Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN GESTIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

PROYECTO
TRABAJO FINAL DE MAESTRÍA

Metodología para la integración de la norma ISO/IEC 27001:2013 en una empresa industrial naviera

AUTOR: LUIS PAOLO TAPIA MONTOYA

DIRECTOR: PATRICIA PRANDINI

MAYO 2020

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Índice General

Lista de Ilustraciones

Lista de tablas

Resumen del Proyecto

La dificultad para identificar adecuadamente el riesgo y las falencias de gestión de la seguridad de la información amenazan a la organización y directamente a su operación y resultan preocupantes ya que pueden condicionar su subsistencia. Por tanto, el departamento de TICs[1] debe poner en práctica las tareas inherentes que le sean requeridas por la entidad, con el fin de mejorar el ambiente de control.

En este contexto, es vital la identificación y revisión de los riesgos, amenazas y vulnerabilidades de los sistemas, identificando las inseguridades que pudieran afectarla y estableciendo las medidas necesarias para alcanzar los objetivos definidos según cada proceso. Estos procesos especifican las actividades propias de la empresa y sus partes interesadas de manera sistematizada, fijando controles que regulen el seguimiento, dando como resultado mejoras específicas y la posibilidad de saber dónde actuar conforme a las normas establecidas.

Para alcanzar dichos objetivos el autor utilizará la metodología exploratorio-descriptiva con un enfoque cualitativo abordando el estudio y análisis de la situación de los procesos desde la perspectiva de la seguridad de la información que estos tratan.

De hecho, la revisión integral de los procesos desde la mirada de la gestión de seguridad de la información permitirá cambios en la cadena de valor, fortaleciendo su confidencialidad, integridad y disponibilidad según lo requiere el negocio y ayudando a los interesados a lograr con eficiencia sus objetivos, frente a un panorama cambiante de amenazas.

El presente trabajo pretende aportar una metodología estándar de implementación de controles en seguridad de la información, aplicada a una empresa industrial naviera, a partir de la identificación de procesos de negocio, buscando recomendar las modificaciones necesarias que le permitan superar la auditoría externa previa a la certificación de la norma internacional ISO/IEC 27001:2013.

[1] **Tecnologías de la Información y la Comunicación** (en inglés *ICT: Information and Communications Technology*). Este concepto hace referencia a las teorías, las herramientas y las técnicas utilizadas en el tratamiento y la transmisión de la información: informática, internet y telecomunicaciones.

Justificación / Fundamentación

Teniendo en cuenta el gradual aumento de información sensible generada por las organizaciones, cada vez es más difícil proteger y controlar los datos, los cuales deben ser tratados de forma segura en las aplicaciones. En este sentido, se pretende perfeccionar los aspectos relacionados con la seguridad de la información debido a que las empresas han entendido que deben contar con procesos estructurados para cumplir con estándares que certifiquen la evaluación, el tratamiento de los riesgos y la mitigación temprana de potenciales incidentes de seguridad, en el menor tiempo posible. La adopción de estándares asegura la disponibilidad de la información para mantener los niveles de competitividad y el estatus vigente, frente al constante cambio tecnológico que día a día enfrentan.

El presente trabajo propone aportar evidencia para demostrar que la adopción de un estándar de seguridad de la información a partir del análisis holístico del área que está a cargo de mantener la infraestructura necesaria para tratar los datos contribuye a un mejor ordenamiento del negocio y constituye una parte esencial de la estrategia de la organización. Asimismo, se busca agilizar los procesos de seguimiento y evaluación de alto nivel, demandas estas de algunas de partes interesadas correspondientes, como por ejemplo los comités y la presidencia de la organización.

Planteamiento del problema

Las dificultades para identificar el riesgo y las falencias a la hora de gestionar la seguridad de la información que amenazan a la organización en su conjunto afectando a todos sus procesos, es un problema que debe atenderse con la mayor prioridad.

De hecho, las empresas enfrentan el peligro de perder información, lo que podría comprometer su operación, entre otras consecuencias negativas. Por tanto, resulta imprescindible una seguridad efectiva, en base a una metodología establecida que contemple todos los procesos y permita mantener la trazabilidad.

El objetivo del trabajo es identificar los controles de seguridad con los que se pueden minimizar las amenazas e identificar y neutralizar las vulnerabilidades que están presentes.

En definitiva, en un mundo globalizado y cada vez más competitivo y caracterizado por pretender alcanzar permanentemente la arista en innovación, cada organización se ha dado cuenta que el recurso más importante es el dato generado a partir de las actividades que lleva adelante y que por lo tanto, debe ser protegido adecuadamente.

En este sentido, es primordial que cuenten con un sistema de gestión de seguridad de la información, que forme parte de los procesos y se integre con la estructura organizativa.

Preguntas Problematizantes

¿Cómo afecta a la organización una insuficiente preocupación profesional por la protección efectiva de la información y la falta de seguimiento sobre los controles a los procesos?

¿Cómo se puede reducir el riesgo de pérdida o daño a la información y a los activos informáticos en la organización?

¿De qué manera se puede asegurar la mejora continua de la seguridad de los sistemas informáticos?

Objetivo general

Identificar los procesos críticos relacionados con la seguridad en la gestión de accesos, activos y aplicaciones, con la finalidad de implementar una metodología que permita determinar los controles de seguridad adecuado, basados en la Norma Internacional ISO/IEC 27001:2013, para asegurar la gestión y mejora continua del Sistema de Gestión de la Seguridad de la Información de la organización.

Objetivos secundarios

- Relevar mediante un esquema de Arquitectura Empresarial, las fases en que se apoyan los procesos de negocios, con énfasis en la gestión de seguridad de la información.
- Identificar brechas relacionadas con el caso de estudio, para determinar un marco de trabajo de fácil comprensión para el cumplimiento en la organización.
- Analizar e identificar los controles de la Norma ISO/IEC 27001:2013 que se deben aplicar para lograr el aseguramiento y mantenimiento del Sistema de Gestión de la Seguridad de la Información.
- Brindar una metodología de gestión adaptada a la seguridad de la información basada en un estándar y en las mejores prácticas para los procesos de la organización.

Hipótesis

La implementación de la Norma ISO/IEC 27001:2013 optimizará los procesos de una empresa constructora naviera, contribuyendo a la mejora de la gestión de la seguridad de su información.

Marco Teórico

El avanzado cambio en el mercado y la evolución de la tecnología debe ser afrontado por las empresas sin importar su naturaleza, tamaño o actividad económica. Su enfoque principal debe ser el de asumir estos cambios como oportunidades de desarrollo. En este aspecto juegan un papel importante los marcos de trabajo y estándares como medios para ayudar al logro de los objetivos del negocio y para contribuir a la mejora de la infraestructura tecnológica que servirá como soporte en los procesos a desarrollar.

En consecuencia, este documento permite explorar cada uno de los conceptos para el desarrollo de un modelo integral, que incluya al negocio, la infraestructura tecnológica utilizada y la metodología de procesos para el planeamiento del proyecto. Por otro lado, se explicarán los controles de seguridad que debe implementar el departamento de sistemas para el desarrollo del proceso de gestión en seguridad de la información. A continuación, se describen los estándares necesarios para el desarrollo del presente trabajo.

Arquitectura Empresarial (TOGAF)

TOGAF (Open Group Architecture Framework) es un estándar desarrollado por The Open Group, cuya versión vigente es TOGAF 9.1. Su objetivo principal es generar un esquema o marco de trabajo de arquitectura empresarial, representada en sistemas de bases de datos, hardware y software para todas las unidades de negocio de la empresa, con la finalidad de impulsar un cambio estratégico expresado a través de la calidad de la información generada. La composición de la Arquitectura empresarial se desarrolla en cuatro capas:

- Arquitectura de negocios: en esta capa se detalla la estrategia global de la empresa tomando en cuenta los cambios a los que se someterá, de acuerdo a los lineamientos de los interesados en un primer proceso de ingeniería de requerimientos.
- Arquitectura de aplicaciones: definida también como arquitectura de soluciones, en este aspecto se manejan las funcionalidades que deben ser desarrolladas de forma individual, para luego relacionarlas directamente con los procesos de negocios.

- Arquitectura de datos: es donde se concentra la información en tablas relacionales, de manera que permiten maximizar la inteligencia de los procesos de negocios.
- Arquitectura de infraestructura tecnológica: es la capa considerada cítrica, que concentra componentes como el software y el hardware que deben respaldar los recursos de base de datos, directorios y otros. Representa la parte física basada en la implementación del marco de trabajo TOGAF.

La metodología TOGAF para la administración del ciclo de vida y el proceso cíclico interactivo de los requerimientos, los gestiona de la siguiente forma:

Fase preliminar: Define el modelo de la arquitectura y el marco de trabajo a utilizar para evaluar los principios del proyecto. Es donde se prepara y se inician las actividades de todo el proceso, se comprenden los entornos de negocios y se establecen los principios y las estructuras del proceso de análisis.

Fase A: Visión de la Arquitectura, se define el alcance de las actividades que identifican a los interesados del proyecto, además mantiene las restricciones del negocio.

Fase B: Arquitectura de Negocios, se identifica la línea base del negocio y se permite la estandarización de las actividades transaccionales y analíticas

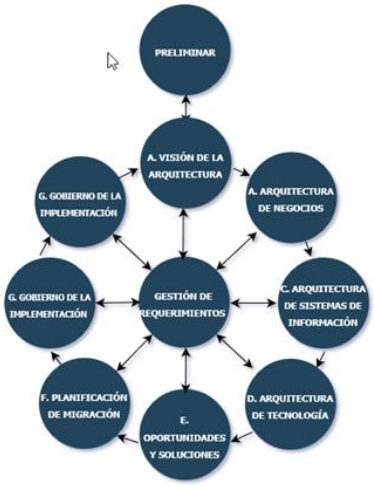
Fase C: Arquitectura de Sistemas de Información, se identifica el dato relacional y la interacción entre bases de datos.

Fase D: Arquitectura de Infraestructura Tecnológicas, se determina el software y hardware que intervienen como soporte de las arquitecturas de información y negocios.

Fase E: Oportunidades y soluciones, se releva lo analizado en la arquitectura de negocio y se detallan las mejoras a implementar.

Fase F: Plan de Migración, se determina los costos, beneficios y riesgos del proyecto y posteriormente, se traza la hoja de ruta para la implementación y migración de la arquitectura general. (The Open Group, 2013)

Ilustración 1 Arquitectura Empresarial TOGAF



Norma ISO/IEC 27001:2013

Esta norma internacional ha sido elaborada y aprobada con la finalidad de proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información. Este estándar internacional fue publicado por la Organización Internacional de Estandarización y por la Comisión electrónica internacional en octubre del 2005 y actualmente es el único aceptado a nivel internacional en seguridad de la información. Se espera que la implementación del sistema de gestión de seguridad de la información se aplique de acuerdo a las necesidades de la organización. Esta norma puede ser utilizada por las partes internas y externas en la entidad, para la evaluación de la información y para cumplir con sus propios requisitos en seguridad de la información. Sin embargo, el orden en que son presentados los requisitos en la norma no refleja su importancia ni implica un orden en el cual deben ser implementados.

Se trata de requisitos genéricos que fueron incluidos para ser aplicados en todas las organizaciones, independientemente del tipo, tamaño o naturaleza.

Para el propósito del presente documento, se expondrá una guía con los controles relativos a gestión de accesos y controles de equipos y respaldo para garantizar el cumplimiento de un sistema de gestión en seguridad de la información.

En consecuencia, la empresa naviera al afrontar un elevado número de riesgos informáticos y las inseguridades que provienen de dentro y fuera de la organización, requiere la adopción de medidas preventivas para contribuir a la seguridad de su información. Por esta razón, la adopción de la Norma ISO/IEC 27001:2013 es una solución apropiada. Por tanto, el SGSI[2] según la Norma ISO/IEC 27001 sigue el enfoque se basa en el Ciclo de Deming para evaluar los riesgos e implantar los controles y estrategias en los procesos, presentándolos según se detalla a continuación:

Mejora

No Conformidad y acción correctiva.

Cuando ocurre una no conformidad, la organización debe:

a) Reaccionar hacia la no conformidad, y según corresponda

1) Tomar acción para controlarla y corregirla: y

2) Liderar con las consecuencias.

b) Evaluar la necesidad de acción para eliminar las causas de la no conformidad, con la finalidad de evitar la recurrencia o la ocurrencia en cualquier otro lugar, mediante:

1) La revisión de la no conformidad

2) La determinación de las causas de la no conformidad.

3) La verificación de si existe una no conformidad similar, o podría darse;

c) La implementación de una acción necesaria;

d) La revisión de la efectividad de las acciones correctivas tomadas; y

e) La implementación de cambios al sistema de gestión de seguridad de la información, si fuera necesario.

Las acciones correctivas deben ser acordes a los efectos de las no conformidades encontradas.

[2](SGSI) Es un conjunto de políticas de administración de la información utilizado principalmente por la ISO/IEC 27001:2013.

La organización deberá conservar la información documentada como evidencia de:
f) La naturaleza de las no conformidades y cualquier acción tomada posteriormente, y
g) Los resultados de las acciones correctivas (Comité Técnico Colectivo ISO/IEC JTC 1, 2013)
Mejora Continua
La organización deberá mejorar de manera continua la idoneidad, adecuación y efectividad del sistema de gestión de la seguridad de la información

Norma ISO/IEC 27002:2013

Es una guía de buenas prácticas que describe los objetivos de control recomendados para implementar un sistema de seguridad de la información según el estándar anterior. No es certificable. La versión 2013 de la norma se estructura en catorce dominios o secciones de seguridad, treinta y cinco objetivos de control que reflejan aquello que se quiera conseguir y un total de ciento catorce controles que hay que implantar. Asimismo, aborda de manera específica cuestiones relativas a criptografía y relaciones con los proveedores. En consecuencia, la Norma ISO/IEC 27002:2013 con relación al estándar ISO/IEC 27001:2013 permitirá la gestión en seguridad de la información para el control y la clasificación de los activos de manera coherente con el modelo de negocio, entre otras cuestiones de seguridad. En consecuencia, el autor propone en el presente documento el uso de la Norma ISO/27002:2013 para el análisis de los procesos al igual considerando las interrelaciones que existen entre ellos y los activos de información implicados.

Norma ISO/IEC 27005:2008

Establece los principios para la gestión de riesgo en seguridad de la información. Diseñada para ayudar a la aplicación de la seguridad de la información usando dicho en enfoque, es aplicable a todo tipo de organización. Está compuesta de doce clausulas y seis anexos que apoyan el desarrollo de cada una de ellas para la implementación de esta norma. El objeto principal de la Norma ISO/IEC 27005:2008 es el respaldo de los conceptos generales especificados en la Norma ISO/IEC 27001:2013 desde la perspectiva del riesgo y el establecimiento de una Declaración de aplicabilidad[3] que contiene los controles asignados para la mitigación de los riesgos de los procesos alcanzados.

Para los fines de la norma ISO/IEC 27005:2008, los términos y definiciones más destacados dados en la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013 se aplican son los siguientes:

1. Impacto: Adverso a los cambios a nivel de los objetivos de negocios alcanzados.
2. Riesgo de seguridad de la información: Potencial de una amenaza para aprovechar las vulnerabilidades de un activo o grupo de activos y por lo tanto, causar daño a la organización. Nota: se mide en términos de una combinación de la probabilidad de un evento y su consecuencia.
3. Eliminación del riesgo: Decisión o acción de retirarse de una situación de riesgo.
4. Comunicación de riesgos: Canje o intercambio de información sobre el riesgo entre el o los que toman las decisiones y otras partes interesadas.
5. Estimación del riesgo: Proceso para asignar valores a la probabilidad y consecuencias de un riesgo.
6. Identificación de riesgo: Proceso para encontrar la lista, y caracterizar elementos de riesgo.
7. Reducción de riesgo: Las acciones tomadas para disminuir la probabilidad, consecuencias negativas o ambas cosas, asociado con un riesgo.

[3]**Declaración de Aplicabilidad,** Es un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar **ISO/IEC 27001** (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad).

8. Retención del riesgo: La aceptación de la carga de la pérdida o beneficio de la ganancia de un riesgo particular.
9. Transferencia de riesgo: Compartir con otra parte de la carga de la pérdida o beneficio de ganancia, para un riesgo.

Criterios Básicos de la Norma

Dependiendo del alcance y objetivos de la gestión de riesgos, se pueden aplicar diferentes enfoques. Este enfoque también puede ser diferente para cada iteración.

Un enfoque de gestión de riesgos adecuado debe seleccionar o desarrollar quien se ocupará de determinar los criterios básicos, tales como: criterios de evaluación de riesgo, los de impacto y los de aceptación del riesgo. Además, la organización debe evaluar si los recursos necesarios están disponibles para realizar la evaluación de riesgo y establecer un plan para su tratamiento, definir e implementar políticas y procedimientos, incluida la aplicación de los controles de monitor seleccionado y monitorear la seguridad de la información y los riesgos asociados a los procesos. A continuación, se listan algunos de los criterios a tener en cuenta:

1. Criterios de evaluación de riesgos: se deben desarrollar para la evaluación de aquellos riesgos de seguridad de la información de la organización, teniendo en cuenta el valor estratégico del proceso de información comercial, de los activos de información involucrados y los requisitos legales y reglamentarios.
2. Criterios de impacto: deben desarrollarse y especificarse en términos del grado de daño a la organización, causados por un evento de seguridad de información teniendo en cuenta las siguientes particularidades:
    a) Nivel de clasificación del activo afectado.
    b) Infracciones de seguridad de la información (por ejemplo, pérdida de la confidencialidad, integridad y disponibilidad), deterioro de operaciones (de partes internas o de terceros), pérdida de valor en el negocio o financiera, alteración de los planes o daños a la reputación.

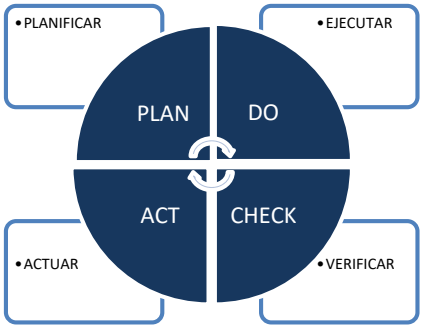
3. Criterios de aceptación del riesgo: la aceptación a menudo depende de las políticas de la organización, sus metas y objetivos y los objetivos de las partes interesadas.
4. Criterios de negocio: referente a los aspectos legales y reglamentarios que pueden afectar las operaciones, las tecnologías y las finanzas.

Por tanto, el autor pretende realizar la evaluación de riesgo en los procesos críticos involucrados en el establecimiento de una declaración de aplicabilidad, que contendrá los controles identificados como propuesta del presente trabajo final de maestría.

Método de estrategia en Calidad, Ciclo de Deming

El ciclo de Deming, también identificado por su acrónimo PDCA por las siglas de Plan (Planificar), Do (Hacer), Check (Verificar) y Act (Actuar), es un método que permite establecer un objetivo y emplear fases para lograr una mejora continua en los procesos. Este método puede aplicarse en cualquier organización, realizando un sistema cíclico y continúo y ejecutando cambios medibles en la gestión del área o sistema sobre el que se desee actuar. A continuación, se presenta el gráfico de Deming y se describen sus fases:

Ilustración 2 Ciclo de Deming



Planificar (Plan): Esta etapa indica qué debemos hacer y cómo vamos a gestionar, revisando los procesos de la empresa señalados como los que requieren especial atención de la alta gerencia, incluyendo la determinación de la técnica o procedimiento adecuado de acuerdo con el propósito que debamos alcanzar y así establecer posible medida para minimizar riesgos.

Ejecutar (Do): En esta fase se empieza a establecer lo planificado anteriormente y los cambios que serán implantados a medida que se ejecute la propuesta.

Verificar (Check): Luego de implantar la mejora son necesarias las mediciones y el seguimiento para verificar los resultados obtenidos.

Actuar (Act): Se inician medidas para corregir y mejorar las desviaciones de acuerdo a los resultados obtenidos. De hecho, para conseguir los mejores resultados debemos aprender de los errores que se van cometiendo. Si dichos resultados luego de las evaluaciones son satisfactorios, se implantará la mejora continua definitiva. (Rodriguez, 2014)

Análisis GAP (brechas)

Es una herramienta utilizada por el análisis estratégico[4], una más entre las muy diferentes disponibles para alcanzar un diagnóstico previo a la formulación estratégica. El análisis gap pretende visualizar los equilibrios o desfases que presentaría la empresa según diferentes formas de enfocar la visión del futuro. Trata de contestar, sucesivamente a dos preguntas claves en la fase de análisis estratégico: ¿Qué está ocurriendo ahora en la empresa y en su entorno? ¿Qué deberíamos estar haciendo para alcanzar determinados objetivos, como por ejemplo la propia supervivencia de la empresa en el mercado? Son cuatro formas de visionar el futuro: extrapolación histórica, prospectiva, competitividad y diversificación.

Como ocurre en otros casos semejantes, la calidad y características de las respuestas del análisis está condicionada por el modelo mental del diseñador de la herramienta. Es decir, las respuestas llevan implícitas la focalización y las relevancias que se pretende visualizar. En este caso se busca reconocer de qué forma el desfase total de la empresa es el resultado

[4] **Análisis estratégico:** es el proceso que se lleva a cabo para investigar sobre el entorno de negocios dentro del cual opera una organización y el estudio de la propia organización, con el fin de formular una estrategia para la toma de decisiones y el cumplimiento de los objetivos.

de la suma de desfases sucesivos, según se vayan aplicando procedimientos de análisis más sofisticados, a través de un recorrido que va desde una simple extrapolación histórica del pasado hasta un análisis de diversificación. Esto va dejando en evidencia desfases o "gaps" que se van acumulando: gap de observación, gap competitivo y gap de diversificación.

Pedagógicamente este instrumento destaca la diferencia básica entre la planificación a largo plazo (PLP), y la planificación estratégica (PE), que está en la visión que cada una tiene del futuro. En la PLP el futuro se pronostica mediante la extrapolación de su desarrollo histórico. La alta dirección asume, en este caso, que el futuro será mejor que el pasado. En la PE no se espera que el futuro sea necesariamente mejor que el ayer, ni tampoco que este (el ayer) sea extrapolable. Para poner en evidencia este hecho, el método lleva a cabo cuatro pasos.

Primer paso: Sobre la línea resultante de la simple extrapolación histórica del pasado se lleva a cabo un análisis prospectivo para identificar las tendencias, amenazas, oportunidades y acontecimientos singulares que puedan hacer cambiar la tendencia histórica. La diferencia entre la simple extrapolación y el análisis prospectivo dará lugar al gap de observación.

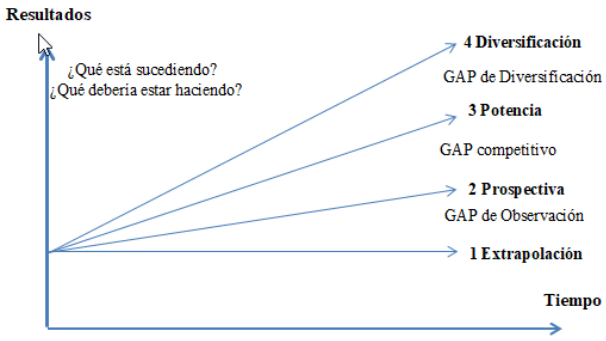
Segundo paso: Se lleva a cabo un análisis competitivo que identifique las mejoras que se puedan obtener mediante el perfeccionamiento de su postura competitiva en las distintas áreas de negocio de la empresa. Mediante el análisis competitivo, se puede apreciar que no todas las áreas son igualmente prometedoras.

Tercer paso: Como consecuencia de la variada situación de cara al futuro, que se aprecia para cada área de negocio, en el tercer paso se lleva a cabo el análisis portafolio mediante el que se comparan las perspectivas de cada área, se establecen prioridades y se asignan recursos estratégicos a las áreas.

La resultante de estos dos análisis, competitivo y portafolio, llevados cabo en el segundo y tercer paso, se configuran una tercera línea luego de la extrapolación y la prospectiva antes mencionadas, llamada la potencia deseable de la empresa que, al enfrentarla con la línea de prospectiva establecida en el segundo paso, provoca el segundo desfase llamado gap competitivo.

Cuarto paso: En algunos casos, la línea de potencia deseable (con una mirada al negocio actual) es inaceptable para la dirección, bien por la vulnerabilidad estratégica del actual portafolio, porque la línea de prospectiva muestra un desequilibrio entre las prospectivas a largo y a corto plazo, o porque las ambiciones de crecimiento están por encima de la línea de prospectiva. En tales casos, el próximo paso a aplicar es el análisis de diversificación que diagnostica las diferencias del actual portafolio para la empresa. Ahora la diferencia entre la línea de potencial actual y la de diversificación, dejará en evidencia el gap de diversificación. A continuación, se muestra el gráfico con las resultantes gap.

Ilustración 3 Herramienta del Análisis estratégico



Fuente: (Coronado F. J., 2003)

El valor estratégico del análisis gap está en que al preparar una estrategia surjan una serie de preguntas clave: qué habilidades, recursos, capacidades y competencias, en definitiva, ventajas competitivas, serían necesarias para alcanzar con éxito o sea el futuro posible elegido. Frente a este perfil ideal que nos conduciría al éxito, la empresa debe ser realista, y evaluar sus actuales debilidades, capacidades, recursos y competencias relativas, lo que le permite identificar las lagunas o gaps significativos existentes. El método se caracteriza por llevar a cabo una investigación en sentido inverso, desde el futuro al presente, desde el perfil competitivo al que se aspira, a la realidad presente. Esta toma de conciencia nos permite orientar, desde el presente, los pasos que debemos empezar a dar ya para alcanzar el futuro

que deseamos. Es el reflejo de una actitud proactiva, de querer influir en el futuro, en lugar de una actitud meramente de ajuste. Es un ejercicio instructivo mediante el cual se toma conciencia de las debilidades y vulnerabilidades que nos impedirán cumplir la misión que nos hemos impuesto, lo que probablemente generará el impulso necesario para crear los puentes que nos permitan salvar las brechas, lagunas o debilidades percibidas. (Coronado F. J., 2003)

Cambio Organizacional

Las propuestas de cambio suelen tener un resultado contraproducente, ya que existen ejecutivos y personal administrativo de distintas áreas que se vuelven negativos ante los diversos enfoques que la organización pretende iniciar en los procesos de transformación digital. Por ende, es importante involucrar a todo el personal y fomentar la comunicación en todos los niveles de la empresa para evitar frenos en el transcurso de los proyectos de cambio. Una estrategia de cambio en la organización implica converger procesos alimentados por las actividades de individuos de distintos niveles de jerarquías. De tal modo, el cambio debe ser abordado sin perder el trabajo colectivo de los diversos actores de la organización. Por otro lado, las reglas laborales que nacen de las implementaciones de un sistema nuevo dan señales a través de cambios de conducta del personal, que deben ser estudiados de acuerdo con el avance del proyecto.

En todo cambio organizacional, la Dirección o el equipo de proyecto a menudo se enfrentan a la resistencia de las personas, aun cuando muchos ejecutivos con experiencia están conscientes de este hecho. Para minimizar el impacto negativo ante el cambio, se evaluarán distintos aspectos primordiales que agilicen la absorción del conocimiento. Algunos de estas reacciones del comportamiento humano se desarrollarán al implementar las normas de seguridad informática. Algunas de ellas se encuentran descritos a continuación:

• Baja tolerancia al cambio
• Resistencia al liderazgo
• Falta de acompañamiento y facilitación
• Ausencia o escasa participación y compromiso

Metodología y técnicas para utilizar

El autor propone como investigación el caso exploratorio / descriptivo con enfoque cualitativo. Inicialmente se realizará un estudio de la situación actual de los procesos organizacionales usando marcos de referencias y buenas prácticas.

Para modelar la ejecución de las acciones y la puesta en marcha de los escenarios, se identificará el proceso más crítico para la organización.

Como explicación analítica se expondrá gráficamente el proceso vinculado a la seguridad de la información para llevar adelante la estrategia de abordaje del problema planteado, sobre la base de los requisitos establecidos por la Norma Internacional ISO/IEC 27001:2013.

En definitiva, para el propósito del presente documento se expondrá una metodología viable de controles de gestión de seguridad de la información, con énfasis en accesos físicos y lógicos, respaldo del dato compartido y gestión de riesgos y de activos de información para la implementación de un estándar en seguridad de la información, de acuerdo a las necesidades del proceso, buscando el agregado de valor a la organización.

Capítulo I

TOGAF para el relevamiento de información en la organización.

En adelante se desarrolla un esquema de relevamiento de seguridad de la información, haciendo uso del Método de Arquitectura Empresarial en sus fases más críticas (ADM[5] por sus siglas en inglés). La norma ISO/IEC 42010:2007 [6]define "arquitectura" como; "La organización fundamental de un sistema, conformada por sus componentes, las relaciones entre ellos y su entorno, así como los principios que gobiernan su diseño y evolución". A continuación, se desplegará las fases que se requieren para lograr el objetivo mencionado, enfocado en la seguridad de la información.

Fase Preliminar: de TOGAF

El presente documento desarrolla un esquema de entorno empresarial identificando las relaciones estratégicas y de gobierno que apoyan al negocio, teniendo presente las unidades organizacionales y los actores involucrados en su entorno de gestión, con el fin de verificar los riesgos informáticos que pudieran limitar la continuidad de las actividades de negocio, así como la gestión de la seguridad de la información. Para esta fase, se describirán las estructuras de gobierno de la organización en que se apoya el proceso crítico "Desarrollo de proyectos", seleccionado como crítico para el aseguramiento de los sistemas de información.

Presentación de la empresa, estructura de gobierno, misión, visión y sus entornos de negocios

La organización es una empresa naviera con más de cuarenta años en el mercado naval ecuatoriano fomentando el desarrollo industrial marítimo y apoyado por la innovación en tecnología. Desde sus inicios ha buscado el desarrollo permanente para competir por ser uno de los astilleros de mayor capacidad productiva industrial naviera del país.

[5] **El ADM,** es un método para obtener las arquitecturas empresariales (negocio, aplicaciones, datos y tecnología) que son específicas en la organización y se fundamenta como el núcleo del marco de referencia TOGAF.
[6]**ISO/IEC 42010: 2007**, Ingeniería de sistemas y software. Práctica recomendada para la descripción arquitectónica de sistemas de software intensivo.

De acuerdo con el Manual para la Planificación Institucional, la organización se fundamenta en un sistema de gestión empresarial que la faculta para articular su estrategia en todos sus niveles. A partir de allí, da inicio a las actividades de alto nivel que permitirán cumplir con la misión, objetivos y metas trazadas en el Plan estratégico.

En definitiva, su objetivo es impulsar soluciones industriales finales que requieren de una estrecha relación con entidades financieras, académicas y reguladoras para crear productos y servicios hacia sus clientes de empresas nacionales e internacionales.

Misión

Ser la primera alternativa para defensa, seguridad en el sector marítimo e industrial a nivel nacional y una alternativa competitiva en el mercado internacional en nuestras líneas de negocio.

Visión

Desarrollar, producir y mantener soluciones sustentables para potenciar la defensa, seguridad y los sectores marítimos e industriales.

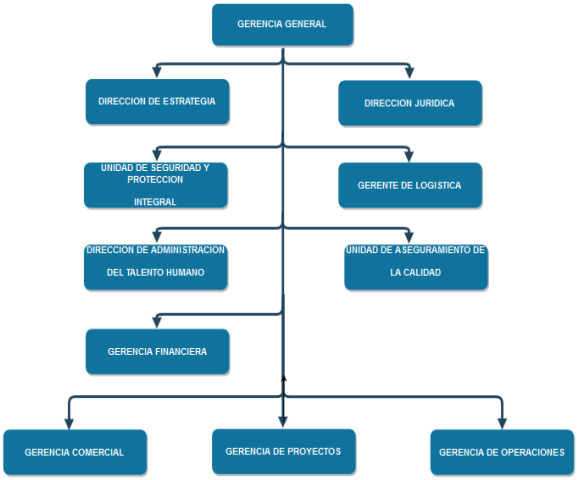
Valores organizacionales

La empresa naviera adopta valores organizacionales que promueven el buen comportamiento humano y resaltan los valores éticos que la empresa requiere. En este sentido, los valores que acreditan el compromiso de los empleados al ser parte de la empresa son los siguientes: lealtad, honestidad, compromiso, respeto, responsabilidad social y equidad.

Estructura Organizativa.

El siguiente cuadro describe la estructura de la entidad, encabezada por la alta gerencia y los departamentos de la organización:

Ilustración 4 Organigrama empresarial



Fuente: Empresa naviera

Modelo de Gestión.

La estrategia de la empresa naviera se encuentra soportada por cinco pilares fundamentales, para que los integrantes de la organización puedan tomar decisiones y que éstas sean comunicadas al personal y para cumplir con las actividades de acuerdo con lo planificado y dentro del alcance de los objetivos. La estrategia es difundida a todo el capital humano de la organización, para lograr el fortalecimiento de la misión y visión empresarial como se muestra en el siguiente gráfico.

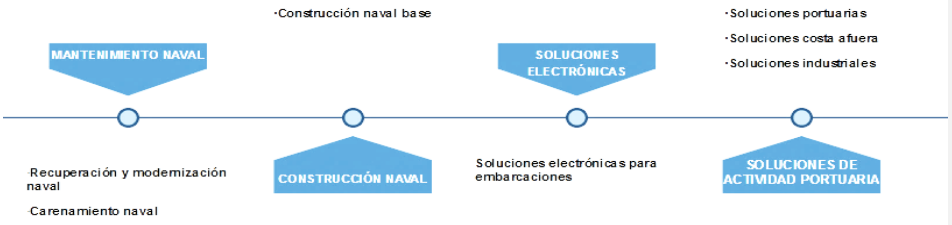
Ilustración 5 Pilares del modelo de gestión Empresa Naviera

Fuente: Empresa Naviera

Lineamientos estratégicos.

La empresa naviera fundamenta su oferta en dos grandes espacios: el desarrollo de productos y la prestación de servicios, los cuales son manejados en cuatro líneas de negocios que se muestran en el siguiente gráfico.

Ilustración 6 Lineamientos estratégicos sobre productos y servicios

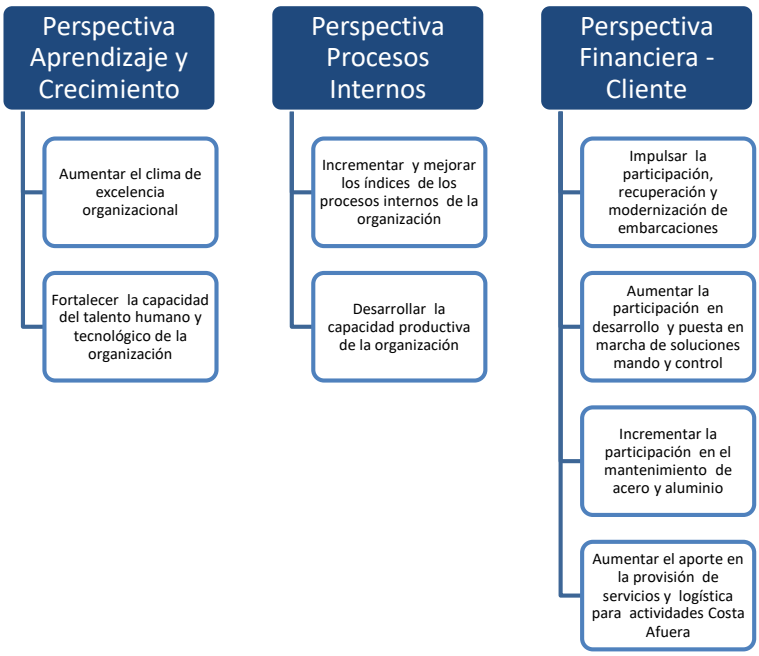


Objetivos Estratégicos.

La empresa naviera ha establecido sus objetivos estratégicos usando la metodología del Balance ScoredCard (BSC), desarrollada por Norton y Kaplan, que permite proporcionar las bases para comunicar el compromiso de la estrategia con las unidades de negocios y llevar acabo las operaciones ejecutadas por la organización. (Robert S. Kaplan, 2000).

Este sistema gerencial de la empresa naviera muestra tres perspectivas que ayudan a balancear y optimizar la gestión en la organización. En adelante se exponen en el siguiente gráfico:

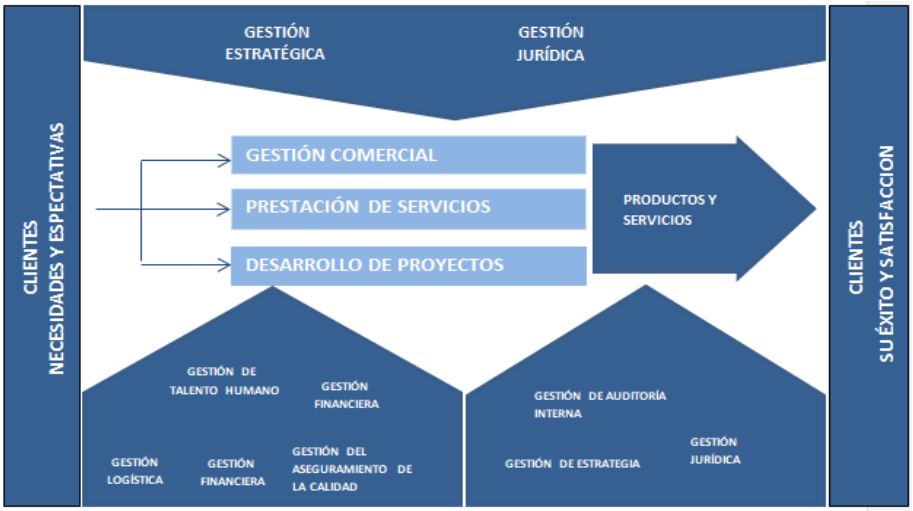
Ilustración 7 Objetitos estratégicos de la empresa según el BSC



Mapa de Procesos de la empresa naviera.

La estructura organizativa de la empresa se encuentra basada en tres procesos, mediante los cuales se desarrollan los productos y servicios que serán entregados al cliente externo. A continuación, se presenta el mapa de procesos macro de la empresa.

Ilustración 8 Mapa de procesos de la empresa naviera



Procesos que agregan Valor.

La organización cuenta con tres procesos claves que agregan valor, a través de los cuales se realizan actividades fundamentales para proveer productos y servicios que la empresa ofrece a sus clientes. Estos procesos se encuentran enfocados sobre los objetivos estratégicos que debe cumplir mediante la operación, los cuales son:

1.- Gestión Comercial: Su cometido es alcanzar las ventas proyectadas en la Planificación anual, que se basa en el Plan Estratégico Institucional. Este objetivo está directamente relacionado con el sistema de Gestión de Calidad.

2.-Prestación de Servicios: Su misión es ofrecer servicios de mantenimiento a las embarcaciones. Sirve de apoyo a la ejecución de los proyectos marítimos y electrónicos, como, por ejemplo, la creación y adecuación de tableros de mando y control para embarcaciones.

3.-Desarrollo de proyectos: Tiene por fin el inicio, control y cierre de proyectos aprobados por la alta gerencia aplicados en actividades marítimas e industriales

Fase A: Visión de TOGAF

Haciendo referencia en esta fase de la arquitectura empresarial de TOGAF, relevaremos los recursos en métodos y procedimientos organizacionales para inspeccionar las correlaciones y requerimientos del estado actual de la organización que en adelante se describen.

Alcance y principios del relevamiento con relación a la Norma ISO/IEC 27001:2013.

El presente Trabajo Final de Maestría utiliza las definiciones de la metodología en arquitectura empresarial para esta fase, exponiendo los productos y servicios de la empresa. Por tanto, el alcance del relevamiento está enfocado concretamente al proceso crítico "Desarrollo de proyectos" como el caso de estudio.

Los principios de la arquitectura empresarial toman forma como directrices generales para el uso y desarrollo de los recursos tecnológicos de la empresa. En este sentido el despliegue futuro de las bases estratégicas serán decisiones pragmáticas en Tecnologías de Información y Comunicaciones. Por ende, para el análisis se ha definido cuatro principios en función de la seguridad de la información correspondiente al proceso "Desarrollo de proyectos", indicados a continuación:

- Destinar recursos a la infraestructura tecnológica a largo plazo, que permita la continuidad operativa del proceso crítico utilizando la capacidad instalada de la empresa.

- Documentar en el sistema de gestión documental el proceso de negocio analizado, de acuerdo con la ejecución, evaluación y control del proyecto y utilizar versionado, si existiera cambios a futuro.
- Comunicar las acciones correctivas y modificaciones que surjan previo a la solución según el de cambios del proceso "Desarrollo de proyectos".
- Aplicar todo cambio o mejora con acuerdo el estándar ISO/IEC 27001:2013.

A continuación, se presenta el siguiente gráfico que se extrae del Mapa de procesos mencionado anteriormente y se identifica la línea base del proceso "Desarrollo de proyectos" de la empresa naviera para su posterior análisis en seguridad de la información, orientando el trayecto inicial a las necesidades, expectativas del cliente y su finalización en la entrega exitosa de productos y servicios.

Ilustración 9 Línea base del proceso "Desarrollo de Proyectos"

En el siguiente diagrama, se muestran las actividades del proceso de “Desarrollo de proyectos”, mostrado en forma sucesiva y lineal para entendimiento del flujo laboral.

Ilustración 10 Actividades del proceso "Desarrollo de Proyectos"

Revisión de las Fases B, C y D de TOGAF que apoyan al proceso de negocio.

Se desplegará la ruta en la cual se revisarán las diferentes arquitecturas tecnológicas que apoyan al proceso crítico “Desarrollo de proyectos”, identificando los subprocesos. A partir del relevamiento, se propondrán sugerencias para el Sistema de Gestión en Seguridad de la Información (SGSI), de acuerdo al relevamiento de las fases B, C y D consideradas crítica para la continuidad del negocio.

Fase B: Arquitectura de Negocios

Esta fase muestra cómo la organización gestiona sus objetivos del negocio y establece la relación de los procesos entre sí, a partir del diseño y la evolución de sus actividades de negocios, procesos y roles.

El objetivo de esta fase es describir los subprocesos del proceso crítico “Desarrollo de proyectos”, que son los siguientes:

Subproceso: Inicio y planificación de proyectos

- Los responsables de esta instancia dependen del Gerente de Proyectos, quién designa al Jefe de Proyectos y da inicio a la gestión, registrando los avances en el acta de constitución del proyecto. Posteriormente dicho documento es legalizado y la designación es comunicada a todos los interesados.
- El jefe del proyecto verifica el documento legalizado y se encarga de crear el registro del proyecto en el sistema informático de Planificación, donde ingresará toda la información y planificación de los proyectos aceptados por la alta gerencia.
- Luego elabora un Plan de proyecto, en el que incluye el cronograma, los aspectos vinculados a la gestión de calidad, las comunicaciones, la configuración, el análisis de riesgo, la logística y el control de cambios, además de la programación en el sistema informático de Planificación de la empresa para luego ser aprobada por el Gerente de proyectos.

Subproceso: Ejecución de proyectos

- En este subproceso se realiza la ingeniería, integración, verificación, transición y validación del producto contratado. Dependiendo de la complejidad, la gerencia de proyectos decidirá contratar o desarrollar la ingeniería para la ejecución del plan de proyecto.

Subproceso: Evaluación y Control de proyectos

- Esta fase se realiza durante la ejecución del proyecto, para lo cual el primer responsable y el Gerente de proyecto evalúan el avance del trabajo, alcance, costos, cronograma, riesgo y calidad, apoyándose en las herramientas informáticas de la empresa naviera.

Cierre del proyecto

- El jefe del proyecto coordina las capacitaciones respectivas con el cliente y al final realiza un reporte destinado a los propietarios del producto entregado.
  El mencionado responsable realiza la entrega de manuales y documentación al cliente externo. Adicionalmente, ejecuta actividades de post entrega conforme a lo acordado en el proceso de negociación. De igual manera, al finalizar, el cliente externo recibe un oficio emitido por el Gerente general o por el Gerente de proyectos para la entrega del producto terminado. A continuación, se presenta en la gráfica los subprocesos antes mencionados.

Ilustración 11 Estado actual de los subprocesos

Justificación de los subprocesos críticos de análisis en la fase de negocio
Durante la fase de negocio, se observaron los siguientes hallazgos con relación a la seguridad de la información:

- La actividad correspondiente al desarrollo de acuerdos para la identificación de requerimientos de clientes se demora y genera retrasos en la formalización de documentación, debido a un sistema de documentación sin versionado y falta de identificación del control de cambios. Por lo tanto, la adopción de un estándar en seguridad de la información permitirá mejoras como, por ejemplo, actualizaciones o

reorganización del gestor documental en línea, designando responsables acordes a las necesidades de las actividades y fomentando el ordenamiento del negocio.

- El seguimiento de las necesidades del cliente externo con respecto a las líneas de negocios de la empresa naviera depende de plataformas informáticas que carecen de actualizaciones, control y seguimiento. Por consiguiente, un sistema en gestión en seguridad de la información ayudará a la optimización del sistema informático.
- Las adquisiciones de insumos y materiales para la ejecución del proyecto presentan demoras de uno a tres meses y requieren seguimiento de organismos externos. En este sentido, la organización busca la disminución de gastos, y con la implementación de un sistema en seguridad de la información, que permitirá también disminuir los incidentes informáticos propios del proceso.
- El servicio Post-Entrega al cliente externo es delegado a terceras personas y se evidencia demora para finalizar la actividad, pudiéndose además afectar el cumplimiento, la confidencialidad y la confiabilidad de los sistemas.

Propósito que justifica el relevamiento de los subprocesos**.**

De acuerdo con lo analizado anteriormente, la revisión de los subprocesos ofrecerá los siguientes beneficios al proceso de Negocio “Desarrollo de Proyectos”:

- Mejorar el uso del Sistema de planificación de recursos empresariales y la plataforma del gestor documental.
- Dinamizar la planificación de los proyectos.
- Agilizar las transacciones.

Fase C: Arquitectura de Sistemas de información.

El objetivo que se persigue al analizar esta fase de arquitectura empresarial es conocer cómo se desarrollan en la empresa los procesos que hacen un uso intensivo de sistemas y bases de datos y su enfoque al presentar la información en aplicaciones informáticas desarrolladas o adquiridas por la institución. El proceso crítico “Desarrollo de proyectos” se sostiene en los

modelos tecnológicos balanceados entre las aplicaciones y las bases de datos que requieren controles para mitigar los riesgos en la ejecución de las actividades propias del proceso.

Según la gestión en los subprocesos, la Gerencia de Proyectos hace uso de plataformas informáticas y de almacenamiento propio, donde registran el ciclo de vida de los proyectos para luego ser aprobados por el Gerente de proyectos.

La empresa naviera cuenta con un Sistema informático de Planificación de Proyectos y un gestor documental en línea que guarda los documentos versionados que residen en el repositorio general de la empresa. De acuerdo con el relevamiento realizado, estas dos plataformas informáticas cuentan con controles de acceso por perfil de usuarios propios de en la gerencia de proyectos

La gestión de los subprocesos de la Gerencia de Proyectos registra cambios constantes en los motores de bases de datos que son el repositorio donde corren las aplicaciones, facilitando el seguimiento de la operación en la empresa. Cabe indicar que la estructura de la base de datos se encuentra en un clúster de alta disponibilidad[7], con instancias debidamente sectorizadas y permisos que el Gerente de proyectos asigna a los usuarios. Sin embargo, como resultado del relevamiento en esta fase se observan procesos que no están debidamente gestionados, los que se citan en la siguiente sección.

Hallazgos encontrados de los subprocesos críticos de análisis en la fase arquitectura de Sistemas de información.

Control y registro de cambios

- No se evidencia un registro de cambios al código fuente en la base de datos, ni la existencia física de la debida autorización gerencial. De la misma forma se encuentran paralizaciones de las aplicaciones de gestión sin dejar un documento formal para registrar las acciones y cambios en el sistema.

[7]Este tipo de **clúster** permite que varios servidores trabajen juntos ofreciendo una **alta disponibilidad** en función de los roles del servidor. Para máquinas virtuales, para aplicaciones de base de datos y aplicaciones de correo.

Eliminación segura de información.

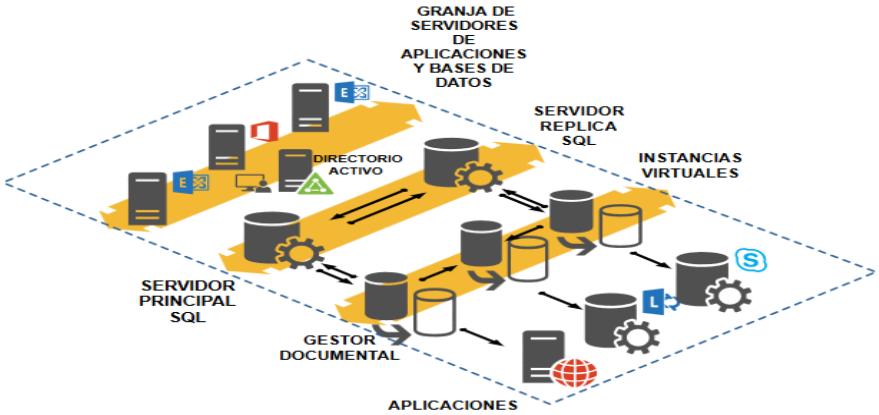
- No existe un plan de eliminación segura de registros e historiales en la base de datos, ni depuración de la información que es enviada como respaldo a cinta magnética.

Mantenimientos periódicos de la base de datos y detección de versiones antiguas de script

- La base de datos no es depurada y solo recibe una escasa revisión. Por ende, carece de documentación que permita un análisis del crecimiento de la base de datos.

La empresa naviera estructura sus recursos informáticos para que el proceso “Desarrollo de Proyectos” despliegue sus actividades ayudado de sistemas de bases de datos y aplicaciones. A continuación, se modela la arquitectura de aplicaciones y datos de la empresa.

Ilustración 12 Arquitectura de datos del proceso "Desarrollo de Proyectos"



Fase D: Arquitectura Tecnológica

Esta es una de las fases más críticas en la que se desarrollan soluciones para hardware, software, comunicaciones y protocolos necesarios que soporten a las exigencias cambiantes del negocio. Para el proceso crítico de análisis se describen los posibles riesgos que paralizarían el negocio.

La empresa naviera cuenta con un centro de datos móvil TIER[8] con características técnicas para el traslado si la empresa así lo requiere, presto a cumplir con todos los cambios tecnológicos y equipado internamente con sensores de humo, sistemas contra incendios, sistema redundante de enfriamiento y una completa arquitectura en alta disponibilidad que evita que se comprometa la actividad continua de las aplicaciones tecnológicas, manteniendo la operación de forma continua.

Para cada tipo de plataforma de hardware o software se definen los puntos siguientes a analizar para el relevamiento de información:

- Responsables del mantenimiento y accesos.
- Ampliación de las redes destinadas a las líneas de negocio.
- Documentación y actualización del consumo del repositorio general.
- Estrategia y plan de migración.
- Plan de mantenimiento en software y hardware de equipos servidores y otros equipos de comunicación.

Hallazgos encontrados en los subprocesos críticos del proceso en la fase arquitectura tecnológica tomando como base los puntos anteriores:

Respecto a los responsables del mantenimiento y accesos

- No existe una revisión mensual documentada de los mantenimientos internos y externos, ni de los accesos al centro de datos.
- No se actualizan los controles que permiten evidenciar el ingreso físico al centro de datos.
- No se documentan los mantenimientos realizados por terceros.
- No existe evidencia de mantenimientos acordados para el hardware y de las actualizaciones requeridas en el caso del software.

Comentado [PP1]: Revisar formato de la llamada o nota

Comentado [LPTM2R1]: Se revisó el pie de pagina

Comentado [PP3R1]: Me parece que sigue sin quedar bien. Podrías revisar nuevamente?

Comentado [LPTM4R1]: Se agrego al pie de página que es la Certificación TIER para data center

Comentado [PP5R1]: No debería estar arriba en lugar de ser un subíndice? Fijate la llamada 7 más arriba.

Comentado [LPTM6R1]: Se arreglo el prefijo

[8] TIER: Se trata de un centro de datos certificado por el Instituto de tiempo y Actividad de los Estados Unidos, que no requiere de paradas o suspensiones del servicio para el reemplazo de equipos o mantenimiento. Posee suministro eléctrico y un sistema de enfriamiento redundante, así como la capacidad de un mantenimiento concurrente.

Respecto a la ampliación de las redes destinadas a los subprocesos en análisis.

- Con los recientes cambios departamentales, el acceso a la red y la disponibilidad de puertos en los equipos de comunicación son limitados.
- No existen planos arquitectónicos de tendido de cables de red.
- Existen cables de red superpuestos y no cuentan con la protección basada en estándares.

Respecto a la documentación y actualización del consumo del repositorio general

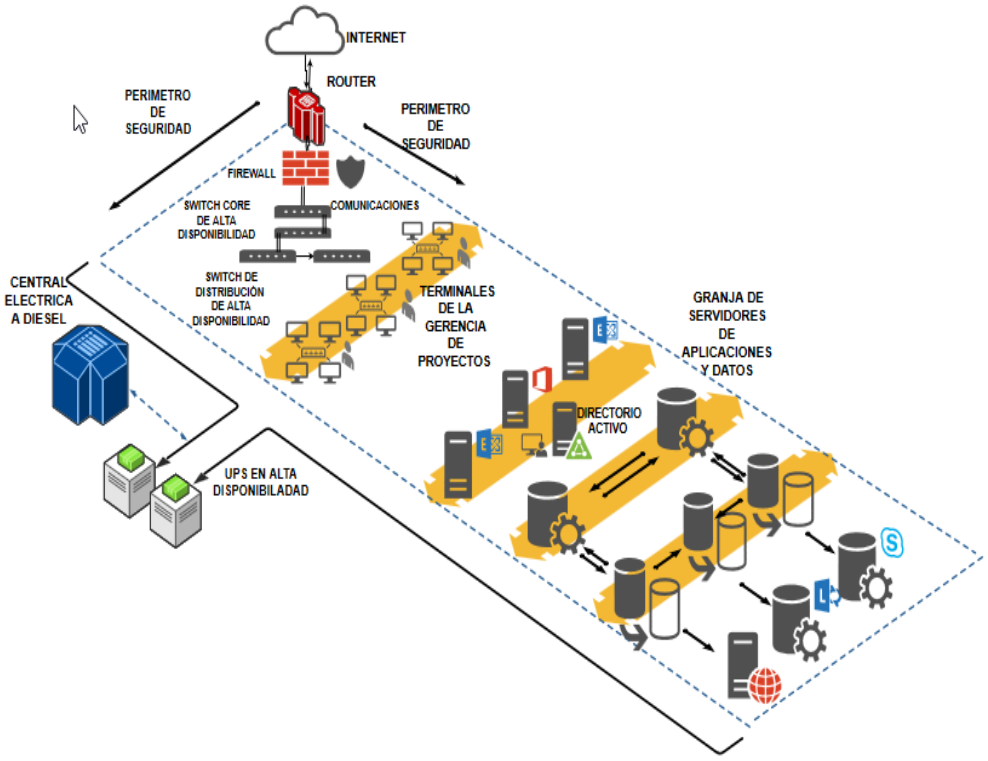
- Se evidencia un importante crecimiento en la base de datos, resultado de los crecientes proyectos y la actualización del gestor documental, que no ha sido debidamente documentado.
- No existe una proyección anual del consumo de espacio en los discos de almacenamiento de información.
- No existen registros de las actualizaciones en los equipos informáticos y discos de almacenamiento.

Respecto a la estrategia y el plan de migración.

- No se evidencia una estrategia de recuperación ante desastres, que indique entre otras cosas, los involucrados para efectuar tan delicada acción y especialmente teniendo en cuenta el gran número de discos virtuales que se encuentran en el esquema de virtualización central de servidores.
- Si fuera requerido un plan de migración en hardware o software, no existen lineamientos de acción ante los posibles desastres informáticos.
- El plan de mantenimiento se realiza con demora y no existe una planificación documentada por áreas y debidamente informada para la viabilidad del trabajo.

A continuación, se presenta la estructura tecnológica que soporta al proceso crítico en análisis, de acuerdo con lo indicado por el personal del departamento de sistemas.

Ilustración 13 Arquitectura tecnológica del Proceso "Desarrollo de Proyectos"

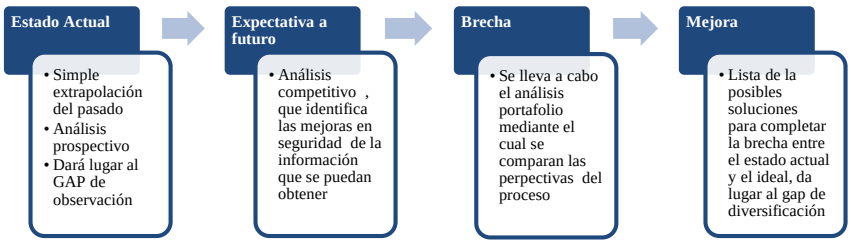


Capítulo II

Análisis de brechas (GAP) del proceso crítico "Desarrollo de procesos".

En este capítulo se presenta un análisis de brechas basado en las fases de referencia de la arquitectura empresarial TOGAF analizado en la sección anterior, que sirve para establecer el estado actual del proceso "Desarrollo de Proyectos" con respecto al aseguramiento de los sistemas de información y su efecto en el negocio. En esta observación se pretende identificar el estado futuro de la seguridad en la información "¿en qué situación estamos? (el estado actual) y ¿en dónde esperamos estar? (una declaración a futuro). Asumiendo como base la definición de la norma ISO/IEC 27001:2013, este Trabajo Final de Maestría se enfocará en los requerimientos y controles de la norma, posicionándose en el Anexo A (Normativa)[9] para la evaluación de los controles. En síntesis, se expone el escenario macro de análisis GAP en la siguiente gráfica.

Ilustración 14 Planificación del análisis GAP para el proceso "Desarrollo de Proyectos"



Fuente: Propia del autor

[9]**Anexo A (Normativa)**, Los objetivos de control y los controles enlistas en el Cuadro A.1 se extraen directamente y están alineados a aquellos detallados en el ISO/IEC 27002:2013.

En nuestro caso, los subprocesos que son soportados por los recursos tecnológicos instalados en la organización requieren ser atendidos. Para ello se efectuó el análisis de las fases del marco de trabajo TOGAF en el proceso "Desarrollo de Proyectos" en el capítulo anterior y se identificaron los parámetros relacionados con la gestión en seguridad de la información por medio de análisis de brechas.

En este sentido, luego de efectuar un servicio de consultoría sobre los asuntos internos críticos relevantes que afectan la capacidad de lograr los resultados esperados en beneficio de la organización, se pretende identificar brechas para el cumplimiento y cuidado de la información del proceso crítico "Desarrollo de proyectos". A continuación, se enuncia la planificación considerando el escenario de partida y el escenario planteado como meta de acuerdo con la norma ISO/IEC 27001:20013.

Estado actual del proceso crítico "Desarrollo de proyectos", GAP de Observación

A efectos de organizar la integración del proceso de negocio al Sistema de Gestión, como en todo proyecto, es necesario conocer la situación en la que se encuentra dicho proceso en cuanto a los objetivos a trazarse y poder planificar las valoraciones más certeras del diseño de la hoja de ruta, considerando como se mencionó el escenario de partida y el planteado como meta. En la siguiente tabla se enuncian los requisitos de la Norma ISO/IEC 27001:2013 especificados en las cláusulas del cuatro al diez requeridos para asegurar conformidad con la Norma Internacional. De este modo, se realiza el GAP de observación.

Tabla 1 . Requisitos de la Norma ISO/IEC 27001:2013 puntualizando el estado actual del proceso

Situación actual del proceso "Desarrollo de proyectos" frente a los requisitos de Norma ISO/IEC 27001:2013		
Requisitos	**Numeración**	**Situación actual del proceso**
4.Contexto de la Organización	4.1,4.2,4.3,4.4	La organización en su entorno de gobierno cuenta con un modelo de gestión perfectamente posicionado, que ayuda a la comunicación vertical hacia sus colaboradores y promueve lineamientos estratégicos que garantizan el desempeño de las líneas de negocios. Con respecto al proceso de estudio, presenta alto interés de partes interesadas con relación a la seguridad de la información. El alcance del SGSI se estableció en el primer capítulo del documento académico. De hecho, la empresa naviera se ha comprometido en establecer, implementar, mantener y mejorar al SGSI de acuerdo con los requisitos de la Norma Internacional.
5. Liderazgo	5.1,5.2,5.3	La alta dirección deberá demostrar liderazgo y compromiso con respecto a la gestión del SGSI, estableciendo políticas y objetivos de la seguridad de la información, garantizando disponibilidad de recursos necesarios para llevar adelante el proyecto y, por último, garantizando la integración del SGSI dentro de los procesos de la organización. Por tanto, el proceso "Desarrollo de proyectos" cuenta con el aval de la gerencia para asegurar su información.
6. Planificación	6.1,6.2	El proceso "Desarrollo de Proyectos no cuenta con la debida planificación que exige la Norma ISO/IEC 27001:2013, para el normal desarrollo de las funciones que se espera del proceso. De hecho, las inconformidades se detallaron en las fases B (negocios), C (Arquitectura de sistemas de información), D (Arquitectura tecnológica) del ADM de TOGAF.

7.Apoyo /Soporte	7.1,7.2,7.3,7.4, 7.5	El proceso "Desarrollo de Proyectos" cuenta con los recursos necesarios para la implementación, mantenimiento y mejora continua de sus competencias. Este requisito requiere que el proceso comunique cambios y estrategias al gerente general, remita documentación y a la vez sea controlado, acciones que no se realizan con propiedad.
8. Operación	8.1,8.2,8.3	El proceso crítico de análisis no cuenta con información de evaluaciones de los riesgos en seguridad de la información ni su debido tratamiento. La organización deberá ser informada y conservar la información documentada con los resultados que origine el tratamiento de los riesgos en seguridad de la información.
9.Evaluación del desempeño	9.1,9.2, 9.3	Este requisito dispone la evaluación del desempeño en seguridad de la información y la efectividad del sistema de gestión de la información. La organización deberá determinar las necesidades que deben ser monitoreadas incluyendo el proceso y los controles de la seguridad de la información. Las auditorías internas son elementos esenciales y deben ser realizadas en intervalos planificados con la finalidad de proporcionar información con respecto al desempeño del SGSI. Como último, el proceso se someterá a la Revisión por parte de la Dirección para verificación del cumplimiento de los objetivos de seguridad de la información. Si bien es cierto la organización cuenta con auditorías internas en seguridad de la información, el personal que trabaja en el proceso "Desarrollo de Proyectos" no conocía la normativa.
10.Mejora	10.1,10.2	Al asegurar la información del proceso "Desarrollo de Proyectos", luego que se ha implantado la gestión de riesgo en sus subprocesos, siendo viable que reaccione a no conformidades y acciones correctivas que permitan cambios si fuera necesario. Sin embargo, revisando las acciones observadas en el primer capítulo para el desempeño de los sistemas de información, no existe evidencia que se esté trabajando en la mejora continua.

Expectativa a futuro en la implementación de la norma ISO/IEC 27001:2013.

En diversas iniciativas internacionales, incluidas las emprendidas por la organización ISO (en español, Organización Internacional de Estándares) con sus guías, se han clarificado los componentes fundamentales de la seguridad de la información. Así se distinguen: los activos, las amenazas, las vulnerabilidades, los riesgos, los impactos y las salvaguardas,

Según lo mencionado por (Heredero & López, 2008) Los activos, son los recursos del Sistema de información (SI) o relacionados con éste, necesarios para que la organización opere correctamente, resguarde su información y alcance los objetivos propuestos por su dirección. Los activos se podrán jerarquizar en función de su composición y estarán relacionados entre sí por el riesgo al que están expuestos. Las características a relevar de cada activo son: su código, descripción, precio unitario, coste de reposición, tiempo máximo de carencia, nivel de mantenimiento de su integridad, los requerimientos en cuanto a su disponibilidad y el nivel de confidencialidad. Los activos pueden ser físicos o lógicos, tangibles o intangibles y se pueden encuadrar en: las personas, el centro de datos y las instalaciones, las computadoras o servidores centrales, el software de base, las computadoras departamentales, la informática de usuario final, incluyendo un posible centro de información las aplicaciones que se procesan, las instancias y ambientes de desarrollo de dichas aplicaciones, los datos y las bases de datos, las comunicaciones y la documentación.

Las amenazas son los eventos que pueden desencadenar un incidente en la organización, produciendo daños o pérdidas inmateriales en sus activos. Se pueden agrupar en clases, siendo sus posibles atributos son: código, nombre, frecuencia (habitualmente subjetiva) y el impacto que podría producir la materialización del riesgo. Por diversas eventualidades que supone amenazas de desastres informáticos podría ser:

Accidentes: averías de hardware y de software, incendio, explosión, suceso natural, excepcional, pérdida de servicio de agua, gas o electricidad, entre otros.

- Por un lado, los daños que se pueden ocasionar en el sistema y una estimación de costes derivados de dichos daños
- Por otro, los costes de implantación y mantenimiento de las medidas apropiadas para su contención.

El presupuesto a invertir en seguridad dependerá de lo crítico de la información que maneje y de los recursos que pueda o quiera asignar la Dirección para su protección.

En este sentido, las expectativas de la Dirección en su afán de salvaguardar los sistemas de información, minimizando el daño permanente de los activos, mantener un sistema de mejora continua para minimizar las amenazas y presentar a los directivos el riesgo residual que la empresa pueda controlar, hace necesario exponer un GAP Competitivo en el proceso crítico "Desarrollo de Proyectos", que en base a lo relevado en el capítulo 1 hace énfasis en la seguridad de la información del negocio, arquitectura de sistemas de información y la arquitectura tecnológica en la que se apoya el proceso. En adelante se presenta una tabla de expectativas que se desea alcanzar con la implementación de la Norma ISO/IEC 27001:2013.

Tabla 2. Expectativas referentes con la implementación de la Norma ISO/IEC 27001:2013

Expectativas del proceso "Desarrollo de proyectos" con la implementación de la Norma ISO/IEC 27001:2013		
Expectativas a futuro	**Fases del ADM TOGAF con mira al proceso crítico**	**Beneficios y su justificación en el proceso**
Reducción de riesgos debido al establecimiento y seguimiento de controles.	Línea base en capa del negocio de los subprocesos. Línea base en capa de Datos y Aplicaciones de los subprocesos. Línea base en capa de Arquitectura Tecnológica de los subprocesos.	Se logrará reducir las amenazas hasta alcanzar un nivel asumible por la organización, contribuyendo a asegurar la continuidad del negocio.
Reducción de costos y derivados de una racionalización de los recursos.		Se eliminan las inversiones innecesarias como las producidas por sobrestimar los riesgos.

La seguridad se considera un sistema y se convierte en una actividad de gestión.		La seguridad deja de ser un conjunto de actividades desorganizadas y pasa a transformarse en un ciclo de vida metódico y controlado en el que participa el personal de la organización.
La certificación del SGSI contribuye a mejorar la competitividad en el mercado.		Causa que las empresas que han conseguido la certificación incrementen su prestigio. El certificado mejora la imagen y confianza de los productos entre clientes, proveedores y socios.

Brechas competitivas desde la mirada de la Norma ISO ISO/IEC 27001:2013.

En adelante se inicia el análisis de competitividad de acuerdo con la gestión de los sistemas de información relevada en el capítulo 1 con respecto a la seguridad de la información, frente a las cláusulas y controles del Anexo A de la Norma ISO/IEC 27001:2013. Por tanto, es necesario definir los interlocutores por agrupación de controles, para hacer el cuestionario a nivel global con los responsables de las áreas con las que interactúa el proceso "Desarrollo de proyectos ". A continuación, se presenta el gráfico donde se observa los controles de la norma en relación con las áreas involucradas en la protección de los activos informáticos del proceso de negocio.

Tabla 3. Interlocutores para el cuestionario GAP ISO/IEC 27001:2013

Controles	Interlocutores
A.5 Políticas de Seguridad de la Información	Dirección + Todos los departamentos
A.6 Organización de la Seguridad de la Información	Director Departamento TI
A.7 Seguridad en los Recursos Humanos	Director RRHH
A.8 Gestión de Activos	Director de Operaciones & Director de TI
A.9 Control de Acceso	Director de Operaciones
A.10 Criptografía	Director de Operaciones & Director de TI
A.11 Seguridad Física y del entorno	Director de Operaciones
A.12 Seguridad en las Operaciones	Director de Operaciones & Director de TI
A.13 Seguridad en las Comunicaciones	Director de Operaciones & Director de TI
A. 14 Adquisición, desarrollo y mantenimiento de sistemas de información	Director del Departamento TI
A.15 Relación con Proveedores	Director de Compras
A.16 Gestión de incidentes de seguridad de la información	Director del Departamento TI
A.17 Gestión de la Continuidad del Negocio	Dirección + Todos los departamentos
A.18 Cumplimiento	Departamento Legal

Una vez identificados los actores que responderán al test de cumplimiento normativo de la ISO/IEC 27001:2013, se listarán los ciento catorce controles de la norma a manera de preguntas que serán respondidas por los interlocutores responsables de la protección de la información y de los activos tecnológicos del proceso “Desarrollo de proyectos”. Estos controles estarán agrupados en tres grupos: Controles de gestión, Controles operacionales y controles técnicos.

El cuestionario incluirá respuestas de tipo: No cumple, Parcial y Cumple con los valores 1, 2 y 3 respectivamente. Posteriormente se presentan las puntuaciones en las preguntas ya relevadas a los interlocutores (ver el Cuestionario GAP ISO 27001 en el Anexo B).

Criterio de evaluación en la brecha competitiva.

De acuerdo con el cuestionario del Anexo B, se asignaron valores para ser analizados cualitativamente, a fin de determinar el nivel de madurez de cada dominio y control y el nivel medio, siendo este último determinado mediante la siguiente fórmula:

Nivel medio de cumplimiento = Puntuación total de cada Control / número de controles totales x 100

Esta fórmula nos entregará el valor medio entre 1 y 3 expresado por el porcentaje total del grupo de control, con el propósito de evaluar el cumplimiento general de la norma. Es importante presentar los resultados del análisis GAP con evaluación, expresados por grupo de control de la siguiente forma:

Controles de Gestión:

- Política de seguridad
- Organización de la información
- Seguridad y cumplimiento

Controles Técnicos

- Gestión de activos, físicos y ambientales
- Seguridad y comunicaciones, gestión de operaciones
- Controles operacionales

Controles Operacionales

- Adquisición, desarrollo y mantenimiento de sistemas
- Control de acceso, gestión de incidentes TI y gestión de la continuidad del negocio.

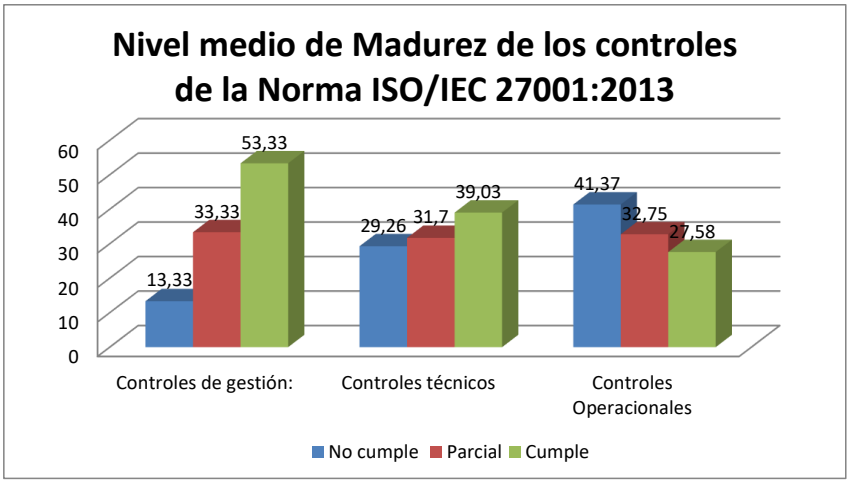
En este aspecto, los resultados por grupo en base a la encuesta realizada a los responsables de la seguridad de la información del proceso de negocio se muestran en la siguiente tabla de resultados:

Tabla 4. Resultados por grupo de controles GAP ISO/IEC 27001:2013

Grupos de controles de la Norma ISO/IEC 27001			
Respuestas	Controles de gestión:	Controles técnicos	Controles Operacionales
No cumple	13,33	29,26	41,37
Parcial	33,33	31,7	32,75
Cumple	53,33	39,03	27,58

Para una mejor interpretación a la tabla anterior, se expone a continuación una ilustración que muestra los datos antes presentados, de los cuales el proceso crítico "Desarrollo de Proyectos" tiene mayor cumplimiento en el grupo de Gestión. Para el resto de los grupos, el cumplimento es parcial, lo que muestra una proliferación de los riesgos no gestionados.

Ilustración 15 Grupo de controles GAP ISO/IEC 27001



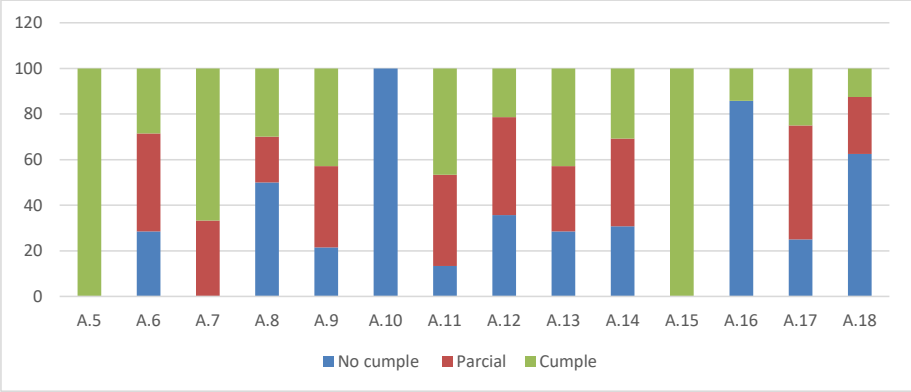
En este mismo sentido tomando los datos de la encuesta, se realizó el análisis por cada dominio para identificar el nivel de esfuerzo necesario para cumplir con la Norma ISO/IEC 27001:2013. Los datos para el análisis son los siguientes:

Tabla 5. Ponderación para cada dominio de la norma ISO/IEC 27001:2013

Controles Anexo A ISO/IEC 27001:2013														
Respuestas	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
No cumple	0	28,57	0	50	21,4	100	13,33	35,7	28,57	30,8	0	85,71	25	62,5
Parcial	0	42,85	33,33	20	35,7	0	40	42,9	28,57	38,5	0	0	50	25
Cumple	100	28,57	66,66	30	42,9	0	46,66	21,4	42,85	30,8	100	14,28	25	12,5

En base a los datos de la tabla 6, la siguiente ilustración evidencia que el proceso crítico ha gestionado y completado los controles con respecto a la Política de seguridad de la información y la relación con proveedores, en un 100 por ciento. Este resultado muestra que, para el proceso de negocio, es prioridad mantener la documentación de la normativa actualizada y su vinculación con los proveedores en orden, dejando de gestionar parcialmente controles técnicos y operacionales e incumpliendo totalmente otros.

Ilustración 16 Nivel de esfuerzo actual en aplicación de controles



Fuente: (INGERTEC, 2013)

Mejoras del análisis GAP en base a la Norma ISO/IEC 27001:2013

Acorde a la observación anterior, podemos destacar que la gestión en seguridad de la información en los controles técnicos y operativos no reciben el tratamiento necesario que el

estándar de la ISO/IEC 27001:2013 exige. Ante este hecho es necesario informar a la alta Gerencia que el proceso crítico “Desarrollo de Proyectos” requiere la atención en las iniciativas tecnológicas. La implementación de un SGSI permitirá un estado futuro en el que se gestionen riesgos residuales y se implemente la mejora continua. En base a las fases de la arquitectura empresarial TOGAF, se expondrán las mejoras visualizando el estado futuro deseado para proteger adecuadamente los sistemas de información que sirven de apoyo al proceso de negocio.

Fase B: Arquitectura de negocios.

- Disponibilidad de mejores prácticas y metodologías para la gestión de sistemas que apoyan al negocio.
- Agilidad y disponibilidad inmediata de la información almacenada en las bases de datos.
- Contribución a la continuidad del negocio, ya que se gestiona adecuadamente cualquier eventual interrupción de las actividades y se resguarda la totalidad de los procesos críticos de la empresa.

Fase C: Arquitectura de sistemas de información.

- Mejora el entorno regulatorio de los sistemas de información.
- Fácil adaptabilidad en nuevos sistemas, bases de datos y disponibilidad de almacenamiento para el emprendimiento de nuevas iniciativas de proyectos.
- Documentación técnica y funcional actualizada para los principales aplicativos del negocio.

Fase D: Arquitectura Tecnológica.

- Disponibilidad de adquirir nuevas tecnologías que ofrece el mercado y así repotenciar la arquitectura tecnológica.
- Fiabilidad de la red corporativa para la transmisión de datos.
- Central robusta en procesamiento de datos con equipamiento monitoreado de acuerdo con la normativa requerida por la alta gerencia.

Capítulo III

Implementación de Controles y aplicación de salvaguardas al proceso "Desarrollo de Proyectos".

En su trayectoria de vida corporativa, la organización ha logrado permanecer a la vanguardia en la exigente demanda de los clientes, entregando productos y servicios finales que requieren de innovación en sus actividades operacionales para alcanzar la excelencia en sus objetivos establecidos en el Plan estratégico institucional.

Por esta razón, la empresa ha tomado iniciativas para mantener la integridad, confidencialidad y disponibilidad de la información que reside en equipos informáticos, redes de datos y almacenamiento que convergen dentro de lo que se conoce como sistemas de información.

Estos sistemas de información están sujetos a permanentes riesgos y amenazas que pueden originarse dentro de la empresa y las que pueda recibir del exterior. Para ello la empresa naviera pretende implementar procedimientos y controles necesarios para mitigar el riesgo y asegurar la continuidad del negocio, los que requieren ser reforzados en forma continua y socializados a todos los miembros de la empresa.

SGSI y su relación con el Ciclo de Deming como parte de la decisión estratégica de la organización.

La empresa naviera con el interés de conseguir la mejora continua en sus procesos ha implementado un Sistema Integrado de Gestión que abarca la gestión medioambiental (norma ISO/IEC 14001:2004), la Gestión de Calidad (norma ISO/IEC 9001:2008) y la Gestión de seguridad y salud ocupacional (norma ISO/IEC 18001:2007). En el año 2015 inicia el proceso de auditoría externa en sistemas integrados de gestión, consiguiendo la certificación por medio del Organismo de Certificación- SGS Ecuador. Con la certificación se lograron los siguientes avances:

1. Equipos de alta tecnología: seguridad y medio ambiente.
2. Personal comprometido con la estrategia empresarial.
3. Infraestructura y su operación adecuada para la operatividad y servicios

4. Personal capacitado en manejo de maquinarias.
5. Implementación de un sistema de gestión documental.
6. Organización orientada a procesos y optimización de recursos. (Mahecha Guzman & Coello, 2016)

Un sistema de gestión de Seguridad de la Información es la idea central que forma los cimientos que se construyen a partir de la norma ISO/IEC 27001:2013 y su gestión se desarrolla mediante un proceso sistematizado, documentado y conocido por toda la organización, con el aval de la Alta Gerencia.

Introducción de la norma ISO /IEC 27005:2008 y definición del enfoque.

En adelante se lleva a cabo una evaluación de riesgos, lo que proporciona información suficiente para determinar con eficacia las acciones necesarias para modificar dichos riesgos a un nivel aceptable. Una vez completada la tarea, sigue el tratamiento del riesgo. Si la información es insuficiente, se llevará a cabo otra iteración de la evaluación de riesgos con el contexto revisado (usando criterios de evaluación de riesgo, de aceptación del riesgo o de impacto),

La eficacia del tratamiento del riesgo depende de los resultados de su evaluación. Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel aceptable residual. En esta situación, otra iteración de la evaluación del riesgo con parámetros modificados de contexto (por ejemplo, la evaluación de riesgos, de aceptación de los riesgos o criterios de impacto), puede ser necesario y seguido por un tratamiento adicional de riesgo.

La actividad de aceptación del riesgo por parte de la alta gerencia tiene que asegurar que se aceptan los riesgos residuales previstos y que éstos son aceptados explícitamente por los responsables de los proyectos Esto es especialmente importante en una situación en la que se omite o se pospone la implementación de controles, por ejemplo, debido a la decisión a no aumentar los costos.

Durante todo el proceso de gestión de riesgos de seguridad de información, es importante que los riesgos y su tratamiento se comuniquen a los administradores involucrados y al personal operativo. Esta información puede ser muy valiosa para gestionar incidentes y puede ayudar a reducir el daño potencial. (Estándar Internacional ISO/IEC 27005, 2018).

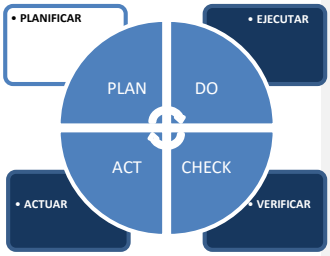
Empleo de la Norma ISO/IEC 27005:2008 como parte del SGSI.

Para efectos del cumplimiento de los requisitos en la norma ISO/IEC 27001:2013, se ha relevado información para el registro de documentos que proporcionan evidencia objetiva de la gestión dentro de la organización con respecto al Sistema de Gestión en seguridad de la información. Bajo el marco del Ciclo de Deming, se hará referencia al primer paso que es la Planificación donde se explica en detalle y se desarrollan a continuación en las siguientes fases para el proceso crítico "Desarrollo de Proyectos" de la empresa.

Fase 1: Planificación

En esta fase se hará referencia al primer paso del ciclo, en el que se explica en detalle y se desarrollan las acciones para hacer frente a los riesgos e identificar las políticas para posteriormente evaluarlas y gestionarlas. También es probable la redefinición de la información por un Auditor Líder de la norma. A continuación, se desarrollan las siguientes etapas para el proceso crítico "Desarrollo de Proyectos" de la empresa.

Ilustración 17 Planificar



Paso 1. Alcance y límites de la norma ISO/IEC 27001:2013.

En el presente documento, del capítulo I se relevó al proceso crítico "Desarrollo de proyectos", mediante la metodología en Arquitectura Empresarial TOGAF, donde se detalla las fases de la arquitectura tecnológica con respecto a los sistemas informáticos de gestión. En consecuencia, se enfatizó en términos de negocio, activos y tecnologías de sistemas de

información que se pretende proteger para la continuidad del negocio, siempre en relación con el proceso crítico escogido “Desarrollo de proyectos”.

Paso 2. Revisión de la Política de Seguridad.

La empresa naviera cuenta con un documento en seguridad de la Información que incluye el marco general y los objetivos de seguridad de la información. Estas directrices establecen los criterios generales con los que se va a evaluar el riesgo y se encuentran aprobadas por la gerencia General. (Gerente General Montenegro Delgado , 2016)

Paso 3. Establecimiento del Comité de Seguridad de la información.

La empresa naviera cuenta con un Comité en Seguridad de la Información que está integrado por:

a) El Gerente de Seguridad de la Información: quien será responsable de convocar regularmente a reuniones o cuando la situación lo amerite, coordinar las acciones del Comité e impulsar la implementación y el cumplimiento de las directrices contenidas en la Política.
b) El responsable de seguridad informática: quien cumplirá funciones relativas a la seguridad de los sistemas de información de la empresa, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en las presentes directrices.
c) Los propietarios de la información: quienes serán responsables de proponer la clasificación de acuerdo con el grado de sensibilidad y criticidad de dicha información, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deben tener permisos de acceso a la información, de acuerdo a sus funciones y competencias.
d) El responsable del Área de Recursos Humanos: cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación a todo el personal de los cambios realizados en ésta. Llevará adelante además la implementación de la suscripción de los Acuerdos de Confidencialidad y las

tareas de capacitación continua en materia de seguridad de la información conjuntamente con el responsable de Seguridad Informática. (Montenegro, 2016, pág. 5)

Paso 4. Declaración del método de evaluación de riesgos.

Como se explicó anteriormente en el marco teórico la norma ISO/IEC 27005:2008, se expone un método de evaluación de riesgos que nos proporciona una lista de amenazas y vulnerabilidades (Ver Anexo A – Lista de amenazas y de Vulnerabilidades). Esta lista se las relaciona directamente con los activos de información para determinar los escenarios más relevantes. A continuación, se identifica la relación entre los activos de información, las amenazas y las vulnerabilidades, descritas por el estándar.

Tabla 6 Variables de Análisis de Vulnerabilidades y Amenazas

Variables	Descripción
Activo	Identificador del activo
Vulnerabilidad	Vulnerabilidad del activo
Amenaza	Amenaza declarada para el activo

En otro orden, para determinar el riesgo, se utilizan los factores frecuencia e impacto. Para el primero, una posible escala a utilizar se detalla a continuación.

Tabla 7 Valores en la frecuencia del riesgo informático

Frecuencia de Riesgo	Valores	Descripción
Bajo	1	Una vez cada año
Medio	2	Dos veces por semestre
Medio alto	3	Dos veces por mes
Alto	4	Una vez por semana

En cuanto al impacto, se lo describe cualitativamente, es decir teniendo en cuenta tanto los daños tangibles como la estimación de los daños intangibles (incluida la información). En este sentido, podría resultar de gran ayuda la realización de entrevistas en profundidad con los responsables del proceso crítico "Desarrollo de proyectos", tratando de determinar cuál es el impacto real de la revelación, alteración o pérdida de la información para la organización, y no solo del elemento TICs que la soporta. Para medir el impacto del daño en la organización, una escala posible es la que se compone de tres niveles, como, por ejemplo: bajo, moderado y alto. En adelante, se agrega la descripción por cada valoración.

Tabla 8 Valoración del impacto del riesgo informático

Valoración	Descripción
Alto	• Pérdida o inhabilitación de recursos críticos. • Interrupción de los procesos de negocio, daños en la imagen y reputación de la organización. • Robo o revelación de información estratégica o especialmente protegida.
Moderado	• Pérdida o inhabilitación de recursos críticos pero que cuentan con elementos de respaldo. • Caída notable en el rendimiento de los procesos de negocio o en la actividad normal de la organización. • Robo o revelación de información confidencial, pero no considerada estratégica.

Bajo	• Pérdida o inhabilitación de recursos secundarios • Disminución del rendimiento de los procesos de negocio. • Robo o revelación de información interna no publicada.

Fuente: (Vieites, 2014)

Paso 5. Identificación de los activos

El proceso crítico "Desarrollo de proyectos" no cuenta con un inventario formal de activos de información. En el presente Trabajo final de Maestría, se propone una forma de identificarlos, clasificarlos y valorarlos. Esta propuesta agrupa los activos con el fin de facilitar la identificación de amenazas y posteriormente la evaluación de riesgo Ver tabla de identificación de los activos en Anexo C.

Paso 6. Valoración de Activos.

En el Anexo B (informativo) de la norma ISO/IEC 27005:2008, se describe la valoración de los activos que se debe identificar. En consecuencia, después de haber detallado los activos de información en la sección anterior, los criterios para la asignación de los valores en el presente trabajo académico se expresarán de acuerdo a la confidencialidad, disponibilidad e integridad que busca la Norma ISO/IEC 27001, con una escala de 1 al 4. A continuación se muestra la tabla con los valores asociados.

Tabla 9 Valoración del dimensionamiento de los activos de información

Valores	Dimensiones		
	Confidencialidad	Disponibilidad	Integridad
1	Activo libre, se puede difundir y es de dominio público	La tolerancia a que el activo no esté disponible es de una semana o un plazo mayor	Los errores o modificaciones no autorizadas no generan ningún impacto al negocio
2	Activo restringido, solo puede ser de uso interno. Si se filtra, no ocasionaría un riesgo	La tolerancia a que el activo no esté disponible es de no más de un día	Los errores o modificaciones no autorizadas generan un impacto leve al negocio
3	Archivo protegido, se debe tener controles para el acceso. Si se llega a filtrar ocasionaría un riesgo moderado al negocio	La tolerancia de que el activo no esté disponible es de no más de una hora	Los errores o modificaciones no autorizadas generan un impacto moderado en el negocio
4	Activo confidencial, información sensible y no se puede difundir bajo ningún concepto. Su filtración ocasionaría un riesgo crítico para el negocio	No se tolera que el activo no esté disponible	Los errores o modificaciones no autorizadas generan un impacto critico al negocio

Dado que se ha establecido el nivel de dimensión propuesto para los activos, el promedio que se obtenga nos permitirá conocer el valor del activo. Por tanto, esta lógica se aplicará a los activos de información del proceso "Desarrollo de Proyectos", según a su importancia. La empresa ha establecido que, si presentan un promedio igual o mayor a tres, los activos serán seleccionados para realizar el análisis de riesgos y su tratamiento, aspectos reflejados en la Declaración de aplicabilidad, siendo estos elementos necesarios para proteger los activos informáticos de la organización. La siguiente tabla presenta los promedios para identificación del valor de los activos, considerando bajo esta caracterización tanto los recursos humanos como informáticos.

Tabla 10 Valoración final de los activos de información

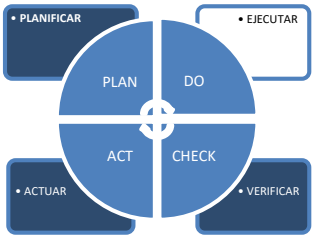
Código	Nombre	Criterios de Valorización			Valor final
		Confidencialidad	Disponibilidad	Integridad	
A1	Gerente de proyectos	2	2	1	2
A2	Jefe de proyectos	1	1	2	1
A3	Lideres de proyectos	2	2	2	2
A4	Ingenieros diseñadores	2	2	1	2
A5	Secretaria	1	1	1	1
S1	Sistema informático de planificación de proyectos	4	4	3	4
S2	Sistema de documentación	3	4	4	4
S3	Sistemas de evaluación y diseño de proyectos	2	2	1	2
H1	Servidor de aplicaciones	4	4	4	4
H2	Servidor de correos	0	3	3	2
H3	Computadoras de escritorios	2	4	4	3
H4	Lector Biométrico	2	3	0	2
H5	Impresoras/copiadoras	3	3	3	3
I1	Internet	2	3	3	3

Código	Nombre	Criterios de Valorización			Valor final
		Confidencialidad	Disponibilidad	Integridad	
B1	Bases de datos	3	3	3	3
R1	Redes informáticas	2	4	2	3
F1	Firewall	3	3	3	3
U1	UPS	0	4	0	1

Fase 2: Hacer

Una vez dado a conocer los pasos de la planificación en el apartado anterior, continuamos con el establecimiento de los controles y procedimientos que requiere el proceso "Desarrollo de Proyectos". En esta etapa es posible que se vuelva a evaluar la información ya identificada como punto de control.

Ilustración 18 Ejecutar



Creación del plan de tratamiento y gestión de los riesgos.

En la planificación se mencionó la metodología de gestión en riesgos descrita en el paso 4 del presente capítulo, que se usará en adelante para la gestión de la seguridad de la información en el proceso de negocio escogido. Como se mencionó, una vez identificados y valorados los activos, es necesario relevar las amenazas y vulnerabilidades a los que están expuestos. Por ende, en el Anexo A (informativo) de la norma ISO/IEC 27005:2008, se presentan ejemplos de amenazas y vulnerabilidades para determinar los escenarios de incidentes que puedan limitar las operaciones propias de la empresa. En el siguiente cuadro, se podrá evidenciar el análisis, considerando un riesgo alto y medio del valor del activo relacionado a los hallazgos relevados en el Capítulo I bajo la referencia de las fases de "TOGAF "utilizadas.

Tabla 11 Relación de vulnerabilidades y amenazas en los activos de información

Código Activo	Nombre del activo	Vulnerabilidad	Amenaza
S1	Sistema informático de planificación de proyectos	Falta de documentación	Error en Uso
		Falta de control de cambios de efectivo	Mal funcionamiento de software
		Falta de copias de seguridad	La manupulación de software
		Eliminación o reutilización de los medios de almacenamiento sin borrado adecuada	Abuso de los derechos
		Falta de seguimiento de auditoria	Abuso de los derechos
		Mala gestión de contraseñas	Forja de derechos
S2	Sistema de Documentación	Falta de respaldo	Error en Uso
		Falta de distribución de accesos	Abuso de los derechos
		Falta de procedimientos para la autorización de la información pública	Abuso de los derechos
		Falta de monitoreo en los recursos de procesamiento de información	Datos de fuentes no confiables
H1	Servidor de aplicaciones	Interfaz de usuario complicada	Error en Uso
		Parametro incorrecto configurado	Error en Uso
		Software distribuido ampliamente	La corrupcion de los datos
		Servicios innecesarios habilitadas	Procesamiento ilegal de datos
H3	Computadoras de escritorios	Sensibilidad a la radiación electromagnetica	Radiación electromagnetica
		Falta de planes de sustitución periodicas	La destrucción de los equipos o medios
		Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Incumplimiento de información sistema de mantenibilidad

Código Activo	Nombre del activo	Vulnerabilidad	Amenaza
H5	Impresoras/copiadoras	Uso incorrecto de equipos compartidos	Error en Uso
I1	Internet	El trafico sencible sin protección	Escuchas ilegales
B1	Bases de datos	Falta de espacion fisico en discos de almacenamientos	Error en Uso
		Falta de mecanismos de autenticación	Data corrupta
		Tabla de contraseñas desprotegidas	Divulgación de la información
		Falta de respaldos	Fallo de equipos
R1	Redes informáticas	falta de pruebas de envio o recepción de un mensaje	La negación de las acciones
		Arquitectura de red insegura	Espionaje remoto
		Conexiones de red publicas no protegidas	El uso no autirizados de equipos
F1	Firewall	Falta de activación de los escudos de protección	Error en Uso
		falta de procedimientos para reportar fallos de seguridad informaticos	El uso no autorizado de equipos

Realizado el análisis anterior sobre las vulnerabilidades y amenazas para el proceso crítico "Desarrollo de Proyectos", se inicia la creación de la Matriz de riesgos abordando sus consecuencias y de acuerdo a los valores de probabilidad e impacto, se obtiene como resultado el nivel de criticidad de los riesgos y el posible tratamiento que se evidencia en la tabla siguiente.

Tabla 12 Matriz de Riesgos de los activos de información.

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R1	S1	Sistema informático de planificación de proyectos	Sin registro de documentación histórica formalizada	Robo de información, acceso no autorizado generación de información corrupta	Improbable	Crítico	Crítico	Reducir
R2			Manipulación incorrecta de información debido a que no cuentan con procedimientos formales	Manejo de información no autorizada	Improbable	Alto	Medio	Retener
R3			Disponibilidad parcial o temporal debido a que no se cuenta con respaldo	Indisponibilidad del aplicativo	Posible	Alto	Alto	Reducir
R4			Accesos de usuarios que ya no se encuentran en la empresa y no se les ha dado de baja formalmente	Robo de información, generación de datos corruptos	Posible	Crítico	Alto	Reducir
R5			Error de datos debido a defectos del aplicativo	Pérdida de información	Improbable	Relevante	Medio	Retener

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R11	H1	Servidor de aplicaciones	Lentitud en el sistema debido a servicios activados innecesariamente	Demora de procesos	Posible	Relevante	Medio	Retener
R12			Falla y lentitud de las aplicaciones debido a que no se encuentran enrutadas correctamente	Servidor no disponible	Improbable	Alto	Medio	Retener
R13			Robo de información por inseguridad de arquitectura en la red	Hurto de información	Probable	Crítico	Crítico	Reducir
R14			Fallos inesperados en el sistema debido a antivirus desactualizado	Raro	Probable	Crítico	Crítico	Reducir
R15			Lentitud del rendimiento del servidor por falta de mantenimiento periódico	Servidor no disponible	Posible	Relevante	Medio	Retener

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R16	H5	Impresoras/copiadoras	Daño de cabezales de impresión	Impedimento de impresión de planos navales	Posible	Relevante	Medio	Retener

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R17	I1	Internet	Configuración errónea de los servicios de actualización de parches de seguridad	Fallas en las actualizaciones de parches de seguridad en los equipos informáticos	Posible	Alto	Alto	Reducir

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R18	B1	Bases de datos	Datos corruptos debido a intromisiones sin autorización	Pérdida de información	Posible	Relevante	Medio	Retener
R19			Error en las transacciones de bases de datos por falta de manteniendo	Datos no confiables	Probable	Crítico	Crítico	Reducir
R20			Divulgación no autorizada de las contraseñas y falta de actualización en la base de claves públicas 10	Data no confiable	Probable	Crítico	Crítico	Reducir
R21			Falta de respaldo de la base de datos	Pérdida de información	Posible	Relevante	Medio	Retener
R22			Falta de soporte técnico y actualizaciones de la base de datos	Indisponibilidad del equipo	Posible	Alto	Alto	Reducir

[10] Es un servidor en el que se almacenan claves públicas, una vez obtenida la clave, se puede utilizar para enviar mensajes cifrados al dueño de la clave pública o bien comprobar la firma digital de un mensaje por el dueño de la clave pública.

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R23	R1	Redes Informáticas	Desconexión total o parcial de la red de datos entre clientes-servidor	Pérdida de comunicación en la red informática	Posible	Alto	Alto	Reducir
R24			Falta de control para el uso de la red privada	Intromisión sin autorización en equipos de red	Probable	Crítico	Crítico	Reducir
R25			Conexión a internet deficiente	Lentitud en la navegación web en las oficinas	Posible	Relevante	Medio	Retener
R26			Falta de estandarización en la red informática	Difícil identificación del cableado informático	Improbable	Alto	Medio	Retener
R27			Acceso libre a equipos de la red	Conexiones no autorizadas	Improbable	Alto	Medio	Retener

ID Riesgo	Código Activo	Nombre de Activo	Riesgo	Consecuencias	Probabilidad	Impacto	Criticidad	Tratamiento
R28	F1	Firewall	Falta de controles y configuraciones de permisos de usuarios	Acceso no autorizado a la red interna y externa	Probable	Crítico	Crítico	Reducir
R29			Falta de controles para los accesos a servidores, computadoras personales y la red	Acceso no autorizado a usuarios internos y externos	Probable	Crítico	Crítico	Reducir
R30			Falta de detección en actividades sospechosas vinculadas a la red	Sin gestión en los firewalls	Posible	Alto	Alto	Reducir

Fuente: **(**Infantas & Diaz, 2017)

En consecuencia, para los riesgos identificados en los sistemas de información que apoyan al proceso "Desarrollo de proyectos "en la tabla anterior se establecieron controles para mitigar los riesgos considerados altos y críticos que la organización debe implementar para el resguardo de su información. A continuación, se presenta la lista de controles seleccionados.

Tabla 13 Lista de controles en seguridad de la información seleccionados.

Id riesgo	Riesgo	Criticidad	Cláusula	Control ISO/IEC 27001:2013
R1	Sin registro de documentación historial formalizada	Crítico	A.12 Seguridad de las Operaciones	A.12.1.2 Se debe mantener un control sobre los cambios en la organización, el negocio y los sistemas que afectan la seguridad de la información
R3	Disponibilidad parcial o temporal debido a que no se cuenta con respaldo	Alto	A.12 Seguridad de las Operaciones A.12.3 Backup	A.12.3.1 Se debe tomar y poner a prueba de manera regular, el backup de copias de la información, software e imágenes del sistema, de acuerdo a la política de backup de la organización
R4	Accesos de usuarios habilitados que no se encuentran en la empresa y no se les ha dado de baja formalmente	Alto	A.9 Control de acceso A.6 organización de la seguridad de la información	A.9.1.1 Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información. A.6.2.2 Se deben implementar políticas y medidas de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.

R8	Invalidación de versionados de documentación debido a falta de control de documentos	Alto	A.8 Gestión de los activos A.6 Organización de la seguridad de la información	A.8.2.3 Se debe desarrollar e implementar procedimientos de manejo de los activos de acuerdo con el esquema de clasificación de la información adoptado por la organización. A.6.1.5 La seguridad de la información debe adaptarse a la gestión de proyecto, independientemente del tipo de proyecto.
R9	Inserción de datos incorrecta por parte del personal	Alto	A.9 Control de acceso	A.9.4.1 Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo con la política de control de acceso. A.9.4.3 Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves. A.11.1.2 Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar sólo pueda hacerlo personal autorizado.
R13	Robo de información por inseguridad de arquitectura en la red	Crítico	A.13 Seguridad de las comunicaciones	A.13.1.1 Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones. A.13.1.3 Se debe segregar grupos de servicios de información, usuarios y sistemas de información

R14	Fallos inesperados en el sistema debido a antivirus desactualizado	Crítico	A.12 Seguridad de las operaciones	A.12.2.1 Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada del usuario.
R19	Error en las transacciones de bases de datos por falta de manteniendo	Crítico	A.12 Seguridad de las operaciones	A.12.1.4 Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.
R20	Divulgación no autorizada de las contraseñas y falta de actualización en la base de claves públicas	Crítico	A.12 Seguridad de las operaciones	A.12.4.1 Se debe llevar a cabo y verificar regularmente eventos de log que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información. A.12.4.2 Se debe proteger contra la falsificación y el acceso no autorizado a los medios y la información del log.
R22	Falta de soporte técnico y actualizaciones de la base de datos	Alto	A.11 Seguridad física y medioambiental	A.11.2.4 Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad.

R23	Desconexión total o parcial de la red de datos entre clientes-servidor	Alto	A.13 Seguridad de las comunicaciones	A.13.1.2 Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todas las redes informáticas e incluirlos en los acuerdos de servicios, ya sea que éstos sean proporcionados por la misma organización o por un tercero.
R24	Falta de control para el uso de la red privada y pública	Crítico	A.13 Seguridad de las comunicaciones	A.13.2.1 Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación. A.13.2.2 Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.
R28	Falta de controles y configuraciones a usuarios	Crítico	A.9 Control de acceso	A.9.2.1 Se debe implementar un proceso registro y des-registro del usuario para habilitar los derechos de acceso. A.9.2.6 Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo o ajustado luego de un cambio.

R29	Falta de controles para los accesos a servidores, ordenadores y la red	Crítico	A.9 Control de acceso	A.9.2.2 Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.
R30	Falta de detección en actividades sospechosas vinculadas a la red	Alto	A.13 Seguridad de las comunicaciones	A.14.1.2 Se debe proteger la información que pasa a través de las redes públicas de actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.
R31	Concientización del personal en temas de Tecnologías de la información	Alto	A.7 Durante el trabajo	A.7.2.2 Todos los trabajadores de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizaciones, de acuerdo con las funciones de trabajo que desempeñen. A.7.2.3 Debe existir un proceso disciplinario formal que debe ser comunicado debidamente, para tomar acción contra los trabajadores que comentan alguna infracción vinculada a la seguridad de la información.

Establecimiento de Controles y políticas para el control de riesgos informáticos.

Una vez identificados los riesgos y establecido el plan de tratamientos para mitigar las vulnerabilidades, se diseña el documento de la "Declaración de aplicabilidad[11]" con el formato que convenga a la organización y para el proceso elegido, respetando lo estipulado en la norma ISO/IEC 27001:2013.

Para ello, se realizó una revisión de los 114 controles que indica la Norma ISO/IEC 27002:2013 y a partir de dicho análisis, se dispuso su aplicabilidad a los sistemas de información del proceso seleccionado. La Declaración requiere que no se omita ningún control y si fuera el caso, que este hecho se pueda justificar en función del proceso de negocio analizado. A continuación, se muestran los campos elegidos para el diseño y elaboración de la declaración de aplicabilidad.

Tabla 14 Campos del documento "Declaración de Aplicabilidad"

Campo	Descripción
Sección	Número de Clausula referenciada de la ISO/IEC 27001:2013
Objetivo	Objetivo de la Clausula
Control	Descripción del control
Aplicación	Sí, si es aplicable al proceso No, si no es aplicable al proceso
Justificación de Exclusión	Justificación de por qué se considera que el control no es aplicable
Justificación de Inclusión	Criterios para la selección de controles, LR: Requerimientos legales, OC: Obligaciones contractuales, BR/BP: Requerimientos del negocio /Mejores Prácticas, BRA: Resultado de Análisis de riesgo
Adopción para el Proceso "Desarrollo de Proyectos"	Descripción de cómo sería la aplicación del control al proceso "Desarrollo de Proyectos"

[11]La **declaración de aplicabilidad** es uno de los tantos documentos que tienen que ser redactados por exigencia de la norma ISO/IEC 27001:2013. Se trata de un informe documentado que detalla los objetivos de control y los controles correspondientes al Sistema de Gestión de Seguridad de la Información (SGSI).

Para efectos de la revisión de controles de seguridad escogidos, se toman los campos expresados en la tabla 16 para el diseño del documento Declaración de Aplicabilidad. En este documento se identifican los controles adoptados y los omitidos por la organización. En el Anexo D, se muestra la revisión del documento mencionado, que es requerido por la norma ISO/IEC 27001:2013 para el registro de los controles que deben ser asumidos e implementados por la empresa naviera. En este caso, el objetivo es asegurar que los sistemas de información respaldan el proceso de negocio "Desarrollo de Proyectos".

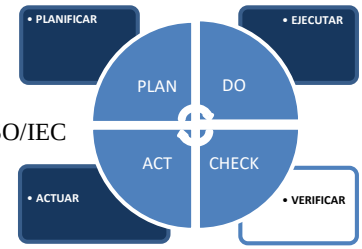
Las políticas que se listan a continuación y que han sido consideradas para la protección de la información del proceso de negocio mencionado, se basan en el documento general "Directrices para la seguridad de la información" que se encuentra en el gestor documental de la empresa naviera.

- Política de Gestión de activos
- Política de la Seguridad de la información ligada a los Recursos Humanos
- Políticas de Gestión de Comunicaciones y Operaciones
- Política de control de accesos
- Política de Desarrollo y Mantenimientos de los Sistemas de Información
- Política de incidentes de Seguridad de la información

Fase 3: Verificar

En adelante se mencionarán los pasos para poder evaluar la efectividad de los 28 controles detallados en el documento de la Declaración de Aplicabilidad. En este sentido, por parte de la Dirección se espera la aprobación de la aceptabilidad del control implementado para mitigar el posible riesgo en los sistemas de información, que es parte del caso de estudio. En este punto se requiere que la organización posea un grupo de actores entrenados en la norma ISO/IEC 27001:2013 para la verificación de los controles y se audite la implementación de las políticas de seguridad,

Ilustración 19 Verificar



realizando la validación de la información a través del juicio de expertos. Los atributos para tener en consideración en la lista de verificación son:

- El actor: Personal calificado para auditar la norma ISO/IEC 27001
- Norma internacional: Norma ISO/IEC 27001:2013.
- Fecha de emisión: Fecha en que se verificó los controles.
- Proceso involucrado: “Desarrollo de Proyectos”.
- Nro. requisito: Número de la sección del control.
- Detalle del requisito: detalle del control seleccionado.
- SI / NO: Si el cumplimiento del control se ejecutó.
- Puntuación: Valor de la aceptabilidad del control establecido por la Gerencia General en el orden >70% No se acepta, >70% y <80% aceptable, >80% aceptación notable
- Evidencia/Observación: Detalle de las novedades encontradas al implementar el control.

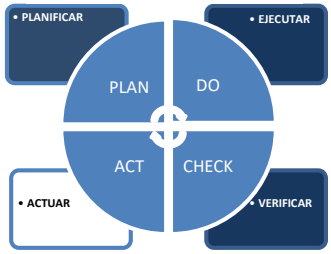
Para este fin se expone el formato de verificación de los controles para el proceso “Desarrollo de Proyectos” (ver Anexo E).

Pasado un tiempo prudencial de tres meses, se obtiene la verificación de los controles, a partir de los procedimientos recomendados por los auditores internos de la organización, a partir de sus conocimientos, experiencia y percepción con la norma ISO/IEC 27001:2013. Esta etapa es de alto nivel y busca redefinir los lineamientos generales que ayudan a la toma de decisiones gerenciales en cuanto a la seguridad de la información.

Fase 4: Actuar

Para esta fase se identificarán los activos de información con el control asociado y la consecuencia luego del control aplicado para mitigar el posible riesgo, que se verá reflejado en las acciones que dispongan en la Revisión por la Dirección para cumplir a futuro con la mejora continua con respecto a la Norma ISO /IEC 27001:2013, que persigue el Ciclo de Deming.

Ilustración 20 Actuar



Por otra parte, de mantenerse la coordinación con la empresa para considerar en cuanto a sugerencias, no conformidades o nuevos lineamientos recibidos por parte de ésta, como consecuencia de su propia revisión y propuestas de mejora en el ámbito de su propio SGSI.
Es así que en esta etapa deberá tenerse en cuenta:

- Identificar no conformidades del SGSI con respecto al proceso crítico “Desarrollo de Proyectos”.
- Definir acciones correctivas y preventivas.
- Evaluar sugerencias y definir la implementación de mejoras.
- Revisar el plan de mejora continua.
- Obtener el “ok” de la Dirección respecto a los cambios propuestos, se ser necesario.
- Comunicar estos cambios y mejoras.
- Monitorear la implementación de estos cambios.

Algunos de estos cambios y mejoras, podrá trascender al alcance del SGSI en cuestión y por ello, podrá ameritar no sólo la aprobación sino un plan compartido con otras áreas involucradas la empresa, tanto en la obtención de recursos necesarios como las etapas de avance y ejecución de estos. En este caso corresponderá, informar de estas mejoras propuestas y requeridas a la Dirección del Comité de Seguridad de la Información y a la Gerencia de la Seguridad de la Información de la empresa para su planificación conjunta. (Mega, 2009).

En base a la planificación, tratamiento del riesgo y la verificación en seguridad de la información al proceso de negocio, se expone los resultados que evidencian al riesgo analizado en el proceso de negocio versus el impacto luego del control aplicado. Ver Anexo F.

Según las tablas del Anexo F, se puede observar la disminución del riesgo relacionado a los activos de información que mantienen en operación al proceso crítico “Desarrollo de Proyectos” y expone el riesgo residual que la organización puede aceptar y gestionar. Por ende, los resultados del presente documento académico fueron el diseño e implementación de controles y políticas de información, acompañados del factor humano que interviene a lo largo del trabajo en el relevamiento de la información del primer capítulo y su participación como auditores internos que evalúan los controles citados en la revisión de la Declaración de aplicabilidad , documento vital de la norma ISO/IEC 27001:2013 para encarar próximas auditorías externas de certificación y la posible acreditación de la norma.

Capítulo IV

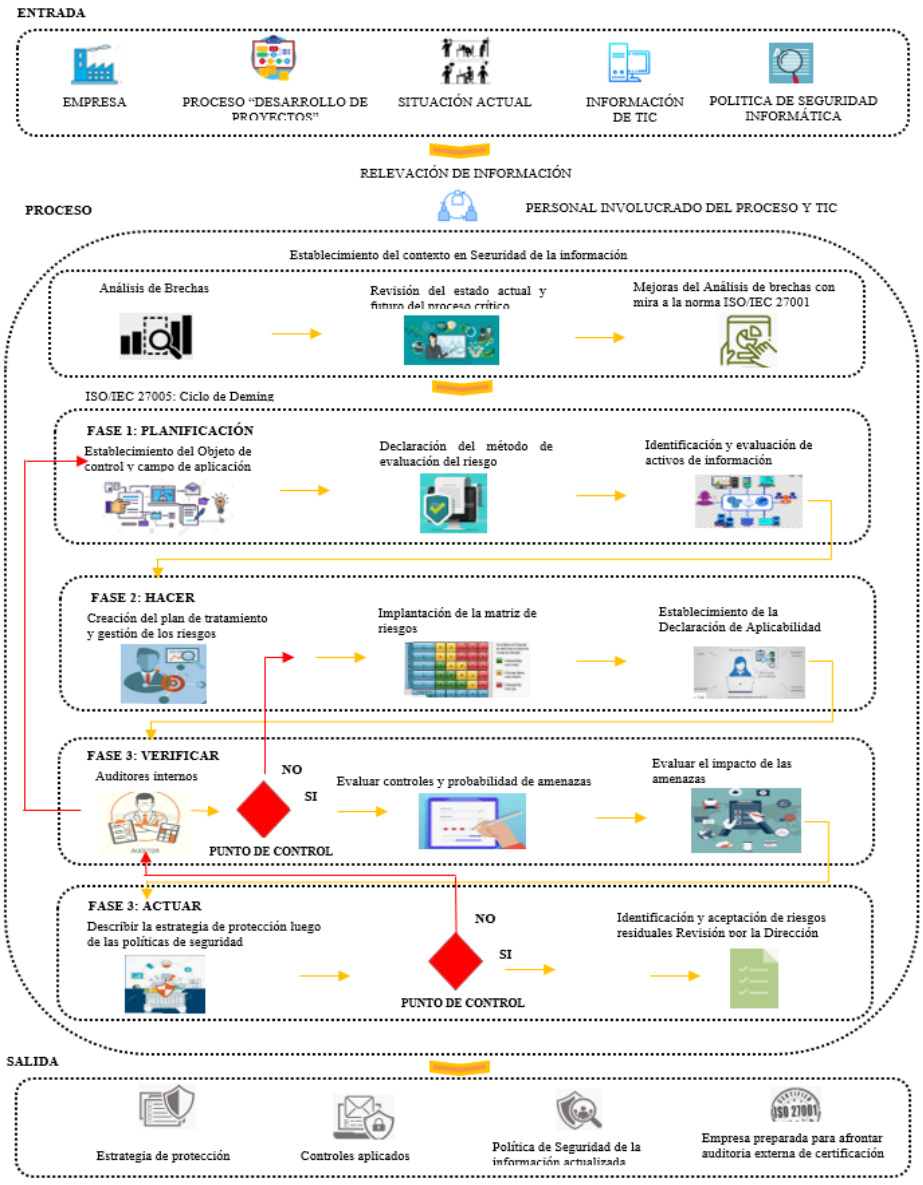
Compendio de la metodología en SGSI al proceso crítico de negocio.

En este capítulo se expone la metodología de forma gráfica a modo de resumen, donde se observará la ruta a seguir en los pasos establecidos para la implementación de la Norma ISO/IEC 27001:2013, combinando los activos de información y el modelo de gestión de riesgos en seguridad de la información descritos anteriormente, que permite a la organización profundizar sus conocimeintos sobre sus activos y los riesgos a los que están expuestos.

El mapa de implementación que muestra las cuatro perspectivas del ciclo de Deming, se inició con el relevamiento de información de la organzación, y los componentes involucrados, que son: la empresa naviera, el proceso "Desarrollo de Proyectos", la información de TICs y su Politica actual en seguridad de información. La información correspondiente a cada uno de estos componentes es relevada en cuanto a las ejecuciones del negocio y la posible afectación de riegos en seguridad de la información haciendo uso de las fases del ADM TOGAF como modelo de relevación de información.

Luego de obtener la información se inició el analisis del estado actual y futuro de la implementación del SGSI, según los requisitos de la norma. De hecho, este analisis permitió observar la gestión huérfana de algunos controles e identificar las políticas de seguridad que requiere el proceso de negocio. En este aspecto, se estableció el criterio de evaluación de riesgos apoyado en la norma ISO/IEC 27005:2008 y su relación con el ciclo de Deming, considerando los conceptos de la ISO/IEC 27002:2013 para la identificación del riesgo, evaluación del riesgo y aceptación del riesgo. En adelante se observará la metodologia propuesta con visión macro basado en los activos de información que apoyan al proceso "Desarrollo de Proyectos", actividad escencial por la organización que ofrece productos y servicios a los clientes finales de la empresa naviera y los puntos de control que pemiten volver a evaluar la información estando en curso el proceso en seguridad de la información.

Ilustración 21 Metodología en seguridad de la información del proceso "Desarrollo de Proyectos"



En el flujo de evaluación del riesgo informático que se expone en la ilustración 21, se identifican dos puntos de control necesarios para volver a evaluar la información del proceso de negocio. El primer punto de control se activa cuando el proceso se encuentra en la fase Actuar, la información es analizada y se observa inconsistencias en los activos de información por ende es enviada para revisión al personal auditor que lo analizará desde la fase de Planificación. Por otro lado, el segundo punto de control es en la fase de Verificar, en esta fase los auditores internos deben volver a revisar los activos de información en la matriz de riesgo y la Declaración de aplicabilidad. De esta forma continúan las fases propias del ciclo de Deming para obtener como salida una estrategia de protección en Seguridad de la información, controles aplicados al riesgo identificado en la fase de planificación, otro documento aceptado y revisado es la Política en seguridad de información. Luego de haber concluido se obtiene un Sistema en seguridad de la información con la probabilidad que la organización se encuentre preparada para auditorías externas en la Certificación de la norma ISO/IEC 27001:2013.

Estrategias para afrontar al cambio en la implementación de un proyecto tecnológico.

La iniciativa de la empresa naviera llevada a cabo con la intención de disminuir el riesgo informático en su proceso más crítico "Desarrollo de Proyectos", incluye toda una estrategia para enfrentar el cambio en la forma de trabajo que el personal ha venido desarrollando en la empresa.

Muchas veces, realizar cambios estructurales o de gestión en la organización implica una alteración en la operación y puede ser visto como amenaza para los intereses de los involucrados. La implementación de un Sistema de Gestión en Seguridad de la Información implica un cambio considerable, regido por controles que deben implantarse o mejorarse y que requieren ser monitoreados según lo exige la norma. Por tal motivo, ante las nuevas definiciones respecto a la gestión de seguridad de la información el capital humano dueño del proceso, podría mostrar cierta resistencia al cambio que la empresa ha decidido emprender.

Como aporte a esta problemática, en este Trabajo Final de Maestría se enuncian a continuación varios métodos para enfrentar la resistencia al cambio que podría experimentarse al implementar los controles aplicables de la norma ISO/IEC 27001:2013.

Posibles causas de resistencia al cambio organizacional

A continuación, se enuncian algunas posibles causas de resistencia al cambio que las personas suelen mostrar:

Baja tolerancia al cambio

Las personas se resisten al cambio porque temen no ser capaces de desarrollar las nuevas habilidades y comportamientos que puede requerir de ellos. Todos los seres humanos tienen una capacidad dada para el cambio, pero en algunos esta limitación es mucho mayor que en otros. El cambio organizacional puede exigir, aunque no sea ésa la intención, que las personas modifiquen su actividad en muchos aspectos y tal vez, rápidamente. Aun cuando los ejecutivos y empleados entiendan la necesidad de realizar cambios en su forma de trabajar, a veces son emocionalmente incapaces de hacer la transición. Esta tolerancia provoca que en ocasiones las personas incluso se resistan a un cambio que consideran bueno. Por ejemplo,

una persona que asume un cargo mucho más importante a raíz de un cambio organizacional probablemente debería sentirse feliz. Sin embargo, también es posible que esa persona se sienta inquieta y se resista a ceder o aceptar ciertos aspectos de la situación actual. Un cargo nuevo y muy distinto le exigirá desarrollar otra conducta, formar otras relaciones y perder algunas actividades y relaciones satisfactorias del cargo actual. Si los cambios son considerables y la persona tiene una baja tolerancia al cambio, podría resistirse enérgicamente por motivos que quizás ni siquiera entienda.

Lidiar con la resistencia.

Muchos ejecutivos subestiman no sólo la variedad de maneras en que las personas pueden reaccionar al cambio organizacional, sino también la influencia positiva que pueden ejercer sobre personas o grupos específico durante un cambio. Además, nuevamente debido a las experiencias pasadas, los ejecutivos a veces no comprenden bien las ventajas y desventajas de los métodos con los que no están familiarizados.

Incomprensión y falta de confianza.

Las personas también se resisten al cambio cuando no comprenden sus implicancias y perciben que las pérdidas podrían ser mucho mayores que las ganancias. Estas situaciones generalmente se dan cuando no existe confianza entre la persona que propone el cambio y los empleados.

Un interés propio con mirada estrecha.

Una de las principales razones por las cuales las personas se resisten a los cambios organizacionales es que piensan que perderán algo valioso. En tales casos, dado que las personas se enfocan en su propio beneficio y no en el de la organización, la resistencia suele manifestarse en “politiquería” o “comportamiento politiquero”. (Kotter & Schlesinger, 2008)
A partir de la presentación de algunas causas por las que el personal muestra resistencia a las exigencias externas e internas que la empresa tiene que afrontar al implementar un SGSI, en la siguiente tabla se mostrará diferentes métodos que podrían emplearse en la gestión del nuevo proyecto en seguridad de la información minimizar.

Tabla 20 Métodos de resistencia al cambio

Método	Situaciones en que se usa comúnmente	Ventajas	Desventajas
Educación y comunicación	Cuando existe falta de comunicación o bien información y análisis inexactos.	Una vez que se les ha persuadido, las personas generalmente ayudarán en la implementación del cambio.	Puede tardar demasiado si existe muchas personas involucradas
Participación y compromiso	Cuando los iniciadores no cuentan con toda la información que necesitan para diseñar el cambio y cuando los demás tienen un poder de resistencia considerable.	Las personas que participan estarán comprometidas con la implementación y cualquier información importante que tengan se integrará al plan de cambio.	Puede tardar mucho si los principiantes diseñan un cambio inadecuado.
Facilitación y apoyo	Cuando la gente se resiste por problemas de adaptación.	Ningún otro método funciona mejor que éste cuando hay problemas de adaptación	Puede tardar mucho, ser costoso y aún asi fallar.
Negociación y acuerdo	Cuando una persona o grupo perderá claramente con el cambio y cuando ese grupo tiene un poder de resistencia considerable.	A veces resulta una manera realtivamente fácil de evitar una resistencia mayor.	En muchos casos puede ser demasiado costoso si alerta a los demas para que negocien su cumplimiento.
Manipulación y cooptación	Cuando las otras tácticas no funcionarán o son demasiado costosas.	Puede ser una solución relativamente rápida y económica ante los problemas de resistencia.	Puede provocar problemas en el futuro si la gente se siente manipulada.
Coerción explícita e implícita	Cuando la rapidez es fundamental y los iniciadores del cambio tienen un poder considerable.	Es un método rápido y puede superar cualquier tipo de resistencia.	Puede ser peligroso si la gente se enoja con los iniciadores.

Métodos posibles para enfrentar la resistencia al cambio.

Para efectos de poder manejar la resistencia al cambio y lograr que la implementación de un SGSI sea aceptada por el personal de la organización, se escogerá de la tabla anterior los métodos que permitan a los usuarios adaptarse a la nueva visión estratégica en seguridad de la información y hacer frente a los nuevos desafíos. Los métodos escogidos para hacer frente a la resistencia laboral son los siguientes:

Educación y comunicación

Para el inicio de este método es necesario educar con anticipación sobre las nuevas definiciones que incluye el SGSI y emprender un sistema de comunicación con ideas que ayuden al personal administrativo y de operación apreciar la necesidad del cambio, lo que conlleva asegurar mediante controles respecto a la seguridad implementada en la información generada y almacenada.

Las acciones requeridas que se deben llevar a cabo se vinculan a la creación de material audiovisual dirigida a los grupos de trabajo y al personal nuevo contratado. Otra acción que ayudaría a dar a conocer las nuevas formas de trabajo es un programa de educación y comunicación para cuando la resistencia se basa en información y análisis inadecuados.

Otra acción en este sentido es la creación de volantes donde la información de los nuevos cambios es comunicada de forma reducida y de fácil comprensión para el personal.

Participación y compromiso

Para que este método tenga éxito y como resultado se obtenga aceptación y viabilidad al despliegue del proyecto en seguridad de la información, es necesario incluir desde un inicio al personal que trabaja en el proceso “Desarrollo de proyectos” en forma activa. Los líderes deben formular preguntas de acuerdo a las acciones que realiza cada equipo de trabajo y sus respuestas deben ser incluidas en el proyecto. De esta forma el personal se sentirá parte del nuevo proceso y entenderán que su participación es valiosa.

Facilitación y apoyo

Otra manera de enfrentar al posible cambio en la organización es brindar apoyo al personal para su fácil adaptación a las exigencias de la Norma ISO/IEC 27001:2013. La empresa debe analizar el nivel de conocimientos con los que cuenta el personal y en base a esto, el proceso debe incluir capacitaciones dirigidas a los empleados y referidas a nuevas habilidades informáticas, y luego se les debe dar tiempo libre para que hagan una retrospectiva en sus funciones y puedan emplear sus nuevos conocimientos en beneficio del proyecto en seguridad de la información.

Conclusiones

1. El establecimiento e implementación de un Sistema de Gestión de la Seguridad de la Información SGSI, para el objetivo y alcance propuesto, permitió identificar los activos críticos de información que apoyan al proceso de negocio "Desarrollo de Proyectos", buscando asegurar la confidencialidad, integridad y disponibilidad de la información involucrada. Para ello, se aplicó un proceso de gestión de riesgos con el fin de contribuir a una mayor protección de dichos activos y garantizar a las partes interesadas, su manejo transparente, adecuado y eficiente. Basar la implementación de un SGSI sobre un proceso serio de gestión de riesgos, le da solidez y realismo ya que permite identificar los activos críticos, las amenazas a las que la empresa está expuesta y las vulnerabilidades que presenta.
2. Se propuso una metodología para mitigar los riesgos a los que estaba expuesto el proceso seleccionado, a través del diseño de políticas en seguridad en base al SGSI, identificando la criticidad e impacto y el posible tratamiento a dar a los riesgos identificados. Al respecto, la elección de una metodología reconocida brindó solidez al proceso de gestión de riesgos.
3. La implementación de la metodología fue realizada sobre la base de una estrategia de evaluaciones realizadas al proceso y de recomendación de lineamientos a cumplir por parte de sus responsables, sobre un esquema de mejora continua. En este sentido, es esencial el involucramiento de todos los responsables y el enfoque de mejora continua, contribuyendo de este modo a un esquema dinámico de seguridad de la información.
4. Se analizó el entorno de negocio del proceso "Desarrollo de proyectos" con la finalidad de identificar a los involucrados y su relación con los activos de información, para la evaluación de los potenciales incidentes informáticos que puedan afectar la operación, de modo de conocer el estado en el que se encontraba el proceso y definir los pasos a seguir para alcanzar los objetivos de seguridad planteados.

5. Se implementó la gestión de riesgos, utilizando como base la norma ISO/IEC 27005:2018, la cual se basa en la ISO/IEC 27001:2013, elegida como base para la implementación del SGSI en la empresa. Al tal fin, se revisaron las políticas de seguridad, con miras al seguimiento de la evolución de los parámetros del negocio en función de amenazas y vulnerabilidades presentes y futuras. En este sentido, toda organización debe ser consciente de que se enfrenta a un panorama cambiante y creciente de amenazas, lo que exige un seguimiento continuo y actualizado.
6. En conclusión, el presente Trabajo Final de Maestría presentó un esquema para la implantación de un SGSI, sobre la base de la norma ISO/IEC 27001:2013, para el aseguramiento del proceso de negocio seleccionado. El trabajo sienta las bases para preparar a la organización para afrontar una auditoría externa de la certificación correspondiente al estándar citado, encaminada hacia una mejora sustantiva de la seguridad de la información en un proceso crítico del negocio.

Recomendaciones

1. Es necesario el apoyo integral de la Gerencia General y el compromiso del personal responsable de los activos de información para el inicio del proyecto de implementación de un SGSI.
2. Una vez que el SGSI es implementado en el proceso de negocio, resulta aconsejable extenderlo a los demás procesos de la empresa, en función de su criticidad para el negocio, para incrementar el nivel de defensa de la organización frente a posibles amenazas internas y externas.
3. Se recomienda fuertemente la revisión periódica del SGSI y la incorporación de nuevos controles, en función a la adquisición de nuevas plataformas o componentes de hardware y software, así como su evaluación y mantenimiento periódicos.
4. Se sugiere que el personal interno del área de auditoría sea capacitado adecuadamente, para hacer frente a los continuos cambios de tecnología y de innovación y sus consecuencias sobre la seguridad de la información.
5. Se recomienda preservar toda evidencia y hallazgos sobre los riesgos informáticos para conservar el historial de gestión y responder ante una auditoría externa del SGSI.
6. Se debe implementar un plan de continuidad del negocio y adiestrar al personal, tanto de aquel que se encargará de la operación informática como del resto de los empleados de la organización que se encuentren involucrados en el proceso. En otras palabras, resulta necesario un programa corporativo de capacitación en seguridad en la información que involucre a todo el personal e incluya también a terceros vinculados a los procesos de la empresa.

Bibliografía

Mahecha Guzman, M., & Coello, G. (2016). Tesis "Desarrollo de un sisitema de información para gestionar la implantación, mantenimiento y mejora continua de un sistema de gestión y seguridad de la información basado en la Norma ISO 27001: 2013". Guayaquil, Guayas, Ecuador.

Andrew Josey, R. H. (2013). *TOGAF Versión 9.1 - Guia de Bolsillo.* Reino Unido: Van Haren Publishing, Zaltbommel.

Andrew Josey, R. H. (2013). *TOGAF Versión 9.1 - Guia de Bolsillo.* Reino Unido: Van Haren Publishing, Zaltbommel.

Comité Técnico colectivo ISO/IEC JTC 1, T. d.-C. (2013). Norma Internacional ISO/IEC 27001 segunda edición .

Comité Técnico Colectivo ISO/IEC JTC 1, T. d.-C. (2013). Norma Internacional ISO/IEC 27001 Segunda Edición .

Comité Técnico Colectivo ISO/IEC JTC1, T. d.-C. (2013). Norma ISO 27001: 2013, Sistema de Gestión Seguridad de Información SGSI.

Comite Técnico Colectivo ISO/IEC JTC1, T. d.-C. (2013-10-01). *NORMA INTERNACIONAL ISO/IEC 27001*.

Comité Técnico ISO/IEC JTC1, T. d. (2008). *Estándar Internacional ISO/IEC 27005.* Reino Unido.

Coronado, F. J. (2003). *Diccionario enciclopédico de estrategia empresarial.* España: Ediciones Diaz de Santos S.A.

Coronado, F. J. (2003). Diccionario enciclopédico de estrategia empresarial. En F. J. Coronado, *Diccionario enciclopédico de estrategia empresarial* (pág. 25). España: Ediciones Diaz de Santos. S.A.

Gerente General CPNV-SP Camilo Montenegro Delgado, D. d. (enero de 2016). Directrices de Seguridad de la Información . Guayaquil, Guayas, Ecuador.

Heredero, C., & López, J. (2008). Dirección y gestión de los sistemas de información en la empresa. España: Esic Editorial.

Infantas, S. F., & Diaz, M. A. (2017). *Diseño e implementación de un sistema de gestión en seguridad de la información para proteger los activos de infromación de la clínica Medcam Perú.* Lima- Perú.

INGERTEC. (2013). Obtenido de https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

INGERTEC, G. (s.f.). *ISO/IEC 27001*. Obtenido de https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

ISACA, (. d. (2012). *Cobit 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Estados Unidos: ISBN 978´-1-60420-282-3.

Kotter , J., & Schlesinger, L. (Julio de 2008). La elección de estrategias para el cambio. *Harvard Business Review*.

Macas Ruiz , E., & Bustamante, W. (28 de Septiembre de 2017). Gobierno de TI: Elección y Aplicación de Buenas Prácticas en Corporación Nacional de Telecomunicación.

Mega, I. G. (2009). *Metodología de implantación de un SGSI en un grupo mpresarial jerárquico* . Montevideo, Uruguay .

Montenegro, G. G.-S. (2016). Directrices de seguridad de la Información. En G. G.-S. Montenegro, *Directrices de seguridad de la Información* (pág. 5). Guayaquil.

PriteshGupta.com. (2013). *ISO/IEC 27002:2013(en)*. Obtenido de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-2:v1:en

reserved, 2. I.—A. (2018). *ISO/IEC 27005:2018(en)*. Obtenido de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27005:ed-3:v1:en

Robert S. Kaplan, D. P. (2000). *El cuadro de Mando Integral The Balanced ScoredCard.*

Rodriguez, P. R. (11 de 09 de 2014). La mejora continua como herramienta para la gestión de proyectos .

Schlesinger, J. P. (2008). *La elección de estrategias para el cambio.*

Senyi Fukusaki Infantas, M. A. (2017). *Diseño e Implementación de un Sistema de Gestión de Seguridad de la información para proteger los activos de información de la clínica Medcam Perú.* Lima-Perú.

Senyi Fukusaki Infantas, M. A. (2017). *Diseño e Implementación de un Sistema de Gestión en Seguridad de la información de la Clínica Medcam Perú.* Lima-Perú.

Stephen A. White PHD, D. M. (2009). *Guia de Referencia y Modelado BPMN.* Estados Unidos, Florida: FutStrat.

The Open Group, A. J. (2013). *TOGAF versión 9.1, Guia de Bolsillo.* Van Haren Publishing Zaltbbommel.

Vieites, A. G. (2014). *Enciclopedia de la Seguridad Informática. 2da Edición* . Madrid-España: Editorial RA-MA.

Anexos

Anexo A. (Informativo) Vulnerabilidades y Métodos para la evaluación de la vulnerabilidad

tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Incumplimiento de información sistema mantenibilidad
	La falta de planes de sustitución periódicas	La destrucción de los equipos o medios
	La susceptibilidad a la humedad, el polvo, la suciedad	El polvo, la corrosión, la congelación
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	La falta de control de cambio de configuración eficiente	Error en uso
	La susceptibilidad a las variaciones de voltaje	La pérdida de la fuente de alimentación
	La susceptibilidad a las variaciones de temperatura	fenómeno meteorológico
	almacenamiento sin protección	El robo de los medios de comunicación o documentos
	La falta de atención a la disposición	El robo de los medios de comunicación o documentos
	la copia no controlada	El robo de los medios de comunicación o documentos
Software	No hay pruebas de software o insuficiente	Abuso de los derechos
	defectos conocidos en el software	Abuso de los derechos
	No 'Cerrar sesión' al salir de la estación de trabajo	Abuso de los derechos
	Eliminación o reutilización de los medios de almacenamiento sin borrado adecuada	Abuso de los derechos
	La falta de seguimiento de auditoría	Abuso de los derechos
	la asignación de derechos de acceso incorrecto	Abuso de los derechos
	software distribuido ampliamente	La corrupción de los datos
	La aplicación de programas de aplicación a los datos erróneos en términos de tiempo	La corrupción de los datos
	interfaz de usuario complicada	Error en uso
	La falta de documentación	Error en uso
	parámetro incorrecto configurado	Error en uso
	fechas incorrectas	Error en uso

	La falta de mecanismos de identificación y autenticación como la autenticación de usuarios	Forja de derechos
	mesas de contraseña no protegidos	Forja de derechos
	La mala gestión de contraseñas	Forja de derechos
	servicios innecesarios habilitadas	procesamiento ilegal de datos
	software inmadura o una nueva	mal funcionamiento de software
	especificaciones confusas o incompletas para desarrolladores	mal funcionamiento de software
	La falta de control de cambio de efectivo	mal funcionamiento de software
	la descarga incontrolada y uso del software	La manipulación de software
	La falta de copias de seguridad	La manipulación de software
	La falta de protección física de los edificios, puertas y ventanas	El robo de los medios de comunicación o documentos
	Falta de presentación de informes de gestión	El uso no autorizado de equipos
Red	La falta de prueba de envío o recepción de un mensaje	La negación de las acciones
	líneas de comunicación no protegidos	escuchas ilegales
	el tráfico sensible sin protección	escuchas ilegales
	Cableado deficiente conjunta	La falta de equipo de telecomunicaciones
	Punto único de fallo	La falta de equipo de telecomunicaciones
	La falta de identificación y autenticación de remitente y el receptor	Forja de derechos
	arquitectura de red insegura	espionaje remoto
	Transferencia de contraseñas en claro	espionaje remoto
	Inadecuado red administración (Resiliencia de enrutamiento)	La saturación del sistema de información
	conexiones de red pública no protegidos	El uso no autorizado de equipos

Personal	Ausencia de personal	El incumplimiento de la disponibilidad de personal
	La insuficiencia de los procedimientos de contratación	La destrucción de los equipos o medios
	formación de seguridad insuficientes	Error en uso
	El uso incorrecto de software y hardware	Error en uso
	La falta de conciencia de seguridad	Error en uso
	La falta de mecanismos de seguimiento	procesamiento ilegal de datos
	el trabajo no supervisado por el exterior o el personal de limpieza	El robo de los medios de comunicación o documentos
	La falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería El uso no autorizado de equipos	

Sitio	El uso inadecuado o negligente de control de acceso físico a los edificios y habitaciones	La destrucción de los equipos o medios
	Ubicación en un área susceptible a las inundaciones	Inundar
	red de energía inestable	La pérdida de la fuente de alimentación
	La falta de protección física de los edificios, puertas y ventanas	Robo de equipos
Organización	Falta de procedimiento formal para el usuario el registro y la cancelación de la matrícula	Abuso de los derechos
	La falta de un proceso formal de revisión de acceso a la derecha (supervisión)	Abuso de los derechos
	La falta o insuficiencia de disposiciones (relativas a la seguridad) en los contratos con los clientes y / o terceros	Abuso de los derechos
	La falta de procedimiento de supervisión de instalaciones de procesamiento de información	Abuso de los derechos
	La falta de auditorías regulares (supervisión)	Abuso de los derechos
	La falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de culpa informes grabado en registros de administrador y operador	Abuso de los derechos
	El incumplimiento servicio inadecuado respuesta de mantenimiento	de información sistema mantenibilidad

	La falta o insuficiencia de disposiciones (relativas a la seguridad de la información) en los contratos con empleados	procesamiento ilegal de datos
	La falta de proceso disciplinario se define en caso de incidente de seguridad de la información	Robo de equipos
	La falta de una política formal sobre el uso del ordenador móvil	Robo de equipos
	La falta de control de los activos fuera del establecimiento	Robo de equipos
	La falta o insuficiente 'escritorio limpio y claro de la pantalla' política	El robo de los medios de comunicación o documentos
	La falta de información de las instalaciones de procesamiento de autorización	El robo de los medios de comunicación o documentos
	Ausencia de establecido vigilancia mecanismos de fallos de seguridad	El robo de los medios de comunicación o documentos
	La falta de revisiones por la dirección regulares	El uso no autorizado de equipos
	La falta de procedimientos para reportar los fallos de seguridad	El uso no autorizado de equipos
	Falta de procedimientos de provisiones el cumplimiento de los derechos intelectuales	El uso de software falsificado o copiado

	La falta o insuficiente Nivel de servicio Acuerdo	Incumplimiento de información sistema mantenibilidad
	La falta de procedimiento de control de cambios	Incumplimiento de información sistema mantenibilidad
	Falta de procedimiento formal para ISMS control de documentación	La corrupción de los datos
	La falta de un procedimiento formal para la supervisión registro ISMS	La corrupción de los datos
	La falta de un proceso formal de autorización de la información pública disponible	Los datos procedentes de fuentes no confiables
	La falta de una adecuada asignación de las responsabilidades de seguridad de la información	La negación de las acciones
	La falta de planes de continuidad	Falla en el equipo
	La falta de política de uso de correo electrónico	Error en uso
	Falta de procedimientos para introducir software en sistemas operativos	Error en uso
	Falta de registros en el administrador y registros del operador	Error en uso
	Falta de procedimientos para clasificado tratamiento de la información	Error en uso
	La falta de responsabilidades de seguridad de la información en las descripciones de puestos	Error en uso

Anexo B. Cuestionario GAP ISO/IEC 27001:2013

Test de cumplimiento de controles del proceso "Desarrollo de proyectos" con la implementación de la Norma ISO/IEC 27001		**No cumple**	**Parcial**	**Cumple**
Controles de gestión:				
A5.- Políticas de Seguridad de la Información				
A5.1	**Dirección de gestión para la seguridad de la información**			
1	¿La Gerencia ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?			3
2	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?			3
A6.- Organización de la Seguridad de la Información				
A6.1				
1	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades en los procesos de negocio?		2	
2	¿Se han segregado en el proceso de negocio las responsabilidades sobre la Seguridad de la Información para evitar usos o accesos indebidos?		2	
3	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes			3

	relacionados con la Seguridad de la Información?			
4	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	1		
5	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?		2	
A6.2	**Dispositivos Móviles y Teletrabajo**			
1	¿Se consideran los requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	1		
2	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?			3
A7.- Seguridad en los Recursos Humanos				
A7.1	**Antes de contratar a un empleado**			
1	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Títulos verificados -Referencias			3
2	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?			3
A7.2	Durante el contrato			

1	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?			3
2	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?		2	
3	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?		2	
A7.3	Terminación del contrato			
1	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?			3
Controles técnicos				
A8.- Gestión de Activos				
A8.1	Responsabilidad sobre los Activos			
1	¿Se ha realizado un inventario de los activos que dan soporte al negocio y de Información?		2	
2	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?			3
3	¿Se han establecido normas para el uso de activos en relación a su seguridad?		2	
4	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?			3
A8.2	Clasificación de la Información			

1	¿Se clasifica la información según su confidencialidad, integridad y disponibilidad en orden a establecer medidas de seguridad específicas?	1		
2	¿Los activos de información son fácilmente identificables respecto a su grado de confidencialidad, integridad y disponibilidad o su nivel de clasificación?			3
3	¿Existen procedimientos para gestionar la información de acuerdo a su clasificación?	1		
A8.3	Manipulación de Soportes			
1	¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado	1		
2	¿Existen procedimientos establecidos para la eliminación de soportes?	1		
3	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado -Etc.	1		
A9.- Control de Acceso				
A9.1	**Requisitos generales para el control de acceso**			

1	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?		2	
2	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?		2	
A9.2	Accesos de Usuario			
1	¿Existen procesos formales de registro de usuarios?			3
2	¿Existen procesos formales para la asignación de perfiles de acceso?			3
3	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?		2	
4	¿Se ha establecido una política específica para el manejo de información clasificada como secreta en cuanto a autenticación y compromisos?	1		
5	¿Se establecen periodos concretos para renovación de permisos de acceso?			3
6	¿Existe un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o un contrato?			3
A9.3	Responsabilidades de los usuarios			
1	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?	1		

A9.4	Control de acceso a sistemas y aplicaciones			
1	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de forma que se restrinjan los requerimientos de información a la actividad específica a desarrollar?		2	
2	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla, etc.?			3
3	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?			3
4	¿Se controla la capacitación y el perfil de las personas que tienen permisos de administración con niveles bajos de Seguridad?		2	
5	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?	1		
A10.- Criptografía				
A10.1	**Control criptográfico**			
1	¿Existe una política para el establecimiento de controles criptográficos?	1		
2	¿Existe un control del ciclo de vida de las claves criptográficas?	1		
A11.- Seguridad Física y del entorno				
A11.1	**Áreas de Seguridad**			
1	¿Se establecen perímetros de seguridad física donde sea necesario, con barreras de acceso?		2	

2	¿Existen controles de acceso en áreas restringidas?			3
3	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc., en áreas de accesibles a personal externo?			3
4	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?			3
5	¿Se controlan las áreas de carga y descarga con procedimientos de control de mercancías entregadas etc.?			3
6	¿Son controlados los puntos de accesos de distribución para el ingreso de personal no autorizado?		2	
A11.2	**Seguridad de los equipos**			
1	¿Se protegen los equipos tanto respecto al medioambiente como a los accesos no autorizados?			3
2	¿Se protegen los equipos contra fallos de suministro de energía?		2	
3	¿Existen protecciones para los cableados de energía y de datos?		2	
4	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?			3
5	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. que puedan contener información de la organización que no es pública?	1		

6	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?	1		
7	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?		2	
8	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?		2	
9	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?			3
Controles Operacionales				
A12.- Seguridad en las Operaciones				
A12.1	**Procedimientos y responsabilidades**			
1	¿Se documentan los procedimientos y se establecen responsabilidades?		2	
2	¿Se controla que la información sobre procedimientos se mantenga actualizada?		2	
3	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?	1		
4	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?			3
A12.2	Protección contra software malicioso			
1	¿Existen sistemas de detección para Software malicioso o malware?			3

A12.3	Copias de Seguridad			
1	¿Se ha establecido un sistema de copias de seguridad acorde con las necesidades de la información y de los sistemas?			3
A12.4	Registros y supervisión			
1	¿Se realiza un registro de eventos? Por ejemplo: -Intentos de acceso fallidos/exitosos, -Desconexiones del sistema o -Alertas de fallos	1		
2	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?		2	
3	¿Se protegen convenientemente y de forma específica los accesos de los empleados o externos autorizados o los de los administradores?		2	
4	¿Existe un control de sincronización de los distintos sistemas?		2	
A12.5	Control del Software			
1	¿Las instalaciones de nuevas aplicaciones de software o las modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?	1		
A12.6	Vulnerabilidad Técnica			
1	¿Se establecen métodos de control para vulnerabilidades técnicas de tipo "hacking ético" o similar?	1		

2	¿Se establecen medidas restrictivas para la instalación de software en cuanto a personal autorizado, evitando las instalaciones por parte de usuarios finales?		2	
A12.7	Auditorias de Sistemas de Información			
1	¿Existen mecanismos de auditoría de medidas de seguridad de los sistemas?	1		
A13.- Seguridad en las Comunicaciones				
A13.1	Seguridad de Redes			
1	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?			3
2	¿Se establecen condiciones de seguridad en los servicios de red, tanto propios como subcontratados?		2	
3	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?			3
A13.2	Intercambio de Información			
1	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?	1		
2	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?	1		
3	¿Se establecen normas o criterios de seguridad en mensajería electrónica?		2	

4	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades			3
A14.- Adquisición, desarrollo y mantenimiento de sistemas de información				
A14.1	Intercambio de Información			
1	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?		2	
2	¿Se especifican los requisitos de Seguridad de la información en el diseño de nuevos sistemas?			3
3	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?			3
A14.2	Seguridad en los procesos de Soporte			
1	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?		2	
2	¿Se gestiona el control de cambios con relación al impacto que puedan tener en los sistemas?	1		
3	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?			3
4	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?	1		
5	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?		2	
6	¿Se realiza una evaluación de riesgos para herramientas de desarrollo de Software?		2	

7	¿Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros?		2	
8	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?	1		
9	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?			3
A14.3	Datos de prueba			
1	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?	1		
A15.- Relación con Proveedores				
A15.1	Seguridad en la Relación con Proveedores			
1	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?		2	
2	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?		2	
3	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro?	1		
A15.2	Gestión de servicios externos			
1	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?			3
2	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?			3
A16.- Gestión de incidentes de seguridad de la información				

A16.1	Gestión de incidentes de seguridad de la información y mejoras.			
1	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?	1		
2	¿Se han implementado canales adecuados para la comunicación de incidentes en la Seguridad de la Información?			3
3	¿Se promueve y se han establecido canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	1		
4	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?	1		
5	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?	1		
6	¿La información que es proporcionada por los eventos en la Seguridad de la Información es adecuadamente tratada para tomar medidas preventivas?	1		
7	¿Existe un proceso para recopilar evidencias sobre los incidentes en la Seguridad de la Información?	1		
A17.- Gestión de la Continuidad del Negocio				
A17.1	Continuidad de la seguridad de la información.			
1	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?		2	

2	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?		2	
3	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?	1		
A17.2	Redundancias			
1	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?			3
A18.- Cumplimiento				
A18.1	Cumplimiento de los requisitos legales y contractuales.			
1	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento en cuanto a: -Protección de Datos Personales -Transacciones Bancarias -Información Protegida -Ley general de Telecomunicaciones -Otras propias del negocio o actividad?		2	
2	¿Existen procedimientos implementados sobre la propiedad intelectual?			3
3	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	1		
4	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	1		

5	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo con la legislación?	1		
A18.2	Revisiones de la Seguridad de la Información			
1	¿Se revisan los controles de la Seguridad de la Información por personal independiente respecto a los responsables de implementar los controles?	1		
2	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la Información?		2	
3	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?	1		

Anexo C. Identificación de los activos de información

Identificador del activo	Nombre de Activo de información	Descripción	Uso en el Proceso	Sub.proceso	Clasificación del activo	Sub-clasificación	Propietario del activo	Ubicación
A1	Gerente de proyectos	Responsable de las desiciones estratégicas y legalización de los proyectos	Desarrollo de proyectos	Planificación de proyectos	Primario	Gerencia	Administrador	Casa Matriz
A2	Jefe de proyectos	Responsable de regisatrar y velar por el cumplimiento de los proyectos	Desarrollo de proyectos	Planificación de proyectos	Primario	Jefatura	Administrador	Casa Matriz
A3	Lideres de proyectos	Encargados de la ingenieria y validación del producto contratado	Desarrollo de proyectos	Ejecución, Evaluación y Control de proyectos	Primario	Recursos humanos	Administrador	Casa Matriz
A4	Ingenieros diseñadores	Responsables del diseño de nuevas embarcaciones	Desarrollo de proyectos	Diseño	Primario	Recursos humanos	Usuario	Casa Matriz
A5	Secretaria	Encargada de actas de entregas	Desarrollo de proyectos	Cierre del proyecto	Primario	Recursos humanos	Usuario	Casa Matriz

Identificador del activo	Nombre de Activo de información	Descripción	Uso en el Proceso	Sub.proceso	Clasificación del activo	Sub-clasificación	Propietario del activo	Ubicación
H2	Servidor de correos	Equipo informatico que soporta la gestión de correos	Todos los usuarios del proceso	Paritícipa en toda la gestión del proceso	Primario	Hardware	Administrador	Casa Matriz
H3	Computadoras de escritorios	Equipo informatico que permite a los usuarios el diseño de embarcaciones	Todos los usuarios del proceso	Paritícipa en toda la gestión del proceso	Primario	Hardware	Administrador	Casa Matriz
H4	Lector Biométrico	Equipo que permite el acceso los departamentos	Para todos los procesos de negocios	Paritícipa en toda la gestión del proceso	Secundario	Hardware	Administrador	Casa Matriz/Sucursal
H5	Impresoras/copiadoras	Equipo que permite obtener planos digitales a fisicos	Todos los usuarios del proceso-diseño	Paritícipa en toda la gestión del proceso	Primario	Hardware	Administrador	Casa Matriz
I1	Internet	Servicio que permite la comunicación al mundo y proveedores	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Red	Administrador	Casa Matriz/Sucursal
B1	Bases de datos	Motor de base de datos para los sistemas de negocios, documentación y correos	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Primario	Administrador	Casa Matriz
R1	Redes informáticas	Cableado y equipos de comunicaciones normalizado entre enquipos informáticos	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Red	Red	Casa Matriz/Sucursal

Identificador del activo	Nombre de Activo de información	Descripción	Uso en el Proceso	Sub.proceso	Clasificación del activo	Sub-clasificación	Propietario del activo	Ubicación
I1	Internet	Servicio que permite la comunicación al mundo y proveedores	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Red	Administrador	Casa Matriz/Sucursal
B1	Bases de datos	Motor de base de datos para los sistemas de negocios, documentación y correos	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Primario	Administrador	Casa Matriz
R1	Redes informáticas	Cableado y equipos de comunicaciones normalizado entre enquipos informáticos	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Red	Administrador	Casa Matriz/Sucursal
F1	Firewall	Equipo de protecc6n de perimetro de seguridad y acceso lógico	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Red	Red	Casa Matriz/Sucursal
U1	UPS	Equipo de protección eléctrico	Para todos los procesos de negocios	Desarrollo de proyectos	Primario	Hardware	Eléctrico	Casa Matriz/Sucursal

Anexo D. Revisión para la elaboración de la Declaración de Aplicabilidad del proceso" Desarrollo de Proyectos"

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / NO	
A.5	Políticas de seguridad de la información								
A.5.1	Gestión de la Gerencia para la seguridad de la información								
A.5.1.1	Políticas de la seguridad de la información	La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.	La empresa cuenta con la Política de la Seguridad de la información					NO	La Política de la seguridad de la información fue comunicada a los trabajadores y partes externas involucradas
A.5.1.2	Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.		X		X	X	SI	Se inicia la revisión de los términos de la Política de seguridad de la información
A.6	Organización de la seguridad de la información								
A.6.1	Organización interna								
A.6.1.1	Funciones y responsabilidades de la seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.				X		SI	Se revisaron las responsabilidades en seguridad de la información

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / NO	
A.6.1.2	Segregación de tareas	Tareas o áreas de responsabilidad de conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizada o involuntaria o el uso inadecuado de los activosde la organización	No representa riesgo					NO	El personal cuenta con tareas debidamentes segregadas
A.6.1.3	Contacto con las autoridades	Se debe mantener contacto adecuado con las autoridades respectivas	No representa riesgo					NO	El personal es informada continuamente sobre el cambio de autoridaes
A.6.1.4	Contacto con grupos especiales de interés	Se debe mantener contacto con grupos especiales de interés u otros forums y asociaciones de profesionales especializados en seguridad	No representa riesgo					NO	El personal del proceso es constantemente invitados a forums de seguridad
A.6.1.5	Seguridad de la información en la gestión del proyecto	La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.		X	X		X	SI	Se implementaron las directrices en la gestión de proyectos para la seguridad de la información
A.6.2	Equipos móviles y trabajo a distancia								
	Objetivo: Garantizar la seguidad del trabajo a distancia y del uso de losequipos móviles								
A.6.2.1	Politicas de los equipos móviles	Se debe adoptar politicas y medidas de soporte de seguridad para el manejo de los riesgos derivados del uso de móviles	No representa riesgo					NO	La organización cuenta con políticas y resticciones en el uso de equipos móviles
A.6.2.2	Trabajo a distancia	Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.					X	SI	Se implementaron reglas de accesos en el firewall para el trabajo a distancia

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.7	Seguridad de los recursos humanos								
A.7.1.	Antes de reclutarlo								
A.7.1.1	Filtración	Se debe llevar a cabo la verificación de los antecedentes de todos los candidatos al empleo de acuerdo a las leyes y regulaciones vigentes y a la ética; y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.	No representa riesgo crítico					NO	El nuevo personal contratado es informado de las regulaciones de la empresa
A.7.1.2	Términos y condiciones de empleo	Los acuerdo contrantatuales con los trabajadores y contratistas debe fijar sus responsabilidades y las de la organización con respecto a la seguridad de la información	No representa riesgo crítico					NO	El personal es debidamente informado en términos y condiciones del empleo
A.7.2	Durante el trabajo								
	Objetivo: Garantizar que los trabajadores y los contratistas sean conscientes y cumplan con las responsabilidades de la seguridad de la información								
A.7.2.1	Responsabilidades de la Gerencia	La Gerencia debe instar a todos los trabajadores y contratistas a aplicar la seguridad de la información de acuerdo a las políticas y procedimientos por la organización	No representa riesgo crítico					NO	Al personal contratato es informado sobre gestión en seguridad de la información
A.7.2.2	Concientización, educación y capacitación sobre seguridad de la información	Todos los trabajadores de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizaciones, de acuerdo a las funciones de trabajo que desempeñen.		X		X		SI	Se implementaron capacitaciones trimestrales al personal interno de la organización

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.7.2.3	Procesos disciplinarios	Debe haber un proceso disciplinario formal que sebe ser comunicado en su lugar , para tomar acción contra los trabajadores que cometan alguna infracción contra la seguridad de la información	No representa riesgo crítico					NO	El personal administrativo y Obrero es comunicado sobre reglamentos de disciplinas en la organización
A.7.3	Término y cambio de empleo								
	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o término del empleo								
A.7.3.1	Término o cambio de responsabilidades de empleo	Se debe definir, comunicar y reforzar a todos los trabajadores y contratistas, las responsabilidades y tareas de seguridad de la información que permanecerán válidos después del término del empleo.	No representa riesgo crítico					NO	El personal es comunicado sobre sus deberes y responsabilidades
A.8	Gestión de los Activos								
A.8.1	Responsabilidades sobre los activos								
	Objetivo: Identificar los activos de la organización y definir las responsabilidades adecuadas de protección								
A.8.1.1	Inventario de activos	Se debe identificar los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos.	No representa riesgo crítico					NO	La empresa cuenta con un sistema de gestión de activos informáticos
A.8.1.2	Propiedad de los activos	Los activos que se encuentren identificados en el inventario deben ser asignados a un "propietario"	No representa riesgo crítico					NO	Los activos son debidamente asignados a sus custodios
A.8.1.3	Uso aceptable de los activos	Se debe implementar, documentar e implementar las reglas para el uso aceptable de la información y de los activos relacionados a la información y a las instalaciones de procesamiento de la información.	No representa riesgo crítico					NO	Se ecuentra documentado el uso aceptable de los activos en el gestor documental

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.8.1.4	Retorno de los activos	Todos los trabajadores y usuarios internos y externos deberán devolver todos los activos de la organización que estén en su posesión una vez terminado su empleo, contrato o acuerdo.	No representa riesgo critico					NO	Se evidencia políticas de retorno de activos al culminar la fecha laboral
A.8.2	Clasificación de la información								
	Objetivo: Garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la organización								
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de los requisitos y valores legales, siendo critica y sensible ante la divulgación y modificación no autorizada.		X	X	X	X	SI	Se implementaron procedimientos categorizandos en clasificación de la información
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar una serie de procedimeientos adecuados para el etiquetado de la información , de acuerdo al esquema de clasificación de la infomación adoptado por la orgacización				X		SI	Se implementaron políticas de etiquetado de los activos de la información
A.8.2.3	Manejo de los activos	Se debe desarrollar e implementar procedimientos de manejo de los activos de acuerdo al esquema de clasificación de la información adoptado por la organización.				X	X	SI	Se implementaron procedimientos de manejos de activos físicos y digitales con delegación de responsables

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.8.3	Manejo de los medios de comunicación								
	Objetivo: Prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación								
A.8.3.1	Gestión de medios de comunicación removibles	Se debe implementar procedimientos para la gestión de los medios de comunicación removibles de acuerdo al esquema de clasificación adoptado por la organización	No representa riesgo critico					NO	Existe la politica de gestión de medios removibles actualizados
A.8.3.2	Disposición de los medios comunicación	Los medios comunicación deben ser desechados de manera segura cuando ya no son necesarios, mediante procedimientos formales.	No representa riesgo critico					NO	Existe procesos formales para la disposición de medios de comunicación
A.8.3.3	Transferencias fisica de los medios de comunicación	Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.	No representa riesgo critico					NO	Existe procesos formales conta el mal uso de medios de comunicación
A.9	Control de acceso								
A.9.1	Requisitos del negocio sobre control del acceso								
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información.				X		SI	Se diseñaron políticas en control de accesos para la gestión del proceso crítico

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.9.1.2	Acceso a la redes y a los servicios de las redes	Los usuarios deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.						NO	Los usuarios cuentan con accesos definidos por rol de gestión
A.9.2	Gestión del acceso al usuario								
	Objetivo: Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios								
A.9.2.1	Registro y des-registro del usuario	Se debe implementar un proceso registro y des-registro del usuario para habilitar los derechos de acceso.			X			SI	Se implementaron accesos de acuerdo al cargo y des-resgistro al término laboral
A.9.2.2	Provisión de acceso al usuario	Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.			X			SI	Se formalizaron accesos a los sitemas de información en caso de algún problema legal en la empresa
A.9.2.3	Gestión de los derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.	No representa riesgo critico					NO	Los accesos son asignados al inicio de la contratación del empleado
A.9.2.4.	Gestión de información de autenticación secreta de usuarios	Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal.						NO	El personal de sistemas gestiona la autenticación secreta de los usuarios

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.9.2.5	Verificación de los derechos de acceso de los usuarios	Los propietarios de los activos deben verificar los derechos de acceso de los usuarios a intervalos regulares.	No representa riesgo					NO	Los accesos son monitoreados por personal de sistemas
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajustado luego de un cambio.					X	SI	Se reforzaron las políticas que desvincula los accesos a los sistemas informáticos y accesos físico a departamentos sensibles
A.9.3	Responsabilidades del usuario								
	Objetivo: Hacer a los usuarios responsables de salvaguardar la autenticación de su información								
A.9.3.1	Uso de información secreta de autenticación	Se debe solicitar a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.	No representa riesgo					NO	El personal es comunicado sobre el uso de información restringida

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.9.4	Control de acceso a sistemas y aplicaciones								
	Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones								
A.9.4.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso.		X			X	SI	Se implementaron políticas de acceso a la información y funciones de los sistemas

A.9.4.2	Procedimiento seguro de logeo	Si así lo requiere la política de control del acceso, se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un procedimiento seguro de logeo.						NO	Los sistemas cuentan con sistemas seguros de logeos
A.9.4.3	Sistema de gestión de la clave	Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.					X	SI	Se establecieron procedimientos en el Directorio Activo para cambio de clave mensual
A.9.4.4	Uso de programas utilitarios de privilegio	Se debe restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación.	No es riesgo para el proceso					NO	Existen políticas de instalación de software en el equipo informático del personal
Sección	**Objetivo**	**Control**	**Justificación de exclusión**	**Justificación de Inclusión**				**Aplicación**	**Adopción del Proceso "Desarrollo de Proyectos"**
				Requerimientos Legales	**Obligaciones contractuales**	**Requerimientos del negocio**	**Resultado de análisis de riesgo**	**SI / No**	
A.9.4.5	Control del acceso para programar el código fuente	Se debe restringir el acceso al programa de código fuente.	No es riesgo para el proceso					NO	Existen políticas sobre el uso y restricción del código fuente
A.10	Criptografía								
	Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información								
A.10.1.1	Política del uso de controles criptográficos	Se debe desarrollar e implementar una política de uso de controles criptográficos para proteger la información.	No es riesgo para el proceso					NO	Existen políticas de manipulación criptográficos en la información
A.10.1.2	Gestión de las claves	Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida.	No es riesgo para el proceso					NO	Existen políticas de gestión de claves criptográficas

A.11	Seguridad física y medioambiental								
A.11.1	Áreas seguras								
	Objetivo: Evitar acceso físico no autorizado, daño e interferencia a la información e instalaciones de procesamiento de la información de la organización.								
A.11.1.1	Perimetro de seguridad física	Se debe determinar y utilizar los perimetros de seguridad para proteger las áreas que contienen información sensible y critica y las instalaciones de procesamiento de la información.	No presenta riesgo para el proceso					NO	El personal informático mantiene reglas de perímetros en seguridad física
A.11.1.2	Controles fisicos de los ingresos	Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.					X	SI	Se implementaron accesos a lugares críticos del proceso de negocio

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI / No	
A.11.1.3	Seguridad de las oficinas, salas e instalaciones	Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	No representa riesgo critico para el proceso					NO	Las instalaciones cuentan con mecanismos físicos y digitales
A.11.1.4	Protección contra las amenazas externas y medioambientales	Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.	No representa riesgo critico para el proceso					NO	Existen políticas de protección contra las amenazas externas y medioambientales
A.11.1.5	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.	No representa riesgo critico para el proceso					NO	El personal informático gestiona reglas para el trabajo en áreas seguras
A.11.1.6	Distribución de las zonas de carga	Los puntos de acceso, tales como las zonas de distribución y carga y otros puntos por los que podría ingresar personal no autorizado a las instalaciones deben ser controlados, y en la medida de lo posible, alejados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	No representa riesgo critico para el proceso					NO	Estan debidamente señalados los luegares seguros de descarga y carga de equipos informáticos
A.11.2	Equipos								
	Objetivo: Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización.								
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.	No representa riesgo critico para el proceso					NO	Existen luegares especializados para el almacenaje de equipos informáticos

Sección	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/No	
A.11.2.2	Servicios públicos de soporte	Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.	No representa riesgo crítico					NO	El personal informático cuenta con servicios públicos en línea para soportes
A.11.2.3	Seguridad en el cableado	Se debe proteger de cualquier interferencia, intercepción o daño	No representa riesgo crítico					NO	El cableado estructurado se encuentra normado bajo políticas de instalación
A.11.2.4	Mantenimiento de los equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	No representa riesgo crítico	X			X	Si	Se establecieron políticas para el mantenimiento del equipo informático
A.11.2.5	Retiro de los activos	El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización	No representa riesgo crítico					NO	Existen políticas para el retiro seguro del equipo informático
A.11.2.6	Seguridad de los equipos y bienes fuera de las instalaciones	Se debe aplicar medidas de seguridad para los activos utilizados fuera de las instalaciones, tomando en cuéntalos diferentes riesgos de trabajar fuera de las instalaciones de la organización.	No representa riesgo crítico					NO	Existen políticas para el trabajo y transporte seguro de los equipos informáticos fuera de las instalaciones
A.11.2.7	Disposición o re-uso seguro de los equipos	Todos los equipos que contienen medios de comunicación de la información deben ser revisados para garantizar que se haya extraído o que se haya sobre-escrito la información sensible y la licencia del software antes de desechar o re-usar el mismo.	No representa riesgo crítico					NO	Existen procedimientos de re-uso de equipos informáticos

Sección	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.11.2.8	Usuario de equipo abandonado (desatendido)	Los usuarios deben garantizar una adecuada protección a los equipos abandonados	No representa riesgo critico					NO	Existen políticas de bloqueos automáticos de equipos en caso de ser desatendidos
A.11.2.9	Política de escritorio y pantallas limpias	Se debe adoptar la política de escritorio limpio de papeles y de medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de la información.	No representa riesgo critico					NO	El personal informático mantienen políticas de escritorios limpios
A.12	Seguridad de las operaciones								
A.12.1	Procedimientos y responsabilidades operaciones								
A.12.1.1	Documentación de los procedimientos operacionales	Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.		X				SI	Se implementaron la politicas para las revisiones permanentes de la documentación generada del proceso de negocio
A.12.1.2	Cambios en la gerencia	Se debe mantener un control sobre los cambios en la organización, el negocio y los sistemas que afectan la seguridad de la información	No representa riesgo critico					NO	El personal informático mantiene roles en los sistemas en caso de cambios departamentales
A.12.1.3	Gestión de la capacidad	Debe ser monitoreado y mejorado el uso de recursos, así como las proyecciones hechas sobre los requisitos de capacidad del futuro, para garantiza el desempeño del sistema.	No representa riesgo critico					NO	El departamento de sistemas garantiza la disponibilidad y capacidad de los sistemas

Sección	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.12.1.4	Separación de ambientes de desarrollo, prueba y de operaciones	Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.				X	X	SI	Se implementaron procedimientos para la separación de ambientes de prueba y producción para reducir cambios no autorizados
A.12.2	Protección contra el malware (programa malicioso)								
	Objetivo: Garantizar que la información y las instalaciones de procesamiento de la información estén protegidos contra el malware								
A.12.2.1	Controles contra el malware	Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada al usuario.					X	Si	Se implementaron revisiones periódicas al software y al antivirus corporativo
A.12.3	Backup								
	Objetivo: Proteger la información contra la pérdida								
A.12.3.1	Backup de la información	Se debe tomar y poner a prueba de manera regular, el back up de copias de la información, software e imágenes del sistema, de acuerdo a la política de back up de la organización.					X	SI	Se implementaron políticas de respaldos a las bases de datos corporativas para ser ejecutados por el personal técnico informático

Sección	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.12.4	Logeo y monitoreo								
	Objetivo: Registrar eventos y generar evidencias								
A.12.4.1	Eventos de logeo	Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información.					X	SI	Se implementaron registros de eventos de accesos por reglas al firewall y los equipos informáticos de la organización

A.12.4.2	Protección de la información del logeo	Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo					X	SI	Se implementaron políticas de control contra la falsificación de logeos
A.12.4.3	Logeo del administrador y operador	Debe logearse las actividades del sistema del administrador y del operador, y los logs deben ser protegidos y revisados de manera regular.	No representa riesgo al proceso					NO	Es revisado con periocidad los log de los sistemas como regla de gestión
A.12.4.4	Sincronización de los relojes	Se debe sincronizar a una sola fuente de tiempo de referencia, los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de la organización o del dominio de seguridad.	No representa riesgo al proceso					NO	El personal informático mantiene sincronizados los relojes del sistema con el Directorio activo

Sección	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.12.5	Control del software operacional								
	Objetivo: Garantizar la integridad de los sistemas operacionales								
A.12.5.1	Instalación del software en los sistemas operacionales	Se debe implementar procedimientos para controlar la instalación del software en los sistemas operacionales	No representa riesgo al proceso					NO	Existen reglas de isntalación de software en los equipos informáticos
A.12.6	Gestión de las vulnerabilidades técnicas								
	Objetivo: Evitar la explotación de las vulnerabilidades técnicas								
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener, de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de la información a ser utilizados; evaluar la exposición de la organización a dichas vulnerabilidades y tomar las medidas adecuadas para manejar los riesgos asociados.	No representa riesgo al proceso					NO	El personal informático se basa en la política de vúlnerabilidades y técnicas para el manejo de riesgos informáticos asociados
A.12.6.2	Restricciones en la instalación de software	Se debe establecer e implementar las reglas que gobiernen la instalación de los softwares.	No representa riesgo al proceso					NO	Existen reglas de instalación de software que mantiene el personal informático

A.12.7	Consideraciones de las auditorías sobre los sistemas de información								
	Objetivo: Minimizar el impacto de las actividades de las auditorías en los sistemas operacionales								
A.12.7.1	Controles de la auditoria sobre los sistemas de información	Se debe planificar cuidadosamente los requisitos y actividades de la auditoria que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio	No representa riesgo al proceso					NO	El personal informático planifica actividades de auditorías para mejoras de gestión

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.13	Seguridad de las comunicaciones								
A.13.1	Gestión de la seguridad de las redes								
	Objetivo: Garantizar la protección de la información en las redes y de sus instalaciones de procesamiento de la información								
A.13.1.1	Controles en las redes	Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones					X	SI	Se implementaron políticas de control en la redes informáticas
A.13.1.2	Seguridad de los servicios de las redes	Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.			X		X	SI	Se implementaron mecanismos de seguridad en los equipos de red y monitoreo de accesos a terceros
A.13.1.3	Segregación en las redes	Se debe segregar grupos de servicios de información, usuarios y sistemas de información					X	SI	Se implementaron segmentaciones de la Red en Vlans para la identificación por departamentos

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.13.2.	Transferencia de la información								
	Objetivo: Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa								
A.13.2.1	Políticas y procedimientos de la transferencia de la información	Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación					X	Si	Se implementaron procedimientos de confidencialidad en el manejo de la información sensible
A.13.2.2	Acuerdos sobre la transferencias de la información	Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.					X	Si	Se implementaron procedimiento de transferencia de información
A.13.2.3	Mensajes electrónicos	Se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.	No representa riesgo					NO	Existen reglas de envios de mensajeria en la organización
A.13.2.4	Confidencialidad o acuerdos no divulgados	Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.	No representa riesgo					NO	Existen los documentos confidenciales del proceso
A.14	Adquisición, desarrollo y mantenimiento del sistema								
A.14.1	Requisitos de seguridad de los sistemas de información								
	Objetivo: Garantizar que la seguridad de la información forme parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos del sistema de la								
A.14.1.1	Análisis y especificaciones de los requisitos de la seguridad de la información	Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.	No representa riesgo al proceso					NO	Existen políticas de requisitos de seguridad de la información para el mejoramiento y gestión de los sistemas

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.14.1.2	Seguridad de los servicios de aplicación en las redes públicas	Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.					X	SI	Se implemenaron reglas de accesos en el firewall para la protección de la información a servidores de amenazas internas y externas
A.14.1.3	Protección de las transacciones de los servicios de aplicación	Se debe proteger la información que provenga de las transacciones se los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.	No representa riesgo al proceso					NO	El personal de sistemas mantiene políticas de revisón de mensajes por roles
A.14.2	Seguridad en los procesos del programa de desarrollo y soporte								
	Objetivo: Garantizar que se diseñe e implemente la seguridad de la información dentro del ciclo del programa de desarrollo de los sistemas de la información								
A.14.2.1	Política del programa de desarrollo seguro	Se debe establecer y aplicar reglas de desarrollo de software y sistemas a los programas de desarrollo dentro de la organización.	No representa riesgo al proceso					NO	El personal de desarrollo mantiene reglas y políticas en escritura de código fuente
A.14.2.2	Procedimiento de control de los cambios de sistemas	Se debe controlar los cambios dentro del ciclo de vida de los programas de desarrollo, mediante el uso de procedimientos formales de control de cambios.	No representa riesgo al proceso					NO	Existen políticas de control de cambios

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.14.2.3	Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional	Luego del cambio de las plataformas operacionales, se debe revisar y verificar las aplicaciones criticas del negocio, para garantizar que no haya un impacto adverso sobre las operaciones o la seguridad organizacional.	No representa riesgo al proceso					NO	El comité de seguridad de la información establece técnicas de control y cambios
A.14.2.4	Restricciones a los cambios de los paquetes de software	No se facilitará la modificación de los paquetes de sistemas; por el contrario, se les limitará a los cambios necesarios y todos los cambios deberán ser estrictamente controlados.	No representa riesgo al proceso					NO	Los cambios en el sistema se encuentran controlodos por reglas del Directorio activo
A.14.2.5	Principios del sistema de seguridad para la ingenieria	Se debe establecer, documentar, mantener y aplicar los principios de sistemas de seguridad para la ingenieria, a todos los esfuerzos de implementación del sistema.	No representa riesgo al proceso					NO	El proceso cuenta con la documentación para limitar los cambios en los sistemas
A.14.2.6	Ambiente seguro del programa de desarrollo	Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo de los sistemas de desarrollo y la integración de los esfuerzos a lo largo del ciclo de vida del programa de desarrollo del sistema.	No representa riesgo al proceso					NO	Los ambientes de desarrollo se encuntran noemalizados y gestionados
A.14.2.7	Programa de desarrollo subcontratado	La organización debe supervisar y monitorear las actividades de desarrollo del sistema del ente subcontratado.	No representa riesgo al proceso					NO	Existen políticas para el control de programas subcontratados
A.14.2.8	Revisión de la seguridad del sistema	Se debe llevar a cabo revisiones de la funcionalidad de la seguridad durante el desarrollo	No representa riesgo al proceso					NO	Existen revisiones mensuales de las funcionalidades de los sistemas

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.14.2.9	Revisión de la aceptación del sistema	Se debe establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos sistemas de información, renovaciones y nuevas versiones.	No representa riesgo al proceso					NO	Personal de sistemas hace revisiones historiales para la aceptación de sistemas
A .14.3	Datos de prueba								
	Objetivo: garantizar la protección de los datos utilizados para la verificación								
A.14.3.1	Protección de los datos de prueba	Los datos de prueba deben ser seleccionados, protegidos y controlados cuidadosamente.	No representa riesgo al proceso					NO	Se evidencia control de datos de prueba
A.15	Relación con los proveedores								
A.15.1	Seguridad de la información en las relaciones con los proveedores								
	Objetivo: Garantizar la protección de los activos de la información a los que los proveedores tiene acceso								
A.15.1.1	Política de seguridad de la información sobre las relaciones con los proveedores	Se debe acordar y documentar los requisitos de seguridad de la relaciones con los proveedores información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización.	No representa riesgo al proceso					NO	Se evidencia requisitos de control relacionones con proveedores en la política de seguridad de la información
A.15.1.2	Consideración de la seguridad en los acuerdos con los proveedores	Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.	No representa riesgo al proceso					NO	Se verifica que el proceso de negocio establece acuerdos contractuales relacionados son la seguridad de la información

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.15.1.3	Cadena de suministro de tecnología de la información y comunicación	Los acuerdos con los proveedores deben incluir los requisitos para el manejo de los riesgos de seguridad de la información relacionados a los servicios de tecnología de la información y la comunicación y a la cadena de suministro del producto	No representa riesgo al proceso					NO	Las políticas de seguridad informática contempla acuerdos con proveedores
A.15.2	A.15.2 Gestión de la prestación del servicio por parte del proveedor								
	Objetivo: Mantener un nivel acordado de seguridad de la información y de la prestación del servicio alineado a los acuerdos del proveedor								
A.15.2.1	Monitoreo y revisión del servicio de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.	No representa riesgo al proceso					NO	Se evidencia el monitoreo y auditoría de los servicios con proveedores
A.15.2.2	Cambios en la gestión del servicio de los proveedores	Se debe gestionar los cambios a la provisión de los servicios prestados por los proveedores, incluyendo el mantenimiento y la mejora de políticas, procedimientos y controles de la seguridad de la información, tomando en cuenta la sensibilidad de la información del negocio, los sistemas y los procesos involucrados asi como la re-evaluación de los riesgos.	No representa riesgo al proceso					NO	Existen reglamentos para la gestión de proveedores dirigido por el Departamento de compras
A.16	Gestión de los incidentes de seguridad de la información								
A.16.1	A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora								
	Objetivo: Garantizar una aproximación consistente y efectiva a la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre los eventos y debilidades de la								
A.16.1.1	Responsabilidades y procedimientos	Se debe establecer responsabilidades de la gerencia y procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información	No representa riesgo al proceso					NO	Existe un Comité de seguridad de la información para emitir responsables

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.16.1.2	Reporte de los eventos de seguridad de la información	Se debe reportar los eventos de seguridad de la información a través de canales adecuados lo más pronto posible.	No representa riesgo al proceso					NO	Existen canales adecuados para reportar los incidentes informáticos
A.16.1.3	Reporte de las debilidades de la seguridad de la información	Se debe instar a los trabajadores y contratistas que hagan uso de los sistemas de información de la organización, a tomar nota e informar acerca de cualquier debilidad que se observe o sospeche con respecto a los sistemas o servicios del sistema de seguridad de la información.	No representa riesgo al proceso					NO	El personal informático reporta mensualmente las debilidades en los sistemas
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Se debe evaluar los eventos de seguridad de la información; y tomar una decisión sobre si deben ser clasificados como incidentes de la seguridad de la información.	No representa riesgo al proceso					NO	La organización periódicamente clasifica los incidentes informáticos
A.16.1.5	Respuesta a los incidentes de seguridad de la información	Se debe responder a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.	No representa riesgo al proceso					NO	El comité revisa periódicamente los incidentes informáticos
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información, con la finalidad de reducir la probabilidad o impacto de futuros incidentes.	No representa riesgo al proceso					NO	La organización cuenta con repositorios para la revisión de lecciones aprendidas

Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.	No representa riesgo al proceso					NO	El personal de sistemas mantiene controles de recolección de evidencias
A.17	Gestión de los aspectos de la seguridad de la información para la continuidad del negocio								
A.17.1	Continuidad de la seguridad de la información								
	Objetivo: La continuidad de la seguridad de la información debe estar incrustada en los sistemas de gestión de la continuidad del negocio de la organización								
A.17.1.1	Continuidad de los planes de seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas, e.g. durante una crisis	No representa riesgo al proceso					NO	Existen Políticas en planes de seguridad de la información
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	No representa riesgo al proceso					NO	Se evalúan controles periódicos para las posibles adopciones
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa.	No representa riesgo al proceso					NO	Se evidencia evaluaciones periódicas en seguridad de la información
Sección	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción del Proceso "Desarrollo de Proyectos"
				Requerimientos Legales	Obligaciones contractuales	Requerimientos del negocio	Resultado de análisis de riesgo	SI/NO	
A.17.2	Redundancias								
	Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de la información								
A.17.2.1	Disponibilidad de instalaciones de procesamiento de la información	Se debe implementar las instalaciones de procesamiento de la información con una capacidad adicional suficiente para cumplir con los requisitos de disponibilidad.	No representa riesgo al proceso					NO	La organización garantiza las instalaciones en buen estado para las funcionalidades del proyecto

A.18	Cumplimiento								
A.18.1	Cumplimiento de los requisitos legales y contractuales								
	Objetivo: Evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad de la información y al cualquier requisito de seguridad								
A.18.1.1	Identificación de la ley aplicable y de los requisitos contractuales	Se debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos legislativos regulatorios y contractuales así como el enfoque de la organización para cumplir con estos requisitos, con respecto a cada sistema de información y a la organización.	No representa riesgo al proceso					NO	El area Legal mantiene vigente la información desarrollada en la organización
A.18.1.2	Derechos de propiedad intelectuales	Se debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derecho de propiedad intelectuales y al uso de productos registrados de software.	No representa riesgo al proceso					NO	La empresa mantiene derechos de propiedad intelectual en todo desarrollo informático realizado en la organización
A.18.1.3	Protección de los registros	Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y lanzamiento no autorizado, de acuerdo a los requisitos legales, regulatorios, contractuales y del mismo negocio.	No representa riesgo al proceso					NO	Los registros son protegidos y respaldados con pericidad
Sección	**Objetivo**	**Control**	**Justificación de exclusión**	**Justificación de Inclusión**				**Aplicación**	**Adopción del Proceso "Desarrollo de Proyectos"**
				Requerimientos Legales	**Obligaciones contractuales**	**Requerimientos del negocio**	**Resultado de análisis de riesgo**	**SI/NO**	
A.18.1.4	Privacidad y protección de la información que permite identificar a las personas	Se debe garantizar la privacidad y la protección de la información que permita identificar a las personas de acuerdo a lo requerido en la legislación y las regulaciones pertinentes, si fuera aplicable.	No representa riesgo al proceso					NO	La alta gerencia evalúa las regulaciones y legislaciones
A.18.1.5	Regulación de los controles criptográficos	Se debe hacer uso de controles criptográficos en cumplimiento con los acuerdos, las leyes y las regulaciones correspondientes.	No representa riesgo al proceso					NO	Se mantienen controles criptográficos para leyes y acuerdos
A.18.2	Revisiones de la seguridad de la información								
	Objetivo: Garantizar que la seguridad de a información sea implementada y operada de acuerdo a las políticas y procedimientos organizacionales								
A.18.2.1	Revisión independiente de la seguridad de la información	Se debe revisar, a intervalos planificados o cuando ocurre algún cambio significativo,, el enfoque de la organización para gestionar la seguridad de la información y su implementación (i.e. objetivos de control, controles, políticas, procesos y procedimientos de la seguridad de la información).	No representa riesgo al proceso					NO	Se mantiene reuniones para revisión de procedimientos de seguridad informática

A.18.2.2	Cumplimiento de las políticas y normas de seguridad de la información	Los gerentes deben revisar regularmente el cumplimiento de los procedimientos y del procesamiento de la información dentro de su área de responsabilidad, de acuerdo a las políticas, normas de seguridad adecuadas y a los otros requisitos de seguridad.	No representa riesgo al proceso					NO	La alta gerencia junto con el comité mantienen reuniones de revisón en políticas de seguridad de la información
A.18.2.3	Revisión del cumplimiento técnico	Se debe revisar regularmente los sistemas de la información con respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	No representa riesgo al proceso					NO	El Proceso mantiene políticas de revisión técnica en nuevos proyectos

Anexo E. Verificación del cumplimiento de controles asignados

Datos Generales					Fecha de emisión
Auditor interno	Luis Tapia				4/5/2020
Norma internacional					Proceso involucrado
ISO/IEC 27001 – Sistema de Gestión en Seguridad de la Información					"Desarrollo de Proyectos"
DESCRIPCIÓN					
N° Requisito	Detalle del requisito	Cumplimiento			Evidencia / Observación
		SI	NO	Puntuación	
A.5	Políticas de seguridad de la información				
A.5.1.2	Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.	X		100%	Se evidencia revisión de la Política de Seguridad informática mediante reuniones realizadas por la Gerencia General
A.6	Organización de la seguridad de la información				
A.6.1.1	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	X		80%	Se evidencia las responsabilidades asigandas en gestión en seguridad de la información por medio de la existencia de documento Directrices de Seguridad de la Información DIT-DDE-016 , / No existem reuniones periódicas del comité en Seguridad de la información
A.6.1.5	La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.	X		100%	Se evidencia el documento PRD-GDP-001 Procedimiento para el Desarrollo de Proyectos v02 1. que informa directrices de procedimientos para inicios de proyectos
A.6.2.2	Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.	X		100%	El personal de Infraestructura técnologica ha implementado reglas de navegación y acceso a teletrabajo desde el Firewall , se evidencia en el sistema.
A.7	Durante el trabajo				
A.7.2.2	Todos los trabajadores de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizaciones, de acuerdo a las funciones de trabajo que desempeñen.		X	0%	No se evidencia capacitaciones frecuentes al personal interno y externo sobre seguridad de la información

A.8	Gestión de los Activos				
A.8.2.1	La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.	X		50%	Existe informe de gestión de capacidad, no existe versionamiento actualizado. INF-TIC-046 PROYECCIONES DE CAPACIDAD INFORMÁTICA
A.8.2.2	Se debe desarrollar e implementar una serie de procedimientos adecuados para el etiquetado de la información, de acuerdo al esquema de clasificación de la información adoptado por la organización	X		100%	Se evidencia procedimientos de etiquetado a los sistemas informáticos adoptado por la empresa
A.8.2.3	Se debe desarrollar e implementar procedimientos de manejo de los activos de acuerdo al esquema de clasificación de la información adoptado por la organización.	X		100%	Se evidencia procedimientos demanejo de activos y asiganción de responsbles en la organización
A.9	Control de acceso				
A.9.1.1	Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información.	X		100%	Se evidencia la existencia de documento Directrices de Seguridad de la Información DIT-DDE-016
A.9.2.1	Se debe implementar un proceso registro y des-registro del usuario para habilitar los derechos de acceso.	X		50%	Se evidencia acciones esporádicas para los des-resgistros del personal en la empresa
A.9.2.2	Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.	X		100%	Se evidencia procedimientos en el sistema para revocar los accesos al personal desvinculado por el personal de talento humano
A.9.2.6	Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajustado luego de un cambio.	X		100%	Se evidencia la eliminación del acceso a los departamentos considerados áreas sencibles en la organización a los trabajadores y personal contratato por contrato temporales
A.9.4.1	Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso.	X		100%	Se evidencia perimetros de seguridad de accesos a la información de acuerdo al rol de los usuarios implementado desde el inicio de la cntratación.
A.9.4.3	Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.	X		100%	Se evidencia reglas de gestión de claves en el Directorio activo que garantiza el cambio de clave mensualmente de forma automática y manual según requiera el usuario

A.11	Seguridad física y medioambiental				
A.11.1.2	Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.	X		100%	Se evidencia el funcionamiento de equipos biométricos para el control de ingresos y registros actualizados en base de datos
A.11.2.4	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	X		70%	Se evidencia el mantenimiento físico y virtual de los equipos informáticos del datacenter , Se observa que falta registros del último semestre de algunos equipos de escritorio
A.12	Seguridad de las operaciones				
A.12.1.1	Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.	X		100%	Se evidencia versionamientos actualizados en el gestor documental del proceso
A.12.1.4	Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.	X		100%	Se evidencia ambientes separados en la base de datos destinados para las pruebas y puesta en producción de los nuvos desarrollos creados para el proceso critico "Desarrollo de Proyectos".
A.12.3	Backup				
A.12.3.1	Se debe tomar y poner a prueba de manera regular, el back up de copias de la información, software e imágenes del sistema, de acuerdo a la política de back up de la organización.	X		100%	Se evidencia en el sistema los periodos de back up configurados para el respaldo de la información y luego almacenado en cinta magnética la data considerada sensible para el proceso critico.
A.12.4	Logeo y monitoreo				
A.12.4.1	Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información.	X		100%	Se evidencia reglas de navegación y de acceso desde el fairewall para todo el personal contratado , de igual manera al personal invitado y proveedores.
A.12.4.2	Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo	X		100%	Se evidencia procedimentos de logeo y des-logeo al personal de la empresa
A.13	Seguridad de las comunicaciones				
A.13.1.1	Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones	X		100%	Se evidencia registros historiales de administración y control de los accesos a la red informática que mantiene en linea a las aplicaciones
A.13.1.2	Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.	X		100%	Se evidencia procedimientos de seguridad en los equipos de la intranet y bloqueos de puertos , donde su apertura es solo por autorización del Oficial de seguridad informática
A.13.1.3	Se debe segregar grupos de servicios de información, usuarios y sistemas de información	X		100%	Se evidencia la segmentación de la red lan por , departamento y servicios (impresoras y telefoina IP) . Al proceso critico está debidamente segmentado su red física .
A.13.2.1	Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación	X		100%	Se evidencia procedimientos de transferencia de información a los distintos departamentos del proceso hacia afuera y de afuera hacia el proceso
A.13.2.2	Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.	X		100%	Se evidencia la transferencia segura de información mediante correo electrónico y por medio dela intranet .
A.14	Adquisición, desarrollo y mantenimiento del sistema				
A.14.1.2	Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.	X		100%	Se evidencia el acceso restringido a la información controlada por roles de usuarios en el sistema de gestión documental del proceso "Desarrollo de Proyectos"

Anexo F. Afectación del riesgo luego del control

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Cláusula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Sistema informático de planificación de proyectos	Improbable	Crítico	Crítico	A.12 Seguridad de las Operaciones	A.12.1.2 Se debe mantener un control sobre los cambios en la organización , el negocio y los sistemas que afectan la seguridad de la información	Probable	Media	Medio
	Posible	Alto	Alto	A.12 Seguridad de las Operaciones A.12.3 Backup	A.12.3.1 Se debe tomar y poner a prueba de manera regular , el backup de copias de la información, software e imágenes del sistema , de acuerdo a la política de Backup de la organización	Posible	Media	Bajo
	Posible	Alto	Crítico	A.9 Control de acceso A.6 organización de la seguridad de la información A.14.1 Requisitos de seguridad de los sistemas de información	A.9.1.1 Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información. A.6.2.2 Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede , procesa o almacena en los lugares de trabajo a distancia. A.14.1.2 Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.	Posible	Media	Bajo

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Cláusula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Sistema de documentación	Posible	Alto	Alto	A.5 Políticas de seguridad de la información A.6 Organización de la seguridad de la información	A.5.1.2 Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos. A.6.1.1 Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	Reducir	bajo	Bajo
	Raro	Relevante	Alto	A.9 Control de acceso	A.9.4.1 Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso. A.9.4.3 Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.	Reducir	Relevante	Bajo

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Cláusula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Equipos y Servidores de Aplicaciones	Posible	Relevante	Medio	A.11 Seguridad fisica y medioambientalA.13 Seguridad de las comunicaciones	A.13.1.1 Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones. A.13.1.3 Se debe segregar grupos de servicios de información, usuarios y sistemas de información A.11.2.4 Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	Reducir	bajo	Bajo
	Improbable	Alto	Crítico	A.12 Seguridad de las operaciones	A.12.2.1 Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada al usuario. A.12.1.4 Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.	Reducir	Relevante	Medio

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Cláusula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Usuarios	Posible	Alto	Medio	A.12 Seguridad de las operaciones	A.12.4.1 Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información. A.12.4.2 Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo.	Reducir	bajo	Bajo
	Raro	Relevante	Medio	A.7.2 Durante el trabajo	A.7.2.2 Todos los trabajadores de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizaciones, de acuerdo a las funciones de trabajo que desempeñen.	Posible	Media	Bajo

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Cláusula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Internet	Posible	Alto	Alto	A.13 Seguridad de las comunicaciones	A.13.1.2 Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero. A.13.2.1 Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación. A.13.2.2 Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.	Posible	Medio	Medio

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Clausula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Bases de Datos	Posible	Crítico	Medio	A.9 Control de acceso	A.9.2.2 Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.	Posible	Relevante	Bajo
	Probable	Alto	Crítico	A.8.2 Clasificación de la información	A.8.2.1 La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.A.8.2.3 Se debe desarrollar e implementar procedimientos de manejo de los activos de acuerdo al esquema de clasificación de la información adoptado por la organización.	Probable	Crítico	Medio

Nombre de Activo	Probabilidad de Riesgo	Consecuencia de riesgo	Impacto del riesgo	Cláusula	Control ISO/IEC 27001:2013	Probabilidad luego del control	Consecuencia luego del control	Impacto del riesgo luego del control
Redes Informáticas	Posible	Alto	Alto	A.13 Seguridad de las comunicaciones	A.13.1.1 Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones A.13.1.2 Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.	Posible	Alto	Bajo
	Probable	Crítico	Crítico	A.13 Seguridad de las comunicaciones	A.13.1.3 Se debe segregar grupos de servicios de información, usuarios y sistemas de información	Probable	Crítico	Medio
Nombre de Activo	**Probabilidad de Riesgo**	**Consecuencia de riesgo**	**Impacto del riesgo**	**Cláusula**	**Control ISO/IEC 27001:2013**	**Probabilidad luego del control**	**Consecuencia luego del control**	**Impacto del riesgo luego del control**
Firewall	Probable	Crítico	Crítico	A.12.4 Logeo y monitoreo	A.12.4.1Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información.	Posible	Relevante	Bajo
	Probable	Crítico	Crítico	A.6.2 Equipos móviles y trabajo a distancia	A.6.2.2 Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.	Probable	Crítico	Bajo