individuales que existen para administrar la seguridad y hacer un uso apropiado de la tecnología y los procesos dentro de la organización. Esta área cubre políticas que abordan todos los tipos de seguridad: en relación al usuario, el sistema y los datos.
Soporte y Recuperación	El soporte y recuperación de datos es esencial para el mantenimiento de la continuidad del negocio frente a un problema o falla del hardware o software. La falta de soporte apropiado y de procedimientos de recuperación puede llevar a una falta de datos y productividad de importancia. La reputación de la compañía y la marca pueden estar en peligro.
Gestión de Ajustes, Parches y	Una buena gestión de ajustes y

Operaciones	**Su Importancia para la Seguridad**
Actualizaciones	actualizaciones resulta importante para ayudar a la seguridad del entorno TI de su organización. La aplicación a tiempo de los ajustes y la actualización del mismo resultan necesarias para ayudar a protegerlo contra vulnerabilidades conocidas y explotables.
La Gente	**Su Importancia para la Seguridad**
Requisitos y Evaluaciones	Los requisitos de seguridad deben ser entendidos por todos aquellos que toman decisiones para que sus decisiones técnicas y comerciales realcen la seguridad más que entren en conflicto con el. La evaluación regular por parte de un tercero puede ayudar a que la compañía revise, evalué, e identifique las áreas plausibles de mejora.
Políticas y Procedimientos	Los procedimientos claros y prácticos para la administración de las relaciones con los proveedores y socios pueden ayudar a proteger la compañía de la exposición a riesgos. Los procedimientos que cubren la contracción y desvinculación de los empleados pueden ayudar a proteger la compañía contra los empleados inescrupulosos o que se han visto

La Gente	Su Importancia para la Seguridad
	contrariados.
Entrenamiento y Concientización	Los empleados deben ser entrenados y concientizados en lo que concierne a las políticas de seguridad y como la seguridad se aplica a las actividades laborales de a diario para no exponer a la compañía a riesgos mayores e inadvertidos.

(Microsoft)

4.2. NEXPOSE

Es una herramienta para la evaluación de vulnerabilidades, auditoria de cumplimiento de políticas y gerenciamiento de planes de remediación diseñado para grandes y pequeñas organizaciones que busquen altos niveles de escalabilidad, rendimiento, personalización y flexibilidad a la hora de implementar un producto de estas características en su infraestructura.

Evalúa vulnerabilidades en aplicativos web, bases de datos, redes, sistemas operativos, y otro tipo de software así también como diferentes dispositivos de red con el objetivo de localizar amenazas, identificar el nivel de riesgo que presentan para la infraestructura e idear un plan de remediación que reduzca de manera significativa el riesgo de seguridad y al mismo tiempo proteja la confidencialidad de los bienes digitales

5. CASO DE ESTUDIO

En este capítulo se muestra el procedimiento que se siguió para la elaboración del Plan de Seguridad de la Información que se realizó en Cotecmar (CORPORACIÓN DE CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO DE LA INDUSTRIA NAVAL, MARÍTIMA Y FLUVIAL**)**

5.1. Descripción del problema

Desde el año 2009 *COTECMAR* (Corporación De Ciencia Y Tecnología Para El Desarrollo De La Industria Naval, Marítima Y Fluvial**)** ha venido realizando grandes

inversiones en tecnologías que han contribuido en el aumento de la productividad de la Corporación, pero que a su vez han dejado abiertos riesgos en cuento a seguridad de la información, debido a que cuando se realizaron los planeamiento y la puesta en marcha de los servicios, no se evaluaron los riesgos que a nivel de seguridad de la información que se produce con la implementación de estas nuevas herramientas.

Esta es una temática que apenas viene estructurándose en la Corporación, ya que por el desconocimiento de sus consecuencias, no se ha realizado un análisis de riesgos que permita definir cuáles serían las debilidades a la que la empresa se encuentra expuesta, esto implicaría poner en riesgo información confidencial y sensible (investigaciones, diseños, patentes, proyectos etc.). Motivo por el cual no se han definido los proyectos a implementar para mitigarlos, así mismo no se ha asignado presupuesto para colocar en marca iniciativas que pudiesen cerrar estas brechas.

Por otra parte, la Corporación en su direccionamiento estratégico plasmó una serie de factores de riesgos en los cuales se evidencian las falencias en la oficina de tecnología de la información y comunicaciones TIC ya que no se cuenta con un Sistema Integrado de Información, Indicadores de medición, Soporte informático (cumplimiento de solicitud, calidad de servicio, servicio oportuno), Variación en tiempo de entrega e información gerencial. (Sistema Integrado de Información), de tal manera que sin este no se facilita el acceso a la información en tiempo real.

Así mismo, esta investigación estará fundamentada en mecanismo de evaluación con el cual se analizó la situación y se identificó los errores o informalidades de algunas procesos que son cruciales para mantener la organización en la oficina de tecnología de la información y comunicaciones TIC , a su vez se pretende realizar un estado del arte, en primera instancia para conseguir elementos de investigación referentes a lo estudiado y determinar en cierta medida cual ha sido el alcance de estos, en segunda instancia se realizara una comparación de dichos elementos y se sacaran conclusiones acerca de cuán importante es ha sido este estudio con el

trascurrir del tiempo, por último se sabrá con que cuenta la Corporación en su infraestructura para dar fundamento a esta iniciativa.

5.2. Alineación con el direccionamiento estratégico

Las necesidades en sistemas de información en las relaciones empresariales han conducido a Cotecmar (Corporación De Ciencia Y Tecnología Para El Desarrollo De La Industria Naval, Marítima Y Fluvial**)** a replantear los procesos internos y externos, soportada bajo una metodología de gestión proveniente del Project Management Institute (PMI).

Cotecmar, ha trazado en su direccionamiento estratégico 2012 -2022 sus Indicadores, metas e iniciativas en tres escenarios diferentes (corto, mediano y largo plazo), en los cuales las tecnologías de la Información y las Comunicaciones TIC´S ha plasmado sus metas en el marco de la variable V13 TIC. (Cotecmar, 2012)

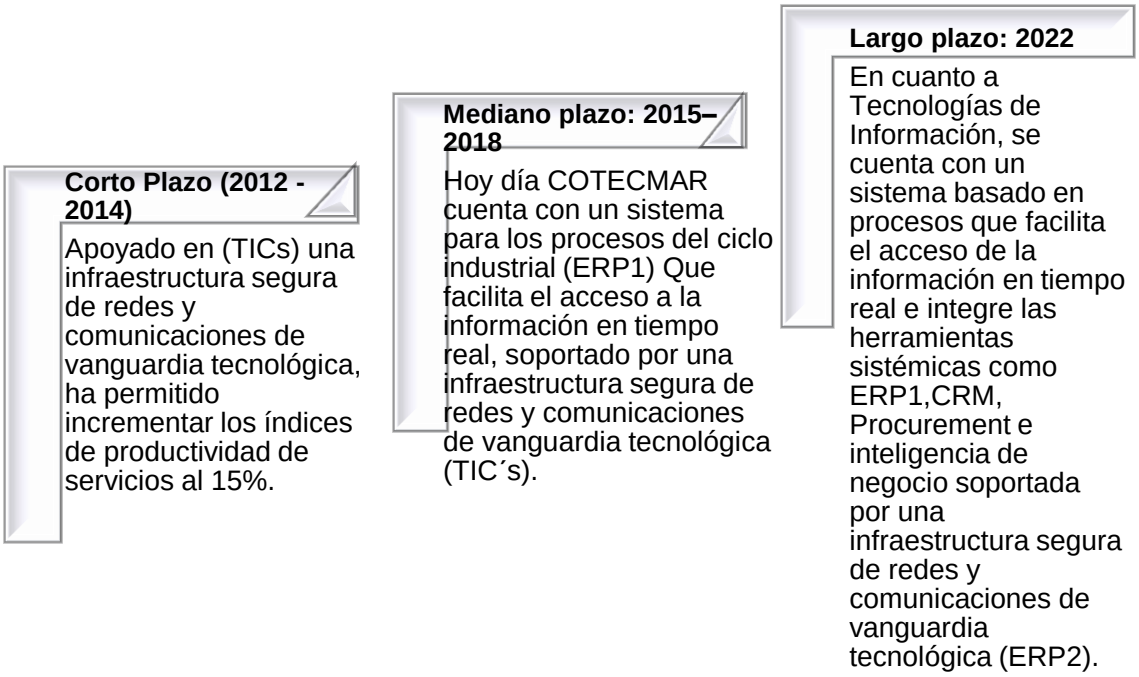


Figura 5-1 *Escenarios estratégicos de TIC según el direccionamiento estratégico de Corporación.*

5.3. Plan de acción

Para alcanzar las metas propuestas en cada escenario la corporación se ha trazado unas estrategias a corto, mediano y largo plazo a través de las cuales proyecta cumplir dicho reto ***Figura 5-2***

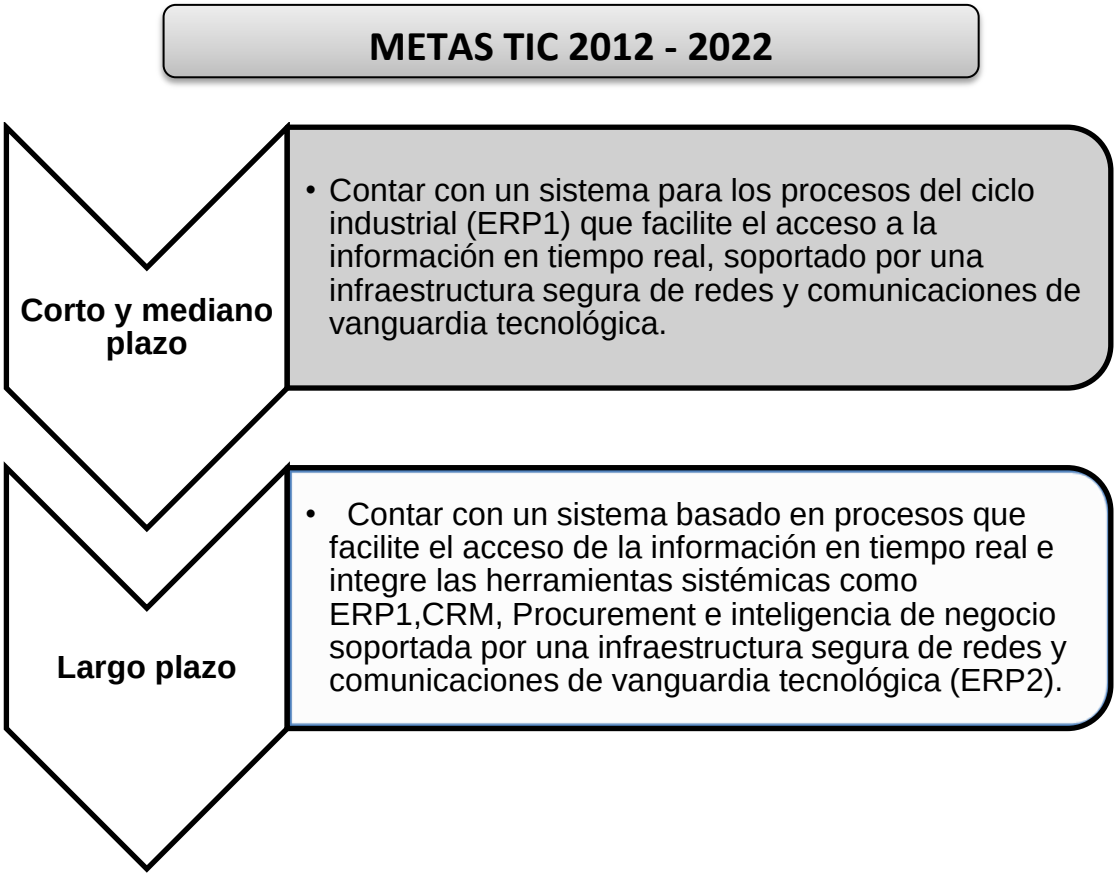


Figura 5-2 *Metas de TIC según el direccionamiento estratégico de Corporación.*

- Implementar un sistema de información que integre los procesos de gerencia de proyectos, financiera, logística y talento humano que garantice la interoperabilidad con los sistemas de ingeniería y de control de acceso.
- Adoptar un Sistema de Gestión de Seguridad de la Información para la Corporación.

- Implementar sistemas satelitales (portal de proveedores- E-Procurement, portal de clientes CRM, Balanced Scorecard -BSC, gestión documental, continuando con Ciclo de vida del producto PLM, Gestión de Cadena de Suministro SCM e Inteligencia de Negocios BI) integrados al sistema de información del ciclo industrial.

- Vigilar e implementar nuevas tecnologías de información y comunicación de vanguardia que contribuyan a la Corporación en posicionamiento en el mercado.

Como estrategia de medición y control la alta dirección de la Corporación ha estructurado el Balance Scorecard donde la variable TIC´S se encuentra dentro de la prospectiva “Aprendizaje y Conocimiento” y cuyo objetivo es “Asegurar la operatividad de servicios de tecnología de la información a través de soluciones seguras, oportunas y sostenibles”.

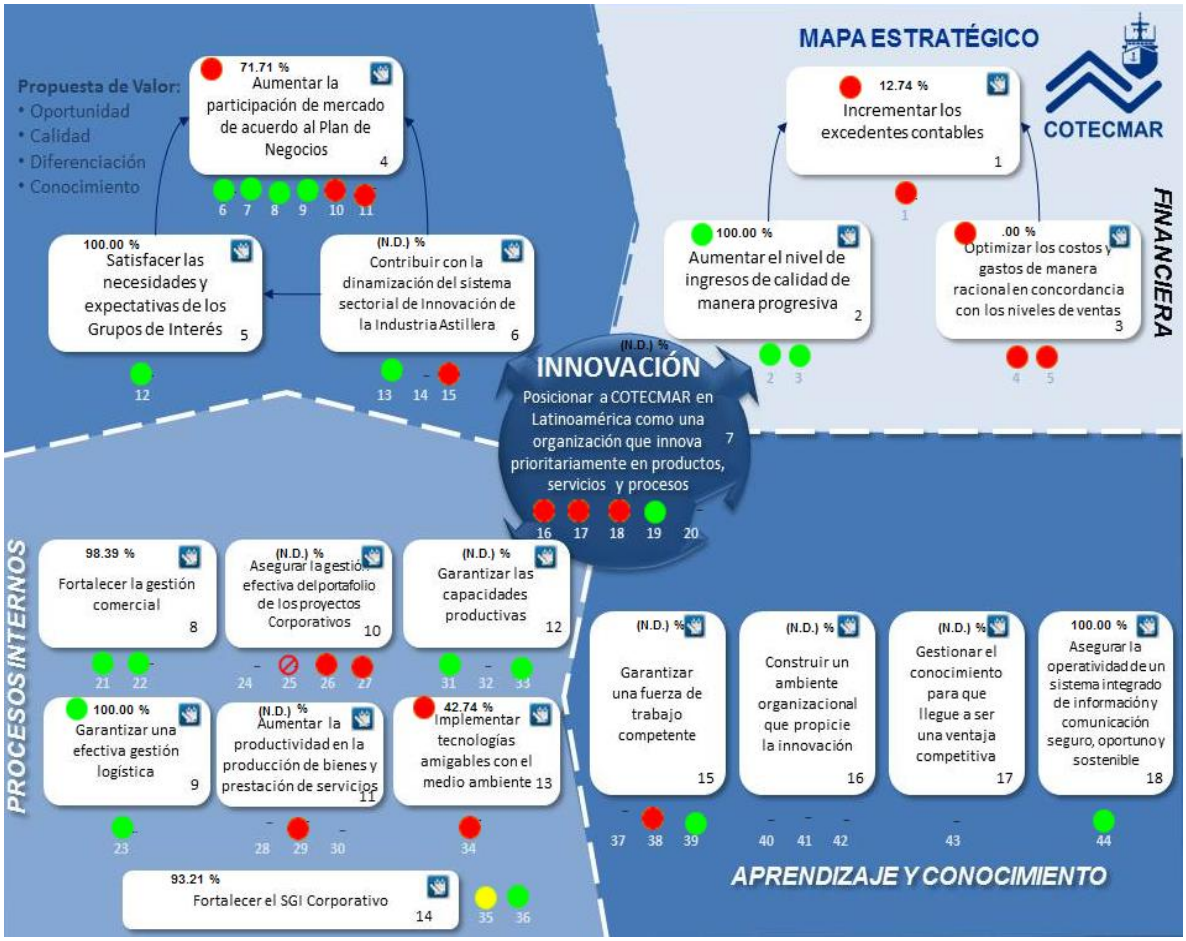


Figura 5-3 *Mapa Estratégico de Cotecmar*

Con el fin de garantizar el cumplimiento de los retos en cada uno de los escenarios Corporativos plasmados en el direccionamiento estratégico, la oficina de Tecnologías de la Información y las Comunicaciones debe de implementar soluciones que apoyen el Core del negocio, cuyas soluciones deben garantizar disponibilidad, oportunidad y seguridad en cada una de las transacciones que se realicen.

Teniendo en cuenta los proyectos tecnológicos a desarrollar por la oficina de TIC´S plasmados en el Plan Estratégico de Tecnología de la información PETI, la coordinación de seguridad de la información de la Corporación debe de implementar una serie de controles que vayan orientados a preservar la Integridad, confidencialidad y disponibilidad de la información contenida en esta herramienta de negocio, a través de técnicas como: Control de acceso, gestión de identidades SIEM, encriptación, certificados y firmas digitales, análisis de amenaza e identificación de vulnerabilidades, gestionado bajo el desarrollo de un plan de seguridad preventiva para cada una de las soluciones tecnológicas que aterrizan cada objetivo estratégico, como se indica a continuación:

Objetivo #1 del mapa estratégico "Incrementar los excedentes contables": La Oficina de tecnología contribuye a este objetivo en la medida que suministrando herramientas de software inicialmente desarrollado in-house y posteriormente con la implantación de una herramienta comercial tipo ERP que integre la sistematización de toda la cadena de valor del proceso de construcción y reparación de buques, con lo que se estará en capacidad de visualizar todas las transacciones que se realizan desde el momento en que se planea una venta, se ejecuta, se entrega el producto y se liquida, las que pasan por la cadena de abastecimiento, por talento humano y financiera y, en tiempo real.

Objetivo #2 "Aumentar el nivel de ingresos de calidad de manera progresiva"*:* para contribuir a este objetivo, la Oficina de TIC´S tiene contemplado implementar en el proyecto ERP II o ERP extendido una solución tipo CRM, con la

que se pueda realizar la gestión del mercadeo estratégico requerida por COTECMAR de manera que contribuya al propósito de crecimiento de las ventas y de financiamiento externo de la innovación, impactando a otras iniciativas como los son: la creación de empresas, al plan de negocios, a la expansión del negocio y por supuesto a la estrategia financiera que se adopte para la Corporación.

Para cada uno de los objetivos del direccionamiento estratégico donde la Oficina de Tecnologías de la Información y comunicaciones le impacta con sus soluciones tecnológicas, la Coordinación de seguridad de la información asegurará cada recurso de acuerdo a los tres pilares de la información de la siguiente forma:

- **Confidencialidad**: a través de la implementación de Control de acceso y criptografía.
- **Integridad:** A través de la implementación de control de acceso y firmas digitales.
- **Disponibilidad:** a través de monitoreo constante, análisis de riesgos, identificación de amenaza y vulnerabilidades y gestión de seguridad preventiva.

5.4. Personal Involucrado

Para el desarrollo del Plan de Seguridad de la Información, fue necesario incorporar el aporte y trabajo de los profesionales de todas las áreas, con el fin de desarrollar adecuadamente los proyectos de interés corporativos. Lo cual permitió dividir las responsabilidades, logrando la especialización en cada uno de los dominios de la norma -ISO 27001, obteniendo resultados de calidad satisfactoria.

Dentro del desarrollo se tuvo presente al siguiente personal:

a. Directivos.

Dada la magnitud y relevancia de la tarea, se tuvo de la participación activa de los más altos directivos de la Corporación ya sea para entregar las orientaciones básicas, como para tomar las decisiones que influyen en el modo de operar . Adicionalmente, fue importante contar con un fuerte liderazgo y compromiso de los directivos que soporte la intervención de los procesos que se buscan mejorar. El rol que cumplen, no puede delegarse sin una significativa pérdida de credibilidad respecto a la seriedad del esfuerzo.

b. Profesionales y técnicos.

La activa participación de profesionales y técnicos seleccionados, que entienden y manejan el desarrollo de los procesos dentro de la Corporación. Para lo anterior, es necesario que cumplan con los perfiles acordes al cargo, dado que ellos entregarán los antecedentes y atenderán los requerimientos en la práctica.

c. Otros funcionarios.

Además, fue necesario incluir a otro personal que pueda ser relevante para el correcto desarrollo del Plan. Cabe mencionar que también se incluyó al personal a cargo de la Gestión de Calidad, dueños de procesos estratégicos del servicio o de procesos de provisión de productos y servicios, personal del área de gestión de riesgo; abogados/as del área jurídica, RRHH, profesionales del área informática, entre otros.

5.5. Diagnostico situación actual de la seguridad de la información en base a la norma ISO 27001

La etapa de diagnóstico fue fundamental, ya que entregaron los lineamientos para el trabajo en las etapas siguientes:

Desde el punto de vista de Seguridad de la Información, se enfatizó la capacidad de generar valor mediante el uso de políticas, estándares y procedimientos de seguridad que, en complemento con las Tecnologías de Información y Comunicaciones (TIC), conforman un sistema de gestión administrado.

Sin embargo, el objetivo no es la incorporación de dichas tecnologías, de la normativa interna o el gobierno corporativo, sino la mejora de la gestión de las instituciones a través de ellas.

En este sentido, es indispensable que los servicios determinaron si sus áreas y divisiones requieren mejoras antes de intervenir en sus procesos, para no generar actividades de control que sean innecesarias, utilizando recursos que pueden aprovecharse en necesidades más urgentes en la corporación.

Es importante destacar que uno de los aspectos relevantes para la aprobación de esta etapa fue la identificación de los activos de información asociados a los procesos de provisión de bienes y servicios, y los riesgos a los que se encuentran sometidos, a fin de poder definir las medidas requeridas para su mitigación.

Es necesario que el encargado como también todos los funcionarios que tengan participación en el llenado del Inventario de Activos, cumplan con la totalidad de los pasos necesarios y requisitos técnicos, con el fin de lograr y asegurar un cumplimiento satisfactorio de la etapa de diagnóstico.

Para efectos del Diagnostico requerido en este sistema, se ha dispuesto una planilla electrónica de la Guía metodológica ISO27001

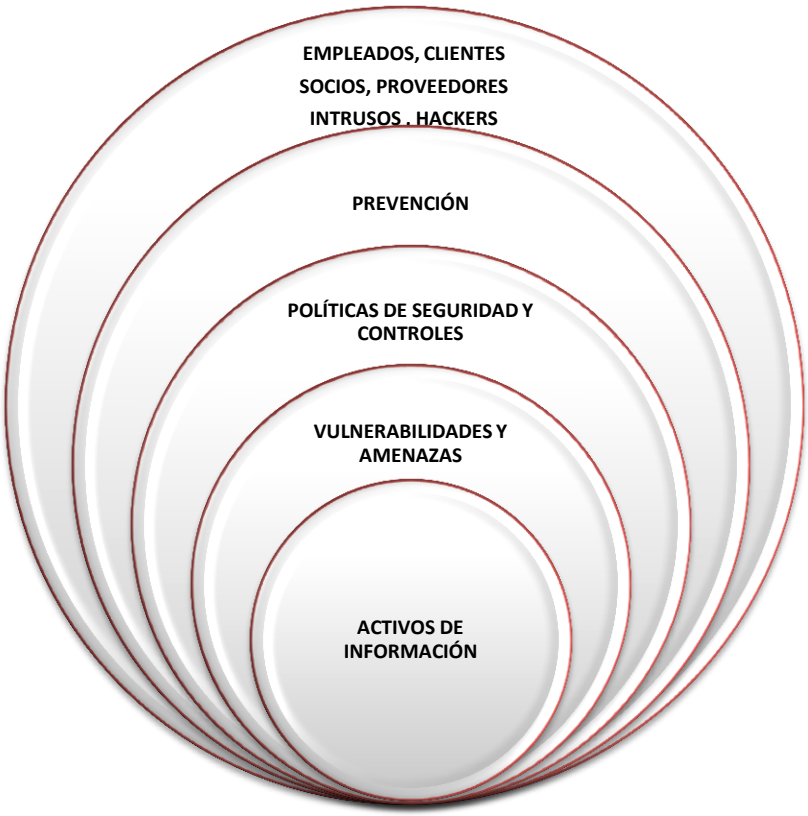
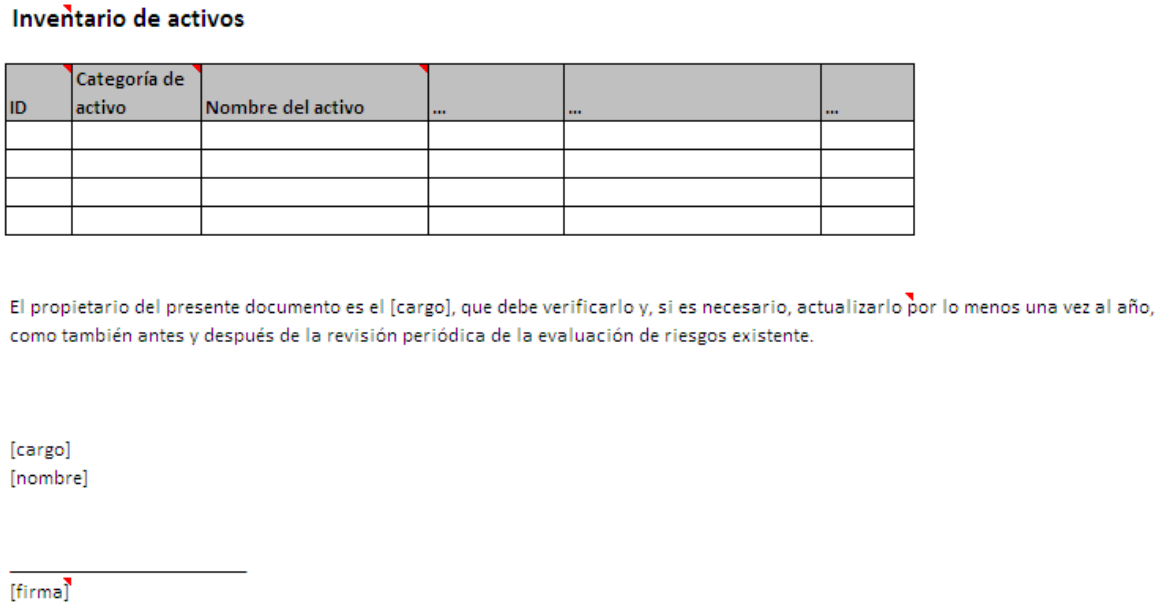


Figura 5-4 Esquema de Acceso a Activos de Información.

5.6. Elaboración del Inventario de Activos de Información.

El diagnóstico tuvo el foco en la correcta identificación de los activos de información de la Corporación, Dichos activos de Información son los que se requiere listar y caracterizar en la hoja Inventario

La elaboración de este inventario, permitió establecer el atributo de Criticidad de cada uno de los activos considerados. Los activos de información que resultaron con criticidad media y Alta fueron considerados para el análisis de riesgos.



Inventario de activos

ID	Categoría de activo	Nombre del activo	...	...	...

El propietario del presente documento es el [cargo], que debe verificarlo y, si es necesario, actualizarlo por lo menos una vez al año, como también antes y después de la revisión periódica de la evaluación de riesgos existente.

[cargo]
[nombre]

_____
[firma]

Figura 5-5 – Plantilla de Inventario de Activos

Con el fin de realizar una adecuada gestión de seguridad de la información y alcanzar los niveles exigibles dentro de la Corporación que contribuya a disminuir los riesgos y minimizar los daños en los activos de información, se realizó una fotografía del estado actual de la Corporación según de la norma ISO 27001 donde se realizó un mapeo por los diferentes dominios de la norma verificando el estado de implementación dentro de la organización:

Figura 5-6. *Dominios Mapeados de la ISO 27001*

Dentro de los 11 dominios mencionados anteriormente, abarcan los 39 objetivos y los 133 controles, donde se evaluó el nivel de implementación de estos dentro de

Caso de estudio: Cotecmar (Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial), en una escala de 1 a 5 de acuerdo a la siguiente clasificación:

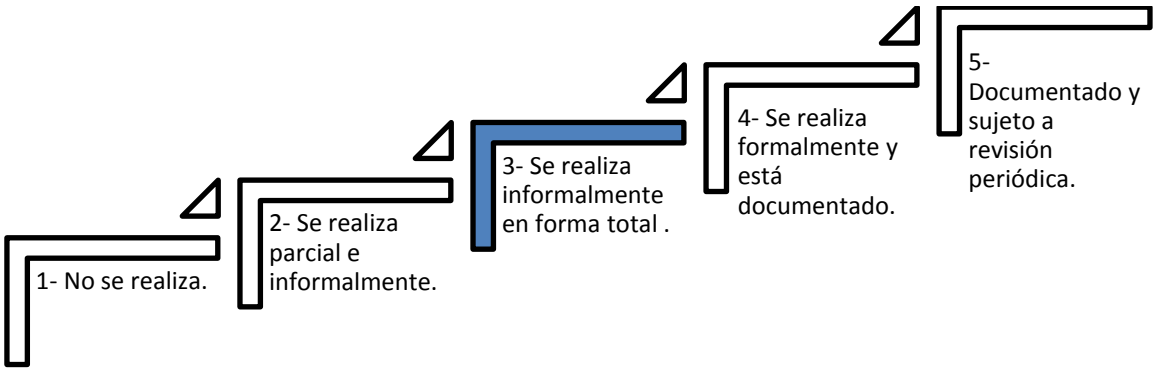


Figura 5-7 *Ítems de escala de evaluación.*

La clasificación a nivel de estado de cumplimiento para los controles de los dominios, se realiza de acuerdo a unos ítems en escala ascendente que muestran en qué fase se encuentra cada uno de los procedimientos, para que sean tomadas las respectivas medidas de control.

5.7. Indicadores de evaluación.

Tabla 5-1. *Indicadores de evaluación.*

Evaluación	Color	Valoración
Aceptable		≥4
Suficiente		<4
Deficiente		≤3
Obtenido		Resultado

Los indicadores de evaluación, muestran una medición general de cada uno de los dominios que se enmarcan en la norma ISO/IEC 27001, lo cual, como anteriormente se mencionaba fueron los criterios para fundamentar el estado actual de la Corporación en cuanto a la seguridad de la información. . Resultados ***de la evaluación***

Índice	Evaluación
3,76	**Suficiente**

Tabla 5-2. *Resultados tabulados por dominios.*

Después de haber realizado la evaluación, se lograron los siguientes resultados tabulados en la Tabla 2. Que expresan un índice porcentual calculado por cada dominio y que fue proporcionado con los indicadores de evaluación antes

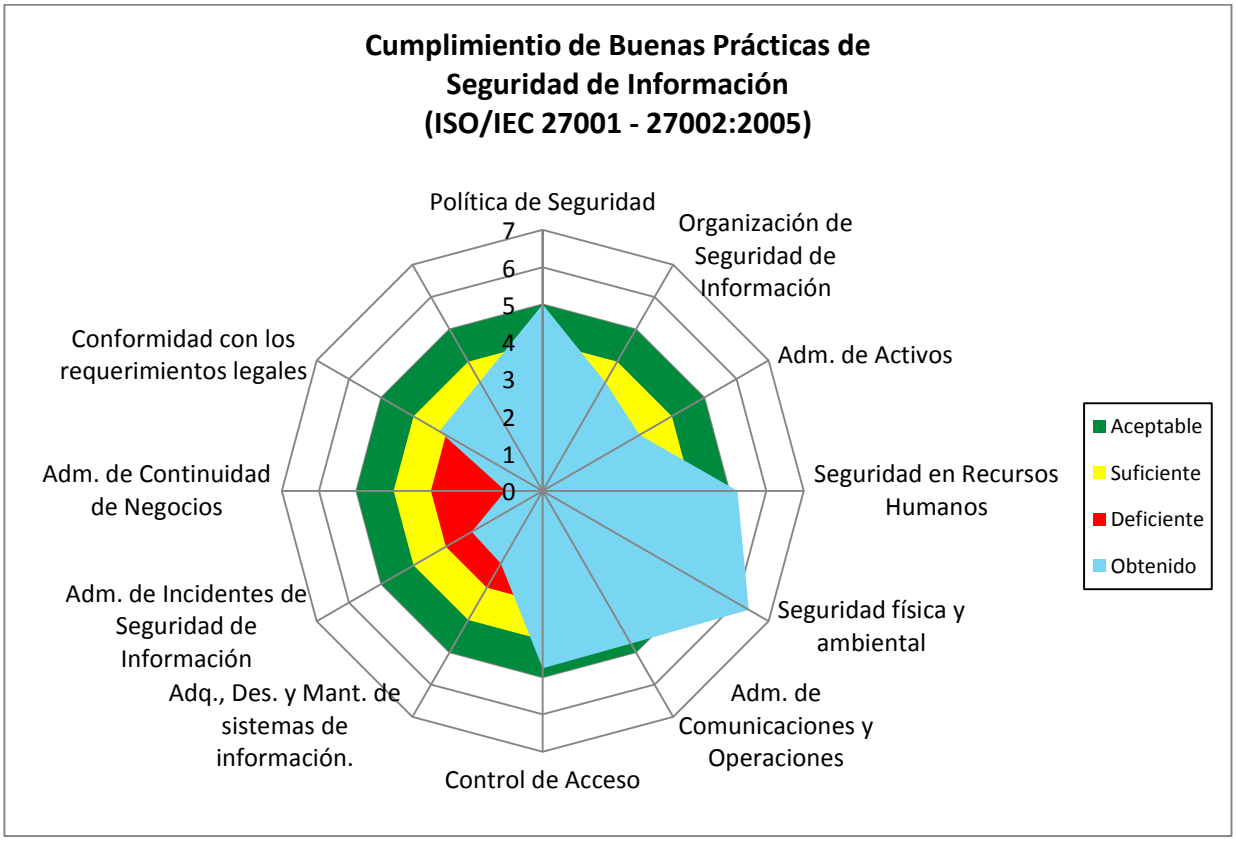
Cláusula	Índice	Evaluación
Política de Seguridad	5,00	Aceptable
Organización de Seguridad de Información	3,36	Suficiente
Adm. de Activos	3,00	Deficiente
Seguridad en Recursos Humanos	5,22	Aceptable
Seguridad física y ambiental	6,38	Aceptable
Adm. de Comunicaciones y Operaciones	4,73	Aceptable
Control de Acceso	4,76	Aceptable
Adq. Des. y Mant. de sistemas de información.	2,25	Deficiente
Adm. de Incidentes de Seguridad de Información	2,20	Deficiente
Adm. de Continuidad de Negocios	1,00	Deficiente
Conformidad con los requerimientos legales	3,20	Suficiente

mencionados. Notamos que en un estado *Deficiente* se encuentran los dominios de administración de continuidad de negocios (1,00), administración de incidentes de seguridad de información (2,20), adquisiciones, desarrollo y mantenimiento de sistemas de información (2,25) y administración de activos (3,00).

En estado de *Suficiente* se tienen los dominios de organización de la seguridad de la información (3,36) y conformidad con los requerimientos legales (3,20) y por

otra parte los dominios *Aceptable* están política de seguridad (5,00), seguridad en recursos humanos (5,22), seguridad física y ambiental (6,38), administración de comunicaciones y operaciones (4,73) y control de acceso (4,76).

Por ultimo nos muestra un total de 3.76, el cual es un promedio global de los anteriores en un estado *Suficiente*.



. Resultados de la evaluación

5.8. Análisis de la Situación

- Teniendo en cuenta el análisis de la herramienta MSAT **Microsoft Security Assessment Tool**, la figura a continuación representa los conceptos de la empresa descritos anteriormente y se basa en las respuestas que se

proporcionó. Se muestran las diferencias entre los resultados de DiDI (***Índice de Defensa en profundidad)*** y los resultados de BRP de la Corporación, organizados por área de análisis.

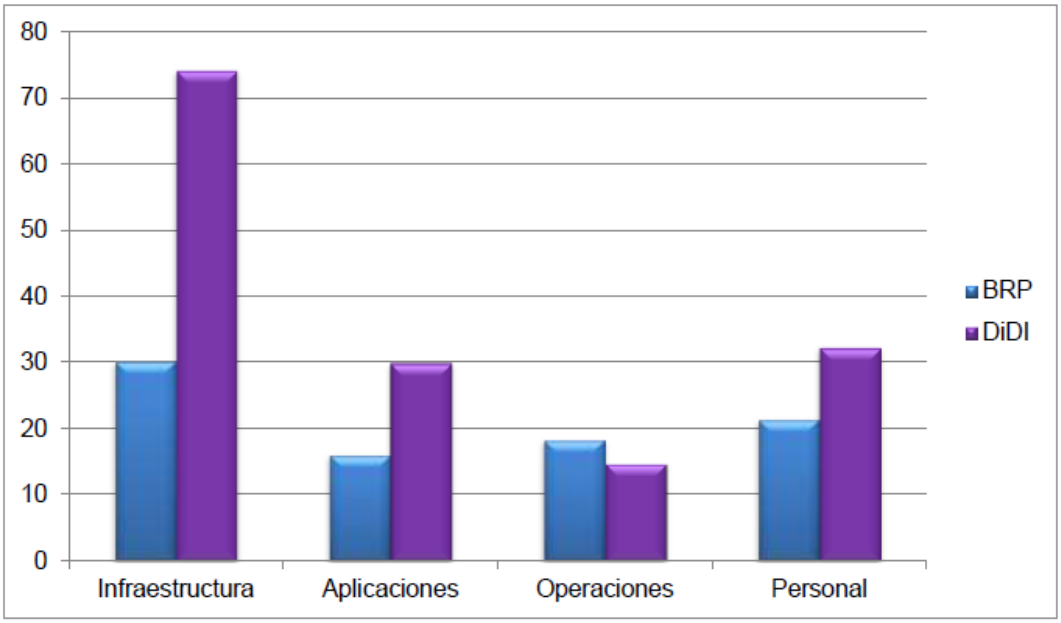
- BRP es una medición del riesgo relacionado al modelo empresarial y al sector de la empresa
- DiDI es una medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en la empresa.
- La madurez de la seguridad es una medición de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de diversas disciplinas.

De igual forma, para el análisis de la situación actual orientada en un contexto técnico con la herramienta MSAT, se tuvo en cuenta otro factor muy importante que es la madurez de la seguridad, que la definen como la medición de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de diversas disciplinas.

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Infraestructura	🔴	🟢
Aplicaciones	🟡	🟢
Operaciones	🟢	🔴
Personal	🟡	🟡

Tabla 5-3 ***Resultados autoevaluación de AoA con relación a la distribución de defensa de riesgo y madurez de la seguridad.***

Esta *Gráfica 1* se encuentra dividida en áreas de análisis, muestra las diferencias en el resultado de la defensa en profundidad



Gráfica 1. *Comparación de los BRP con DiDI en las áreas de análisis (AoA).*

1. La puntuación del BRP (Perfil de riesgos para la empresa) va de 0 a 100. Una puntuación más alta significa un riesgo posible aumentado al que está expuesta la corporación en esta área de análisis. Es importante tener en cuenta que una puntuación de 0 no es posible.
2. DiDI (Índice de Defensa en profundidad) también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno donde se han tomado más medidas para implementar estrategias de DiDi en el área de análisis específica.
   La puntuación DiDI no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno.

5.8.1. Madurez de la Seguridad

La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a

través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centrar los programas de seguridad de la empresa.

Los indicadores con los que se evalúa la madurez de la seguridad son los siguientes:

Básica: Algunas medidas proactivas de seguridad utilizadas como mecanismo de defensa inicial; respuesta a incidentes y operaciones aun en forma muy reactiva.

Estándar: Capas múltiples de defensa utilizadas para respaldar una estrategia definida.

Optimizada: Protección efectiva de lo correcto, en forma correcta y garantía de uso constante de las mejores prácticas recomendadas.

5.8.2. Tarjeta de puntuación

De acuerdo con las respuestas que se dieron acerca de la situación actual de la Corporación para la evaluación de riesgos, las medidas de defensa se calificaron de la siguiente forma.

Leyenda: ● Cumple las mejores prácticas recomendadas ● Necesita mejorar ● Carencias severas

Infraestructura	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
Antivirus	●
Antivirus - Equipos de escritorio	●
Antivirus - Servidores	●
Acceso remoto	●
Segmentación	●
Sistema de detección de intrusiones (IDS)	●
Inalámbrico	●
Autenticación	●
Usuarios administrativos	●
Usuarios internos	●
Usuarios de acceso remoto	●
Directivas de contraseñas	●
Directivas de contraseñas-Cuenta de administrador	●
Directivas de contraseñas-Cuenta de usuario	●
Directivas de contraseñas-Cuenta de acceso remoto	●
Cuentas inactivas	●
Gestión y control	●
Informes sobre incidentes y respuesta	●
Creación segura	●
Seguridad física	●
Aplicaciones	●
Implementación y uso	●
Equilibrio de carga	●
Clústeres	●
Aplicación y recuperación de datos	●
Fabricante de software independiente (ISV)	●
Desarrollado internamente	●
Vulnerabilidades	●
Diseño de aplicaciones	●
Autenticación	●
Directivas de contraseñas	●
Autorización y control de acceso	●
Registro	●
Validación de datos de entrada	●
Metodologías de desarrollo de seguridad de software	●
Almacenamiento y comunicaciones de datos	●
Cifrado	●
Cifrado - Algoritmo	●

Operaciones	●
Entorno	●
Host de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●
Directiva de seguridad	●
Clasificación de datos	●
Eliminación de datos	●
Protocolos y servicios	●
Uso aceptable	●
Gestión de cuentas de usuarios	●
Regulación	●
Directiva de seguridad	●
Gestión de actualizaciones y revisiones	●
Documentación de la red	●
Flujo de datos de la aplicación	●
Gestión de actualizaciones	●
Gestión de cambios y configuración	●
Copias de seguridad y recuperación	●
Archivos de registro	●
Planificación de recuperación ante desastres y reanudación de negocio	●
Copias de seguridad	●
Dispositivos de copia de seguridad	●
Copias de seguridad y restauración	●
Personal	●
Requisitos y evaluaciones	●
Requisitos de seguridad	●
Evaluaciones de seguridad	●
Directiva y procedimientos	●
Comprobaciones del historial personal	●
Directiva de recursos humanos	●
Relaciones con terceros	●
Formación y conocimiento	●
Conocimiento de seguridad	●
Formación sobre seguridad	●

5.8.3. Iniciativas de Seguridad

Se tiene que la evaluación para identificar el estado actual del entorno de tecnología de información y comunicaciones basado en la herramienta MSAT arrojó una serie resultados específicos, los cuales fueron fundamentados en el estándar internacional ISO/IEC 27001:2005 y la metodología NIST SP 800-30 que tienen en común una solución para la seguridad de la información a nivel organizacional. Cabe enfatizar que la principal función de la herramienta MAST es determinar los riesgos a los que se enfrenta una infraestructura informática y las medidas que ha adoptado para combatirlos, además de sugerir medidas adicionales para contribuir aún más a la reducción del nivel de riesgos.

Este procedimiento se llevó a cabo de la siguiente manera, se valoraron cuatros áreas de análisis especificas o medidas de defensa, estas son *infraestructura*, *aplicaciones*, *operaciones* y *personal*. Para empezar con el primer área tenemos que la *infraestructura* se encuentra en un estado "*necesita mejorar"* puesto que los indicadores de defensa del perímetro, autenticación, gestión y control y estación de trabajo, se están efectuando parcialmente y requieren ciertas mejores para que lleguen a un equilibrio conveniente y así cumplir con las mejores prácticas en seguridad de la información.

En segunda instancia se examinó el área de las *aplicaciones*, la cual se halla en un estado de "*carencias severas*" esto quiere decir que los factores de utilidad y uso, almacenamiento y comunicaciones de datos se efectúan de manera insuficiente y contrariamente el factor de diseño de aplicaciones se realiza de manera regular, entregando así de manera general en esta área el valor más bajo en su escala de puntuación.

En tercera instancia se analizó el área de las *operaciones*, cuyo estado también es de "*carencias severas*" pues los indicadores de entorno, directiva de seguridad, actualizaciones y gestión de actualizaciones, copias de seguridad y recuperación

son planificados y documentados de manera insuficiente, es decir no puede darle cumplimiento a las buenas prácticas requeridas.

Por último se realizó el análisis del área referente al "*Personal*" la cual se encuentra en un estado de "*carencias severas*" debido a que algunos de sus componentes como requerimientos y revaluaciones, directivas y procedimientos, formación y conocimientos, los cuales son apoyados con la gestión del talento humano no se están implementado de la mejor forma ocasionando una falla intolerable dentro del rango de valoración de la herramienta.

En las siguientes áreas no cumplen las mejores prácticas recomendadas por MSAT y deben dirigirse a aumentar la seguridad de su entorno.

Prioridad alta	Prioridad intermedia	Prioridad baja
• Acceso remoto • Usuarios administrativos • Planificación de recuperación ante desastres y reanudación de negocio • Desarrollado internamente • Creación segura	• Conocimiento de seguridad • Validación de datos de entrada • Formación sobre seguridad • Usuarios de acceso remoto • Archivos de registro	• Copias de seguridad • Antivirus - Equipos de escritorio • Antivirus - Servidores • Directivas de contraseñas-Cuenta de administrador • Directivas de contraseñas-Cuenta de usuario

Tabla 5-4 ***Subcategorías de áreas de análisis que no cumplen las mejores prácticas.***

5.9. Evaluación Detallada

Teniendo en cuenta los Ítem anteriores, en esta sección se encuentran los resultados detallados para cada categoría, así como las mejores prácticas, recomendaciones y referencias. Las recomendaciones son prioritarias.

5.9.1. Áreas de Análisis

La siguiente tabla enumera las áreas incluidas para el análisis de alto nivel de esta evaluación de riesgos para la seguridad y explica la relación entre cada área y la seguridad. La sección "Detalles de la evaluación" describe los niveles de seguridad de su empresa (según las respuestas aportadas en la evaluación) con respecto a cada una de estas áreas. Asimismo, se indican las prácticas más reconocidas del sector, además se ofrecen recomendaciones para implantar tales prácticas.

Categoría	Importancia para la seguridad
Perfil de riesgos para la empresa (BRP)	
Perfil de riesgos para la empresa (BRP)	Comprender como la propia naturaleza de la empresa afecta a los riesgos es importante a la hora de decidir dónde aplicar los recursos que ayuden a paliar tales riesgos. El reconocimiento de las áreas le permitirá optimizar la asignación del presupuesto de seguridad.
Infraestructura	
Defensa del perímetro	La defensa del perímetro trata la seguridad del perímetro de la red, donde su red interna conecta con el exterior. Este es su primer escudo protector contra los intrusos.
Autenticación	Los procedimientos estrictos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no accedan sin autorización a la red mediante ataques locales o remotos.
Gestión y control	La gestión, supervisión y el registro adecuados son elementos vitales para mantener y analizar los entornos informáticos. Estas herramientas son aún más importantes después de un ataque, cuando se necesita un análisis del incidente.
Aplicaciones	
Implantación y utilización	Cuando se implantan aplicaciones críticas para la empresa, hay que asegurar la seguridad y la disponibilidad de esas aplicaciones y de los servidores. El mantenimiento continuo es imprescindible para ayudarle a asegurarse de que los errores de seguridad se corrigen y que no se introducen nuevas vulnerabilidades en el entorno.
Diseño de aplicaciones	Un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, la autorización, y la validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad para acceder a información confidencial.
Almacenamiento y comunicaciones de	La integridad y confidencialidad de los datos son dos de las prioridades que

datos	debe garantizar cualquier empresa. La pérdida o el robo de datos puede afectar negativamente tanto a los ingresos de una entidad como a su reputación. Es importante comprender como las aplicaciones controlan y protegen los datos críticos.
Operaciones	
Entorno	La seguridad de una empresa depende de los procedimientos operativos, los procesos y las pautas que se aplican en el entorno. Pueden aumentar la seguridad incluyendo más que meras defensas tecnológicas. La capacidad del equipo de operaciones para mantener la seguridad del entorno depende de forma crucial de la documentación exacta del entorno y de las pautas.
Directiva de seguridad	La política de seguridad corporativa hace referencia a las directivas y a pautas individuales para regular el uso adecuado y seguro de las tecnologías y los procesos de la empresa. Esta área incluye las directivas para todos los aspectos de la seguridad, como los usuarios, los sistemas y los datos.
Gestión de actualizaciones y revisiones	La gestión adecuada de actualizaciones y revisiones es un factor importante para la seguridad del entorno informático de las empresas. La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y aquellas que podrían ser un frente de ataque.
Copias de seguridad y recuperación	Las copias de seguridad y la recuperación de datos son imprescindibles para el mantenimiento de la continuidad de los servicios comerciales en caso de un accidente o fallo de hardware o de software. La falta de procedimientos adecuados para realizar copias de seguridad y recuperación podría producir una pérdida significativa de datos y de productividad.
Personal	
Requisitos y evaluaciones	Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí. Las evaluaciones periódicas realizados por terceros independientes pueden ayudar a la empresa a revisar, evaluar e identificar las posibles mejoras.
Directivas y procedimientos	Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa. Los procedimientos para contratar aspirantes y finalizar sus contratos pueden proteger a la empresa contra empleados sin escrúpulos o descontentos.
Formación y conocimiento	Los empleados deben recibir formación para que sean conscientes de cómo las medidas de seguridad afectan a sus actividades diarias, para que no expongan a la empresa a mayores riegos de forma inadvertida.

5.10. Resultados de la evaluación del riesgo

Dicha evaluación se fundamentó en algunas normativas y metodologías internacionales que tiene como objetivo implantar buenas prácticas de seguridad de la información a nivel corporativo y en esta oportunidad servirán de guía a el *Plan Estratégico de Seguridad de la Información* de Cotecmar, abordando toda la temática referente a aplicaciones, servicios, infraestructura, personal y operaciones que deben estar regulados bajo unas políticas de seguridad de la información en un contexto organizacional.

Por tanto, como fue mencionado anteriormente en el diagnóstico del riesgo se emplea la metodología NIST SP 800-30 (*Guía de Gestión de Riesgos para Sistemas de Tecnología de Información*), la cual se basa en una matriz de nivel de riesgo de 3x3 de probabilidad de amenaza (alta, media y baja) y el impacto de la amenaza (alto, medio y bajo), con la cual se procura encontrar resultados acertados, que permitan disminuir el grado de riesgo que compromete a la Corporación. Seguidamente se ilustran las tablas que establece dicha metodología para realizar el proceso de evaluación de riesgo.

Escala de riesgo: Alto (> 50 hasta 100), Medio (>10 hasta 50) y Bajo (1 hasta 10).

Probabilidad de Amenaza	**Impacto**		
	Bajo (10)	**Medio (50)**	**Alto(100)**
Alta (1.0)	Bajo 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100

Media (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Baja (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10

Tabla 5-5*Matriz de nivel de riesgo según metodología NIST SP 800-30*

(Nist 800-30)

Las definiciones de la probabilidad de amenaza se explican mediante la siguiente tabla:

Nivel de Probabilidad	Definición de Probabilidad
Alta	La fuente de amenaza está altamente motivada y es lo suficientemente capaz, y los controles para prevenir que se explote una vulnerabilidad son inefectivos.
Media	La fuente de amenaza está motivada y es capaz, pero los controles implementados pueden impedir la explotación exitosa de una vulnerabilidad.
Baja	La fuente de amenaza carece de motivación y capacidad, o los controles implementados previenen la explotación de una vulnerabilidad, o al menos la dificultan significativamente.

Tabla 5-6 *Definición de Probabilidad de Amenaza*

(Nist 800-30)

Las definiciones de magnitud de impacto se explican mediante la siguiente tabla:

Tabla 5-7 Definición de Magnitud de Impacto

Magnitud de Impacto	Definición de Magnitud de Impacto
Alta	La explotación de una vulnerabilidad (1) puede resultar en una alta pérdida de los principales activos tangibles o recursos, (2) puede significar violación, daño o dificultad de la misión, reputación o interés de la organización, (3) puede resultar en muerte humana
Media	La explotación de una vulnerabilidad (1) puede resultar en una Pérdida de los activos tangibles o recursos, (2) puede significar violación, daño o dificultad de la misión, reputación o interés de la
Baja	La explotación de una vulnerabilidad (1) puede resultar en la pérdida de algunos activos tangibles o recursos, (2) puede afectar notablemente a la misión, reputación o interés de la organización.

Caracterización del Sistema

Dentro del inventario de activos críticos que se incluyó para la evaluación de los riesgos, estuvo un grupo de servidores y aplicaciones in-house y ERP relevantes para el negocio, que actualmente cumplen con la sistematización de procesos en varias áreas de la Corporación. A continuación se mostrar una tabla con los activos críticos de TIC:

Tabla 5-8. *Activos críticos de la Corporación que fueron evaluados.*

ACTIVOS CRITICOS DE TECNOLOGÍA DE LA INFORMACIÓN	
Activo / Servicio	**Descripción**
Servidor SUITE VISION	Servidor para herramienta de BSC para manejo de información gerencial
Servidor TSM	Servidor de herramienta que realiza las copias de seguridad a todos los servidores
Servidor Microsoft Lync Server 2010	Servidor donde corre la plataforma de comunicaciones unificadas, que integra distintos formatos de comunicación (mail, chat, telefonía IP, etc.)
EDGE Server Lync 2010	Servicio de Lync para enrutar llamadas entrantes y salientes
Servidor INFOR ERP XA	Servidor de producción de la herramienta ERP que optimiza procesos de ingeniería, configuración, manufactura y ensamblaje a pedido y elaboración a stock.

Controlador de Dominio Bogotá	Servidor que tiene como función administrar toda la información correspondiente a usuarios y recursos de la sucursal Bogotá
Controlador de Dominio Primario Mamonal	Controlador de dominio principal que administra toda la información correspondiente a usuarios y recursos de sede Mamonal
Controlador de Dominio Secundario Mamonal	Controlador de dominio de respaldo del controlador de dominio principal de sede Mamonal
Antivirus Trend Micro	Servidor de antivirus corporativo para la detención y eliminación de virus informáticos.
File Server SUB, DIRCON y DIRFAD	Servidor de archivos de las direcciones de construcciones, financiera y submarinos
File Server DIDESI	Servidor de archivos de la dirección de Investigación, desarrollo e Innovación
Servidor de	Servidor donde corren todas las aplicaciones

Aplicaciones In-house	desarrolladas in house de la Corporación.
Servidor Tribon Mamonal	Servidor de herramienta de diseño e ingeniería de buques sede Mamonal
Servidor Microsoft Exchange	Servidor donde corre el servicio de cuentas de correo electrónico de usuarios.
Servidor Microsoft SharePoint	Servidor donde correo la herramienta de colaboración Share Point (PKM)
Controlador de dominio Bocagrande	Controlador de dominio administra toda la información correspondiente a usuarios y recursos de sede Bocagrande
Servidor Tribon Bocagrande	Servidor de herramienta de diseño e ingeniería de buques sede Bocagrande
Servidor FTP	Servidor de FTP- compartir archivos.

Identificación de Amenazas

Para el estudio fueron consideradas una serie de amenazas potenciales y sus acciones asociadas, que son descritas en sus categorías como ambientales, humanas, técnicas y organizacionales, las cuales son aplicables a la oficina de tecnología de información y comunicaciones.

Tabla 5-9. *Fuentes de Amenazas*

Amenazas Ambientales	
Fuentes de Amenaza	**Acciones de Amenaza**
Movimiento telúrico	• Destrucción infraestructura física (edificación/hardware). • Daño al personal.
Tormenta Eléctrica	• Falla eléctrica (suspensión del servicio de energía eléctrica). • Daño de equipos.
Inundación	• Falla eléctrica • Daño en equipos y redes de datos • Perdida de información • Indisponibilidad de servicios
Falla Eléctrica/Suspensión del servicio de energía eléctrica	• Daño de equipos. Indisponibilidad de los servicios. • Fallo en la integridad de la información. • Desconfiguración de aplicaciones y/o servicios.
Humedad/Sobrecalentamiento	• Daño de equipos. • Incomodidad para el personal y usuarios en el desenvolvimiento de sus actividades.

Animales (roedores, insectos, aves)	• Daños en equipos.

Tabla 5-10. *Fuentes de Amenazas*

Amenazas Humanas	
Fuentes de Amenaza	**Acciones de Amenaza**
Pérdida de Personal	• Suspensión y desorganización del soporte y de las tareas que se encuentran a su cargo.
Hacker, cracker	• Ingeniería social. • Intrusión al sistema, allanamiento. • Acceso no autorizado al sistema.
Vandalismo	• Daño de equipos. • Penetración al sistema. • Manipulación al sistema.
Personal y usuarios internos (deficiente capacitación, descontento, malicia, negligencia, error, deshonestidad, o empleados cesados, limpieza incorrecta, frustración)	• Chantaje. • Abuso de computación. • Fraude y robo. • Abuso de computación. • Fraude y robo. • Pérdida de confidencialidad e integridad de los datos: entrada de datos falsificados, corrompidos. • Destrucción negligente de equipos, cables y datos. • Código malicioso (Ej. virus, bomba lógica, caballo de Troya). • Venta/intercambio de información personal. • Fallas del sistema. • Intrusión al sistema.

	• Sabotaje al sistema. • Acceso no autorizado al sistema.
Incorrecta administración del sistema y de los derechos de acceso a los datos	• Fallas en el sistema. • Accesos no autorizados. • Pérdida de confidencialidad. • Utilización innecesaria de recursos.
Robo	• Costos para reposición de equipos. • Inoperatividad del sistema. • Falta de disponibilidad. • Pérdida de confidencialidad.

Tabla 5-11. *Fuentes de Amenazas*

Amenazas Técnicas	
Fuente de Amenaza	**Acciones de Amenaza**
Falla en un componente	Falla en las operaciones del sistema. Daño en equipos.
Falla del proveedor de Internet	Suspensión de aplicaciones y servicios (que dependan del servicio de Internet).
Inoperatividad de controles existentes	• Falta de protección de los activos/recursos. • Daño de los activos/recursos. Accesos no autorizados. • Falla en el sistema
Vulnerabilidades o errores de software	• Falla en el sistema. • Falta de protección de los activos/recursos. • Pérdida de confidencialidad, integridad y disponibilidad.

Virus, bombas lógicas, caballo de Troya(código malicioso)	• Falla en el sistema. • Pérdida de confidencialidad, integridad y disponibilidad.

Tabla 5-12 Fuentes de Amenaza

Amenazas Organizacionales	
Fuente de Amenaza	**Acciones de Amenaza**
Falta o insuficiencia de reglas	• Deficiencia en la gestión de recursos y operaciones. • Pérdida de confidencialidad de la información.
Monitoreo insuficiente de las Medidas de Seguridad TI	• Incidentes que afecten a la imagen y seguridad de la organización.
Uso no controlado de recursos	• Falla o daño de los recursos y/o del sistema. • Mal uso de los recursos por parte del personal y usuarios.
Pobre ajuste a cambios en el uso de TI	• Falla en el sistema.
Falta de, o inadecuada documentación	• Daños en la operación. Mantenimiento inadecuado.
La estrategia para el sistema de red y el sistema de gestión no está establecida	• Problemas de instalación, configuración y operación de nuevos componentes en la red y en el sistema de gestión. Conexiones no autorizadas a la red
Falta de estaciones de trabajo estandarizadas	• Dificultad en la instalación y mantenimiento. • Dificultad en la seguridad TI

Falta o insuficiencia de Gestión de la Seguridad de TI	• Falta de responsabilidad del personal. • Inadecuado soporte de gestión. • Inadecuados requerimientos estratégicos y conceptuales. • Inversión insuficiente o mal encaminada. • Impracticabilidad de conceptos de salvaguardas. • Falla para actualizar los procesos TI.
Falta de licencias de software propietario y/o violación de derechos de autor	• Sanciones legales.

Identificación de Vulnerabilidades

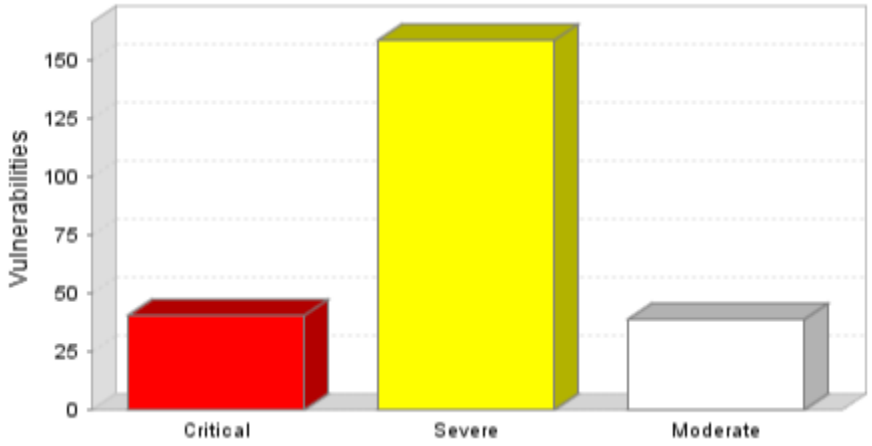
A continuación se presentan las vulnerabilidades criticas detectas a través del estudio del estado actual de la oficina de tecnología de información, las cuales se categorizan como ambientales, técnicas, humanas y organizacionales. También se incluyeron las vulnerabilidades críticas detectadas por las herramientas de auto escaneo Nexpose.

De acuerdo con la herramienta Nexpose se pudieron identificar 237 vulnerabilidades. De ellos, 40 eran vulnerabilidades críticas, las cuales requieren inmediata atención.

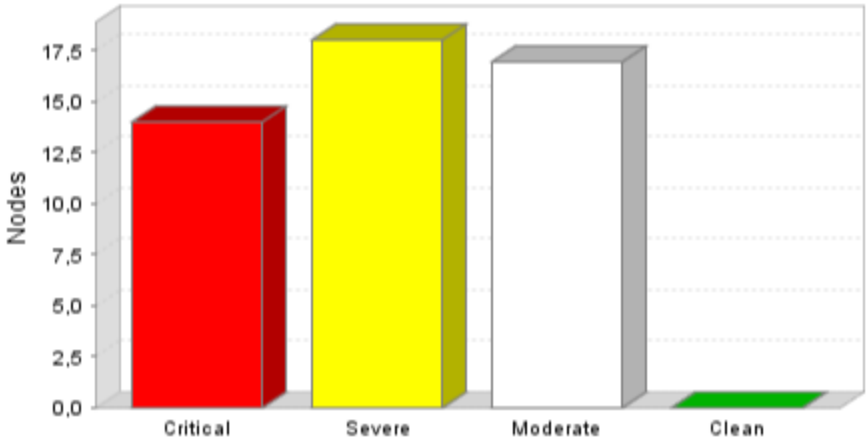
158 vulnerabilidades fueron graves, estas son a menudo más difíciles de explotar y no pueden proporcionar el mismo acceso a los sistemas afectados.

Había 39 vulnerabilidades moderadas. Estas a menudo proporcionan información a los atacantes que pueden ayudarles a montar ataques

posteriores de la red. Estos también deben fijarse en el momento oportuno, pero no son tan urgentes como las otras vulnerabilidades.



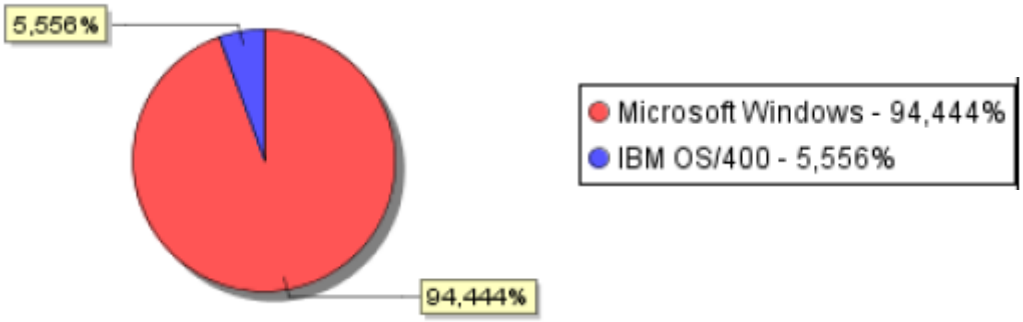
Gráfica 2- Vulnerabilidad por gravedad



Gráfica 3- ***Nodos de gravedad de las vulnerabilidades***

Había 2 sistemas operativos identificados durante esta exploración. El sistema operativo Microsoft Windows se encontró en 17 sistemas, por lo que es el sistema operativo más común.

Hubo 42 servicios encontrados estar corriendo durante esta exploración.



Gráfica 4 - Sistema Operativos más comunes

En las siguientes tablas se pueden observar las vulnerabilidades que se identificaron por la herramienta Nexpose.

Tabla 5-13 Vulnerabilidades

Vulnerabilidades Ambientales
No se tiene generadores de energía eléctrica de respaldo para las diferentes sedes de Cotecmar, (actualmente sólo se tiene para la planta Mamonal).
Daño de equipos y servidores producto de fallas y tormentas eléctricas.
Daño en equipos y servidores producto de inundación.
Des configuración de equipos y aplicaciones por fallas ambientales.
Daño en equipos de cómputo y aires acondicionados producto de sobrecalentamiento y/o humedad, produciendo pérdida de información.
Daños en equipos y cableado por roedores.

Tabla 5-14 Vulnerabilidades Humanas

Vulnerabilidades Humanas
El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades de seguridad.
Existe desconocimiento sobre el debido manejo de la información.
No Identificación de riesgos relacionados con partes o personas externas.
Ausencia de directrices de seguridad en el trato con clientes de la corporación.
No existe proceso disciplinario para los empleados que abran brechas de seguridad.
No hay controles suficientes para asegurar la validación y no alteración de los datos (integridad).
No hay controles suficientes para asegurar la validación y no alteración de los datos (integridad), y que las funciones del sistema trabajan para lo que han sido destinadas.
No hay controles que restrinjan la instalación de paquetes de software por usuarios finales.
No hay documentación suficiente que explique el uso del software/hardware.
No se protege suficientemente la integridad de los datos y aplicaciones.
Los usuarios pueden ejecutar remotamente código arbitrario.
Descentralización de las responsabilidades de seguridad de la información

Vulnerabilidades Técnicas
No están identificados las operaciones críticas y sus respaldos.
Falta de revisión de los controles de seguridad del sistema.
Las versiones de los paquetes usados en el levantamiento de servicios y aplicaciones no están actualizadas y/o libres de fallas o errores.
No se administra el sistema para reducir posibles vulnerabilidades.
Existen vulnerabilidades de software que permiten obtener información de la red y re direccionar maliciosamente el tráfico.
Se puede obtener información clave de red, sistema operativo, servicios que están corriendo, programas instalados de los equipos, e información sensible mediante el acceso a recursos o por escaneos de red.
Las configuraciones de algunos de los servicios no se realizan tomando en cuenta la seguridad de la información.

Tabla 5-15 Vulnerabilidades Técnicas

Paso 4. Análisis de Controles Paso 5. Determinación de Probabilidad Paso 6. Análisis del Impacto

Paso 7. Determinación del Riesgo.

A continuación se ilustra una tabla donde se agrupan los pasos 4, 5, 6 y 7 de la metodología NIST SP 800-30, esta muestra los riesgos existentes junto con valoración, de acuerdo a la evaluación de probabilidad y análisis del impacto que cada riesgo presente. Así mismo se indican los controles según sea la amenaza establecida.

Vulnerabilidades	Fuentes de Amenazas	Probabilidad	Impacto	Riesgo	Controles
CATEGORIA: AMBIENTALES		Valoración			
No se tiene generadores de energía eléctrica de respaldo para las diferentes sedes de Cotecmar, (actualmente sólo se tiene para la planta Mamonal).	Falla eléctrica (suspensión del servicio de energía eléctrica).	Medio	Alto	Medio	Adquirir e instalar generadores eléctricos para las plantas bocagrande.
Daño de equipos y servidores producto de fallas y tormentas eléctricas.	Tormenta Eléctrica	Bajo	Alto	Bajo	ACEPTAR
Daño en equipos y servidores producto de inundación.	Inundación	Medio	Alto	Medio	TRASFERIR El riego a proveedor de seguros.
Desconfiguración de equipos y aplicaciones por fallas ambientales.	Movimiento telúrico	Bajo	Bajo	Bajo	ACEPTAR
Daño en equipos de cómputo y aires acondicionados producto de sobrecalentamiento y/o humedad, produciendo pérdida de información.	Humedad/Sobrecalentamiento	Medio	Alto	Medio	Realizar inspección constante del sistema electrico y ductos de agua potables con el fin de prevenir incidentes.

Tabla 5-16 Determinación del Riesgo Ambientales

Vulnerabilidades	Fuentes de Amenazas	Probabilidad	Impacto	Riesgo	Controles
CATEGORIA: HUMANAS		Valoración			
El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades de seguridad.	Pérdida de Personal	Alto	Alto	Alto	Realizar capacitaciones y divulgación semestral sobre las políticas y controles de seguridad existentes en la Corporación.
Existe desconocimiento sobre el debido manejo de la información.	Hacker, cracker	Alto	Alto	Alto	Realizar divulgación a funcionarios existentes y a los que ingresan sobre las mejores prácticas y manejo de la información.
No Identificación de riesgos relacionados con partes o personas externas.	Vandalismo	Bajo	Medio	Bajo	ACEPTAR
Ausencia de directrices de seguridad en el trato con clientes de la corporación.	Personal y usuarios internos	Medio	Alto	Medio	Socialización de directrices de seguridad a clientes Corporativos.
No existe proceso disciplinario para los empleados que abran brechas de seguridad.	Personal y usuarios internos	Medio	Alto	Medio	Incluir dentro del reglamente interno del trabajo las sanciones previstas por incumplimiento a las directrices de seguridad de la información.

No hay controles suficientes para asegurar la validación y no alteración de los datos y aplicaciones (integridad).	Incorrecta administración del sistema y de los derechos de acceso a los datos	Alto	Alto	Alto	Implementar cotroles eficientes para garantizar la integridad tales como control de acceso y firmas digitales.
No hay controles que restrinjan la instalación de paquetes de software por usuarios finales.	Personal y usuarios internos	Alto	Alto	Alto	Implementar por controlador de dominio la inhabilitación automática de privilegios administrativos del usuasrio final sobre las estaciones de trabajo.
No hay documentación suficiente que explique el uso del software/hardware.	Hacker, cracker	Alto	Medio	Medio	Centralizar (en lo posible de manera electrónica) y bajo segmentación de roles, perfiles y privilegios la consulta de dicha información por parte del personal interesado.
Los usuarios pueden ejecutar remotamente código arbitrario.	Hacker, cracker	Medio	Alto	Medio	Implementar soluciones que demarquen las zonas de memoria no ejecutable, para evitar ser explotadas.

Tabla 5-17 Determinación del Riesgo Humanas

Vulnerabilidades	Fuentes de Amenazas	Probabilidad	Impacto	Riesgo	Controles
CATEGORIA: TECNICAS		Valoración			
No están identificadas las operaciones críticas y sus respaldos.	Falla en un componente	Alto	Alto	Alto	Identificar los procesos críticos del negocio dentro de un plan de continuidad del negocio.
Falta de revisión de los controles de seguridad del sistema.	Inoperatividad de controles existentes	Medio	Alto	Medio	Centralizar y revisar las configuraciones y parametrizaciones de los diferentes sistemas operativos y herramientas.
Las versiones de los paquetes usados en el levantamiento de servicios y aplicaciones no están actualizadas y/o libres de fallas o errores.	Vulnerabilidades o errores de software	Alto	Alto	Alto	Realizar monitoreo constante de los diferentes parches y actualizaciones con el fin de implementar los que sean pertinentes para el negocio.
No se administra el sistema para reducir posibles vulnerabilidades.	Inoperatividad de controles existentes	Alto	Alto	Alto	Inspeccionar los diferentes servicios y aplicaciones de TIC´S con el fin de realizar una evaluación de vulnerabilidades por lo menos de manera semestral.

Existen vulnerabilidades de software que permiten obtener información de la red y redireccionar maliciosamente el tráfico.	Vulnerabilidades o errores de software	Alto	Alto	Alto	Realizar escaneo de puerto, y protocolos de red con el fin de evitar que código o herramientas mal intensionadas obtengan información de la red.
Las configuraciones de algunos de los servicios no se realizan tomando en cuenta la seguridad de la información.	Inoperatividad de controles existentes	Alto	Alto	Alto	Que toda solicitud de acceso a herramienta tecnológica, implementación y/o cambio sea validada por el área de seguridad de la información.
Las cuentas de usuario invitado y sesión anónima se encuentran habilitadas y no son monitoreadas.	Virus, bombas lógicas, caballo de Troya(código malicioso)	Medio	Alto	Medio	Validar las conexiones remotas y cuentas por defecto e invalidarlas en lo posible (sin afectar el normal funcionamiento de los servicios tecnológicos)

Tabla 5-18 Determinación del Riesgos Técnicas

Vulnerabilidades	Fuentes de Amenazas	Probabilidad	Impacto	Riesgo	Controles
CATEGORIA: ORGANIZACIONALES		Valoración			
No se cuenta con planes de continuidad del negocio que incluyan seguridad de la información en la Corporación.	Falta o insuficiencia de Gestión de la Seguridad de TI	Alto	Alto	Alto	Realizar un plan de continuidad del negocio para la Corporación.
No se realiza verificación periódica de los sistemas de información para asegurar conformidad con los estándares de implantación de seguridad.	Monitoreo insuficiente de las Medidas de Seguridad TI	Alto	Medio	Medio	Realizar monitoreo período de los sistemas de información y verificar el cumplimiento de estos con respecto a los estándares.
No se tiene contacto con autoridades que regulen la seguridad de la información a nivel nacional para las organizaciones.	Falta o insuficiencia de Gestión de la Seguridad de TI	Medio	Medio	Medio	Realizar contacto con entidades de seguridad de la información con el fin de escalar requerimientos en caso de ser necesario. (CSIRT de la policía. etc..)
No se evalúa periódicamente el riesgo al que se encuentra expuesta la Corporación,ni se ha determinado un nivel aceptable de riesgo.	Falta o insuficiencia de Gestión de la Seguridad de TI	Medio	Alto	Medio	Realizar una evaluación semestral del riesgo referente a seguridad de la información, con los respectivos planes de miigación.
No hay control de cambios en los sistemas de información.	Pobre ajuste a cambios en el uso de TI	Medio	Alto	Medio	Normalizar e implementar el procedimiento de control de cambios para TIC´S

El personal no entiende el riesgo de los sistemas a su cargo.	Falta o insuficiencia de Gestión de la Seguridad de TI	Alto	Alto	Alto	Realizar concientización de los riesgos a los que se expone cada funcionario producto de la utilización de las herramientas tecnológicas y de la información allí contenida.
No existe un plan de seguridad que gestione la Seguridad TI.	Falta o insuficiencia de Gestión de la Seguridad de TI	Alto	Alto	Alto	Formular e implementar un plan de seguridad de la información para el corto, mediano y largo plazo.
No se realizan auditorias internas en las cuales se revisen los procedimientos de seguridad de la información que se dan en la organización.	Falta o insuficiencia de Gestión de la Seguridad de TI	Medio	Alto	Medio	Gestionar dentro de la organización la creación de un área de auditoría interna.

Tabla 5-19 Determinación del Riesgo Organizacional

Paso 9. Documentación de Resultados

Después de que se elaboró la evaluación de riesgos basada en la metodología NIST SP 800-30 fueron estimados los niveles de la probabilidad de ocurrencia de una vulnerabilidad potencial, el impacto de las fuentes de amenazas y los riesgos a los que encuentra expuesto la Corporación, mediante unos valores de "*Alto*", "*Medio*" y "*Bajo*", según se establecen en la metodología antes mencionada.

Cabe resaltar que en esta matriz de evaluación de riesgo se realizó una agrupación de vulnerabilidades, fuentes de amenazas y controles que podrían mitigar o eliminar los riesgos identificados. También se debe tener en cuenta que aquellos riesgos de nivel "alto" son la prioridad principal para ser disminuidos en un tiempo corto, ya que pueden comprometer con facilidad el activo más importante de la Corporación (Información). Dentro de los controles a ejecutar de estos riesgos se tiene, realizar capacitaciones y divulgación semestral sobre las políticas y controles de seguridad existentes en la Corporación, realizar divulgación a funcionarios existentes y a los que ingresan sobre las mejores prácticas y manejo de la información, implementar controles eficientes para garantizar la integridad tales como control de acceso y firmas digitales, centralizar los derechos de acceso a los diferentes sistemas de información de la Corporación y fortalecer el equipo de trabajo del proyecto, entre otros que están especificado en la matriz de evaluación riesgo.

Así mismo los riesgos de nivel "Medio" se deben considerar seguidamente relevante, ya que a pesar de que no se encuentran en un nivel alto, no quiere decir que no impactaran sobre los activos críticos de la compañía en un largo plazo. Dentro de los controles a ejecutar de estos riesgos tenemos, Adquirir e instalar generadores eléctricos para las plantas Bocagrande, Realizar inspección constante del sistemas eléctricos y ductos de agua potables con el fin de prevenir incidentes, Incluir dentro del reglamente interno del trabajo las sanciones previstas

por incumplimiento a las directrices de seguridad de la información, entre otros que están especificado en la matriz de evaluación riesgo basada en la metodología NIST SP 800-30.

Por ultimo mencionaremos los riesgos de nivel "*Bajo*" los cuales contrariamente a los dos anteriores sencillamente deben ser aceptados, porque aunque no dejan de ser un riesgo latente para la Corporación, en algunos casos su ocurrencia no depende de esta.

CONCLUSIONES

En toda esta investigación se puede concluir en varios puntos que se detallan a continuación:

1. Situación Actual: Se realizó un análisis del estado actual de seguridad de la Corporación. Para ello el análisis de riesgos evaluó el nivel actual, luego se definió a dónde quiere llegar la Corporación y se determinó actividades necesarias para cerrar esa brecha.

2. De acuerdo al cumplimiento de la norma ISO 27001, se identificó por medio del estado del arte de los dominios, en un nivel de “Suficiente” con un 3.76 a la Corporación, de cumplimiento respecto a un nivel máximo de 5 puntos, esto en cuanto a la situación actual de la gestión de seguridad de la información.

   Los dominios sobre los cuales se debe realizar mayor trabajo son: administración de activos con un puntaje de 3.0, adquisición, desarrollo y sostenimiento de Sistemas de Información con puntaje de 2.25, administración de incidentes de seguridad de la información con un puntaje de 2.20 y administración de continuidad de negocio con un puntaje de 1.0.

3. Se plasmó iniciativas o proyectos a corto, mediano y largo plazo requerido para el cierre de las brechas identificadas en el estado del arte y las valoraciones de riesgos.

4. El Alinear el direccionamiento estratégico de la corporación permitió levantar la visión del proyecto alineada con la visión del negocio e

identificar los objetivos corporativos a los cuales se apunta desde el área de seguridad de la información.

5. De acuerdo a los resultados arrojados al proceso de Gestión de Riesgos De acuerdo por la herramienta de autoevaluación MSAT, para el análisis de Riesgos y Nexpose para detectar las vulnerabilidades, riesgos y amenazas se indicó que las áreas de análisis "aplicaciones", "operaciones" y "personal" de la Corporación, se encuentra en un nivel de "**carencias severas**" el cual puede ser corregido colocando en prácticas las iniciativas que esta misma propone

6. A través de la evaluación del riesgo realizada con base a la metodología NIST SP 800-30, se pudo determinar las brechas de seguridad (vulnerabilidades Vs. Amenazas), que permitió identificar los controles que se deben implementar para los riesgos que en materia de seguridad de la información se encuentra expuesta la Corporación.

7. Se hace imprescindible la realización de cada uno de las iniciativas sugeridas en este proyecto de investigación en aras de continuar con el proceso para obtener la certificación del "Sistema de Gestión de Seguridad de la Información" de la norma internacional ISO 27001.

RECOMENDACIONES

- Se recomienda establecer en las organizaciones la administración de seguridad de la información, es decir involucrar a todo el personal del área en la administración de la seguridad con el debido apoyo total de las TIC (Tecnologías de la Información y las Comunicaciones).
- Fomentar la conciencia del empleado para garantizar que no haya fuga de la información.
- Realizar Auditorías a la Seguridad de la Información de las empresas para tener un conocimiento de sus vulnerabilidades y que procedimientos seguir para minimizar los riesgos.
- Proporcionar al área de sistemas los recursos necesarios para mantener la seguridad de la Información en la empresa.

Orientadas al Caso de Estudio *(Cotecmar - Corporación De Ciencia Y Tecnología Para El Desarrollo De La Industria Naval, Marítima Y Fluvial)*

De acuerdo al estado de seguridad encontrado en el estado del arte los diferentes dominios de la norma ISO 27001 y las vulnerabilidades detectadas con herramientas como MSAT a continuación:

EN BASE LOS DOMINIOS DE LA NORMA ISO 27001

A continuación se presentan recomendaciones a implementar en los diferentes dominios de la norma ISO 27001 cuya valoración se encuentra entre los niveles 1 y 2 de una escala nivel 5, donde 1 corresponde a “No se realiza” y 2 a “se realiza parcialmente e informalmente”:

Organización de Seguridad de Información			
N°	**Controles**		**Recomendaciones**
1.	Participación de la Gerencia en Seguridad de Información.	La gerencia debe prestar apoyo activo a seguridad dentro de la organización a través de directrices claras, participación demostrable, asignaciones explícitas y conocimiento de sus responsabilidades en seguridad de información.	Se recomienda la creación de un comité de seguridad integral, que incluya las funciones de seguridad de la información cuyas funciones estén definidas corporativamente mediante directiva permanente.
2.	Coordinación de Seguridad de Información	Las actividades de seguridad de información deben ser coordinadas por representantes de las diferentes partes de la organización con roles y funciones laborales relevantes.	Se recomienda implementar la política y distribuir de la mejor forma los roles y funciones a las personas directamente involucradas en el tema de seguridad de la información en la corporación.
3.	Asignación de responsabilidades de seguridad de información	Todas las responsabilidades de seguridad de información deben estar claramente definidas.	Se recomienda centralizar las responsabilidades de cada proceso de seguridad de la información, fortalecer el equipo

			de trabajo y documentar con claridad el propósito de cada proceso.
4.	Proceso de autorización para la instalaciones de procesamiento de información	Debe existir un proceso definido e implantado para la autorización gerencial de nuevas instalaciones de procesamiento de información.	Se recomienda documentar los procesos de instalación que requieran autorización de la alta gerencia, con el fin de regularizar y sean evidenciados.
5.	Contacto con autoridades	Debe mantenerse contactos apropiados con autoridades relevantes.	Se recomienda establecer contactos con autoridades a nivel nacional que regulen la seguridad informática como son el COLCERT, El Comando Conjunto Cibernético y El Centro Cibernético Policial.
6.	Contacto con grupos de interés especial	Debe mantenerse contacto apropiado con grupos de interés especial u otros foros especializados y asociaciones profesionales.	Se recomienda establecer contactos con empresas líderes en seguridad de la información a nivel nacional e internacional, y suscribirse a foros y comunidades expertas en este tema.
7.	Revisiones independientes de seguridad de información	El acercamiento de la organización a la administración de seguridad de información y su implantación, deben ser revisados de manera independiente a intervalos planificados o cuando ocurra un cambio significativo en la implantación de seguridad.	Se recomienda programar revisiones continuas a las políticas de seguridad y procedimientos que se implantaron, para constatar su vigencia y garantizar la seguridad de la información de la organización.

8.	Identificación de riesgos relacionados con partes externas	Los riesgos para la información de la organización y sus instalaciones de procesamiento producidos por procesos de negocios que involucren partes externas deben ser identificados y los controles apropiados deben ser implantados antes de entregar acceso.	Se recomienda implementar una política de control al ingreso de todo el personal de entidades externas que realice trabajos con la información de la corporación, con el fin de establecer clausuras de confidencialidad de dicha información.
9.	Directriz de seguridad en el trato con clientes	Todos los requerimientos de seguridad identificados deben ser señalados antes de entregar acceso a los clientes a la información de la organización o sus activos.	Se recomienda implantar una política en donde se establezcan clausuras de confidencialidad con los clientes en cuento a seguridad de la información que sea manipulada en las instalaciones de la corporación.
Administración de Activos			
#	**Control**		**Recomendaciones**
10.	Inventario de Activos	Todos los activos deben estar claramente identificados, elaborando y manteniendo un inventario de todos los activos relevantes.	Se recomienda centralizar el proceso de inventario a nivel general de todos los activos con que cuenta la oficina de TIC y mantenerlo constantemente actualizado.
11.	Guías para clasificación	La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización.	Se recomienda poner en marcha la política de clasificación de la información para priorizarla y brindarle la protección adecuada a la misma.
12.	Manejo y etiquetado de información	Un apropiado conjunto de procedimientos para etiquetado y manejo de información debe ser desarrollado e implantado en conformidad con el esquema de	Se recomienda implementar la política de manejo y etiquetado de la información para que pueda ser fácilmente identificada y tengo una mejor organización

		clasificación adoptado por la organización.	para la persona encargada.
Seguridad en Recursos Humanos			
#	**Control**		**Recomendaciones**
13.	Capacitación, educación y entrenamiento en seguridad de información.	Todos los empleados de la organización y, cuando sea relevante, los contratistas y los usuarios de terceras partes deben recibir capacitación, entrenamiento y actualizaciones regulares en las políticas y procedimientos de la organización que sean relevantes a su función laboral.	Se recomienda realizar divulgación de las buenas prácticas en seguridad de la información a usuarios finales, mediante capacitaciones y charlas con el fin de crear una cultura de concientización acerca de cómo preservar y proteger el activo principal de la organización.
14.	Proceso disciplinario	Debe existir un proceso disciplinario formal para aquellos empleados que produzcan brechas de seguridad.	Se recomienda promulgar una política de seguridad que permita sancionar a los usuarios que vulneren los controles o mecanismos de seguridad existentes en la corporación.
15.	Remoción de derechos de acceso	Los privilegios de acceso de todos los empleados, contratistas y usuarios de terceras partes a información o instalaciones de procesamiento deben ser removidos al término del empleo, contrato o acuerdo. En caso de cambio de función, deben ser ajustados.	Se recomienda centralizar el procedimiento para que sea la coordinación seguridad de la información en conjunto con el área de recursos humanos los encargados de la remoción de usuarios del sistema y aplicaciones específicas.

Seguridad física y ambiental			
#	Control		Recomendaciones
16.	Ubicación y protección de equipos	El equipamiento debe ser ubicado o protegido para reducir los riesgos producidos por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Se recomienda instaurar normas de protección que permitan reducir el riesgo dando una buena ubicación y protección los equipos. Así mismo considerar una variabilidad del espacio donde se albergan los equipos críticos para que cumpla las condiciones recomendables.
17.	Seguridad de equipos fuera de las instalaciones propias	La seguridad debe aplicarse a los equipos fuera de los instalaciones físicas de la organización tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización	Se recomienda instruir al usuario final para que se concientice de los riesgos que puedo sufrir la información al salir de las instalaciones, instalar herramientas de encriptación de la información y adquirir pólizas de seguro para la protección de equipos que salen de las instalaciones.
18.	Seguridad en el reciclaje y deshecho de equipos	Todos los ítems de equipamiento que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier información sensible o software licenciado ha sido eliminado o sobrescrito previo a su eliminación.	Se recomienda poner en acción política de seguridad que establece procedimiento formal para el proceso de eliminación de la información confidencial en equipos.
19.	Remoción de propiedad	El equipamiento, información o software no debe ser sacado de las instalaciones físicas de la organización sin autorización previa.	Se recomienda mantener un procedimiento documentado para la salida de equipos de las instalaciones de la corporación e implementar un mecanismo para hacerle seguimiento hasta que este sea retornado.

Administración de Comunicaciones y Operaciones			
#	Control		Recomendaciones
20.	Procedimientos documentados de operación	Procedimientos operacionales deben ser documentados, mantenidos y puestos a disposición de todos los usuarios que los necesiten.	Se recomienda realizar un levantamiento de todos los procesos y procedimiento de la oficina de TIC y de igual manera debe mantenerse actualizado y en constante revisión.
21.	Administración de cambios	Los cambios en instalaciones de procesamientos de información y sistemas deben ser controlados.	Se recomienda implementar procedimiento para tener una mejor administración de los cambios que se realizan en el sistemas, aplicaciones y en equipos y puedan ser evidenciados de las mejor forma.
22.	Separación de instalaciones de desarrollo, pruebas y operación	Las instalaciones de desarrollo, prueba y producción deben estar separadas para recudir el riesgo de acceso no autorizado o cambios en el sistema en producción.	Se recomienda ejecutar la separación del desarrollo, pruebas y producción en todas las aplicaciones existentes en la organización para poder disminuir el riesgo de ser vulnerados por personal no autoriza.
23.	Aceptación de sistemas	Criterios de aceptación para nuevos sistemas, actualizaciones y nuevas versiones deben ser establecidos y deben ejecutarse pruebas apropiadas de él o los sistemas antes de su aceptación.	Se recomienda documentar detalladamente este procedimiento para evidenciar posibles fallas e inconvenientes que se pueden presentar a corto, media o a largo plazo después del proceso de implementación de dicho sistema.

24.	Controles contra código malicioso	Controles de detección, prevención y recuperación deben ser implantados para protegerse contra el código malicioso. Debe implantarse un procedimiento de concientización de usuarios.	Se recomienda concientizar al usuario final para que no sea engañado y pueda tomar medidas en el momento de que se produzca un acontecimiento con códigos maliciosos. Además este proceso debe ser documentado para llevar un seguimiento de estas afectaciones.
25.	Eliminación de medios	Los medios deben ser eliminados, de manera segura, utilizando procedimientos formales, cuando no vayan a ser requeridos.	Se recomienda emprender la política de eliminación de medios, de tal manera que la información no sea extraída con fines maliciosos (borrado seguro) y de igual manera debe documentarse formalmente.
26.	Procedimientos de manejo de información	Procedimientos de manejo y almacenamiento de información deben ser establecidos para proteger esta información de divulgaciones no autorizadas o mal uso.	Se recomienda establecer una política de seguridad para este procedimiento, de tal forma de que se lleve un buen control tanto de la información física como lógica que se maneja en la corporación.
27.	Seguridad de la documentación de sistemas	El sistema de documentación debe estar protegido contra acceso no autorizado.	Se recomienda centralizar el proceso de documentación de los sistemas apoyándose en la coordinación de seguridad informática, para que exista una mejor organización y un constante seguimiento.
28.	Procedimientos y políticas de intercambio de información	Política forma de intercambio, procedimientos y controles deben ser implantados para proteger el intercambio de información a través de todos los tipos de facilidades de comunicación.	Se recomienda poner en marcha la política de seguridad de la información que contempla el procedimiento de intercambio de información y debe ser instaura para cualquier medio de comunicación en que se emita.

29.	Sistemas de información de negocios	Políticas y procedimientos deben ser desarrollados e implantados para proteger la información asociadas con la interconexión de sistemas de información de negocios.	Se recomienda realizar una implementación completa para que el sistema de información funciones de la mejor manera y siempre cumpla con los pilares de la seguridad (confidencialidad, integridad y disponibilidad).
30.	Transacciones en línea	La información involucrada en transacciones en línea debe ser protegida para prevenir transmisiones incompletas, pérdidas de ruta y alteraciones, divulgación, duplicación o replicación no autorizada de los mensajes.	Se recomienda iniciar mecanismos de seguridad como firmas digitales y certificados digitales para asegurar las transacciones en línea que se realicen en la corporación.
31.	Monitoreo de Uso de sistemas	Procedimientos para monitorear el uso de las instalaciones de procesamiento de información deben ser establecidos y los resultados del monitoreo de actividades deben ser revisados regularmente.	Se recomienda evidenciar este procedimiento mediante documentación formal de manera permanente y que sirva de constancia ante cualquier incidente que se pueda presentar en el sistema.
32.	Protección de la información de registro.	Las instalaciones e información de registros deben ser protegidas contra la alteración y acceso no autorizados.	Se recomienda tener una política de seguridad donde se tenga un procedimiento formal en el que se otorgue privilegios solo a personal autorizado para que acceda a estos registro del sistema y evitar que sean alterados o accedidos por personal no autorizado

Control de Acceso			
#	Control		Recomendaciones
33.	Política de Control de Acceso	Una política de control de acceso debe ser establecida, documentada y revisada basándose en los requerimientos de negocios y seguridad.	Se recomienda implementar y documentar procedimiento de control de acceso para garantizar la seguridad de la información de la Corporación.
34.	Administración de Contraseñas de usuarios	La asignación de contraseñas debe ser controlada a través de un proceso formal de administración.	Se recomienda cifrar todas las contraseñas de usuarios y documentar el procedimiento para que sea realizado de manera formal.
35.	Revisión de derechos de acceso de usuarios	La administración debe revisar periódicamente los privilegios de acceso según un procedimiento formal.	Se recomienda realizar revisiones constantes de las políticas de acceso a usuarios para evitar accesos no autorizados y procurar formalidad documental.
36.	Política de Escritorio y Pantalla limpios	Una política de escritorios limpios de papeles y medios removibles y una política de pantallas limpias de para instalaciones de procesamiento de información deben ser adoptadas.	Se recomienda poner en marcha la política de escritorio y pantallas limpias, para que la información no este alcance ni pueda ser manipulado en caso que se realiza un acceso no autorizado.
37.	Política de Uso de Servicios de Red.	Los usuarios tendrán acceso a aquellos servicios de red a los que han sido específicamente autorizados.	Se recomienda autorizar a los usuarios solo los servicios que requieran en la red y también divulgar la política del uso de estos, para que sean utilizados de

			la mejor forma.
38.	Control de rutas de redes	Controles de ruteo deben implantarse en las redes para asegurar que las conexiones de computadores y flujos de información no producirán brechas en la política de control de acceso a las aplicaciones de negocios.	Se recomienda pedir la documentación a la entidad que presta este servicio y realizar controles periódicos a esta configuración para evitar abrir brechas lógicas en la red. Adicionalmente se recomienda realizar escaneos de red para detectar conexiones indeseadas.
39.	Uso de herramientas del sistema	El uso de herramientas de sistema capaces de sobrescribir controles de sistemas y aplicaciones debe ser restringido y estrictamente controlado.	Se recomienda implementar control por los sistemas de información (Dominio) para evitar que usuarios con privilegios no administrativos instalen software y/o herramientas de escaneo.
40.	Time-out de sesiones	Las sesiones inactivas deben ser eliminadas después de un periodo predefinido de inactividad.	Se recomienda adoptar la política de sesiones inactivas y formalizar la documentación que se necesita para evidenciarla.
41.	Limitación del tiempo de conexión	Tiempos de restricción de conexiones deben ser utilizados para brindar seguridad adicional a las aplicaciones de alto riesgo.	Se recomienda accionar política de seguridad la cual limita de tiempos de conexión, ofreciendo integridad y disponibilidad del sistema.

Adquisición, desarrollo y mantenimiento de sistemas de información.			
#	Control		Recomendaciones
42.	Validación de datos de entrada	Los datos de entrada a aplicaciones deben ser validados para asegurar que los datos son correctos y apropiados.	Se recomienda ejecutar validaciones de los datos de entrada de las aplicaciones, por su respectivo responsable.
43.	Control de procesamiento interno	Puntos de verificación deben ser incluidos en las aplicaciones para detectar cualquier corrupción de información por errores de procesamiento o actos deliberados.	Se recomienda generar puntos de verificación por el responsable de la aplicación y de igual manera documentar el procedimiento con detalles específicos.
44.	Validación de datos de salida	Los datos de salida de las aplicaciones deben ser validados para asegurar que el procesamiento y la información almacenada es correcta y apropiada a la circunstancias.	Se recomienda ejecutar validaciones de los datos de salida de las aplicaciones, por su respectivo responsable.
45.	Administración de llaves	Debe existir Administración de Llaves criptográficas para apoyar el uso de técnicas criptográficas por parte de la organización.	Se recomienda implementar herramienta de encriptación de información y definir política de seguridad que enfatiza en la administración de llaves criptográficas para brindar confidencialidad de la información a la Corporación.
46.	Control de Software	Deben existir	Se recomienda mantener

	Operacional	procedimientos implantados para controlar la instalación de software en sistemas operacionales.	controles en su totalidad de este procedimiento y difundir la política de seguridad a los usuarios finales de la organización, adicionalmente implementar controles por sistemas de información.
47.	Protección de datos de prueba de sistemas	Los datos de prueba deben ser cuidadosamente seleccionados, protegidos y controlados.	Se recomienda instaurar la política de protección de datos de prueba, con el fin de controlar y ofrecer la confidencialidad, integridad y disponibilidad de la información.
48.	Control de acceso a código fuente de programas	El acceso al código fuente de programas debe ser restringido.	Se recomienda que se centralice el control de los códigos fuentes de las aplicaciones, con la intensión de guardar confidencialidad y disponibilidad de estos.
49.	Procedimiento de Control de Cambios	La implantación de controles debe ser controlada a través del uso de un procedimiento formal de control de cambios.	Se recomienda documentar estrictamente cada cambio que se realice a los sistemas o aplicaciones, para formalizar de una manera forma el procedimiento.

50.	Revisión técnica de aplicaciones después de cambios al sistema operativo	Cuando un sistema cambie, las aplicaciones de negocios críticas, deben ser revisadas y probadas para asegurar que no existe un impacto adverso en las actividades de la organización o en la seguridad.	Se recomienda que el responsable de soporte realice seguimiento a los usuarios finales cuando se dé un cambio del sistema operativo para garantizar la continuidad de la operación y también sea registrado cada cambio para evidenciarlo en error futuros.
51.	Fuga de información	Oportunidades de fuga de información deben ser prevenidas.	Se recomienda implementar mecanismos y herramientas para prevenir y detectar fugas de información.
52.	Desarrollo de software externalizado	El desarrollo de software externalizado debe ser supervisado y monitoreado por la organización.	Se recomienda realizar supervisión y monitoreo del software durante toda su implementación y puesta en marcha en la Corporación, garantizar que todo desarrollo quede documentado.
53.	Control de vulnerabilidades técnicas	Información oportuna acerca de vulnerabilidades técnicas de sistemas información debe ser obtenida, la exposición de la organización a estas vulnerabilidades debe ser evaluada y las medidas apropiadas deben	Se recomienda implementar varias herramientas de detección y control de vulnerabilidades, con el fin de corroborar la información de cada uno y así tomar decisiones sobre las vulnerabilidades más críticas que tenga el sistema.

		tomarse en función del riesgo.	

Administración de Incidentes de Seguridad de Información			
#	Control		Recomendaciones
54.	Reportar eventos de seguridad de información	Eventos de seguridad de información son reportados a través del canal administrativo más rápido posible.	Se recomienda que los eventos de seguridad de la información sean reportados a través de un proceso formal de mesa de servicio.
55.	Responsabilidades y procedimientos	Procedimientos y responsabilidades administrativas deben establecerse para asegurar la rápida, efectiva y ordenada respuestas a incidentes de seguridad de información.	Se recomienda definir responsabilidades en materia de seguridad de la información de acuerdo al responsable de cada componente (Aplicaciones, Bases de datos, infraestructura y seguridad) centralizar el monitoreo de las responsabilidades y procedimientos a través del encargado de la seguridad de la información, con el fin de establecer una mejor organización y cumplimiento de estos servicios en la organización.

56.	Aprendizaje de incidentes de seguridad de información.	Deben existir mecanismos implantados para permitir que los tipos, volúmenes y costos de los incidentes de seguridad de información sean cuantificados y monitoreados.	Se recomienda realizar un plan de lecciones aprendidas de seguridad de la información, con el fin de prevenir y estimar cualquier riesgo de seguridad que se pueda presentar en la organización.
57.	Recolección de evidencia	Cuando se tome una acción seguimiento contra una persona u organización después de un incidente de seguridad de información involucrando una acción legal (ya sea civil o criminal), deberá recolectarse, retenerse y presentarse evidencia en conformidad con las reglas de recopilación de evidencia de la jurisdicción correspondiente.	Se recomienda adquirir e implementar herramientas de análisis forense con el fin de recolectar con la debida cadena de custodia las evidencias que podría llegar, dependiendo de la criticidad, a estrados judiciales.

Administración de Continuidad de Negocios			
#	**Control**		**Recomendaciones**
58.	Incluyendo la seguridad de información en el proceso de administración de continuidad del negocio	Un proceso de administración de continuidad de negocios debe ser desarrollado y mantenido a través de la organización. Este debe considerar los requerimientos de seguridad de información necesarios para la continuidad de los negocios de la organización.	Se recomienda realizar un BIA (análisis de impacto del negocio) con el fin de realizar el documento de definición de continuidad del negocio donde se contemple los procesos críticos a salvaguardar en la organización.
59.	Assessment del Riesgo y Continuidad de Negocios	Los eventos que pueden producir interrupciones a los procesos de negocios deben ser identificados,	Se recomienda realizar un BIA (análisis de impacto del negocio) con el fin de realizar, el documento de definición de continuidad del negocio donde se contemple los procesos críticos a salvaguardar en la organización.
60.	Diseño e implantación de planes de continuidad que incluyan seguridad de información.	Los planes deben ser desarrollados e implantados para mantener y restaurar las operaciones y asegurar la disponibilidad de la información al nivel requerido y las escalas de tiempo requeridas después de una interrupción o falla de procesos críticos de negocios.	Se recomienda realizar definición de los procesos críticos del negocio, la información que se debe respaldar ante una eventualidad y los tiempos mínimos y máximos en que esta debe de entrar en producción.

61.	Marco de trabajo para planificación de continuidad de negocios	Un marco de trabajo único de planes de continuidad de negocios debe mantenerse para asegurar que todos los planes son consistentes, para cumplir consistentemente los requerimientos de seguridad de información, y para identificar prioridades para pruebas y mantenimiento.	Se recomienda realizar un plan centralizado de continuidad del negocio donde se contemple donde se identifiquen requerimientos de seguridad de la información, se identifiquen prioridades y se realice pruebas de acción para salvaguardar la información ante incidentes.
62.	Pruebas, mantenimiento y revaluación de planes de continuidad de negocios	Los planes de continuidad de negocios deben ser probados y actualizados regularmente para asegurar que son efectivos y oportunos.	Se recomienda realizar pruebas periódicas del plan centralizado de continuidad del negocio y de cada uno de sus componentes.
Conformidad			
#	**Control**		**Recomendaciones**
63.	Derechos de Propiedad Intelectual (IPR)	Procedimientos apropiados deben ser implantados para asegurar conformidad legal, regulatoria y contractual en el uso de material considerando que podría estar sujeto a derechos de propiedad y el uso de productos de	Se recomienda colocar en marcha la política de seguridad de la información que involucra la temática de propiedad intelectual y considerar todos sus lineamientos para proteger cualquier material que se considere de propiedad intelectual para la organización.

		software propietario.	
64.	Regulación de controles criptográficos.	Controles Criptográficos deben ser usados en conformidad con todos los acuerdos, leyes y regulaciones relevantes.	Se recomienda implementar controles criptográficos en la Corporación para proteger legalmente la información crítica que se manejada dentro ella.
65.	Verificación de conformidad técnica	Los sistemas de información deben ser verificados regularmente para asegurar conformidad con los estándares de implantación de seguridad.	Se recomienda programar una constante verificación de los estándares que se manejan con respecto a la seguridad de la información.
66.	Controles para auditoria de sistemas de información	Los requerimientos de auditoria de sistemas de información y actividades de verificación involucradas deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocios.	Se recomienda manejar una programación de las auditorias de sistemas de información, con el fin de controlar y evitar todo tipo de dificultades en las tareas que se realizan a diario en la organización.

67.	Protección de herramientas de auditoria de sistemas	El acceso a las herramientas de auditoria de sistemas de información debe ser protegido para prevenir cualquier mal uso o compromiso.	Se recomienda implementar herramientas de auditoría de los sistemas de información. Aumentar los controles en los registros de auditorías generados por los dispositivos y también planificar auditorías internas referentes al tema de seguridad de la información.

EN BASE A HERRAMIENTA MSAT

A continuación se presentan recomendaciones a implementar a partir del escaneo realizado por la herramienta de autoevaluación MSAT, donde nos muestra las falencias que se tienen en las áreas de análisis (AoAs). Las recomendaciones que se tendrán en cuenta serán de las áreas que fueron valoradas con un nivel de "carencias severas".

Infraestructura		
Categoría	**Subcategoría**	**Recomendaciones**
Defensa del perímetro	Acceso remoto	Estudie utilizar la autenticación multifactor para la conexión de usuarios remotos a través de Internet a los recursos corporativos. Revise con regularidad la lista de acceso de los usuarios en el dispositivo VPN.
Autenticación	Usuarios administrativos	Considere implantar otro factor de autenticación para disminuir el riesgo de accesos no autorizados. Piense en poner en práctica controles avanzados para la gestión de cuentas y el registro de acceso de cuentas.

Gestión y control	Informes sobre incidentes y respuesta	Establezca procedimientos para la creación de informes de incidentes y sus respuestas, problemas o preocupaciones sobre seguridad. Designe un equipo de respuesta de emergencia que incluya representantes de varias disciplinas, incluidas tecnologías, recursos humanos y legales para responder a todos los incidentes y problemas de seguridad.
Gestión y control	Creación segura	Aplique una directiva que solicite una revisión periódica de las configuraciones predeterminadas de los cortafuegos para tener en cuenta los cambios en las aplicaciones o los servicios utilizados.

Fuente: Reporte de herramienta MSAT

Aplicaciones		
Categoría	**Subcategoría**	**Recomendaciones**
Implementación y uso	Equilibrio de carga	Piense en utilizar equilibradores de carga de hardware en el primer nivel de los servidores Web para obtener una mayor disponibilidad. El equilibrador de carga muestra una sola dirección IP (virtual) al exterior que se asigna a todas las direcciones de cada servidor Web en el clúster.

Implementación y uso	Clústeres	Para asegurar una disponibilidad alta de las bases de datos críticas y de los archivos compartidos, piense en utilizar mecanismos de clúster.
Implementación y uso	Aplicación y recuperación de datos	Todas las aplicaciones de líneas comerciales deberían evaluarse periódicamente para su seguridad, someterse a procesos regulares de copias de seguridad, documentarse a fondo y contar con planes de contingencia en caso de que se produzcan fallos.
Implementación y uso	Fabricante de software independiente (ISV)	Continúe desarrollando aplicaciones clave propias, pero si posteriormente decide obtenerlas de un tercero, asegúrese de que podrá seguir disponiendo de servicio técnico y actualizaciones periódicas para los software clave de su empresa, o que el fabricante independiente de los mismos puede ofrecerle el código de origen en caso de que ya no pueda prestar dicho servicio para la aplicación.
Implementación y uso	Desarrollado internamente	Intente trabajar con el equipo de desarrollo interno para recibir periódicamente revisiones y actualizaciones de las aplicaciones utilizadas. Cuando aparezca una revisión, pruébela completamente en el entorno de laboratorio antes de utilizarla. Trabaje con el equipo de desarrollo para revisar las configuraciones de las aplicaciones y garantizar así una máxima

		seguridad.
Implementación y uso	Vulnerabilidades	Visite los sitios de los fabricantes y otros proveedores de soluciones de seguridad para detectar vulnerabilidades de la aplicación. Piense en una evaluación independiente para que un tercero pueda valorar el diseño de la seguridad de la aplicación e identificar otros problemas que necesiten más mecanismos de seguridad.
Diseño de aplicaciones	Metodologías de desarrollo de seguridad de software	Amplíe el uso de las herramientas de prueba de software de seguridad como parte instrumental de todos los planes de desarrollo de seguridad. Establezca un programa de formación de metodologías de desarrollo de seguridad de software con el objeto de mejorar la capacidad del personal para desarrollar código seguro.
Almacenamiento y comunicaciones de datos	Cifrado	Para aplicaciones que procesan datos confidenciales, opte por el cifrado con un algoritmo estándar del sector para la transmisión y el almacenamiento de datos.

Fuente: Reporte de herramienta MSAT

Operaciones		
Categoría	**Subcategoría**	**Recomendaciones**
Entorno	Host de gestión	Piense en utilizar estaciones de trabajo de gestión distintas para administrar los servidores y dispositivos de red por un protocolo seguro. Utilice SSH o VPN para asegurar los protocolos de gestión de texto sin formato. Debe reforzar las estaciones de trabajo de administración y poner en práctica controles de contraseñas fuertes basados en las capacidades del sistema host y las aplicaciones de gestión.
Directiva de seguridad	Protocolos y servicios	Colabore con el equipo de seguridad y comercial para establecer las pautas de los protocolos y servicios permitidos en el entorno corporativo y documente estas pautas. A continuación, audite los dispositivos necesarios (cortafuegos, dispositivos VPN, encaminadores, etc.) para asegurarse de que están configurados de forma acorde a las pautas documentadas.
Directiva de seguridad	Regulación	Las directivas son reglas y prácticas que especifican cómo se puede utilizar de forma adecuada un entorno informático. Si no existen directivas, no existe mecanismo alguno para definir ni hacer cumplir los controles dentro del entorno. Planifique inmediatamente el desarrollo de las directivas necesarias de acuerdo con los estándares de aplicación y gestión de la compañía.
Gestión de actualizaciones y	Documentación de la red	Trabaje con el grupo de ingenieros de red para que desarrollen en primer lugar los diagramas de la red externa. A continuación, dedíquese a los diagramas de la red interna.

revisiones		Limite el acceso a estos diagramas a un grupo del personal, principalmente a los equipos de TI y de seguridad.
Gestión de actualizaciones y revisiones	Gestión de actualizaciones	Desarrolle una directiva para la actualización de los sistemas operativos y todas las aplicaciones utilizando las pautas de prácticas recomendadas. Actualice en primer lugar los sistemas externos y de Internet, a continuación, los sistemas internos críticos y, por último, todos los sistemas no críticos.
Gestión de actualizaciones y revisiones	Gestión de cambios y configuración	Considere la puesta en práctica de un proceso formal de gestión para las configuraciones y los cambios para probar y documentar todas las actualizaciones antes de su puesta en práctica.
Copias de seguridad y recuperación	Planificación de recuperación ante desastres y reanudación de negocio	El equipo de seguridad debe repasar los archivos de registro cada día para buscar actividades sospechosas o anómalas. Considere utilizar una solución MOM (Microsoft Operations Manager) para controlar los archivos de registro del DMZ y de los servidores críticos de red. Si se producen entradas críticas de archivos de registro, MOM enviará alertas a los miembros del equipo adecuados.
Copias de seguridad y recuperación	Dispositivos de copia de seguridad	Desarrolle directivas y procedimientos para el almacenamiento y la gestión de los dispositivos de copias de seguridad utilizando las mejores prácticas recomendadas. Estas directivas deben tratar los sistemas críticos necesarios para la continuidad de la actividad empresarial.
Copias de seguridad y recuperación	Copias de seguridad y restauración	Desarrolle una directiva que demande pruebas regulares de los procedimientos de copias de seguridad y restauración. Este proceso se deberá documentar correctamente para que los encargados de TI puedan restaurar las operaciones en caso

		de producirse un desastre. En primer lugar, desarrolle los procedimientos de copias de seguridad y restauración para los sistemas críticos para la continuidad de la empresa y, a continuación, para el resto de sistemas y datos de menor importancia.

Fuente: Reporte de herramienta MSAT

Personal		
Categoría	**Subcategoría**	**Recomendaciones**
Requisitos y evaluaciones	Evaluaciones de seguridad	La asignación de niveles de importancia a cada componente de la infraestructura informática permite que la mayoría de los recursos se apliquen a aquéllos equipos establecidos como los más críticos, por lo que los sistemas que son menos críticos reciban menos recursos. Como consecuencia, se aplican con mayor eficacia los escasos recursos de seguridad en aquellos sistemas que los necesitan más.
Directiva y procedimientos	Comprobaciones del historial personal	Cree una directiva que requiera una comprobación del historial personal y financiero de las nuevas incorporaciones que vayan a ocupar puestos importantes. A la larga, esta directiva deberá englobar a todos los nuevos empleados, independientemente del puesto.
Directiva y procedimientos	Relaciones con terceros	El personal interno debería configurar los sistemas siguiendo una simulación de creación. Según las necesidades de la empresa, pueden ser soluciones viables tanto la gestión propia como la subcontratada. Si se subcontratan los servicios, los requisitos de seguridad

		deberían tratarse en el contrato y los acuerdos de nivel de servicio (SLA) deberían garantizar el cumplimiento de tales requisitos. Debe desarrollar directivas y procedimientos formales para los distintos tipos de relaciones con terceros con el acuerdo común de toda la empresa. Para ello, haga partícipe a los diversos equipos empresariales. Si las directivas se elaboran correctamente, los riesgos a los que está expuesta la empresa se verán reducidos.

BIBLIOGRAFÍA

- *[1]. Search Security.com. Definitions. Consultada en Octubre 2012 en http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci211622,00.html.*

- *[2]. Network Working Group. Site Security Handbook. Internet Engineering*
- *Task Force [En línea, p. 14]. Consultado en Octubre 2012 en http://www.ietf.org/rfc/rfc2196.txt.*

- *[3]. ISO/IEC 27001:2005 – Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos. Desarrollada por British Standards Institution*

- *[4]. NIST SP 800- 30 Risk Management Guide for Information Technology Systems- Recommendations of the National Institute of Standards and Technology, Gary Stone burner, Alice Goguen, and Alexis Feringa.*

- *[5]. Saint-Germain, R. Information Security Management Best Practice Based on ISO/IEC 17799. Londres, p. 60*

- *[6] M. Farias-Elinos, M. C, Mendoza-Diaz y L. Gómez-Velazco. "Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática". Techno-Legal aspects of Information Society and New Economy: an Overview. Information Society book series, 2003*

- *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST 800-30 Guía de Gestión de Riesgos de Sistemas de Tecnología de la Información. Gaithersburg: 2002, 2 p*

- (s.f.). Recuperado el Feb de 2013, de Security: Security.com

- (s.f.). Obtenido de Nist: www.nist.org/

- (2005). ISO27001:2005. En *Cláusula 3.3.*
- Cotecmar. (2012). *Análisis Prospetiva Estratégica .* Cartagena.
- (s.f.). ISO 27001: 2005. cláusula 3.2.
- *ISO27001*. (s.f.). Recuperado el 23 de 09 de 2013, de www.iso27001.es
- *iso27001.es*. (s.f.).
- (s.f.). ISO27001: 2005, Cláusula 3.8.
- Nist 800-30 . (s.f.).
- Tena, J. G.-J. (2003). *Protocolos Criptográficos y Seguridad en Redes.* Servicio de Publicaciones- Universidad de Cantabria.

ANEXOS

Anexo 1 *ISO 27001:2005 Cumplimiento de buenas prácticas*

- **Política de seguridad**

5 Política de Seguridad **5.1 Política de Seguridad de Información**			**Observación**	**Evaluación**	**5,00**
Objetivo: Para proporcionar una dirección y apoyo de la gerencia a la seguridad de la información de acuerdo a los objetivos de negocios, leyes y regulaciones relevantes.					
5.1.1	Documento de política de seguridad de información.	*Control* Un documento de política de seguridad de información debe ser aprobado por la gerencia, publicado y comunicado a todos los empleados y partes externas interesadas.	Si se cuenta con una política de seguridad de la información en proceso de revisión.	3.- Se realiza informalmente en forma total	
5.1.2	Revisiones de la política de seguridad de información	*Control* La política de seguridad de información debe ser revisada, a intervalos planificados o si ocurren cambios significativos, para asegurar la continuidad de su pertinencia, adecuación y efectividad.	que está en proceso de revisión y aprobación por la gerencia.	3.- Se realiza informalmente en forma total	

Anexo 2 *ISO 27001:2005 Cumplimiento de buenas prácticas*

- **Organización de seguridad de información**

6 Organización de Seguridad de Información **6.1 Organización Interna**			**Observaciones**	**Evaluación**	**3,364**
Objetivo: Para administrar la seguridad de información dentro de la organización.					
6.1.1	Participación de la Gerencia en Seguridad de Información.	*Control* La gerencia debe prestar apoyo activo a seguridad dentro de la organización a través de directrices claras, participación demostrable, asignaciones explícitas y conocimiento de sus responsabilidades en seguridad de información.	La gerencia se encuentra comprometida, pero no existe formalidad por escrito, como lo es un comité de seguridad de la información, que esta propuesto como ente certificador de las actividades realizadas.	2.- Se realiza parcial e informalmente	
6.1.2	Coordinación de Seguridad de Información	*Control* Las actividades de seguridad de información deben ser coordinadas por representantes de las diferentes partes de la organización con roles y funciones laborales relevantes.	Esta planteado en la política de SI pero no se encuentra implementado en la actualidad.	1.- No se realiza	
6.1.3	Asignación de responsabilidades de seguridad de información	*Control* Todas las responsabilidades de seguridad de información deben estar claramente definidas.	Muchas de las actividades de SI se están llevando a cabo, pero no están documentados a nivel de procesos y procedimientos, ni se ha identificado claramente en algunos procesos los responsables.	2.- Se realiza parcial e informalmente	
6.1.4	Proceso de autorización para la instalaciones de procesamiento de información	*Control* Debe existir un proceso definido e implantado para la autorización gerencial de nuevas instalaciones de procesamiento de información.	Existen procedimientos en el area en los cuales no son necesarios las autorizaciones de la alta gerencia, como son instalacion de computadores o dispositivos. Pero en la implementacion de elementos mas relevantes como son sistemas de información y servidores si se requiere autorizacion formal. El procedimiento no esta documentado.	2.- Se realiza parcial e informalmente	
6.1.5	Acuerdos de Confidencialidad	*Control* Requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de protección de información deben ser identificados y revisados regularmente.	Acuerdos de confidencialidad definido, documentad, aprobado y en mejoracontinua administrado por la oficina jurídica.	5.- Documentado y sujeto a revisión periódica	

6.1.6	Contacto con autoridades	*Control* Debe mantenerse contactos apropiados con autoridades relevantes.	Actualmente desde el área de seguridad de la información no se cuentan con estos contactos. En el área de seguridad física si.	1.- No se realiza
6.1.7	Contacto con grupos de interés especial	*Control* Debe mantenerse contacto apropiado con grupos de interés especial u otros foros especializados y asociaciones profesionales.	Se realiza suscripciones a foros internacionales de seguridad de la información, pero no se tiene contacto con comunidades locales.	2.- Se realiza parcial e informalmente
6.1.8	Revisiones independientes de seguridad de información	*Control* El acercamiento de la organización a la administración de seguridad de información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de información) deben ser revisados de manera independiente a intervalos planificados o cuando ocurra un cambio significativo en la implantación de seguridad.	Se enceuntra en su primer momento de revisión por la alta gerencia, no se cuenta con procedimeinto documentado.	2.- Se realiza parcial e informalmente
6.2 Partes Externas				
Objetivo: Para mantener la seguridad de la información de la organización y sus instalaciones de procesamiento que será accedida, procesada, comunicada a, o administrada por partes externas.				
6.2.1	Identificación de riesgos relacionados con partes externas	*Control* Los riesgos para la información de la organización y sus instalaciones de procesamiento producidos por procesos de negocios que involucren partes externas deben ser identificados y los controles apropiados deben ser implantados antes de entregar acceso.	Actualmente no se miden los riesgos de asignar accesos a entidades externas.	1.- No se realiza
6.2.2	Directriz de seguridad en el trato con clientes	*Control* Todos los requerimientos de seguridad identificados deben ser señalados antes de entregar acceso a los clientes a la información de la organización o sus activos.	No se cuenta con un documento donde se le notifique al cliente las responsabilidades a nivel de seguridad de la información.	1.- No se realiza
6.2.3	Directriz de seguridad en acuerdos con terceras partes	*Control* Los acuerdos con terceras partes que involucren acceso, procesamiento, comunicación o administración de información de la organización o sus instalaciones de procesamiento, o la adición de productos o servicios para instalaciones de procesamiento de información debe cubrir todos los requerimientos de seguridad relevantes.	En el acuerdo de confidencialidad adminsitrado por la oficina jurídica se cuenta con clausulas que delimitan las responsabilidades del uso de la información, sin embargo se debe revisar para garantizar que se realice de acuerdo a este control.	5.- Documentado y sujeto a revisión periódica

Administración de activos

7 Administración de Activos 7.1 Responsabilidad por activos			Observación	Evaluación	3,00
Objetivo: Para asegurar y mantener protección apropiada de los activos organizacionales.					
7.1.1	Inventario de Activos	*Control* Todos los activos deben estar claramente identificados, elaborando y manteniendo un inventario de todos los activos relevantes.	Se maneja parcialmente los inventarios de activos ya que activos fijos maneja un inventario general desde cierto monto quedando por fuera algunos activos de menor valor. TIC´S maneja inventario parcial de los activos de tecnología.	2.- Se realiza parcial e informalmente	
7.1.2	Propiedad de activos	*Control* Toda la información y activos relacionados con las instalaciones de procesamiento de información deben ser apoderadas por partes designadas de la organización.	Se cuenta con responsables de administración de los diferentes servicios de Tecnología, se encuentra docuemntado mas no validado.	3.- Se realiza informalmente en forma total	
7.1.3	Uso aceptable de activos	*Control* Reglas para el uso aceptable de la información y los activos asociados con instalaciones de procesamiento de información deben ser identificadas, documentadas e implantadas.	Actualmente se cuenta con formato de entrega de equipos móviles donde se dan lineamientos de uso, las demás reglas se contemplan en la política de seguridad de la información que está en proceso de revisión.	3.- Se realiza informalmente en forma total	
7.2 Clasificación de Información					
Objetivo: Para asegurar que la información recibe el adecuado nivel de protección.					
7.2.1	Guías para clasificación	*Control* La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización.	Esta definido el compromiso en la política de seguridad de la Información que esta en proceso de revisión y firma.	1.- No se realiza	
7.2.2	Manejo y etiquetado de información	*Control* Un apropiado conjunto de procedimientos para etiquetado y manejo de información debe ser desarrollado e implantado en conformidad con el esquema de clasificación adoptado por la organización.	Esta definido el compromiso en la política de seguridad de la Información que esta en proceso de revisión y firma.	1.- No se realiza	

Seguridad en recursos humanos

8 Seguridad en Recursos Humanos			Observaciones	Evaluación	5,2222
8.1 Previo al empleo					
Objetivo: Para asegurar que los empleados, contratistas y usuarios de terceras partes comprenden sus responsabilidades, que estas son acordes con sus roles y reducir el riesgo de hurto, fraude o uso malicioso de instalaciones.					
8.1.1	Roles y responsabilidades	*Control* Los roles y responsabilidades de seguridad de empleados, contratistas y usuarios de terceras partes deben estar identificados y documentados en conformidad con la política de seguridad de información de la organización.	Se encuentra en el docuemnto de políticas que se encuentra en revisión.	3.- Se realiza informalmente en forma total	
8.1.2	Investigación de antecedentes (Screening)	*Control* La verificación de antecedentes de todo candidato a empleado, contratista o usuario de tercera parte debe conducirse en conformidad con las leyes relevantes, regulaciones, ética y proporcionalmente a los requerimientos del negocio, la clasificación de la información a que tendrá acceso y los riesgos percibidos.	Se realiza por la oficina de seguridad física ante cualquier vinculación o acceso a las instalaciones de COTECMAR, se encuentra documentado en el sistema de gestión de calidad y esta sujeto a mejoramiento continuo.	5.- Documentado y sujeto a revisión periódica	
8.1.3	Términos y condiciones del empleo	*Control* Como parte de sus obligaciones contractuales, empleados, contratistas y usuarios de tercera parte deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual definirá sus obligaciones y las de la organización en relación a seguridad de información.	Se encuentra adjunto a la política de seguridad de la Información en revisión, que se anexará a los contratos laborales.	3.- Se realiza informalmente en forma total	
8.2 Durante el empleo					
Objetivo: Para asegurar que todos los empleados, contratistas y usuarios de terceras partes están enterados de las amenazas y preocupaciones en seguridad de información, sus responsabilidades y compromisos, y están preparados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y reducir el riesgo de error humano.					
8.2.1	Responsabilidades administrativas	*Control* La administración debe instar a los empleados, contratistas y usuarios de terceras partes a cumplir con la seguridad en conformidad con las políticas y procedimientos establecidos por la organización.	Se encuentra adjunto a la política de seguridad de la Información en revisión, que se anexará a los contratos de empleados y contratistas. No para todo contratista aplica, sólo para los que prestan servicios.	3.- Se realiza informalmente en forma total	

8.2.2	Capacitación, educación y entrenamiento en seguridad de información.	*Control* Todos los empleados de la organización y, cuando sea relevante, los contratistas y los usuarios de terceras partes deben recibir capacitación, entrenamiento y actualizaciones regulares en las políticas y procedimientos de la organización que sean relevantes a su función laboral.	Se contempla realizar una vez se firme la directiva de política.	1.- No se realiza
8.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal para aquellos empleados que produzcan brechas de seguridad.	Parte del proceso disciplinario se contempla en la política de seguridad de la información que complementará la oficina jurídica.	1.- No se realiza
8.3 Término o cambio de empleo				
Objetivo: Para asegurar que empleados, contratistas y usuarios de tercera parte abandonan la organización o cambian de función de manera ordenada				
8.3.1	Responsabilidades de término de contrato	*Control* Las responsabilidades de ejecutar el término o cambio del empleo deben estar claramente y asignadas	Se encuentra documentado en el cese de personal, pero a nivel procedimental de debe	5.- Documentado y sujeto a revisión periódica
8.3.2	Reintegro de activos	*Control* Todos los empleados, contratistas y usuarios de terceras partes deben reintegrar los activos de la organización que estén en su poder al momento del término del empleo, contrato o acuerdo.	Se realiza y se enuentra documentado en cese de personal.	5.- Documentado y sujeto a revisión periódica
8.3.3	Remoción de derechos de acceso	*Control* Los privilegios de acceso de todos los empleados, contratistas y usuarios de terceras partes a información o instalaciones de procesamiento deben ser removidos al término del empleo, contrato o acuerdo. En caso de cambio de función, deben ser ajustados.	El procedimiento se encuentra docuemntado, pero en ocaciones Talento Humano no realiza la notificación a tiempo al área de TIC´S.	2.- Se realiza parcial e informalmente

Seguridad física y ambiental

9 Seguridad física y ambiental 9.1 Áreas Seguras			Observaciones	Evaluación	6,38
Objetivo: Para prevenir acceso físico no autorizado, daño e interferencia a las premisas de la organización e información.					
9.1.1	Perímetro de Seguridad Física	*Control* Un perímetro de seguridad (barreras como muros, puertas de acceso controladas con tarjeta o una recepción) debe ser definido para proteger áreas que contengan información o instalaciones de procesamiento.	Se encuentra implementado y controlado por la oficina de seguridad física, normalizado dentro del documento "Plan de Protección de la Instalación Portuaria".	5.- Documentado y sujeto a revisión periódica	
9.1.2	Controles de ingreso físico	*Control* Las áreas seguras deben estar protegidas por controles de ingreso apropiados para asegurar que sólo el personal autorizado podrá acceder.	Se encuentra implementado y controlado por la oficina de seguridad física, normalizado dentro del documento "Plan de Protección de la Instalación Portuaria".	5.- Documentado y sujeto a revisión periódica	
9.1.3	Asegurando oficinas, salas e instalaciones	*Control* Seguridad física para oficinas, salas e instalaciones debe ser diseñada y aplicadas	Se encuentra implementado y controlado por la oficina de seguridad física, normalizado dentro del documento "Plan de Protección de la Instalación Portuaria".	5.- Documentado y sujeto a revisión periódica	
9.1.4	Protección contra amenazas externas y ambientales	*Control* Protección física contra daño producido por fuego, inundaciones. Terremotos, explosiones, desordenes sociales y otras formas de desastres naturales o producidos por el hombre deben ser diseñados y aplicados.	Se encuentra implementado y controlado los desastres por fuego por la oficina de seguridad física. Se enceuntra documentado en los docuemntos Plan de Protección de la Instalación Portuaria", matriz de riesgos corporativos y plan de evacuación de la planta Mamonal.	5.- Documentado y sujeto a revisión periódica	
9.1.5	Trabajando en áreas seguras	*Control* Protección física y guías para trabajar en áreas seguras deben ser diseñadas y aplicadas.	Se realiza actualmente y se controla por la oficina de seguridad física y seguridad industrial. Se encuentra documentado en el sistema gestión de calidad.	5.- Documentado y sujeto a revisión periódica	
9.1.6	Áreas de acceso público, carga y despacho.	*Control* Puntos de acceso tales como áreas de carga y despacho u otros puntos que podrían permitir el acceso a personas no autorizadas deben ser controlados y, si es posible, aislados de las instalaciones de procesamiento de información para evitar accesos no autorizados.	"Se realiza y se encuentra documentado en los documentos Evaluación y Plan de Protección de la Instalación Portuaria "	5.- Documentado y sujeto a revisión periódica	

9.2 Seguridad de Equipamiento				
Objetivo: Para prevenir la pérdida, daño, hurto o compromiso de los activos e interrupción de las actividades de la organización.				
9.2.1	Ubicación y protección de equipos	*Control* El equipamiento debe ser ubicado o protegido para reducir los riesgos producidos por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	El centro de datos no cumple con las normas de proteccion requeridas porque la corporacion no cuenta con el espacio ni el presupuesto para sublir esta necesidad, pero se cuenta con un sistema contra incendios. Y los demas componente estan bien ubicados y protegidos en la Corporación.	2.- Se realiza parcial e informalmente
9.2.2	Herramientas de apoyo	*Control* El equipamiento debe ser protegido de interrupciones en el suministro de energía y otras interrupciones producidas por fallas en las herramientas de apoyo.	Se cuenta con un sistema de Ups solo en el centro de datos principal porque es la prioridad al momento que ocurre una interrupcion, las otras sucursales no cuenta con este sistema. No se cuenta con un canal de respaldo del servicio de internet.	3.- Se realiza informalmente en forma total
9.2.3	Seguridad del cableado	*Control* El cableado de energía y telecomunicaciones que transporta los datos o soporte servicios debe ser protegido de intervenciones o daño.	Se cumple con las normas EIA/TIA 568 A y 568 B, las cuales estan estandarizadas a nivel mundial para garantizar el cableado estructura de la Corporación. Se implementa de forma total.	4.- Se realiza formalmente y está documentado
9.2.4	Mantenimiento de equipos	*Control* El equipamiento debe ser correctamente mantenido para asegurar la continuidad de su disponibilidad e integridad.	Se tiene un contrato con Ousourcing para llevar a cabo de forma periodica el proceso de mantenimeinto de equipos y ups. El mtto de servidores es realizado por persanal del area. Este proceso esta complemetamente documentado.	5.- Documentado y sujeto a revisión periódica

9.2.5	Seguridad de equipos fuera de las instalaciones propias	*Control* La seguridad debe aplicarse a los equipos fuera de los instalaciones físicas de la organización tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización	No se ha realizado la concientización de los usuarios respecto a la protección de la información en equipos que se saquen de las instalaciones de COTECMAR, ni se ha asegurado los mismos.	1.- No se realiza
9.2.6	Seguridad en el reciclaje y deshecho de equipos	*Control* Todos los ítems de equipamiento que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier información sensible o software licenciado ha sido eliminado o sobrescrito previo a su eliminación.	No se realiza, no se cuenta con procedimiento definido ni implementado.	1.- No se realiza
9.2.7	Remoción de propiedad	*Control* El equipamiento, información o software no debe ser sacado de los emplazamientos físicos de la organización sin autorización previa	Se cuenta con un procedimeinto docuementado e implemnetado de ingreso y salida de equipos. No se cuenta con un control efectivo de retorno del activo.	2.- Se realiza parcial e informalmente

Administración de comunicaciones y operaciones

10 Administración de Comunicaciones y Operaciones 10.1 Procedimientos y responsabilidades operativas			Observaciones	Evaluación	4,73
Objetivo: Para asegurar la correcta y segura operación de las instalaciones de procesamiento de información.					
10.1.1	Procedimientos documentados de operación	*Control* Procedimientos operacionales deben ser documentados, mantenidos y puestos a disposición de todos los usuarios que los necesiten.	Se realiza parcialmente. Se encuentra en proceso de documentación y algunos de implementación.	2.- Se realiza parcial e informalmente	
10.1.2	Administración de cambios	*Control* Los cambios en instalaciones de procesamientos de información y sistemas deben ser controlados.	Existe formato de cambios y proceso documentado pero no se encuentra implementado.	2.- Se realiza parcial e informalmente	
10.1.3	Segregación de tareas	*Control* Las tareas y áreas de responsabilidad deben estar segregadas para reducir la oportunidad de modificación o mal uso, no autorizado o accidental, de activos de la organización.	Se encuentra segmentada las responsabilidades de los diferentes administradores, sin embargo esta sujeto a medición y mejora.	4.- Se realiza formalmente y está documentado	
10.1.4	Separación de instalaciones de desarrollo, pruebas y operación.	*Control* Las instalaciones de desarrollo, prueba y producción deben estar separadas para recudir el riesgo de acceso no autorizado o cambios en el sistema en producción.	no se cuenta con los tres ambientes de desarrollo, pruebas y producción.	2.- Se realiza parcial e informalmente	
10.2 Administración de servicios entregados por terceros					
Objetivo: Para implantar y mantener el nivel apropiado de seguridad de información y de prestación de servicios en conformidad con los acuerdos de prestación de servicio de terceros					
10.2.1	Prestación de Servicios	*Control* Asegurar que los controles de seguridad, definiciones de servicios y niveles de prestación incluidos en el acuerdo de prestación de servicios de terceros están implantados, operativos y son mantenidos por el tercero.	Se encuentra especificado de manera global en el documento de políticas en revisión por la gerencia.	3.- Se realiza informalmente en forma total	

10.2.2	Monitoreo y revisión servicios de terceros	*Control* Los servicios, reportes y registros entregados por el tercero deben ser monitoreados y revisados regularmente, y debe llevarse a cobo una auditoria periódicamente.	Si se realiza formalmente una revision de metas trazadas por la oficina con respecto al los servicios prestado por terceros, evaluando asi dicho servicio y acertividad.	4.- Se realiza formalmente y está documentado
10.2.3	Administración de cambios de servicios de terceros	*Control* Los cambios en la entrega del servicio, incluyendo mantenimiento y mejora de las políticas de seguridad de información existentes deben ser administrados, tomando en cuenta la criticidad de los sistemas y procesos de negocios involucrados y el re-assessment de los riesgos.	Se realizan acuerdos para concertar al respecto, sobre los cambios que pueden surgir en el trascursos del contrato ya pactado. Este proceso es informalmente llevado aunque se cuenta con soportes como lo son los contratos..	3.- Se realiza informalmente en forma total
10.3 Aceptación y planificación de sistemas				
Objetivo: Para minimizar el riesgo de fallas en los sistemas.				
10.3.1	Administración de capacidades	*Control* El uso de los recursos debe ser monitorear, ajustado y deben realizarse proyecciones de los requerimientos de capacidad futura para asegurar el desempeño del sistema	Se según la necesidad de cada sistema van diagnosticando la capacidad que se debe tener y en caso de requerir mas, si se cuenta con el recurso se toma la decision sino se consulta con la dirección.	3.- Se realiza informalmente en forma total
10.3.2	Aceptación de sistemas	*Control* Criterios de aceptación para nuevos sistemas, actualizaciones y nuevas versiones deben ser establecidos y deben ejecutarse pruebas apropiadas de él o los sistemas antes de su aceptación.	Se ejecutan las pruebas pertinentes para la implementacion de cada sistema, pero este procedimiento no se encuentra documentado en la oficina.	2.- Se realiza parcial e informalmente

10.4 Protección contra código malicioso y código móvil				
Objetivo: Para proteger la integridad del software y la información				
10.4.1	Controles contra código malicioso	*Control* Controles de detección, prevención y recuperación deben ser implantados para protegerse contra el código malicioso. Debe implantarse un procedimiento de concientización de usuarios.	Se realiza parcialmente y no se encuentra documentado.	2.- Se realiza parcial e informalmente
10.4.2	Controles contra código móvil	*Control* Donde se autorice el uso de código móvil, la configuración debe asegurar que la autorización de código móvil opera de acuerdo a una política de seguridad claramente definida, y la ejecución de código móvil no autorizado está prevenido	Se enceuntra definido en la política de seguridad de la información en proceso de revisión, sin embargo actualmente en la Corporación no aplica debido a que no se prestan servicios a través de móviles.	0.- No aplica
10.5 Respaldos				
Objetivo: Para mantener la integridad y la disponibilidad de la información y las instalaciones de procesamiento.				
10.5.1	Respaldos de información	*Control* Copias de respaldo de información y softw are deben realizarse y probarse periódicamente en conformidad con la política de respaldo acordadi	Se realiza, esta documentado y esta sujeto a revisión y mejora en las pruebas de restauración.	5.- Documentado y sujeto a revisión periódica
10.6 Administración de Seguridad de Redes				
Objetivo: Para asegurar la protección de la información en redes y la protección de la infraestructura de apoyo.				
10.6.1	Controles de Red	*Control* Las redes deben ser administradas y controladas adecuadamente, para asegurar su protección contra amenazas, y para mantener la seguridad de los sistemas de información y aplicaciones que la utilizan, incluyendo la información en tránsito.	Se realiza control de la red mediante aplicaciones de administración, las cuales permiten gestionar la información que puede ser violada. Este proceso no esta documentado.	3.- Se realiza informalmente en forma total
10.6.2	Seguridad de los servicios de red	*Control* Las características de seguridad, niveles de servicio y requerimientos de todos los servicios de red deben estar identificados e incluidos en cualquier acuerdo de nivel de servicios de red, si estos servicios son prestados “in-house” o son externalizados.	Se cuenta con unas clausuras con el ISP y Outsourcing, que indican en cierta medida con lo que deben cumplir ambas partes,para mantener un buen servicio de redes que se utiizan en la Corporación.	4.- Se realiza formalmente y está documentado

10.7 Manejo de Medios				
Objetivo: Para prevenir la divulgación no autorizada, modificación o destrucción de activos, y la interrupción de las actividades de negocios.				
10.7.1	Administración de medios removibles	*Control* Deben existir procedimientos implantados para la administración de medios removibles.	Se encuentra implementados pero no docuemntados.	3.- Se realiza informalmente en forma total
10.7.2	Eliminación de medios	*Control* Los medios deben ser eliminados, de manera segura, utilizando procedimientos formales, cuando no vayan a ser requeridos.	No se cuenta con un procedimiento formalizado e implementedo para el borrado seguro de la información.	1.- No se realiza
10.7.3	Procedimientos de manejo de información	*Control* Procedimientos de manejo y almacenamiento de información deben ser establecidos para proteger esta información de divulgaciones no autorizadas o mal uso.	Se realiza para los sistemas de información y se controla con los permisos de acceso por roles. Pero no se encuentra implementado para información contenida en documentos físicos.	2.- Se realiza parcial e informalmente
10.7.4	Seguridad de la documentación de sistemas	*Control* El sistema de documentación debe estar protegido contra acceso no autorizado.	Este control no esta documentafo	1.- No se realiza
10.8 Intercambio de Información				
Objetivo: Para mantener la seguridad de información y software intercambiado con una organización u otra entidad externa				
10.8.1	Procedimientos y políticas de intercambio de información	*Control* Política forma de intercambio, procedimientos y controles deben ser implantados para proteger el intercambio de información a través de todos los tipos de facilidades de comunicación.	se encuentra documentado en el docuemento de políticas de Seguridad de la Información en revisión por parte de la gerencia. No se contempla la seguridad de redes inalambricas.	2.- Se realiza parcial e informalmente

10.8.2	Acuerdos de intercambio	*Control* Acuerdos deben establecerse para el intercambio de información y software entre organizaciones y partes externas.	Se realiza con el documento de acuerdo de confidencialidad elaborado por la oficina jurídica.	5.- Documentado y sujeto a revisión periódica
10.8.3	Medios físicos en tránsito	*Control* Los medios que contengan información deben ser protegidos contra acceso no autorizado, mal uso o daño durante el transporte más allá de los limites físicos de la organización.	Serealiza el control de trasporte de los activos con información importante para el negocio, pero actualmente no se encuentra documentado.	3.- Se realiza informalmente en forma total
10.8.4	Mensajería electrónica	*Control* La información enviada a través de mensajería electrónica debe ser protegida apropiadamente.	Se encuentra establecida en el documento de políticas de Seguridad de la Información y se enceuntra pendiente por implementación servicos RMS de microsoft.	3.- Se realiza informalmente en forma total
10.8.5	Sistemas de información de negocios	*Control* Políticas y procedimientos deben ser desarrollados e implantados para proteger la información asociadas con la interconexión de sistemas de información de negocios.	Se encuentra implementado parcialmente para la información contenida en los sistemas de información, no se encuentra documentado e implementado para la información almacenada en otros medio.	2.- Se realiza parcial e informalmente
10.9 Servicios de Comercio Electrónico				
Objetivo: Para asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.				
10.9.1	Comercio electrónico	*Control* La información involucrada en comercio electrónico que transita a través de redes públicas debe ser protegida de actividades fraudulentas, conflictos contractuales, divulgación y modificaciones no autorizadas.	No se realizan actualmente en la corporación actividades de comercio electrónico tales como portales de proveedores y clientes.	0.- No aplica
10.9.2	Transacciones en línea	*Control* La información involucrada en transacciones en línea debe ser protegida para prevenir transmisiones incompletas, pérdidas de ruta y alteraciones, divulgación, duplicación o replicación no autorizada de los mensajes.	No se ceunta con firmas digitales y certificados digitales para asegurar las transacciones en los sistemas de información.	1.- No se realiza

10.9.3	Información disponible a público	*Control* La integridad de la información disponible en sistemas de acceso público debe estar protegida para prevenir modificaciones no autorizadas.	Se realiza y se controla a través de contrato de tercerización del proveedor de servicio de la página web, que es el único servicio al público.	5.- Documentado y sujeto a revisión periódica
10.10 Monitoreo				
Objetivo: Para detectar actividades de procesamiento de información no autorizados.				
10.10.1	Registros de auditoria	*Control* Registros de las actividades de los usuarios, excepciones y eventos de seguridad deben producirse y resguardarse por un periodo predeterminado para ser utilizado en futuras investigaciones y monitoreos de control de acceso.	Se encuentra implementado los logs de auditoría en los sistemas de información, pero el procedimiento no se encuentra documentado.	3.- Se realiza informalmente en forma total
10.10.2	Monitoreo de Uso de sistemas	*Control* Procedimientos para monitorear el uso de las instalaciones de procesamiento de información deben ser establecidos y los resultados del monitoreo de actividades deben ser revisados regularmente.	Monitoreo de los sistemas se realiza por parte de onfrsestructura tecnológica, pero no se encuentra documentado el procedimiento.	2.- Se realiza parcial e informalmente
10.10.3	Protección de la información de registro.	*Control* Las instalaciones e información de registros deben ser protegidos contra la alteración y acceso no autorizados.	Se tiene registro de los logs de transacciones y/o auditoría de los sistemas, se realiza backups de estos y se controla el acceso por autenticación de usuarios con roles de administrador, pero no se tiene docuemntado y se filtra a un segundo log los registros netamente de seguridad.	2.- Se realiza parcial e informalmente

10.10.4	Registros de Administrador y Operador del Sistema	*Control* Las actividades de administradores y operadores deben ser registradas.	Se registran las actividades de todos los usuarios tanto funcionales como técnicos en los logs de los sistemas, pero no se ceuntra docuemntado el procedimiento.	3.- Se realiza informalmente en forma total
10.10.5	Registros de Fallas	*Control* Las fallas deben ser registradas, analizadas y las medidas apropiadas deben tomarse.	En este proceso esta involucrado la mesa de ayuda, que es donde se gestionan todos los incidentes que se puedan tener, asi mismo se llevan a cabo unos indicadores de miden el numero de fallas obtenida en los periodos.	4.- Se realiza formalmente y está documentado
10.10.6	Sincronización de Reloj	*Control* Los relojes de todos los sistemas que procesan información relevante en una organización o dominio de seguridad deben estar sincronizados con una fuente de señal horaria confiable y previamente acordad	Este proceso si se encuentra implementado, se cuenta con una sincrononizacion total de los sistemas de información con los que cuenta la Corporación y cada uno de los elementos involucrados que lo requieran.	5.- Documentado y sujeto a revisión periódica

Control de acceso

11 Control de Acceso			Observaciones	Evaluación	4,8400
11.1 Requerimientos de negocios para control de acceso					
Objetivo: Para controlar el acceso a la información.					
11.1.1	Política de Control de Acceso	*Control* Un política de control de acceso debe ser establecida, documentada y revisada basándose en los requerimientos de negocios y seguridad.	la política de control de acceso se encuentra incluida dentro del documento de políticas de seguridad de la información. A nivel de control de acceso se realiza de manera parcial.	2.- Se realiza parcial e informalmente	
11.2 Administración de accesos de usuarios					
Objetivo: Para asegurar acceso autorizado de usuarios y prevenir el acceso no autorizado a sistemas de información.					
11.2.1	Registro de Usuarios	*Control* Debe existir un procedimiento formal de registro y eliminación para entregar y revocar acceso a todos y cada uno de los sistemas de información y servicios.	El procedimieto existe, esta implementado y docuemntado pero esta pendiente por validación.	3.- Se realiza informalmente en forma total	
11.2.2	Administración de Privilegios	*Control* La asignación de y uso de privilegios debe ser restringida y controlada	Se realiza a través de la solicitud de servicios a través de la mesa de ayuda y es autorizado por el jefe inmediato.	4.- Se realiza formalmente y está documentado	
11.2.3	Administración de Contraseñas de usuarios	*Control* La asignación de contraseñas debe ser controlada a través de un proceso formal de administración.	Se encuentra implementado parcialmente y hasta donde las herramientas comerciales y de desarrollo in house lo permitán. **No se encuentra cifradas las contraseñas en las herramientas de desarrollo in house.**	2.- Se realiza parcial e informalmente	

11.2.4	Revisión de derechos de acceso de usuarios	*Control* La administración debe revisar periódicamente los privilegios de acceso según un procedimiento formal.	El proceso lo realiza cada administrador de aplicación o servicio mas no se encuentra documentado.	2.- Se realiza parcial e informalmente
11.3 Responsabilidades de usuarios				
Objetivo: Para prevenir el acceso no autorizado y el compromiso o hurto de información o instalaciones de procesamiento de información.				
11.3.1	Uso de Contraseña	*Control* Los usuarios deben seguir buenas prácticas de seguridad en el uso y selección de contraseñas.	Se realiza a nivel de socialización, concientización y divulgación del buen uso de las contraseñas.	5.- Documentado y sujeto a revisión periódica
11.3.2	Equipos desatendidos por el usuario	*Control* Los usuarios deben asegurar la protección de sus equipos cuando estos no están apropiadamente atendidos.	Se enceuntra docuemntado en el docuemnto de políticas de seguridad de la información. Su implementación se realiza mediente control de acceso y políticas de bloqueos a través del controlador del dominio.	3.- Se realiza informalmente en forma total
11.3.3	Política de Escritorio y Pantalla limpios	*Control* Una política de escritorios limpios de papeles y medios removibles y una política de pantallas limpias de para instalaciones de procesamiento de información deben ser adoptadas.	Esta contenplado dentro del documento de políticas, pero aún no s eha divulgado.	2.- Se realiza parcial e informalmente
11.4 Control de Acceso a Redes				
Objetivo: Para prevenir el acceso no autorizado a los servicios de red.				
11.4.1	Política de Uso de Servicios de Red.	*Control* Los usuarios tendrán acceso a aquellos servicios de red a los que han sido específicamente autorizados.	Esta contenplado dentro del documento de políticas, pero aún no s eha divulgado.	2.- Se realiza parcial e informalmente
11.4.2	Autenticación de usuarios para conexiones externas.	*Control* Métodos de autenticación apropiados deben ser usados para controlar el acceso de los usuarios remotos.	Se contempla dentro de la política de Seguridad de la Información. Se tiene métodos de autenticación seguros para conexiones a la red de usuarios remotos, a través de VPNs, pero no se cuenta con procedimiento formal documentado.	3.- Se realiza informalmente en forma total

11.4.3	Identificación de equipos en redes.	*Control* Identificación automática de equipos debe ser considerada como una forma de autenticar conexiones desde ubicaciones o equipos específicos.	Todos los equipos de la red de la Corporacion se encuenta identificados. Este procedimiento se encuenta completamente implementado, pero no documentado	3.- Se realiza informalmente en forma total
11.4.4	Protección de puertos de configuración y diagnóstico remoto.	*Control* Los puertos físicos y lógicos de diagnostico y configuración deben ser controlados.	si se realiza procedimiento de bloqueo de puerto usb y acceso remoto. No se encuentrada documentado.	3.- Se realiza informalmente en forma total
11.4.5	Segregación de redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes.	cada grupo de usuario se encuentra dentro de una subred diferente, para evitar cualquier amenaza y por estandares. Este proceso se encuentra documentado.	4.- Se realiza formalmente y está documentado
11.4.6	Control de conexiones a redes	*Control* En redes compartidas, especialmente aquellas extendidas más allá de los límites físicos de la organización, la capacidad de los usuarios para conectarse a la red debe estar restringida, alineada con la política de control de acceso y los requerimientos de las aplicaciones de negocios (ver 11.1).	ciertos usuarios de acuerdo a los requerimientos, tienen acceso a las aplicaicones del negocio por VPN. Este procedimiento no se encuentra documentado.	3.- Se realiza informalmente en forma total
11.4.7	Control de rutas de redes	*Control* Controles de ruteo deben implantarse en las redes para asegurar que las conexiones de computadores y flujos de información no producirán brechas en la política de control de acceso a las aplicaciones de negocios.	si se realiza procedmiento pero es contralado atravez de terceros. no se encuentra documentado	2.- Se realiza parcial e informalmente

11.5 Control de acceso al sistema operativo				
Objetivo: Para prevenir acceso no autorizado a los sistemas operativos.				
11.5.1	Procedimientos de Log-on seguro	*Control* El acceso a los sistemas operativos debe ser controlado por un proceso de "login seguro".	Se encuentra docuemntado en el docuemnto de políticas. Se realiza logon seguro de usuarios autenticandose contra un servidor controlador de dominio.	3.- Se realiza informalmente en forma total
11.5.2	Identificación y autenticación de usuarios	*Control* Todos los usuarios deben tener un único identificador (user ID) para su uso personal, y una técnica adecuada de autentificación debe ser elegida para verificar la identidad del usuario.	Se encuentra implementado y documentado en la directiva de políticas de seguridad de la Información y en el documento de políticas técnicas de administración de usuarios y contraseñas.	5.- Documentado y sujeto a revisión periódica
11.5.3	Sistemas de administración de contraseñas	*Control* Los sistemas para el manejo de contraseñas serán interactivos y asegurarán el uso de contraseñas de calidad.	Se encuentra documentado en el documento de políticas de seguridad de la información y políticas técnicas, se ecuentra implementado en las herramientas comerciales, y en las de desarrollo in house hasta donde estas lo permiten.	5.- Documentado y sujeto a revisión periódica
11.5.4	Uso de herramientas del sistema	*Control* El uso de herramientas de sistema capaces de sobrescribir controles de sistemas y aplicaciones debe ser restringido y estrictamente controlado.	El acceso a herramientas del sistema se restringe a través control de acceso con los roles perfiles y provilegios de cada usuario, pero no se ha documentado, ni revisado periodicamente.	1.- No se realiza
11.5.5	Time-out de sesiones	*Control* La sesiones inactivas deben ser eliminadas después de un periodo predefinido de inactividad.	ese procedimiento no se encuentra implementado, ni documentado.	1.- No se realiza
11.5.6	Limitación del tiempo de conexión	*Control* Tiempos de restricción de conexiones deben ser utilizados para brindar seguridad adicional a las aplicaciones de alto riesgo.	no se realiza procedmiento para limitar el tiempo de conexión de los usuarios al sistema.	1.- No se realiza

11.6 Control de acceso a Aplicaciones e Información				
Objetivo: Para prevenir el acceso no autorizado a información involucrada en sistemas de aplicación.				
11.6.1	Restricción de acceso a la información	*Control* El acceso a funciones de sistemas de aplicación e información por parte de usuarios y personal de soporte debe estar restringido en conformidad con la política de control de acceso definida.	El acceso a la información contenida en aplicaciones se realiza con control de acceso,por segmentación de roles y responsabilidades de administrador, desarrollador y usuario final.	5.- Documentado y sujeto a revisión periódica
11.6.2	Aislamiento de sistemas sensibles	*Control* Los sistemas sensibles debe tener un ambiente de computo dedicado (aislado).	Se ha identificado informalmente las aplicaciones críticas del negocio y corren en ambientes dedicados, pero no se encuentra dicha clasificación documentada.	3.- Se realiza informalmente en forma total
11.7 Computación móvil y teletrabajo				
Objetivo: Para asegurar la seguridad de información cuando se emplea facilidades de computación móvil y teletrabajo.				
11.7.1	Computación móvil y comunicaciones	*Control* Una política formal debe ser implantada y las medidas apropiadas de seguridad deben ser adoptadas para protegerse contra los riesgos de emplear computación móvil y las actividades de teletrabajo.	Se encuentra docuemntada en el docuemnto de políticas de seguridad de la información.	3.- Se realiza informalmente en forma total
11.7.2	Teletrabajo	*Control* Una política, planes operacionales y procedimientos deben ser desarrollados e implantados para actividades de teletrabajo.	Se encuentra documentada la política de teletrabajo, pendiente la implementación y documentación del procedimeinto.	3.- Se realiza informalmente en forma total

Adquisición, desarrollo y mantenimiento de los sistemas de información

12 Adquisición, desarrollo y mantenimiento de sistemas de 12.1 Requerimientos de seguridad de sistemas de información			Observaciones	Evaluación	2,38
Objetivo: Para asegurar que la seguridad es una parte integral de los sistemas de información.					
12.1.1	Especificación y análisis de requerimientos de seguridad	*Control* Declaraciones de requerimientos de negocios para nuevos sistemas de información o extensiones de los existentes deben especificar requerimientos de controles de seguridad.	Se realiza y se encuentra documentado en las políticas de seguridad de la información en revisión por la alta gerencia.	3.- Se realiza informalmente en forma total	
12.2 Procesamiento correcto en aplicaciones					
Objetivo: Para prevenir errores, perdida, modificación no autorizada o mal uso de información en aplicaciones.					
12.2.1	Validación de datos de entrada	*Control* Los datos de entrada a aplicaciones deben ser validados par asegurar que los datos son correctos y apropiados.	la validacion de los entradas de datos de las aplicaciones no se realiza por la coord. De aplicaciones. Esta tarea no corresponde a la coordinacionde aplicaciones	1.- No se realiza	
12.2.2	Control de procesamiento interno	*Control* Puntos de verificación deben ser incluidos en las aplicaciones para detectar cualquier corrupción de información por errores de procesamiento o actos deliberados.	no se realizan puntos de verificacion por la coordinacion, pero si se realiza validacion de programacion y la interconexion con la base de datos.	1.- No se realiza	
12.2.3	Integridad de mensajes	*Control* Requerimientos para asegurar la autenticidad y proteger la integridad de los mensajes en aplicaciones deben ser identificados y controles apropiados deben ser identificados e implantados.	Se encuentra definido en la política de seguridad de la información en revisión por la gerencia, pero no se enceuntra implementada.	3.- Se realiza informalmente en forma total	
12.2.4	Validación de datos de salida	*Control* Los datos de salida de las aplicaciones deben ser validados para asegurar que el procesamiento y la información almacenada es correcta y apropiada a la circunstancias.	la validacion de los salidas de datos de las aplicaciones no se realiza por la coord. De aplicaciones. Esta tarea no corresponde a la coordinacionde aplicaciones	1.- No se realiza	

12.3 Encriptación				
Objetivo: Para proteger la confidencialidad, autenticidad o integridad de información a través de métodos criptográficos.				
12.3.1	Política de uso de controles criptográficos	*Control* Una política acerca del uso de controles criptográficos para la protección de información debe ser desarrollada e implantada	Se encuentra definido en la política de seguridad de la información en revisión por la gerencia, pero no se enceuntra implementada.	3.- Se realiza informalmente en forma total
12.3.2	Administración de llaves	*Control* Debe existir Administración de Llaves criptográficas para apoyar el uso de técnicas criptográficas por parte de la organización.	Se encuentra definido en la política de seguridad de la información en revisión por la gerencia, pero no se enceuntra implementada.	1.- No se realiza
12.4 Seguridad en los sistemas de archivos				
Objetivo: Para asegurar la seguridad de los sistemas de archivos.				
12.4.1	Control de Softw are Operacional	*Control* Deben existir procedimientos implantados para controlar la instalación de softw are en sistemas operacionales.	Se encuentra docuemntado en el documento de políticas, hay algunos controles pero no implementados de manera total.	2.- Se realiza parcial e informalmente
12.4.2	Protección de datos de prueba de sistemas	*Control* Los datos de prueba deben ser cuidadosamente seleccionados, protegidos y controlados.		2.- Se realiza parcial e informalmente
12.4.3	Control de acceso a código fuente de programas	*Control* El acceso al código fuente de programas debe ser restringido.	se cuenta los codigos fuentes para efectuar control de acceso para cambios. Pero si se debe implementar seguridad en el codigo fuentes. No se realiza procedimiento	1.- No se realiza

12.5 Seguridad en los procesos de desarrollo y soporte				
Objetivo: Para mantener la seguridad del software de aplicación de sistemas e información.				
12.5.1	Procedimiento de Control de Cambios	*Control* La implantación de controles debe ser controlada a través del uso de un procedimiento formal de control de cambios.	se realiza una notificacion de cambio por el jefe del area y luego se implementa cambio sin ser documentado.	2.- Se realiza parcial e informalmente
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	*Control* Cuando un sistema cambie, las aplicaciones de negocios criticas, deben ser revisadas y probadas para asegurar que no existe un impacto adverso en las actividades de la organización o en la seguridad.	los usuarios hacen la revision y notifican fallas de la aplicaciones posteriormente	1.- No se realiza
12.5.3	Restricción en los cambios a paquetes de softw are	*Control* Modificaciones a los paquetes de softw are deben ser desincentivadas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	no se realiza cambio a herramientas licenciadas	1.- No se realiza
12.5.4	Fuga de información	*Control* Oportunidades de fuga de información deben ser prevenidas.	No se cuenta con herramienta de prevención y detección de fuga de información.	1.- No se realiza
12.5.5	Desarrollo de softw are externalizado	*Control* El desarrollo de softw are externalizado debe ser supervisado y monitoreado por la organización.	se revisa en la parte tecnica antes de la implementacion de estos software, el usuario final es quien realiza revision funcional de los software externo.	2.- Se realiza parcial e informalmente
12.6 Administración de vulnerabilidades técnicas				
Objetivo: Para reducir el riesgo de “explotación” de vulnerabilidades técnicas publicitadas.				
12.6.1	Control de vulnerabilidades técnicas	*Control* Información oportuna acerca de vulnerabilidades técnicas de sistemas información debe ser obtenida, la exposición de la organización a estas vulnerabilidades debe ser evaluada y la medidas apropiadas deben tomarse en función del riesgo.	Se realiza captura de vulnerabilidades de los sistemas de información a través de logs de transacciones y Bitácora de auditoría (Journal) , pero no se encuentra un procedimeinto definido.	2.- Se realiza parcial e informalmente

Administración de incidentes de seguridad de información

13 Administración de Incidentes de Seguridad de Información 13.1 Reportar vulnerabilidades y eventos de seguridad			Observaciones	Evaluación	2,20
Objetivo: Para asegurar que los eventos de seguridad de información y las vulnerabilidades asociadas son comunicadas de forma que permita tomar acciones correctivas oportunas.					
13.1.1	Reportar eventos de seguridad de información	*Control* Eventos de seguridad de información son reportados a través del canal administrativo más rápido posible.	En la actualidad no existen, se propuso en la directiva de políticas que estas sean generadas a través de un comité de seguridad.	1.- No se realiza	
13.1.2	Reportar vulnerabilidades de seguridad	*Control* Todos los empleados, contratistas y usuarios de terceros, ya sea de sistemas de información y/o servicios, deben ser involucrados en la detección y reporte de cualquier debilidad o sospecha observada en sistemas o servicios.	Este procedimiento se realiza de manera total, documentado a traves de correo electrónico, pero debe ser documentado formalmente.	3.- Se realiza informalmente en forma total	
13.2 Administración y mejora de incidentes de seguridad de información					
Objetivo: Para asegurar que se emplea una aproximación efectiva y consistente para la administración de incidentes de seguridad de información.					
13.2.1	Responsabilidades y procedimientos	*Control* Procedimientos y responsabilidades administrativas deben establecerse para asegurar la rápida, efectiva y ordenada respuestas a incidentes de seguridad de información.	Los procedimientos y responsables a nivel de seguridad de la información estan definidos parcialmente, ya que algunas de las funiconalidades de esta Coordinación se realizan de manera descentralizada.	2.- Se realiza parcial e informalmente	
13.2.2	Aprendizaje de incidentes de seguridad de información.	*Control* Debe existir mecanismos implantados para permitir que los tipos, volúmenes y costos de los incidentes de seguridad de información sean cuantificados y monitoreados.	Aun no se enceuntra implementado este control.	1.- No se realiza	
13.2.3	Recolección de evidencia	*Control* Cuando se tome una acción seguimiento contra una persona u organización después de un incidente de seguridad de información involucrando un acción legal (ya sea civil o criminal), deberá recolectarse, retenerse y presentarse evidencia en conformidad con las reglas de recopilación de evidencia de la jurisdicción correspondiente.	No se realiza aún en la Corporación.	1.- No se realiza	

Administración de continuidad de negocios

14 Administración de Continuidad de Negocios					
14.1 Aspectos de Seguridad de información en Administración de Continuidad de Negocios			**Observaciones**	**Evaluación**	**1,00**
Objetivo: Para evitar la interrupción de actividades de negocios y para proteger los procesos críticos de negocios de los efectos producidos por una falla mayor de sistemas de información o un desastre y asegurar su reconstitución oportuna					
14.1.1	Incluyendo la seguridad de información en el proceso de administración de continuidad del negocio	*Control* Un proceso de administración de continuidad de negocios debe ser desarrollado y mantenido a través de la organización. Este debe considerar los requerimientos de seguridad de información necesarios para la continuidad de los negocios de la organización.	No se realiza procedimiento, apenas se esta investigando como implementar esta metodologia	1.- No se realiza	
14.1.2	Assessment del Riesgo y Continuidad de Negocios	*Control* Los eventos que pueden producir interrupciones a los procesos de negocios deben ser identificados,	No se realiza procedimiento, apenas se esta investigando como implementar esta metodologia	1.- No se realiza	
14.1.3	Diseño e implantación de planes de continuidad que incluyan seguridad de información	*Control* Los planes deben ser desarrollados e implantados para mantener y restaurar las operaciones y asegurar la disponibilidad de la información al nivel requerido y las escalas de tiempo requeridas después de una interrupción o falla de procesos críticos de negocios.	No se realiza procedimiento, apenas se esta investigando como implementar esta metodologia	1.- No se realiza	
14.1.4	Marco de trabajo para planificación de continuidad de negocios	*Control* Un marco de trabajo único de planes de continuidad de negocios debe mantenerse para asegurar que todos los planes son consistentes, para cumplir consistentemente los requerimientos de seguridad de información, y para identificar prioridades para pruebas y mantenimiento.	No se realiza procedimiento, apenas se esta investigando como implementar esta metodologia	1.- No se realiza	
14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad de negocios	*Control* Los planes de continuidad de negocios deben ser probados y actualizados regularmente para asegurar que son efectivos y oportunos.	No se realiza procedimiento, apenas se esta investigando como implementar esta metodologia	1.- No se realiza	

Conformidad con los requerimientos legales

15 Conformidad 15.1 Conformidad con los requerimientos legales			Observaciones	Evaluación	3,20
Objetivo: Para evitar brechas con respecto de cualquier ley, estatuto, regulación u obligación contractual y cualquier requerimiento de seguridad.					
15.1.1	Identificación de legislación aplicable	*Control* Todos los estatutos, regulaciones y requerimientos contractuales y el acercamiento de la organización para satisfacerlos debe estar explícitamente definido, documentado y actualizado para cada sistema de información y la organización.	Se encuentra documentado en la política de seguridad de la Información en revisión por la oficina jurídica.	3.- Se realiza informalmente en forma total	
15.1.2	Derechos de Propiedad Intelectual (IPR)	*Control* Procedimientos apropiados deben ser implantados para asegurar conformidad legal, regulatoria y contractual en el uso de material considerando que podría estar sujeto a derechos de propiedad y el uso de productos de softw are propietario.	Se realiza medeinte: - contratao de trabajo - convenios con acuerdo de confidencialidad - contratos de compras y venta tienen elementos de propiedad intelectual. Pero esta en revisión la Directiva transitoria "política propiedad intelectual"	2.- Se realiza parcial e informalmente	
15.1.3	Protección de registros de la organización	*Control* Los registros importantes deben ser protegidos de perdida, destrucción y falsificación, en conformidad con los estatutos, regulaciones, obligaciones contractuales y requerimientos de negocios.	El control de la documentación física se realiza por la oficina de archivo, se cuenta con directiva de gestión de archivo y correspondencia, pero no se encuentra con procesos o procedimientos normalizados. La información digital se encuentra protegida por control de acceso, pero tampoco se encuentra documentado el procedimiento.	3.- Se realiza informalmente en forma total	
15.1.4	Protección de datos y privacidad de la información personal	*Control* La protección de datos y la privacidad debe ser asegurada como sea requerido por la legislación, regulaciones y, si es aplicable, cláusulas contractuales.	Se contempla dentro del documento de políticas en proceso de revisión.	3.- Se realiza informalmente en forma total	

15.1.5	Prevención del mal uso de instalaciones de procesamiento de información.	*Control* El usuario debe ser disuadido de utilizar las instalaciones de procesamiento de información para propósitos no autorizados.	Se contempla dentro del documento de políticas en proceso de revisión y socialización al usuario final.	3.- Se realiza informalmente en forma total
15.1.6	Regulación de controles criptográficos.	*Control* Controles Criptográficos deben ser usados en conformidad con todos los acuerdos, leyes y regulaciones relevantes.	aun no se han implementado controles criptográficos en la Corporación.	1.- No se realiza
15.2 Conformidad con política y estándares de seguridad, y conformidad técnica				
Objetivo: Para asegurar conformidad de los sistemas con las políticas y estándares de seguridad organizacionales.				
15.2.1	Conformidad con políticas y estándares de seguridad	*Control* Los administradores deben asegurarse que todos los procedimientos de seguridad con sus áreas de responsabilidad son ejecutados correctamente para alcanzar conformidad con las políticas y estándares de seguridad.	Contemplado dentro del documento de políticas en revisión.	3.- Se realiza informalmente en forma total
15.2.2	Verificación de conformidad técnica	*Control* Los sistemas de información deben ser verificados regularmente para asegurar conformidad con los estándares de implantación de seguridad.	Actualmente no se realiza	1.- No se realiza
15.3 Consideraciones de auditoria de sistemas				
Objetivo: Para maximizar la efectividad de los procesos de auditoría de los sistemas de información y minimizar su interferencia.				
15.3.1	Controles para auditoria de sistemas de información	*Control* Los requerimientos de auditoria de sistemas de información y actividades de verificación involucradas deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocios.	Actualmente no se realiza auditoría interna, sólo las externas realizada por l la revisoría fiscal y Contraloría General de la Nación.	1.- No se realiza
15.3.2	Protección de herramientas de auditoria de sistemas	*Control* El acceso a las herramientas de auditoria de sistemas de información deben ser protegidos para prevenir cualquier mal uso o compromiso.	Actualmente no se realiza auditoría interna, sólo las externas realizada por l la revisoría fiscal y Contraloría General de la Nación.	1.- No se realiza

Anexo 3 -Tabla de evaluación de los dominios de la norma ISO/IEC 27001

	Lista de Verificación	
		Puntaje General

Cláusula	Indice	Evaluación
Política de Seguridad	5,00	Aceptable
Organización de Seguridad de Información	3,36	Suficiente
Adm. de Activos	3,00	Deficiente
Humanos	5,22	Aceptable
Seguridad física y ambiental	6,38	Aceptable
Operaciones	4,73	Aceptable
Control de Acceso	4,84	Aceptable
Adq., Des. y Mant. de sistemas de información.	2,38	Deficiente
Información	2,20	Deficiente
Adm. de Continuidad de Negocios	1,00	Deficiente
Conformidad con los requerimientos legales	3,20	Suficiente

Indice	Evaluación
3,76	Suficiente

Anexo 4- Cuestionario MSAT

Preguntas y respuestas

Las siguientes respuestas se proporcionaron como entrada en esta evaluación.

Cuestión de la evaluación	Su respuesta
Business Risk Profile	
Número de equipos de escritorio y portátiles que se utilizan en su empresa:	Mas de 500
Número de servidores que se utilizan en su empresa:	Más de 25 servidores
¿Tiene su empresa una conexión permanente a Internet?	Sí
¿Acceden los clientes y fabricantes a su red o sistemas internos a través de Internet?	No
¿Alberga su empresa algunos servicios de aplicaciones externas, como por ejemplo, un portal o un sitio Web, para sus socios o clientes externos?	No
¿Dispone su empresa de servicios que usen los clientes internos y externos en el mismo segmento de red?	No
¿Se conectan directamente los socios o clientes externos a los sistemas internos de la aplicación para acceder a los datos, actualizar los registros o gestionar de cualquier otra forma la información?	No
¿Se utilizan los mismos componentes de infraestructura de aplicación, como por ejemplo, bases de datos en apoyo de las aplicaciones externas y los servicios corporativos internos?	No

¿Permite su empresa que los empleados o los contratistas accedan remotamente a la red corporativa interna?	Sí
¿Se permite que los empleados puedan utilizar sistemas que no sean de producción en la red corporativa general, como por ejemplo, servidores Web personales o equipos que actúen como hosts de "proyectos personales"?	Sí
Aparte de los dispositivos de cinta y de copia de seguridad, ¿permite su empresa procesar la información confidencial o de propiedad fuera de las instalaciones?	Sí
En el caso de que los sistemas de seguridad se vieran comprometidos, ¿afectaría ello significativamente la capacidad comercial de su empresa?	Sí
¿Comparte su empresa espacio de oficinas con otras entidades?	Sí
¿Se desarrollan aplicaciones en su empresa?	Sí
¿Permite su empresa que los desarrolladores de software se conecten de forma remota a los recursos de desarrollo corporativos o que desarrollen remotamente código para	No

¿Desarrolla o pone en venta su empresa algunos productos de software para el uso de clientes, socios o el mercado en general?	No
¿Se permite que los desarrolladores prueben o desarrollen los sistemas en sitios remotos o inseguros?	No
¿Actúa el personal de TI como guardianes (en contraposición a los desarrolladores) de la línea de aplicaciones comerciales?	No
Según los procedimientos de su empresa, ¿es necesario la actuación de un tercero para almacenar, procesar o distribuir los datos?	No
¿Se almacenan o procesan los datos del cliente en un entorno compartido con los recursos corporativos?	No
¿Recurre a fabricantes independientes de software para complementar la oferta de servicios empresariales?	No
¿Obtiene su empresa ingresos por ofrecer servicios que incluyen el procesamiento o la minería de datos?	No
Los datos que procesan las aplicaciones de su empresa, ¿se consideran confidenciales o vitales para las operaciones comerciales de sus clientes?	Sí
¿Se ofrecen aplicaciones comerciales críticas a través de conexiones a Internet?	No
¿Quiénes son los usuarios objetivos de las aplicaciones principales de su entorno?	Empleados internos
¿Cómo acceden los usuarios a las aplicaciones principales?	Solamente desde la red interna

¿Está conectada su red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados?	No
¿Obtiene su empresa ingresos por servicios basados en el almacenamiento o la distribución electrónica de datos, como por ejemplo, archivos de medios o documentación?	No
En los últimos seis meses, ¿se ha sustituido radicalmente algún componente tecnológico de gran importancia?	No
¿La actividad de su empresa depende de la recepción o el procesamiento de datos por parte de socios, fabricantes o terceros?	No
Un incidente que afecte a las aplicaciones o a las infraestructuras orientadas a los clientes, como un apagón o el fallo de una aplicación o hardware, ¿afectaría significativamente a sus ingresos?	Sí
¿Almacena su empresa datos confidenciales de sus clientes o de importancia vital?	Sí
Los componentes de infraestructura y las aplicaciones del cliente, ¿dependen del acceso a recursos de su entorno?	No

¿Comparte su empresa los componentes de infraestructura y aplicaciones entre varios clientes?	No
¿Considera que los recursos de TI son un requisito para su empresa?	Sí
¿Utilizan todos los empleados de su empresa equipos informáticos para desarrollar su trabajo?	No
¿Subcontrata su empresa el mantenimiento o la propiedad de alguna parte de su infraestructura?	Sí
¿Tiene su empresa algún plan a medio o largo plazo para la selección y utilización de componentes de nuevas tecnologías?	Sí
¿Cree que su empresa participa en la adopción rápida de las nuevas tecnologías?	Sí
¿Selecciona e implanta su empresa nuevas tecnologías basadas en acuerdos de licencias y asociaciones existentes?	Sí
¿Limita su empresa las opciones relacionadas con la tecnología a aquellas que conoce actualmente el personal de TI?	No
¿Amplía su empresa su red mediante la adquisición de nuevas empresas con sus entornos correspondientes?	No
¿Permite su empresa que los empleados descarguen a sus estaciones de trabajo datos corporativos o datos confidenciales de los clientes?	Sí
¿Limita su empresa el acceso a la información en función de los roles de los usuarios?	Sí

¿Amplía su empresa su red mediante la adquisición de nuevas empresas con sus entornos correspondientes?	No
¿Permite su empresa que los empleados descarguen a sus estaciones de trabajo datos corporativos o datos confidenciales de los clientes?	Sí
¿Limita su empresa el acceso a la información en función de los roles de los usuarios?	Sí
¿Implanta su empresa nuevos servicios o aplicaciones antes de evaluar los posibles riesgos para la seguridad?	No
¿Cambia su empresa periódicamente las credenciales de las cuentas con privilegios?	Sí
¿Cambia su empresa las credenciales de las cuentas con privilegios cuando el personal deja de trabajar en la empresa?	Sí
Seleccione la opción que mejor defina el sector profesional de su empresa:	Fabricación (discreto)
Seleccione el número de empleados de su empresa:	Más de 500 empleados
¿Su empresa tiene más de una oficina?	Sí
¿La actividad de su empresa se desarrolla en un mercado de gran competencia o de investigación, en el que el robo de material intelectual o el espionaje son temas de gran preocupación?	Sí
¿Cambia muy a menudo el personal técnico en su empresa?	Sí

Infraestructura	
¿Utiliza su empresa cortafuegos u otros controles de acceso en los perímetros de la red para proteger los recursos corporativos?	Sí
¿Aplica su empresa estos controles en todas las oficinas?	Sí
¿Utiliza su empresa una zona neutral (normalmente conocida como 'zona desmilitarizada' o DMZ) para separar las redes internas y externas de los servicios albergados?	Sí
¿Alberga su empresa servicios relacionados con Internet en la red corporativa?	No
¿Utiliza su empresa software de cortafuegos basado en hosts para proteger los servidores?	Sí
¿Utiliza su empresa hardware o software de detección de intrusiones para identificar los ataques a la seguridad?	Sí
Seleccione los tipos de sistemas de detección de intrusiones (IDS) utilizados:	IDS basado en red (NIDS)
¿Se utilizan soluciones antivirus en el entorno?	Sí
Seleccione los sistemas que utilizan soluciones antivirus:	Servidores de correo electrónico
	Hosts del perímetro (pasarelas, proxies, relés, etc.)
	Equipos de escritorio
	Servidores

¿Se puede acceder a la red de la empresa de forma remota?	Sí
Seleccione quién se puede conectar a la red de forma remota:	Empleados
¿Se utiliza la tecnología de red privada virtual (VPN) para la conectividad segura a los recursos corporativos de los usuarios remotos?	Sí
¿Puede la VPN limitar la conectividad a una red aislada en cuarentena hasta que el cliente haya superado todas las comprobaciones de seguridad necesarias?	Sí
¿Se utiliza autenticación multifactor (token o tarjeta inteligente, etc.) para los usuarios remotos?	No
¿Tiene la red más de un segmento?	Sí
¿Se segmenta la red para separar los servicios de clientes externos y servicios extranet de los recursos corporativos?	Sí

¿Agrupa su empresa los hosts en segmentos de redes según los roles o servicios similares ofrecidos?	Sí
¿Agrupa su empresa los hosts en segmentos de redes para ofrecer únicamente los servicios necesarios a los usuarios que se conectan?	Sí
¿Se ha creado y documentado un plan para regular la asignación de direcciones TCP/IP a los sistemas según los segmentos necesarios?	No
¿Dispone la red de opciones de conexión inalámbrica?	Sí
¿Cuáles de los siguientes controles de seguridad se usan para regular las conexiones a las redes inalámbricas?	Cambio del nombre de red predeterminado/predefinido (conocido también como Identificador del conjunto de servicio o SSID) del punto de acceso Activar Acceso protegido de fidelidad inalámbrica (WPA) Activar restricciones de dirección por hardware (también conocido como Control de acceso al medio, o MAC) Conectar el punto de acceso a la red fuera del cortafuegos o en un segmento separado de la red de cable
¿Existen controles para hacer cumplir las directivas de contraseñas en todas las cuentas?	Sí

¿Cuáles de las soluciones siguientes se han instalado en las estaciones de trabajo y los portátiles de los empleados?	Software de cortafuegos particular
¿Su organización cuenta con procedimientos de respuesta ante incidentes formales?	No
¿Se han aplicado controles de seguridad físicos para garantizar la seguridad de los activos de la empresa?	Sí
¿Cuáles de los siguientes controles de seguridad se utilizan?	Sistema de alarma instalado para detectar e informar de intrusiones
	Equipos de red (conmutadores, cableado, conexión a Internet) en habitaciones cerradas con acceso restringido
	Los equipos de red se encuentran además en un armario cerrado
	Los servidores están en una habitación cerrada con acceso restringido
	Los servidores se hallan también en armarios cerrados
	Los materiales impresos confidenciales se almacenan en armarios cerrados
¿Cuáles de los siguientes controles de acceso físico se utilizan?	Tarjetas de identificación para empleados y visitantes
	Acompañantes de visitantes
	Registros de visitantes

Aplicaciones	
¿Dispone su empresa de una línea de aplicaciones comerciales (LOB)?	Sí
¿Utiliza macros personalizadas para las aplicaciones de Office (como, por ejemplo, Word, Excel o Access)?	Sí
¿Qué mecanismos tiene su empresa para asegurar una disponibilidad alta de las aplicaciones? Seleccione los mecanismos utilizados de la lista siguiente:	Ninguno
¿Ha desarrollado un equipo interno de desarrollo algunas de las aplicaciones principales de su entorno?	Sí
¿Proporciona con regularidad el equipo de desarrollo interno las actualizaciones de software y seguridad, así como la documentación sobre los mecanismos de seguridad?	No
¿Los consultores/proveedores de terceros han desarrollado alguna aplicación clave implementada en su entorno?	No
¿Qué metodologías de desarrollo de seguridad de	Ninguna

software se practican en su empresa? (Seleccione todas las respuestas que correspondan)	
¿Conoce su empresa las vulnerabilidades de seguridad que existen actualmente en las aplicaciones de su entorno?	No
¿Su empresa proporciona formación sobre seguridad para el personal de desarrollo y pruebas?	No
¿Su empresa confía en herramientas de software como parte del proceso de prueba y auditoría para el desarrollo de software seguro?	No
¿Existen controles para hacer cumplir las directivas de contraseñas de las aplicaciones principales?	Sí
Seleccione los controles de contraseña implantados en las aplicaciones principales:	Contraseñas complejas Caducidad de las contraseñas
En la siguiente lista, seleccione el método de autenticación más común de las aplicaciones principales:	Contraseña compleja
¿Tienen las aplicaciones principales del entorno mecanismos para limitar el acceso a los datos y las funciones confidenciales?	Sí
¿Guardan las aplicaciones principales del entorno mensajes en archivos de registro para su análisis y auditoría?	Sí
Seleccione los tipos de eventos que se registran:	Intentos de autenticación fallidos

	Autenticaciones correctas
	Errores de la aplicación
	Cambios en los datos
	Cambios en las cuentas de usuarios
¿Las aplicaciones utilizadas validan los datos de entrada?	Sí
Seleccione los tipos de entrada que validan las aplicaciones:	Usuarios finales
¿Cifran las aplicaciones principales los datos confidenciales y críticos de la empresa que se encargan de procesar?	No
Operaciones	
¿Es la empresa la que gestiona el entorno o se contrata los servicios de un tercero?	La empresa gestiona el entorno
¿Utiliza la empresa hosts de gestión dedicados a la administración segura de los sistemas y dispositivos del entorno?	No
¿Se utilizan cuentas de registro individuales para las actividades normales en contraposición con las	No

actividades administrativas o de gestión?	
¿Garantiza la empresa a los usuarios el acceso administrativo a sus estaciones de trabajo y equipos portátiles?	Sí
¿Se comprueba periódicamente los cortafuegos para garantizar que funciona según lo previsto?	No
¿Su organización mantiene planes de recuperación ante desastres y de reanudación de negocio?	No
¿Existe un modelo para asignar niveles de importancia a los componentes del entorno informático?	No
¿Existen directivas para la regulación del entorno informático?	No
¿Hay un proceso documentado para la creación de hosts? Si la respuesta es afirmativa, ¿de qué tipo? (¿Para qué tipos de hosts hay un proceso de creación documentado?)	Ninguno
¿Hay pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa? Seleccione la opción adecuada:	No hay directivas
¿Su organización dispone de un proceso formal bien documentado para la eliminación de datos en medios electrónicos y en formato impreso?	No
¿Su organización dispone de un esquema de clasificación de datos con directrices de protección de datos asociadas?	No

¿Hay un proceso de gestión para las configuraciones y los cambios?	No
¿Existe un proceso establecido para las directivas de actualización y revisión?	No
¿Existe una directiva establecida por la que se regule la actualización de productos de detección basados en firmas?	Antivirus
¿Hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los hosts?	No
¿Existen diagramas exactos de la arquitectura y del flujo de datos de las aplicaciones principales?	Sí
Seleccione los tipos de aplicaciones de las que existen diagramas:	Sólo aplicaciones internas
¿Está activado en el entorno el registro de los eventos producidos en los hosts y los dispositivos?	Sí
¿Toma medidas la empresa para proteger la información incluida en los registros?	El sistema operativo y las aplicaciones están configuradas para no sobrescribir eventos
¿Revisa la empresa periódicamente los archivos de registro?	Sí
¿Con qué frecuencia se revisan los registros?	Según sea necesario

¿Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente?	Sí
¿Existen directivas y procedimientos para el almacenamiento y la gestión de los dispositivos de copias de seguridad?	No
¿Existen directivas para la comprobación periódica de los procedimientos de copias de seguridad y restauración? Estas directivas, ¿están documentadas?	No
Personal	
¿Hay en su empresa individuos o grupos que sean responsables de la seguridad?	Sí
¿Tienen estos individuos o grupos experiencia en el tema de la seguridad?	Sí
¿Estos individuos o grupos se ocupan de establecer los requisitos de seguridad de las tecnologías nuevas y existentes?	Sí
¿En qué etapa del ciclo de vida de la tecnología suele participar este equipo o individuo encargado de la seguridad?	Planificación y diseño
¿Existen responsabilidades y roles definidos para cada individuo que participa en la seguridad de la información?	Sí
¿Realiza su empresa evaluaciones de la seguridad del entorno a través de terceros?	No
¿Realiza su empresa evaluaciones de la seguridad del entorno de forma interna?	No

¿Realiza la empresa comprobaciones del historial personal como parte del proceso de contratación?	No
¿Hay un proceso formal para la salida de la empresa de los empleados?	Sí
Seleccione las opciones para las que exista un proceso formal para la salida de la empresa de los empleados:	Salidas hostiles Salidas amistosas
¿Hay una directiva formal para las relaciones con terceros?	No
¿Hay un programa de divulgación de las medidas de seguridad en su empresa?	No
¿Se ofrece a los empleados formación relacionada con el cargo que desempeñan en la empresa?	Sí
Seleccione las opciones que correspondan en la siguiente lista:	Preparación para incidentes y reacción