UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACION Y SISTEMAS

"MODELO DE PROCESOS PARA LA IMPLEMENTACION DE LA NORMA ISO 27001 EN LA CONCESIONARIA TERRAPUERTO TRUJILO S.A. DURANTE EL AÑO 2017"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACION Y SISTEMAS

LÍNEA DE INVESTIGACIÓN: Gestión de sistemas de información

AUTOR: Br. Edward Jean Carlos Llanos Paredes

ASESOR: **Ing. Enrique Cárdenas Rengifo**

TRUJILLO - PERÚ

2017

Presentación

Señores Miembros del Jurado:

Dando cumplimiento al Reglamento de Grados y Títulos de la "Universidad Privada Antenor Orrego", para optar el título Profesional de Ingeniero de Computación y Sistemas, es grato poner a vuestra consideración, la presente tesis titulada:

"MODELO DE PROCESOS PARA LA IMPLEMENTACION DE LA NORMA ISO 27001 EN LA CONCESIONARIA TERRAPUERTO TRUJILO S.A. DURANTE EL AÑO 2017"

Este trabajo de investigación es el resultado de esfuerzo, donde he plasmado todos los conocimientos y experiencias adquiridas a lo largo de mi formación profesional, complementado además con la orientación y apoyo de mi asesor y todas aquellas personas que colaboraron durante el desarrollo del Proyecto.

Atentamente,

Br. Edward Jean Carlos Llanos Paredes

Trujillo, julio del 2017

Dedicatoria

A mis padres, que me han apoyado inmensurablemente durante los años de mi vida universitaria y por la confianza que depositaron siempre en mí, ya que gracias a su esfuerzo y ejemplo estoy alcanzando poco a poco mis metas y objetivos.

A mis familiares que en los momentos más difíciles me apoyaron y me dieron la ánimos y fuerza para continuar.

A Dios, por ser quien nos guía por el camino del bien y nos da las fuerzas necesarias para seguir y no desfallecer en el intento.

Agradecimientos

Siendo el presente trabajo, resumen de nuestro esfuerzo a lo largo de la carrera siempre demostrando nuestro grado de responsabilidad, compañerismo, respeto y gratitud para aquellas personas que son valiosas que hacen posible esta tesis, a ustedes también está mi especial agradecimiento.

A mi asesor, Ing. Luis Enrique Cárdenas Rengifo, por su desmedido apoyo valioso e invalorable colaboración y guía importante a lo largo del desarrollo de la misma

A la empresa Concesionaria Terrapuerto Trujillo por el apoyo y confianza para la realización de esta tesis.

Resumen

La presente tesis tiene por objetivo realizar un modelo de procesos para la implementación de la norma ISO 27001 en la Concesionaria Terrapuerto Trujillo, al verse comprometida de forma indirecta con la normativa publicada en el año 2016, donde se indica que se tiene que resguardar y administrar de forma correcta la información de la empresa bajo la normativa ISO 27001.

Para ello se aplica las etapas basadas en el framework Spark, las cuales serán tomadas para la creación de dicho modelo de procesos para la empresa Concesionaria Terrapuerto Trujillo S.A. demostrando que, las etapas que presenta este framework, la realización del modelo de procesos para la implementación se dará en un mayor porcentaje de noventa por ciento de los requerimientos, políticas y controles que exige la norma técnica peruana para que se cumpla en la empresa con respecto al Sistema de Gestión de Seguridad de la información.

Abstract

The present thesis aims to create a process model for the implementation of the ISO 27001 standard in the Terrapuerto Trujillo Concessionary, being indirectly compromised with the regulations published in 2016, which indicate that it has to be safeguarded and administered In a correct way the information of the company under the norm ISO 27001.

For this purpose, the stages based on the Spark framework are applied, which will be taken for the creation of this process model for the company Terraces Trujillo S.A. Demonstrating that the stages of this methodology, the implementation of the model of processes for implementation will be given in a greater percentage of ninety percent of the requirements, policies and controls required by the Peruvian technical standard to be met in the company with With respect to the Information Security Management System.

Índice

Índice de Tablas

Índice de Gráficos

I. INTRODUCCIÓN

Los medios de transporte se han convertido de suma importancia para las personas y los avances tecnológicos y la gran cantidad de empresas abocadas en este rubro pueden dar fe de ello. (Ferreiro, 2006) Pero con estas mejoras también vienen algunas complicaciones, si hablamos del medio de transporte más común sin duda nos estaremos refiriendo a los automóviles, estos son de gran utilidad ya que están hechos para desplazarse a distancias cortas y largas sin mayor problema, estos se podrían decir que en la actualidad han generado que sea el medio de transporte público más común y por lo tanto ha hecho que deba regularse y organizarse de manera efectiva para que sea un beneficio y no un problema. (Euronews, 2013) En este punto es en el que nace el concepto de Terrapuerto o Terminal terrestre, que como concepto organiza y regula el transporte público de distancias medias y largas, las grandes ciudades de los países más desarrollados acuñaron este concepto debido a lo que la experiencia les fue enseñando.

En nuestro continente se ha visto el crecimiento de países como Argentina, Ecuador, Brasil y otros, este crecimiento sin duda ha llevado a estos países a tener problemas de primer mundo como lo son el transporte público. (Maciel, 2014)En el caso de Brasil específicamente fue un problema que se tuvo que atacar contundentemente debido a la magnitud del caos que vivía en muchas áreas pobladas, planteando reformas y un gran plan de culturización en el cual se está haciendo posible generar un cambio oportuno.

(Penagos, 2011) Perú es un país en vías de crecimiento y el transporte público no es la excepción. Recientemente se están llevando a cabo muchos proyectos como el metropolitano y el tren eléctrico en Lima o la construcción de terminales terrestres como Terminal Plaza Norte, El Terminal Terrestre de Moquegua o El Terminal Terrestre de Arequipa, son muestras de las medidas que se están tomando para afrontar el hecho de que el país crece y demanda una mejor organización en el transporte público.

Trujillo es una de las principales ciudades del Perú y a la vez un destino turístico concurrido, la aparición de agencias de transporte interprovincial han ido en aumento en estos últimos años generando bienestar a la ciudad debido a la diversidad que hay al momento de tomar una elección sobre qué servicio consumir, pero a la vez ha traído incomodidades debido al tráfico y ruido que su actividad genera, ya que éstas se encuentran ubicadas en el casco urbano de la ciudad. (Castro, 11) La Municipalidad Provincial de Trujillo en vista de todo lo que estaba ocurriendo se planteó la tarea de solucionarlo, mediante la construcción de un Terrapuerto, el cual albergaría a todas estas empresas centralizando así las actividades de todas estas.

Concesionaria Terrapuerto Trujillo es una organización que presta sus servicios a empresas de transporte provincial, con el fin de buscar una formalidad de todas estas empresas de transporte y además brindar seguridad y comodidad a las personas que desean viajar al interior del país.

Existen varios procesos que se realizan para tener un total control y registro de actividades que las empresas de transporte realizan en la Concesionaria Terrapuerto de Trujillo.

(Peruano, 2016) En inicios del 2016 se declara el uso obligatorio de la NTP / ISO IEC 27001:2014 para todas las entidades Integrantes del Sistema Nacional de Informática, la cual se denota la importancia del activo más preciado de las empresas que es la Información, la cual considera que toda la información de la empresa tiene que ser correctamente resguardada y administrada según la necesidad por personas idóneas y de confianza, este activo tiene que ser reconocido con tal importancia por todas las empresas al ver casos de robo de información, sustracción o alteración de la misma.

En el Terrapuerto Trujillo existen diversos sistemas de información siendo los principales el sistema de Recaudación (Sistema de cajas), Sistema de Parking Buses y sistema contable. Estos sistemas contienen información valiosa para la empresa ya que la información que es registrada en las mismas sirve para controlar y

registrar información de ingresos que hay a la empresa y además que sirve para toma de decisiones estratégicas.

Sin embargo, dicha información se ve expuesta a robo o alteración, o sin ningún respaldo de la misma, lo cual en anteriores gestiones se ha dado y por lo mismo ha generado desorden e inconsistencias para las diversas áreas, como tal evidencian los informes encontrados por dichos motivos.

En este caso particular, los sistemas se encuentran instalados en las diversas áreas según los requerimientos que se necesitan para las mismas, pero además se ha instalado sistemas básicos en áreas de empresas terciarias con el fin de tener una mejor operación de las actividades que se realizan en el Terrapuerto, lo cual es un peligro inminente ya que puede haber una sustracción de información por alguno de sus trabajadores y también por los propios trabajadores del Terrapuerto ya que no existe políticas ni mecanismos de seguridad para el correcto uso y limitación de esta información.

Es por ello, que en el presente proyecto de investigación plantea como solución, el modelo para la implementación de la norma ISO 27001:2014 en la Concesionaria Terrapuerto Trujillo con el fin de identificar y analizar el nivel en el que se encuentra la seguridad de la información en la empresa.

El problema a resolver es el siguiente: **¿En qué medida un modelo de procesos permite implementar la norma ISO 27001:2014 en la concesionaria Terrapuerto Trujillo S.A.?**

Para dar respuesta a esta pregunta se plantea la siguiente Hipótesis: **Un modelo de procesos construido con el framework Spark implementará en un 90 por ciento la norma ISO 27001:2014 en la empresa Concesionaria Terrapuerto Trujillo S.A.**

Siendo el Objetivo principal: **Medir el nivel de implementación de la norma ISO 27001 para la empresa Concesionaria Terrapuerto Trujillo S.A. mediante un modelo de procesos basado en el framework Spark**

Y cuyos objetivos específicos son los siguientes:

- Realizar una revisión sobre modelado de procesos

- Elaborar el modelo de procesos para la implementación de la norma ISO 27001 en la empresa Concesionaria Terrapuerto Trujillo S.A. utilizando el framework Spark
- Construir un prototipo del modelo de procesos para demostrar la implementación de la norma ISO 27001 en un 90% utilizando Bizagi.
- Realizar una prueba de aceptación del prototipo del modelo de proceso de implementación de la norma ISO 27001.
- Identificar en que porcentaje se llega a implementar la norma ISO 27001 en la empresa Concesionaria Terrapuerto Trujillo S.A.

Esta investigación es necesaria al evaluar el estado actual de la protección de los activos de la empresa, desde la información digital, los documentos y activos físicos como son computadoras y redes, hasta los conocimientos de los empleados y trabajadores que laboran en la empresa Concesionaria Terrapuerto Trujillo S.A.

Dicha investigación es viable gracias a las facilidades con la información que brinda la empresa Concesionaria Terrapuerto Trujillo S.A.

II. MARCO TEÓRICO

1.1. Antecedentes

(Seclén Arana, 2016) en su trabajo de investigación nos dice que Las principales limitaciones y problemas que vienen enfrentando las entidades del sector público en la implementación del SGSI se dividen en 8 categorías los cuales distribuyo en 3 niveles

I. Nivel Estratégico

1.1. Una Política Estratégica de Estado en Seguridad de la Información

II. Nivel Operativo: 04 pilares operacionales

2.1. Una gestión eficiente de la seguridad de información,

2.2. Apoyo institucional de la Alta Dirección

2.3. Una adecuada organización del SGSI

2.4. Aplicación efectiva de la normatividad en seguridad de información

III. Nivel Técnico: Compuesta de 03 partes

3.1. Desarrollo integral institucional de la NTP

3.2. Contar con un presupuesto nacional para la seguridad de la información

3.3. La especialización técnica de profesionales en SGSI como prioridad nacional

Así como también las estrategias y metodologías que vienen aplicando las entidades públicas que ya han completado la ejecución es iniciar con la identificación y ordenamiento de sus procesos a través de la ISO 9001 como soporte de gestión por procesos. Estas instituciones han confirmado que para completar las fases de implementación del SGSI, es muy importante tener claros los procesos de negocio de la institución, otro factor a tener en cuenta es el presupuestal y el último factor es de profesionalización de especialistas en seguridad de información en el Estado.

(Tola Franco, 2015) En su trabajo de investigación de implementación de un sistema de gestión de seguridad para una consultoría y auditoría aplicando la norma iso 27001, nos indica lo siguiente:

1. Lo primordial el establecimiento del alcance de una actividad ya que delimita el campo de acción y el uso de recursos.
2. Establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización

desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia

3. La adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que 117 se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos
4. Es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.
5. Implementar controles o salvaguardas, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización
6. La mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales

(Huamán Monzón, 2014) En su trabajo de investigación de diseño para procedimientos de auditoria para la verificación del cumplimiento de la norma ISO 27001 en instituciones públicas nos indica Se necesita recabar la información necesaria mediante la solicitud de los documentos oficiales, registrados y difundidos de la empresa, así como también, mediante entrevistas personales con la(s) personas(s) a cargo en las áreas relacionadas al objeto de auditoría.

1. **Determinar el alcance** que tendrá la Auditoría. Para ello se revisará la documentación de la empresa que se hayan compuesto al implementar los controles sugeridos por la NTPISO/ IEC 17799:2007.
2. **La definición del objetivo general** dependerá de varios factores. Entre los más importantes y más recurridos se encuentran: El mandato y el cometido de una de las entidades (Control Interno, Gerencia General o Contraloría General de la República) que sea específico para la auditoría a realizar y que pueda escapar del cumplimiento de cualquiera de las normas anteriormente mencionadas. Leyes y regulación interna pertinentes a la empresa auditada y que guardan relación con las normas auditadas

(los denominados cuestionarios de control interno) ya que estos factores podrían modificar (ampliar) el objetivo de la auditoría de cumplimiento.

3. **Procedimientos para establecer los criterios de la auditoría** dependiendo del documento de declaración de aplicabilidad de la empresa.
4. **Procedimiento para el levantamiento de evidencias**, teniendo acceso a esta información se podrá realizar luego la clasificación de los controles de acuerdo a la declaración de aplicabilidad.
5. **Procedimiento para la documentación de hallazgos,** el cual contempla mostrar los resultados de la recopilación de evidencias frente a los criterios de auditoria.
6. **Procedimiento para la documentación de conclusiones y recomendaciones.**

(David Aguirre, 2014) En su trabajo de investigación del diseño de un sistema de SGSI para la empresa SERPOST del Perú S.A. nos indica que existen factores externos que se necesitan para la implementación del sistema SGSI (Sistema indicado por la norma ISO 27001 para implementar) como son la intervención y el apoyo de la alta gerencia, fundamental para el levantamiento de la información, así mismo la difusión de las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, otro factor es la necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI.

1.2. Definiciones

- **Modelo**. – (School, 2014) (Blog "Retos para ser Directivo" 2014) Desde la década de los 60, el modelado ha evolucionado hasta convertirse en una herramienta indispensable para la representación de una empresa, procesos de las mismas o como guía de algo que se requiera.

  Se trata de un documento escrito que detalla los aspectos más significativos de una compañía. En él caben desde los más generales, como el diseño organizacional o el mapa de jerarquías, hasta las más puntuales, como el sistema informático empleado por los trabajadores, además de ser una representación de la realidad por medio de abstracciones. Los modelos enfocan ciertas partes importantes de un sistema (por lo menos, aquella

que le interesan a un tipo de modelo específico), restándole importancia a otras

El documento debe expresar con claridad los elementos que forman parte de la identidad corporativa y la filosofía de una compañía. Cuanto más preciso sea, el negocio quedará plasmado con mayor fidelidad.

Entre los usos más comunes del modelado está la organización de procesos que tienen que ver con el diseño organizacional, la planificación estratégica, el diseño de la arquitectura empresarial o la gestión de la calidad.

Sin embargo, el modelado no es una herramienta exclusiva de las etapas previas a la puesta en marcha de una compañía. También es muy común emplearla en fases posteriores, sobre todo en aquellas en las que se realizan procesos de negocio.

- **Proceso**. – (Jaén, 2015) Un proceso es un conjunto de actividades planificadas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado. Se estudia la forma en que el Servicio diseña, gestiona y mejora sus procesos (acciones) para apoyar su política y estrategia y para satisfacer plenamente a sus clientes y otros grupos de interés.

  (DefinicionMX, 2014) Un proceso es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico. Los procesos son mecanismos de comportamiento que diseñan los hombres para mejorar la productividad de algo, para establecer un orden o eliminar algún tipo de problema. El concepto puede emplearse en una amplia variedad de contextos, como por ejemplo en el ámbito jurídico, en el de la informática o en el de la empresa. Es importante en este sentido hacer hincapié que los procesos son ante todo procedimientos diseñados para servicio del hombre en alguna medida, como una forma determinada de accionar.

- **Modelo de implementación. –** (hernandez, 2013) El Modelo de Implementación es comprendido por un conjunto de componentes y subsistemas que constituyen la composición física de la implementación del sistema. Entre los componentes podemos encontrar datos, archivos, ejecutables, código fuente y los directorios. Fundamentalmente, se describe la relación que existe desde los paquetes y clases del modelo de diseño a subsistemas y componentes físicos.

  Un diagrama de implementación muestra:

  - Las dependencias entre las partes de código del sistema (diagramas de componentes).
  - La estructura del sistema en ejecución (diagrama de despliegue).

- **Seguridad. –** (Huamán Monzón, 2014) A continuación, se presentará los conceptos relacionados a seguridad como son: activo, seguridad de la información, amenaza y vulnerabilidad.

  - **Activo**. - Elemento impreso o digital que contenga información, así como todo sistema conformado por software, hardware y su documentación pertinente que cree, maneje y procese información para una organización; también se puede incluir a la infraestructura tecnológica donde se desenvuelven dichos sistemas. Se considera activo esté o no registrado contablemente
  - **Seguridad de la Información.** - La ISO/IEC 27000:2009 define la Seguridad de Información como la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas. (ISO 2009). También amplia el concepto añadiendo que es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

- **Amenaza**. - Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización
- **Vulnerabilidad**. - La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas

- **Seguridad de la información.** – (David Aguirre, 2014) Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran [NTP ISO/IEC 17799].
- **ISO 27001.-** (Huamán Monzón, 2014) Se refiere a las normas internacionales del International Organization for Standardization (ISO). Pertenecen a la familia de normas ISO 27001. El objetivo de la ISO 27001 es que la empresa sea capaz de priorizar y seleccionar controles en base a sus posibilidades y a sus necesidades/riesgos de seguridad. Es que los riesgos se analicen y se gestionen, que la seguridad se planifique, se implemente y, sobre todo, se revise y se corrija y mejore. La ISO 27001 se ha modificado para adaptarse a la nueva estructura de alto nivel utilizado en todas las normas de Sistemas de Gestión, lo que simplifica su integración con otros sistemas de gestión.

  (López, 2014) La NTP especifica los requisitos para el establecimiento, implantación, la puesta en funcionamiento, control, revisión, mantenimiento y mejoramiento de un Sistema de Gestión de Seguridad de la Información de una organización

  Adopta la aplicación de un sistema de procesos dentro de una organización, junto con la identificación y la interacción de estos procesos, así como su gestión, adoptando el modelo “Plan-Do-Check-Act”, que se aplica para estructurar todos los procesos del Sistema de Gestión de Seguridad de la Información. Este proceso requiere:

Imagen 1 Modelo Plan-Do-Check-Act

Fuente: (López, 2014)

- Establecer el SGSI: Crear política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en correspondencia con las políticas y objetivos generales de la organización.
- Implementar y operar el SGSI: Implementar y manejar la política, controles y procedimientos SGSI.
- Monitorear y revisar el SGSI: Evaluar y, donde sea aplicable, calcular el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para revisión
- Mantener y mejorar SGSI: Tomar acciones correctivas y preventivas, establecidas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

- **BPMN.** – (David Aguirre, 2014) Notación para el modelado de procesos por sus siglas en inglés, es “un estándar que provee a una organización la capacidad de entender y comunicar entre sí los distintos procedimientos propios del negocio en una notación gráfica. De igual forma, permite

conocer cuál es el rendimiento actual de la organización al trabajar con otras empresas".

El objetivo principal de BPMN es el proporcionar un estándar para el modelado de procesos de la organización. Fue desarrollada por el BPMI (Business Process Management Initiative) que es parte de la OMG (Object Management Organization) desde que las 2 organizaciones se fusionaron en el 2005. Actualmente se encuentra en la versión 2.0 la cual fue emitida en marzo del 2011.

Como resultado se tienen los procesos de la organización en un BPD (Business Process Diagram) utilizando una técnica de diagrama de flujo muy similar al diagrama de actividades del estándar UML reduciendo así la brecha que existe entre el modelado de procesos y la implementación de los mismos.

Justificación: Al ser un estándar orientado al modelamiento de procesos, facilita el entendimiento de los procesos del negocio debido a su practicidad para ver los procesos en distintos niveles, diferenciando macro procesos de micro procesos, reduciendo la carga visual y facilitando la lectura del modelo.

El modelamiento de procesos dentro de un sistema de gestión de seguridad de información es vital, debido a que se deben conocer los procesos que están dentro de su alcance para asegurar el correcto levantamiento de activos de información y asignar los controles necesarios para asegurar la disponibilidad, integridad y confidencialidad de los mismos.

- **Framework Spark**. – (Bizagi Spark, 2015) Spark es un moderno modelo de gestión de proyectos que consiste de tres etapas, diseñadas para entregar rápidos resultados y alcanzar el mejoramiento de procesos a largo plazo. Lo cual permite ayudar a iniciar poco a poco, pensando en grande y escalar rápido, Spark está basado en métodos de gestión de proyectos ágiles que eliminan las implementaciones monolíticas y rígidas del pasado.

El Marco de Trabajo Bizagi Spark se basa en tres pasos claves (Impulsar, fortalecer y Expandir). Cada uno se construye como el primer proceso, por la cual cualquiera que sea su estado de madurez en BPM, el proceso será el mismo.

1. Impulsar: Bizagi QuickStart

(QuickStart, 2015)El programa QuickStart es un paquete de trabajo diseñado para entregar a tiempo rentabilidad. Utilizando técnicas probadas, modernas y ágiles, este es el primer paso de nuestro marco general de implementación de Spark, lo que lo pone en el camino no sólo para ganancias a corto plazo, sino también para el éxito a largo plazo de BPM.

Paquete de inicio rápido	Implementación de 7 semanas	Criterios de inicio rápido
✓ Plantilla del proyecto: Actividades, Hitos, Entregables, ... ✓ Matriz de evaluación de procesos ✓ Metodología ágil - Modelo de Proceso de Negocio - Análisis y Diseño: definición de alto nivel - Construcción de procesos ✓ Soporte de gestión de cambios ✓ Apoyo directo	Plan de proyecto: ✓ **3 días:** Selección de proceso ✓ **5 días:** especificación de "alto nivel" ✓ **20 días:** Compilación ágil ✓ **5 días:** Prueba de aceptación por parte del usuario ✓ **2 días:** Soporte en directo y absorción del usuario Recursos: **Cliente:** Proceso Propietario y especialista en integración **Bizagi:** Analista de Negocios y Analista Técnico Revisión bimensual de los patrocinadores	✓ Proceso seleccionado de la evaluación ✓ Involucrar negocios y TI ✓ Integraciones realizadas por el cliente a tiempo y compatibles con el estándar de integración de Bizagi ✓ No hay cambios relevantes después de la fase de Análisis y Diseño ✓ Diseño de Interfaz de Usuario Bizagi 'Estándar'

Tabla 1 Tabla Proceso Bizagi QuickStart

Fuente: (QuickStart, 2015)

QuickStart aplica métodos probados durante el proceso ágil de scrum para solicitar retroalimentación de los principales interesados, tanto de negocios como de TI, para asegurar una alineación precisa entre todos los requisitos.

Promover el trabajo en equipo de las mejores prácticas y aumentar el éxito del proyecto mediante la implementación de sesiones estructuradas de comunicación cara a cara y de retroalimentación.

Beneficios de QuickStart:

Aumento de los niveles de colaboración empresarial y de TI

Utilizando la Herramienta de Evaluación de Procesos de Bizagi, se ayuda a seleccionar el primer proceso correcto, luego usar métodos ágiles para definir, construir y validar la liberación a las partes interesadas del negocio, incluyendo demostraciones regulares de la solución de trabajo. A lo largo del proceso, se utiliza métodos obtenidos durante la metodología ágil de scrum para gestionar las principales expectativas empresariales y de TI.

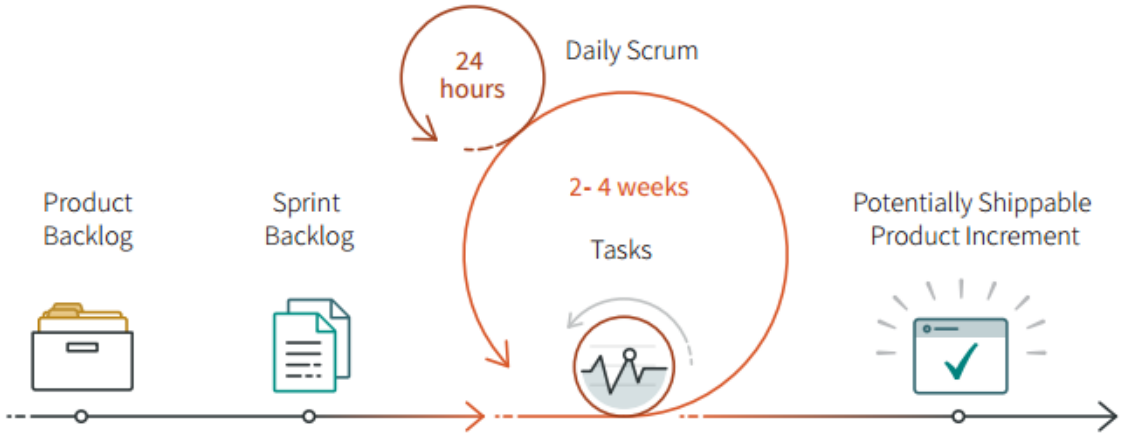


Imagen 2 Procesos de QuickStart

Fuente: (QuickStart, 2015)

Adopción mejorada del usuario final

Los beneficios son de dos tipos: Se alivia la carga de su personal interno para obtener resultados más rápidos; Facilita el conocimiento adquirido, acortando así masivamente la curva de aprendizaje.

Herramienta de Evaluación de Procesos Bizagi

La herramienta de evaluación de procesos de Bizagi es un marco de medición analítica que permite a ambas partes decidir qué proceso es el

mejor candidato de QuickStart. El proceso seleccionado alcanzará una puntuación objetivo para permitir la entrega (en producción)

Dentro de 7 semanas.

Cada proceso potencial se evalúa en:

- Impacto empresarial - ¿cuánto valor tendrá?
- Madurez del proceso: ¿qué nivel de comprensión del proceso existe?
- Complejidad - integración, flujos de procesos y reglas de negocio

2. Fortalecer: OnTarget

(OnTarget, 2015) La Metodología OnTarget define la fase de Impulsar de Framework Spark y ayuda a establecer las mejores prácticas ya que replica su éxito QuickStart en nuevas áreas de su negocio.

El objetivo del enfoque Impulsar es integrar las disciplinas clave dentro de su negocio para implementar gradualmente Bizagi en toda su empresa y potencialmente optimizar cientos de procesos.

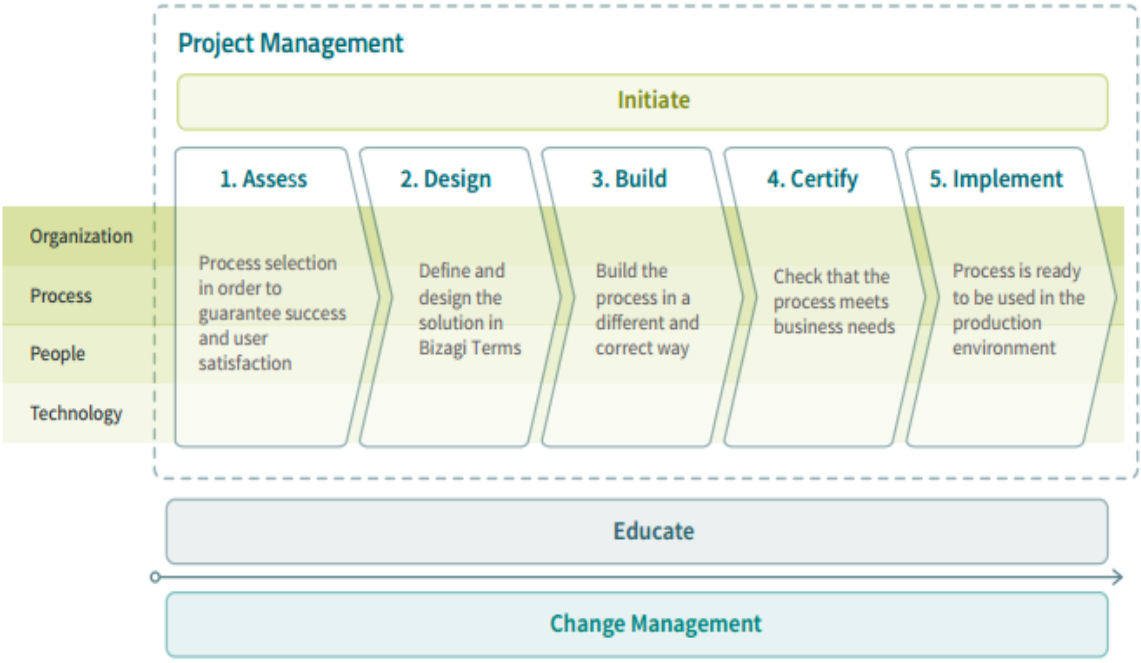


Imagen 3 Etapas de la Fase Fortalecer del framework Spark

Fuente: (OnTarget, 2015)

OnTarget comienza con el desarrollo de un plan de transferencia de conocimiento para "cerrar la brecha" combinando la formación avanzada y el intercambio pragmático de habilidades. Esto es para ayudarle a entregar el segundo proceso en usando el rigor del framework.

Completar con éxito esta fase de empoderamiento proporcionará a su empresa una base sólida para posteriormente formar un Hub de Fábrica de Procesos BPMS de Bizagi y automatizar sucesivamente los procesos de una manera consistente utilizando la funcionalidad completa de Bizagi BPMS.

Descripción de los pasos de la metodología OnTarget

- ✓ Evaluar

  Si ya se ha entregado QuickStart (etapa Impulsar del framework Spark), un segundo proceso correcto para automatizar ya puede ser aparente. Sin embargo, si se omitió QuickStart, puede aplicar la herramienta de evaluación de procesos de Bizagi para ayudarle a seleccionar posibles candidatos de proceso, hasta un máximo de diez. Se consideran tres dimensiones del análisis de Selección de Procesos: Impacto Empresarial, Vencimiento del Proceso y Complejidad

- ✓ Diseño

  Funcional

  Incorpora las mejores prácticas para definir y diseñar los detalles de la solución en términos de Bizagi basados en los requisitos del negocio. Esencialmente se trata de cerrar la brecha entre los requisitos funcionales y la funcionalidad específicas de la aplicación Bizagi. Es muy importante que los requerimientos de los usuarios sean efectivamente capturados y verdaderamente representados.

  Técnico

  Transfiera los conocimientos de mejores prácticas a su equipo de BPM creando el Documento de Diseño Técnico de Bizagi. Esto define en que

se detalle la solución desde un punto de vista técnico basado en el diseño funcional definido en la fase anterior.

- ✓ Construir

  Al crear una solución de trabajo tangible en Bizagi, se puede potenciar modelar y desarrollar el proceso seleccionado en Bizagi e integrar todos los componentes que forman parte de la aplicación.

  Durante la fase de construcción se modela el proceso seleccionado, se crea la estructura de datos, se desarrollan y validan las plantillas y se configuran los comportamientos de los campos junto con las reglas y políticas comerciales de soporte.

- ✓ Certificar

  Esta etapa ayudará a certificar que su configuración de proceso BPMS de Bizagi cumple con los requisitos de negocio especificados en la fase de diseño y está lista para su implementación en el entorno de producción.

- ✓ Implementar

  La solución Bizagi certificada se puede llevar al entorno de producción. La transferencia de conocimiento se proporciona desarrollando un plan estructurado, utilizando la plantilla de mejores prácticas de Bizagi. El plan es una tarea crítica para asegurar que se alcancen los objetivos del proyecto. Al final de esta fase, la aplicación Bizagi BPMS completamente configurada ejecutará el proceso seleccionado en un entorno de producción.

3. Expandir

(Bizagi Spark, 2015) *Proporcionar BPM a nivel global en toda la empresa*

El paso final del marco Spark se basa en sus éxitos anteriores y proporciona el conocimiento y las herramientas que necesita para

establecer un servicio compartido BPM global utilizando el modelo COE de Bizagi.

- Mapear estratégicamente Bizagi a la arquitectura de su empresa
- Alinee su hoja de ruta de BPM con sus controladores estratégicos corporativos
- Definir las mejores prácticas de BPM para su organización
- Medir y mejorar su desempeño de BPM

- **Bizagi. –** (Bizagi, 2013) Herramienta que permite la colaboración entre las unidades de negocio y TI, por medio de la rápida construcción y experimentación de aplicaciones de proceso, aumentando la productividad operacional, manteniendo el control de TI.
  - Aplicaciones de procesos modelados
  - Facilita la experimentación por medio de herramientas intuitivas
  - Reutilización de todos los objetos de negocio
- **SGSI. –** (López, 2014) Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

  La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Fundamentos:

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

- **ISO.-** (Peña, 2015) Las normas ISO son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos. La alta competencia internacional acentuada por los procesos globalizadores de la economía y el mercado y el poder e importancia que ha ido tomando la figura y la opinión de los consumidores, ha propiciado que dichas normas, pese a su carácter voluntario, hayan ido ganando un gran reconocimiento y aceptación internacional.

  Las normas ISO son establecidas por el Organismo Internacional de Estandarización (ISO), y se componen de estándares y guías relacionados con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización.

- **ISO 27001 Sistema de Gestión de Seguridad de la Información.-** (López, 2014) SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

  En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

  La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (SGSI Blog especializado, 2014)Contiene una serie de cláusulas que conforman un Sistema de Gestión de Seguridad de la Información. De entre ellas hoy hablaremos de la quinta, Liderazgo.

  Se trata de una sección formada por:

  - Liderazgo y compromiso
  - Política
  - Roles, responsabilidades y autoridades en la organización

  En este artículo abordaremos la primera parte: Liderazgo y compromiso.

  (IsoTools, 2017) La determinación del alcance del Sistema de Seguridad de la Información, ha sido una de las principales novedades incluidas en la revisión de norma ISO 27001.

  Concretamente al definir el alcance del Sistema de Seguridad de la Información, se busca como principal objetivo clarificar cual es la información a la que se quiere dar protección, con independencia de dónde se halle, cómo se almacene o quién pueda acceder a la misma.

Veamos a continuación qué novedades se introducen en relación al alcance del Sistema de Seguridad de la Información tras la actualización última de 2013 de la norma ISO 27001.

Requisitos de la norma ISO 27001, para determinar el alcance del Sistema de Seguridad de la Información

A la hora de definir el alcance del Sistema de Seguridad de la Información bajo los fundamentos de ISO 27001 debemos tener en cuenta:

- Análisis de los aspectos tanto internos como externos de cara a lograr un entendimiento de la organización.
- Identificar las partes interesadas

Analizar las interrelaciones entre lo que ocurre dentro del Sistema de Gestión de Seguridad de la Información y el mundo externo, es lo que denominamos análisis de las interfaces y dependencias.

Además de lo anterior, es también recomendable incluir en el documento que recoge el alcance del Sistema de Seguridad de la Información, información respecto a la ubicación y las unidades organizativas que integran la organización,

Vamos a centrar la atención en el tercer de los puntos a considerar al determinar el alcance del Sistema de Seguridad de la Información, es decir cómo tratar las interfaces y dependencias entre las actividades realizadas por la organización y el mundo del exterior.

III. MATERIAL Y MÉTODOS

3.1. Material

3.1.1 Población

Todos los criterios que la norma ISO 27001 sugieren que están plasmados en el modelo de implementación.

3.1.2 Muestra

Como para obtener el modelo de implementación se requieren todas las practicas o criterios de la norma 27001, la muestra es igual a la población (7 criterios). Como la muestra es menos de 30 no se aplica fórmula de cálculo de muestra.

3.1.3 Unidad de Análisis

La unidad de análisis es el modelo de implementación para la norma ISO 27001 en la empresa Concesionaria Terrapuerto Trujillo S.A.

3.2. Método

3.2.1 Tipo de Investigación

El tipo de investigación será de forma Aplicada

3.2.2 Diseño de Investigación

El diseño que se usará será el cuasi-experimental

3.2.3 Variables de estudio y operacionalización

V. INDEPENDIENTE (VI), X = Modelo de procesos construido con el framework spark

DIMENSIONES	INDICADORES
X_1=Modelo de procesos	X_{11}: Nro de Etapas o fases X_{12}: Nro de entregables o resultados
X_2=Proceso	X_{21}: Nro de diagramas procesos X_{22}: Nro de descripciones de procesos X_{23}: Nro de indicadores por proceso

Tabla 2 Variables Independientes

V. DEPENDIENTE (VD), Y = implementación de la norma iso 27001

DIMENSIONES	INDICADORES
Y_1=Procesos en cada área o criterio	Y_{11}:% de proceso implementados
Y_2=Criterios o áreas	Y_{21}:% de criterios o áreas implementadas

Tabla 3 Variables Dependientes

3.2.4 Instrumentos de recolección de Datos

Revisión documental de los diferentes modelos para implementación de una norma.

Se utilizará el medio de entrevistas para determinar el nivel de cumplimiento e identificar el estado actual de la seguridad en la empresa.

3.2.5 Procedimientos y análisis de datos

Revisión documental de los diferentes modelos de implementación de la norma ISO 27001.

Se utilizará un check-list para caracterizar el modelo y para describir los cumplimientos que indica la norma ISO 27001.

Se utilizará encuestas para determinar el nivel de aceptación del modelo de implementación.

3.2.6 Técnicas de análisis de datos

Los datos recolectados serán procesados de forma estadística descriptiva e inferencial, utilizando una hoja de cálculo que será elaborado por los investigadores.

3.2.7 Modelos estadísticos de análisis de datos

Para el análisis de los datos desde la perspectiva estadística utilizará el modelo estadístico de T-student

IV. RESULTADOS

Para el siguiente informe se realizó una corta entrevista con la gerencia y jefes de áreas (total de 7 personas) con el fin de identificar el conocimiento y disposición que tienen los trabajadores de la empresa con referente a la norma ISO 27001 que se basa en la seguridad de la información de una empresa, además se realizó un check-list con el fin de cumplir con la primera etapa de la framework Spark, donde se evaluará el estado en que se encuentra la empresa con respecto a las políticas, criterios y normas que indica se deben cumplir la norma ISO 27001 en conjunto con los criterios que indica la ISO 27002 que va asociada para el cumplimiento de la primera.

Para representar los resultados se presenta el siguiente gráfico.

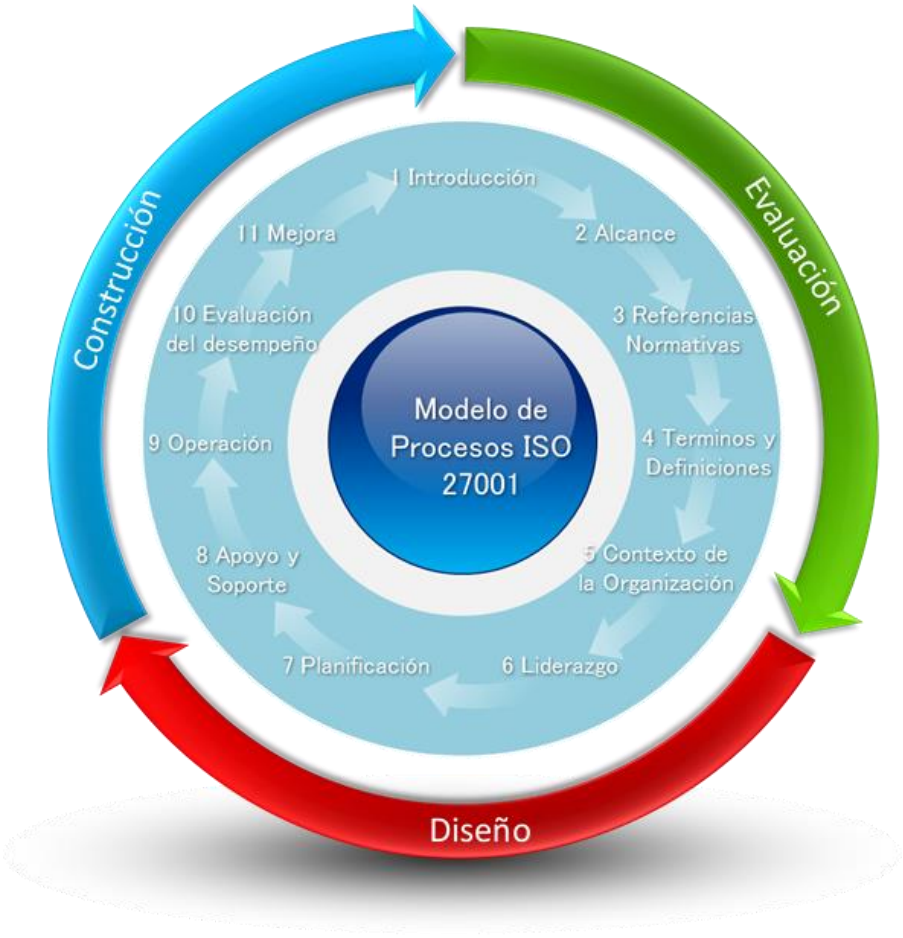


Imagen 4 Representación de orden de resultados

Resultados Entrevista

1. ¿Qué conocimientos tiene sobre seguridad de la información?

   Conclusiones:

   Lo relacionan con la seguridad que se brindan en los sistemas de información.

2. ¿Cómo considera usted la seguridad de la información en la empresa y por qué?

   Conclusiones:

   Lo consideran en un nivel intermedio, ya que relacionado por el concepto que tienen de la seguridad de la información, que es brindada por los sistemas de información, cuenta con logueos por cada usuario en los sistemas que se manejan en la empresa.

3. ¿Cómo utiliza la información proporcionada en su área?

   Conclusiones:

   Cada jefe de área considera que la información proporcionada en su área es fundamental e importante para la empresa.

4. ¿Cuenta con políticas internas del área para mejorar la seguridad de la información?

   Conclusiones:

   Solo 1 área cuenta con políticas internas de su área, que tienen asignaciones especificas por cada trabajado, sin embargo, no cuenta con algún documento que oficialice dichas políticas internas.

5. ¿Qué piensa de la seguridad en el manejo de la información proporcionada por los sistemas que utiliza para su área?

   Conclusiones:

   Intermedio, ya que algunos sistemas cuentan con información general para todos los usuarios creados.

6. ¿Considera usted que es necesario implementar la normativa ISO 27001 en la empresa Concesionaria Terrapuerto Trujillo? ¿Por qué?

   Conclusiones:

Si, por que mejorará la seguridad y restricciones para la información que se maneja en la empresa.

7. ¿Cree que la implementación la normativa ISO 27001 dificultará los trabajos realizados por el área?

   Conclusiones:

   Sí, pero se tiene claro que es un beneficio a largo plazo a la empresa.

8. ¿Cubre las necesidades de su área con respecto a la seguridad de la información?

   Conclusiones:

   Sí, se plantearon bien los requerimientos para que sean tomados en cuenta para la implementación.

Resultados de Check List:

(Kumar, 2014) En la siguiente tabla se resume los criterios indicados en la norma ISO 27001 basandos en la norma ISO 27002

Chequeo de Cumplimiento

Un formato condicional ha sido proveído bajo el campo "Estado (%)" y se menciona abajo:

1 a 25		No cumple con los criterios necesarios
26 a 75		Cumplimiento en cierta parte de los criterios necesarios
76 a 100		Cumple con los criterios necesarios

En el campo "Observaciones" se comentó la evidencia que se identificó o los comentarios sobre la implementación

En el campo "Estado (%)" se escribe el nivel de cumplimiento sobre la escala mencionada más arriba

Si alguno de los controles no es aplicable, se colocará "NA" o algo que denote que ese control en particular no es aplicable para la organización.

En el Anexo 01 se detalla el check-list completo y detallado que se usó para los resultados mostrados en las siguientes tablas en la empresa Concesionaria Terrapuerto Trujillo

Dominio	Estado (%)
Políticas de Seguridad	20%
Organización de la Seguridad de Información	50%
Administración de Activos	48%
Seguridad de Recursos Humanos	49%
Seguridad Física y Ambiental	54%
Gestión de Comunicaciones y Operaciones	42%
Control de Acceso	37%
Desarrollo y Mantenimiento de Sistemas de Información	34%
Gestión de Incidentes de Seguridad de Información	54%
Administración de la Continuidad de las Actividades de la Empresa	33%
Cumplimiento	44%

Tabla 4 Resumen Check List

Dominio	Objetivos	% Grado de cumplimiento
	Aspectos Generales	40
	Sanciones Previstas por incumplimiento	10
	Revisión de la Política de Seguridad	10
	Infraestructura de la Seguridad de la Información	29
	Seguridad Frente al Acceso por Parte de Terceros	50
	Tercerización	70
	Inventario de Activos	73
	Clasificación de Información	40
	Rotulado de la Información	30
	Previo al Empleo	57
	Durante al Empleo	23
	Terminación o Cambio de empleo	67
	Perímetro de Seguridad Física	70

	Controles Físicos de Entrada	30
	Protección de Oficinas, Recintos e Instalaciones	80
	Trabajando en Areas Seguras	40
	Aislamiento de las Áreas de Recepción y Distribución	40
	Ubicación y Protección del Equipamiento y Copias de Seguridad	63
	Suministros de Energía	80
	Seguridad del Cableado	55
	Mantenimiento de Equipos	63
	Seguridad de los Equipos Fuera de las Instalaciones.	45
	Disposiciones de Seguridad de Reutilización de Equipos	50
	Política de Escritorio Limpio y Pantalla Limpia	0
	Retiro de los Bienes	80
	Procedimientos y Responsabilidades Operativas	36
	Planeamiento y Aceptación de Sistemas	65
	Manejo de Entrega de Servicios Tercerizados	22
	Protección contra código malicioso	50
	Copias de Respaldo	53
	Administración de la Red	50
	Manejo de Medios	20
	Intercambio de Información	38
	Requerimientos para el Control de Acceso	50
	Administración de Accesos de Usuarios	17
	Responsabilidades de Usuarios	40
	Control de Acceso a la Red	36
	Controles de Acceso a Sistemas Operativos	31
	Control de Acceso a las Aplicaciones y a la Información	65
	Monitoreo del Acceso y Uso de los Sistemas	30
	Computación Móvil y Trabajo Remoto	30
	Requerimientos de Seguridad de los Sistemas de Información	23
	Seguridad en los Sistemas de Aplicación	31
	Controles Criptográficos	42
	Seguridad de los Archivos de Sistemas	43
	Seguridad de los Procesos de Desarrollo y Soporte	30
	Reportando Eventos de Seguridad y Vulnerabilidades	17

	Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras	38
Administración de la Continuidad de las Actividades de la Empresa	Aspectos de Seguridad en la Gestión de la Continuidad del Negocio	33
	Cumplimiento con Requerimientos Legales	45
	Revisiones de la Política de Seguridad y la Compatibilidad Técnica	73
	Consideraciones de Auditoría de Sistemas	30
	Sanciones Previstas por Incumplimiento	30

Tabla 5 Resultado Check List controles

Modelo de implementación de Norma ISO 27001

NTP 27001 en la Empresa Concesionaria Terrapuerto Trujillo S.A.

Control de cambios

Tabla 6 Tabla Control de Cambios o versiones

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1.0.0			Equipo del proyecto	Creación del documento
2.0.0			Equipo del proyecto	Ajustes al documento
2.0.1			Equipo del proyecto	Versión aprobada

Términos y condiciones de uso

"Se especifica y detalla los Términos y Condiciones para los que se tendrá uso el documento de Modelo de Implementación de la Norma ISO 27001"

El uso de esta "Política de Seguridad de la Información para la Concesionaria Terrapuerto Trujillo S.A. se rige por los términos y condiciones que a continuación se mencionan. Quien acceda a este documento conoce, entiende y acepta los términos relativos a su utilización y que a continuación se detallan:

La presente "Política de Seguridad de la Información" fue aprobada por la Gerencia y Directores de la empresa Concesionaria Terrapuerto Trujillo S.A., en virtud de las facultades conferidas por la Decisión Administrativa Nº XXXX y por la Resolución XXXXXX, con el objeto de facilitar a las áreas y personal correspondiente de la empresa, la redacción o bien adecuación de la Política de Seguridad de la Información.

Queda expresamente prohibido su uso para fines comerciales.

Las personas autorizadas para usar la "Política Modelo" la pueden copiar, modificar y reproducir únicamente para aquellos fines a los cuales está destinada.

La "Política de Seguridad de la información" de ninguna manera sustituye o modifica la normativa vigente aplicable a cada empresa.

1. Introducción

1.1. General

"Texto cuyo contenido se hace para una presentación preliminar del informe, en el cual se explica por qué, para qué y para quién ha sido realizado, además se explica un poco de trata el tema a exponer en el informe, este no debe contener muchos detalles porque se repetiría en el desarrollo real del informe, debe abarcar desde la toma de decisión para realizar el documento hasta su culminación"

En inicios del 2016 se declara el uso obligatorio de la NTP / ISO IEC 27001 para todas las entidades Integrantes del Sistema Nacional de Informática, la cual se denota la importancia del activo más preciado de las empresas que es la Información, la cual considera que toda la información de la empresa tiene que ser correctamente resguardada y administrada según la necesidad, por personas idóneas y de confianza, este activo tiene que ser reconocido con tal importancia por todas las empresas al ver casos de robo de información, sustracción o alteración de la misma.

En diciembre del 2016, la gerencia convocó a especialistas y encargados en las áreas de sistemas de las empresas asociadas al grupo empresarial que pertenece la empresa Concesionaria Terrapuerto Trujillo S.A., con el fin de conocer sus opiniones respecto a una estrategia de seguridad informática para que se implemente y se cumpla con la norma indicada a inicio de año. De estas reuniones surgió la necesidad de que la empresa implemente la norma basándose de un modelo y siguiendo un framework para cumplir con todos los criterios de la norma de Seguridad de la Información.

En consecuencia, se conformó un grupo de trabajo con el objeto de implementar la norma técnica peruana 27001 correspondiente a la Seguridad de la Información en la empresa y que este trabajo sirviera de punto de partida para la elaboración de las políticas correspondientes en cada empresa del grupo. Dicho grupo de trabajo decidió basar el modelo en la norma ISO 27001 e ISO 27002, como un marco de referencia para la seguridad de la información en una entidad.

El presente modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

2. Alcance

"Especifica los requisitos mínimos y máximos para el establecimiento, implementación, mantenimiento y mejora continua del sistema de seguridad de la información dentro del contexto de la organización."

Este modelo será de aplicación en la empresa Concesionaria Terrapuerto Trujillo S.A. con el fin de una implementación de la norma ISO 27001 la cual servirá para sus revisiones periódicas que se efectuarán con carácter semestral.

3. Referencias Normativas

"Se indica los documentos que serán usados en parte o en su totalidad para la implementación de la norma ISO 27001 en la empresa."

- ISO 27001
- ISO 27002
- Evaluación Norma ISO 27001
- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM

4. Términos y Definiciones

"Se debe indicar definiciones o significados de términos que sean usados en el documento para entendimiento general"

A los efectos de este documento se aplican las siguientes definiciones:

Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: Se garantiza que la información sea accesible sólo a

aquellas personas autorizadas a tener acceso a la misma.

- **Integridad**: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad**: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación**: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio**: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad**: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información**: Referido a que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

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

- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información**: Se refiere al hardware y software operados en la empresa o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la empresa, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la empresa.

Administración de Riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas de la empresa, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Responsable de Seguridad Informática

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la empresa que así lo requieran.

Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

5. Contexto de la Organización

"Se detalla el contexto que existe en la organización con el fin de tener un entendimiento de la empresa." (Morales, 2015)

5.1. Conocimiento de la organización y su contexto

Contexto Interno

"Se deberá determinar los asuntos internos y externos que sean relevantes para su propósito y que afectan su capacidad para lograr el o los resultados de la empresa."

5.1.1. Productos y Servicios

"Acá detallamos los productos y servicios que ofrecemos a nuestros clientes"

Concesionaria Terrapuerto Trujillo es una organización que presta sus servicios a empresas de transporte provincial, con el fin de buscar una formalidad de todas estas empresas de transporte y además brindar seguridad y comodidad a las personas que desean viajar al interior del país.

Existen varios procesos que se realizan para tener un total control y registro de actividades que las empresas de transporte realizan en la Concesionaria Terrapuerto de Trujillo.

A los pasajeros se les brinda servicios de Cable, Wifi, Seguridad, Cafeterías, Servicios Higiénicos, Video Vigilancia, Tiendas y Cargadores Públicos

5.1.1.1. Importancia Relativa

"La importancia relativa se refiere a la importancia que tienen los productos y servicio claves para las finanzas de nuestra organización"

Los mayores ingresos para la empresa son de ochenta por ciento de los ingresos por servicio prestados a las empresas de transporte y comerciales, mientras que el 20 por ciento, es producido por los pasajeros.

5.1.1.2. Logística

"Se refiere a la forma que funciona la cadena logística para la entrega de productos y/o servicios, es recomendable especificar el tiempo."

Promedio de entrega del servicio desde que el momento que cliente ingresa a las instalaciones del Terrapuerto.

5.1.1.3. Clima Organizacional

"Al menos debemos cubrir los 3 puntos siguientes, además de agregar cualquier otro punto que consideremos destacar del clima organizacional de nuestra empresa."

Misión

"Se indica la misión que tiene la empresa"

Brindar servicio de atención, ingeniería, mantenimiento y administración de operaciones, con excelencia, oportunidad y responsabilidad social; mediante estándares de calidad seguridad y salud ocupacional, y preservación del medioambiente para contribuir al desarrollo.

Visión

"Se indica la visión que tiene la empresa en unos años"

Ser reconocida como una empresa de servicios líder en el mercado nacional e internacional, con excelencia en su modelo de gestión y procesos de innovación, para mejorar la calidad de vida a sus trabajadores, generar bienestar social, y contribuir al desarrollo sostenible.

Valores

"Se detalla los valores que tiene la empresa en unos años"

Integridad, Respeto, Lealtad, Transparencia y Solidaridad.

5.1.2. Perfil de la fuerza de trabajo

5.1.2.1. Cantidad

"Agregamos y explicamos las estadísticas de nuestros colaboradores, cantidad de hombres, mujeres, contratados directamente y subcontratados."

En la organización contamos con 48 trabajadores los cuales 35 son hombres y 14 mujeres.

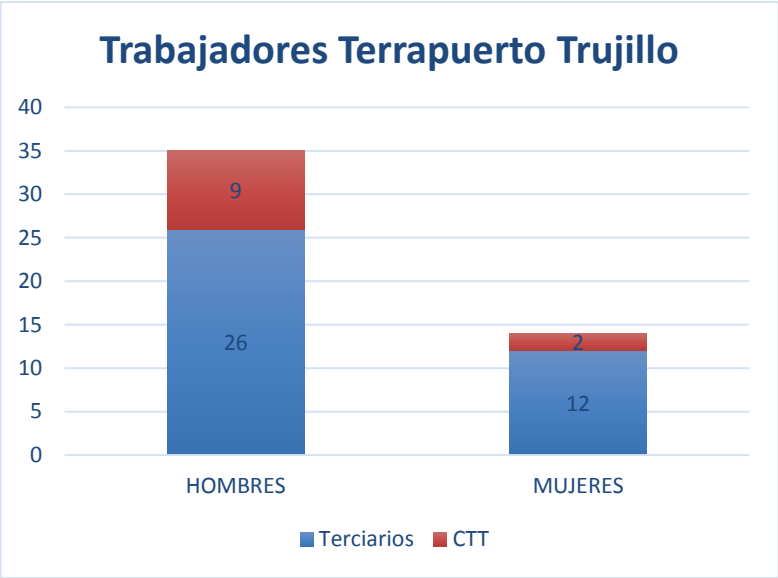


Imagen 5 Grafico Trabajadores

5.1.2.2. Grado Académico

Siempre apoyados en datos estadísticos provistos por RRHH, agregamos con el nivel de detalle que se considere pertinente, el grado académico de los trabajadores.

En la empresa contamos con 21 trabajadores con estudios superiores, 9 con estudios inconclusos o en curso y 18 sin estudios superiores.

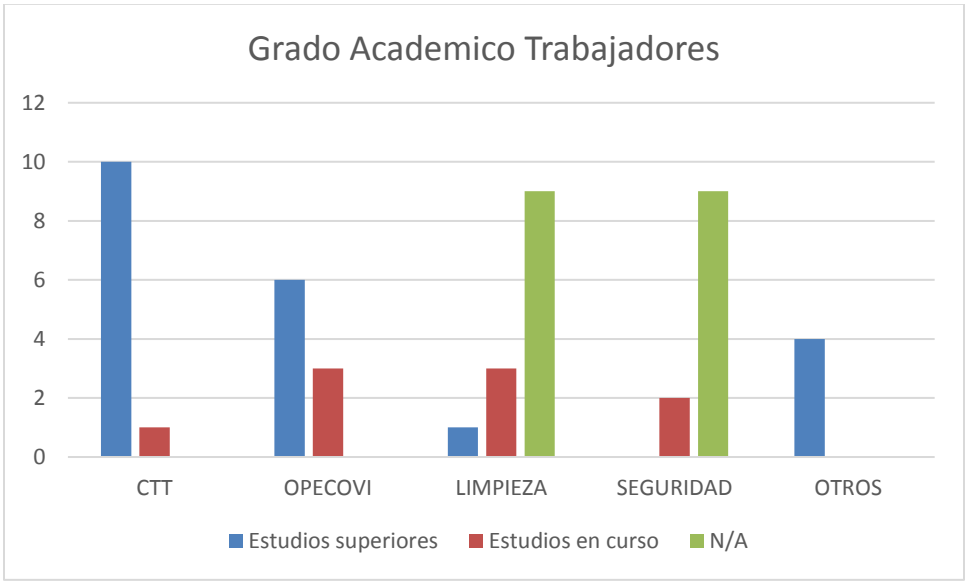


Imagen 6 Grafico grado académico Trabajadores

5.1.2.3. Nivel socioeconómico

Usando de base, las tablas de ingreso nacionales del país donde opere nuestra organización, ubicaremos en que grupos se encuentran los colaboradores

Nuestros trabajadores pertenecen en su mayoría a la primera clase con respecto a ingresos promedio del mercado laboral en el Perú.

850 - 1000	53%
1000 - 1500	9%
1500 - 2000	15%
2000 - 3000	21%
3000 - 5000	0%
5000 - 10000	0%
10000 - 20000	3%

Tabla 7 Nivel socioeconómico trabajadores

5.1.3. La organización

En esta parte, especificamos todo lo referente a la estructura organizacional de la empresa.

5.1.3.1. Esquema de la organización

(Insertamos el organigrama de la empresa)

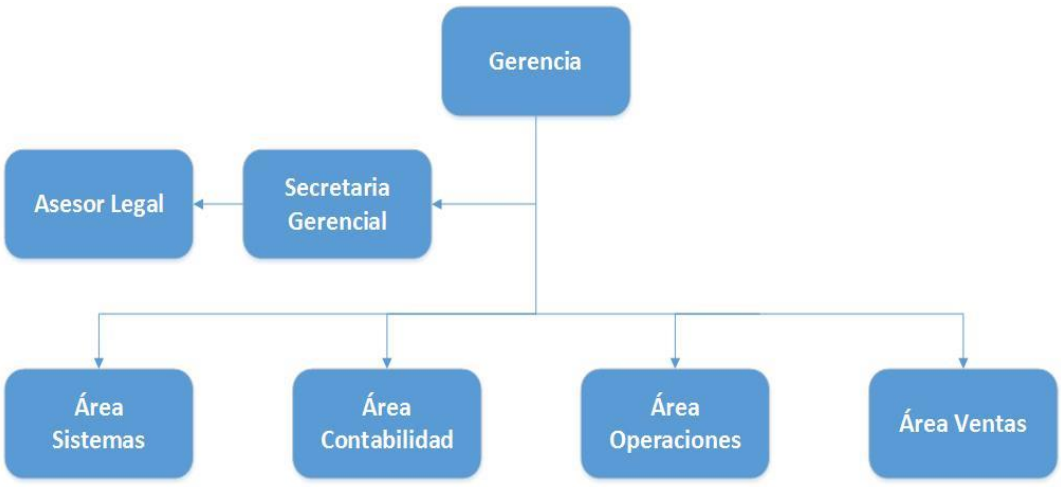


Imagen 7 Organigrama

5.1.3.2. Requisitos especiales de Calidad, Ambiente, Salud y/o Seguridad de la información

Se explica los requisitos especiales según sea nuestro producto y servicio.

La empresa Concesionaria Terrapuerto Trujillo es una empresa que brinda servicios de embarque y desembarque por lo que sus principales requisitos son la atención al público y a los buses las 24 horas del día, los 365 días del año.

5.1.3.3. Infraestructura

Detallamos nuestra infraestructura física y Tecnológica

La empresa cuenta con una infraestructura física valorizada en aproximadamente 40 millones de soles y con equipos tecnológicos valorizados en más de 5 millones de soles lo cual hace que la empresa tenga la disponibilidad de sus servicios al público las 24 horas por 365 días todos los años.

5.1.3.4. Requerimientos regulatorios

Son los Reglamentos internos y externos que afectan nuestras operaciones.

El Terrapuerto Trujillo es una concesión con la municipalidad distrital de Trujillo, por lo que se le reporta mensualmente cualquier actividad (compras, gastos, ingresos, etc), así mismo en algunos casos se tienen tramites que necesitan aprobación por ambas partes para que se puedan realizar.

5.1.3.5. Normas de Calidad, Ambiente, Salud y Seguridad de la información

Se refiere a las leyes del país, directamente relacionadas a la certificación que tenga nuestra empresa, es decir, Reglamentos ambientales, Reglamentos de Seguridad Ocupacional etc.

La empresa anualmente renueva los certificados correspondientes que son requeridos por ley, casos de INDECI, SUNAT, etc.

Entorno Externo

5.1.4. Mercado

5.1.4.1. Clientes

"Se indica los tipos de clientes que tiene la empresa."

Los clientes de la empresa se dividen en 3 grupos:

- Empresas de Transporte
- Locatarios Comerciales
- Pasajeros

5.1.4.2. Competencia

"Se indica los tipos de competencia que tiene la empresa o en el rubro"

Competencia directa con terminales informales o paraderos.

5.1.4.3. Grupos de interés

"Se indica las personas, grupos u organizaciones que se ven afectadas, de forma directa o indirecta, por las actividades o decisiones de la empresa."

CASA Construcción y Administración S.A. Es una empresa peruana dedicada a la Industria de la Construcción. Fue fundada en 1975 y desde el inicio de sus actividades CASA se ha caracterizado por buscar la excelencia y la calidad total en todos los servicios que ofrece, buscando ante todo la plena satisfacción del cliente y el fiel cumplimiento de todos los compromisos asumidos.

CASA desde su constitución como empresa asumió el reto de elaborar y construir importantes proyectos de ingeniería en todo el Perú, inició sus actividades en el área de Edificación Privada y Pública, se consolidó posteriormente como Empresa Constructora de obras viales, obras de saneamiento (agua y desagüe), obras hidráulicas, obras de electrificación y portuarias.

5.1.5. Proveedores

Especificamos los tipos de proveedores que tenemos, como es la interacción con ellos, que requisitos mínimos deben poseer para cumplir con los requerimientos de la empresa y específicamente con los requisitos de nuestro Sistema de Gestión.

Tipos de proveedores

Proveedor de bienes

Proveedor de servicios

Proveedores de recursos

Clasificación de Proveedores

Proveedores Normales

Proveedores Confiables

Proveedores Específicos

Proveedores Convenio

5.1.5.1. Asociados

En caso de tener asociados, distribuidores o similares lo mismo que el punto anterior

La empresa CASA es nuestro principal asociado, por lo que cuando se necesite un apoyo de la misma presta sus servicios o personal de sus empresas pertenecientes al grupo.

5.1.5.2. Requisitos clave en su cadena de suministro

Los requisitos clave para todos los proveedores y asociados que están relacionadas a la cadena de suministros vital, para que no se interrumpan las Operaciones de la empresa.

Los requisitos fundamentales para la operación son el cumplimiento con los plazos acordados y mantenimiento de equipos.

5.2. Conocimiento de las necesidades y expectativas de las partes interesadas

Este apartado señala que la organización está obligada a determinar:

- *Las partes interesadas pertinentes para el Sistema de Gestión de Seguridad de la Información.*
- *Los requisitos de las partes interesadas.*

Los requisitos de las partes interesadas están orientados a la inclusión de los requisitos legales y reglamentarios y las obligaciones contractuales.

Las partes interesadas para la implementación del SGSI son los directores, gerencia y el área de sistemas ya que por su parte las áreas gerenciales buscan tener a buen resguardo la información y el área de sistemas comprende que la información está bajo su cargo en la empresa. Otra parte interesada de forma externa viene a ser la Municipalidad de Trujillo ya que al ser una Concesión aplica de forma indirecta la norma publicada a inicios del año 2016.

5.3. Determinación del alcance del sistema de seguridad de la información

"Al definir el alcance del Sistema de Seguridad de la Información, se busca como principal objetivo determinar los límites y la aplicabilidad del sistema de seguridad de la información"

El alcance de la implementación del SGSI se dará para información propia de la empresa Concesionaria Terrapuerto Trujillo S.A. por lo que afectará directamente a todas sus áreas, pero para el cumplimiento de la misma necesitará apoyo e información que le faciliten de sus empresas terciarias.

5.4. Sistema de gestión de seguridad de la información

"Se deberá establecer, implementar, mantener y mejorar de manera continua el sistema de seguridad de la información, de acuerdo a los requisitos de la Norma Internacional"

Las Políticas de Seguridad de la Información se desarrollarán para protegen a la empresa de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Empresa.

Los principios de la Política de Seguridad serán parte de la cultura organizacional, para esto, se debe asegurar un compromiso manifiesto de los directores y gerencia, así como de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Esta Política se aplica en todo el ámbito de la Empresa Concesionaria Terrapuerto Trujillo S.A. a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Todos los encargados de las Unidades Organizativas, directivos y gerencia son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la empresa, cualquiera sea el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades de la empresa aprueban esta Política y son responsables de la autorización de sus modificaciones.

La implementación se realizará a través del framework propuesto y evaluada previamente a la implementación por lo permitirá posteriormente realizar los mismos pasos para mejorar y mantener de forma continua el cumplimiento de la misma.

6. Liderazgo

6.1. Liderazgo y compromiso

"Se detalla el liderazgo que se debe tener por parte de la gerencia o directores, las acciones que tomaran para la implementación de la norma."

La alta dirección tomará el liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información basándose en los siguientes criterios:

- Asegurar que tanto la política de seguridad como los objetivos de seguridad sean establecidos y al mismo tiempo que dichos objetivos sean compatibles con la dirección estratégica de la organización.
- Asegurar que los requisitos del Sistema de Gestión de Seguridad de la Información están integrados en los procesos de la organización.
- Garantizar la disponibilidad de los recursos necesarios para el Sistema de Gestión de Seguridad de la Información.
- Comunicar la importancia de una gestión de la seguridad de la información eficaz y la conformidad con los requisitos del SGSI.
- Corroborar que el SGSI va a lograr alcanzar los resultados previstos.
- Contribuir a la eficacia del SGSI mediante el apoyo a las personas.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la dirección, y así demostrar su liderazgo aplicado a sus áreas de responsabilidad.

6.2. Política

"Se detalla las políticas de seguridad de información que se implementarán, los cuales deben tener los propósitos y objetivos que busca la organización para la implementación de la SGSI."

En la Concesionaria Terrapuerto Trujillo S.A. la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales la empresa implementa una política de Seguridad que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados

6.2.1. Políticas generales de seguridad de la información

La Concesionaria Terrapuerto Trujillo, ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

- **Organización de la Seguridad de la Información**

  Orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación.

- **Manejo de Activos**

  Destinado a mantener una adecuada protección de los activos del Organismo.

- **Seguridad de Recursos Humanos**

  Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.

- **Seguridad Física y Ambiental**

  Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Organismo.

- **Gestión de las Comunicaciones y las Operaciones**

  Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

- **Control de Accesos**

  Orientado a controlar el acceso lógico a la información.

- **Desarrollo y Mantenimiento de los Sistemas**

  Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

- **Gestión de Incidentes de Seguridad de Información**

  Orientado a administración de identificación y acciones con los incidentes que afecten a la seguridad de la información.

- **Administración de la Continuidad de las Actividades de la Empresa**

  Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

- **Cumplimiento**

  Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos y de los requisitos de seguridad.

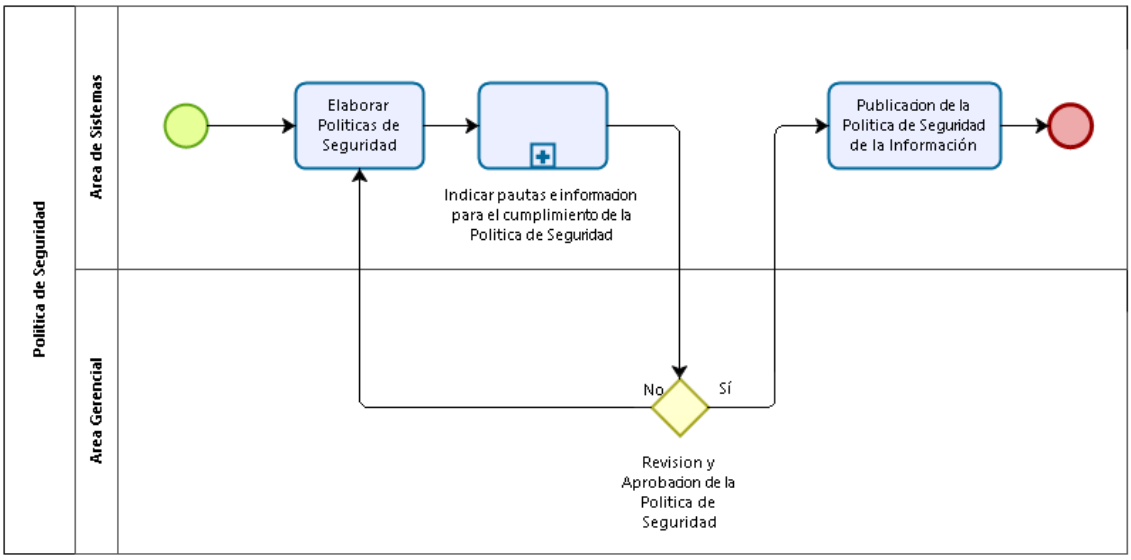


Imagen 8 Flujograma Política de Seguridad.

6.2.1.1. Organización de la Seguridad de la Información

Generalidades

"Información general de la organización concerniente a la Seguridad de la Información."

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades del Organismo.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades de la empresa pueden requerir que terceros accedan a información interna, o bien puede ser

necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

"Objetivo para el cual se desarrolla la organización de la Seguridad de la Información."

El objetivo primordial es administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con empresas especializadas para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la empresa.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a todos los recursos del Organismo y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Flujograma

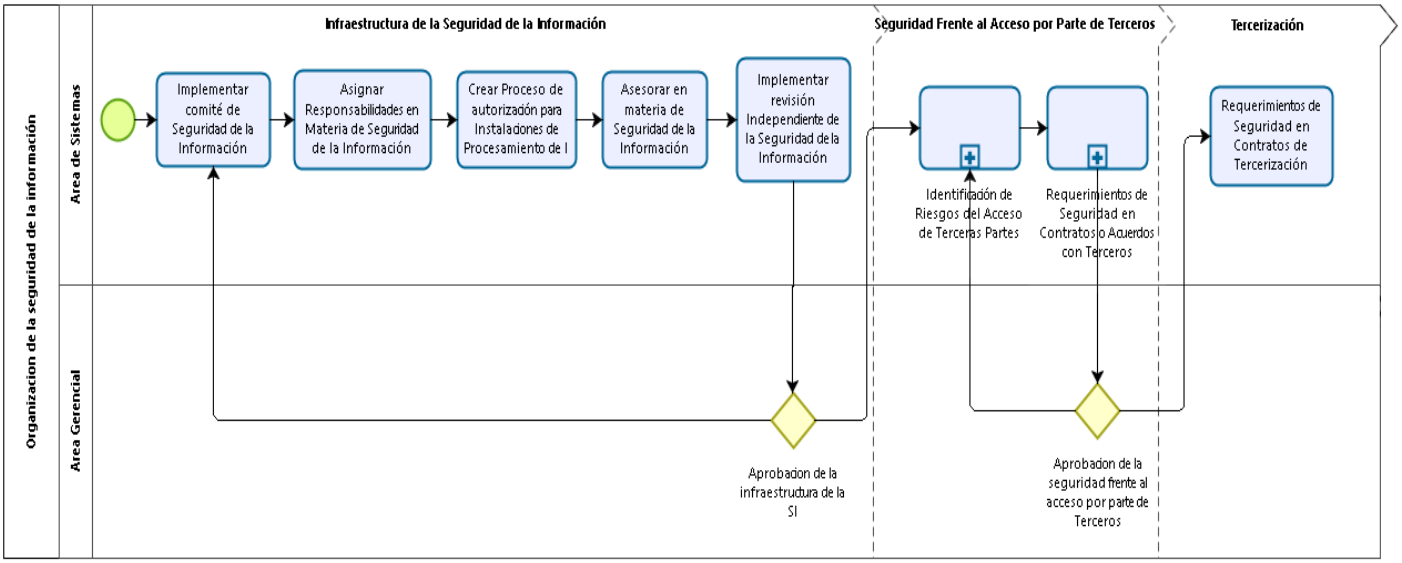


Imagen 9 Flujograma Organización de la seguridad de la información

Responsabilidad

"Se especifica encargados y asignaciones de tareas para el funcionamiento de la organización de la Seguridad de la Información."

El Responsable de Seguridad Informática asistirá al personal del Organismo en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información del Organismo y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los Responsables de las Unidades Organizativas cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El Responsable del Área de Administración cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

El Responsable del Área Legal participará en dicha tarea. Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Organismo

6.2.1.2. Manejo de Activos

Generalidades

"Información general de la clasificación y control de activos concerniente a la seguridad de la información."

La empresa debe tener un conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo debe ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la empresa.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

"Objetivo para el cual se desarrolla la clasificación y control de activos."

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Flujograma

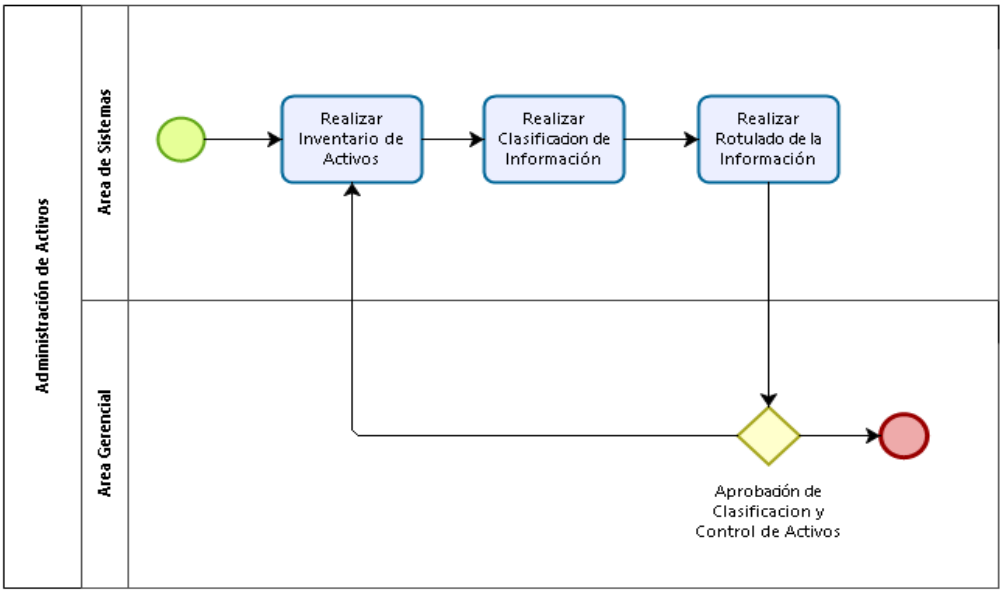


Imagen 10 Flujograma Administración de Activos

Responsabilidad

"Se especifica encargados y asignaciones de tareas para la clasificación y control de activos."

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, así mismo son los encargados de documentar y mantener actualizada la clasificación efectuada y de definir las funciones, que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia, sea cumplido de acuerdo a lo establecido en la presente Política.

6.2.1.3. Seguridad de Recursos Humanos

Generalidades

"Información general de la seguridad personal concernientes con la seguridad de la Información"

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo y evitarlo en el futuro.

Objetivo

"Objetivo para el cual se desarrolla el punto de seguridad personal."

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la empresa.

Flujograma

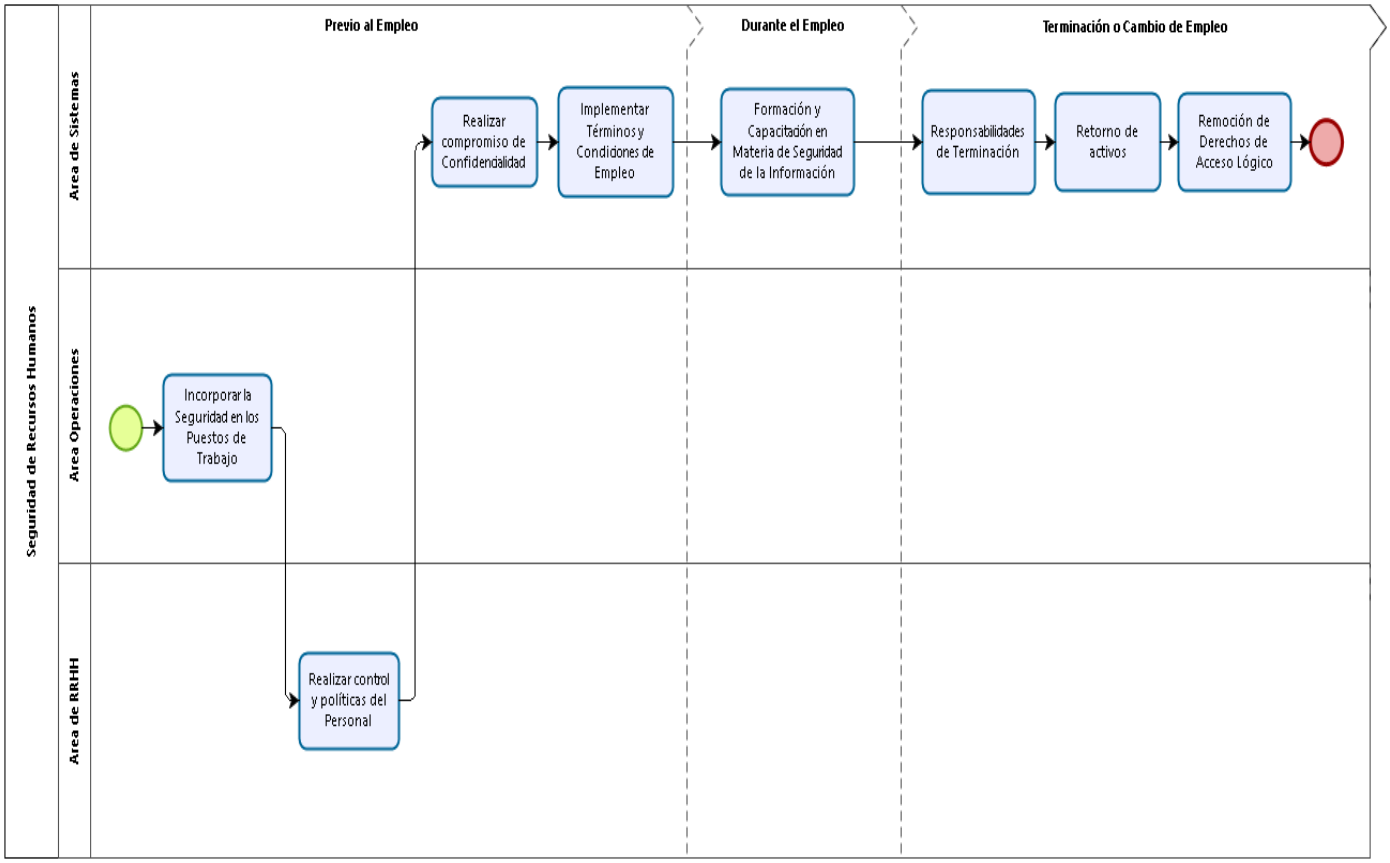


Imagen 11 Flujograma Seguridad de los Recursos Humanos

Responsabilidad

"Se especifica encargados y asignaciones de tareas para la seguridad personal."

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen

funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Organismo es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

6.2.1.4. Seguridad Física y Ambiental

Generalidades

"Información general de la seguridad física y ambiental concerniente a la seguridad de la información."

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la empresa. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

Objetivo

"Objetivo para el cual se desarrolla el punto de seguridad física y ambiental."

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones inadecuadas para la seguridad de la información de la empresa.

Proteger el equipamiento de procesamiento de información crítica para la empresa ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático, que alberga la información de la empresa.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la empresa: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Flujograma

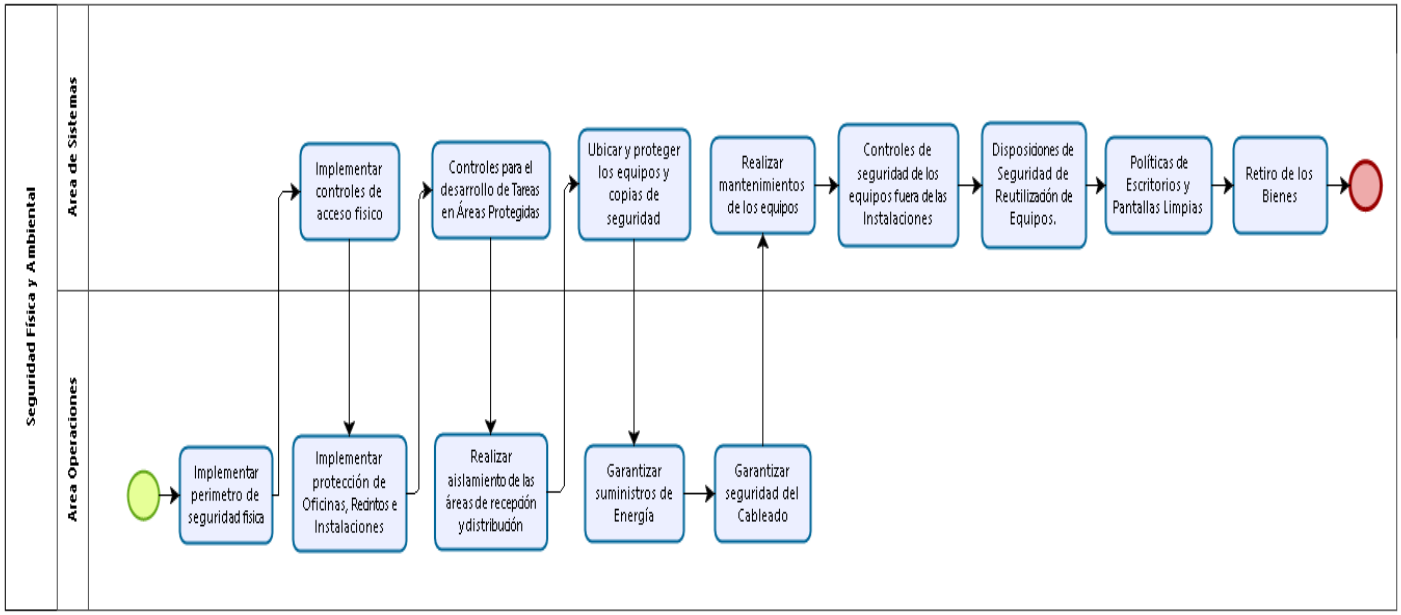


Imagen 12 Flujograma Seguridad Física y Ambiental

Responsabilidad

"Se especifica encargados y asignaciones de tareas para la seguridad física y ambiental."

El Responsable de Seguridad Informática definirá junto con el Responsable del Área Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos y controlará su implementación. Asimismo,

verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las a las áreas restringidas bajo su responsabilidad.

Todo el personal del Organismo es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

6.2.1.5. Gestión de Comunicaciones y Operaciones

Generalidades

"Información general de la gestión de comunicaciones y gestión de operaciones que se realizan en la empresa concerniente a la seguridad de la información."

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

"Objetivo para el cual se desarrolla la gestión de comunicaciones y operaciones."

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

Flujograma

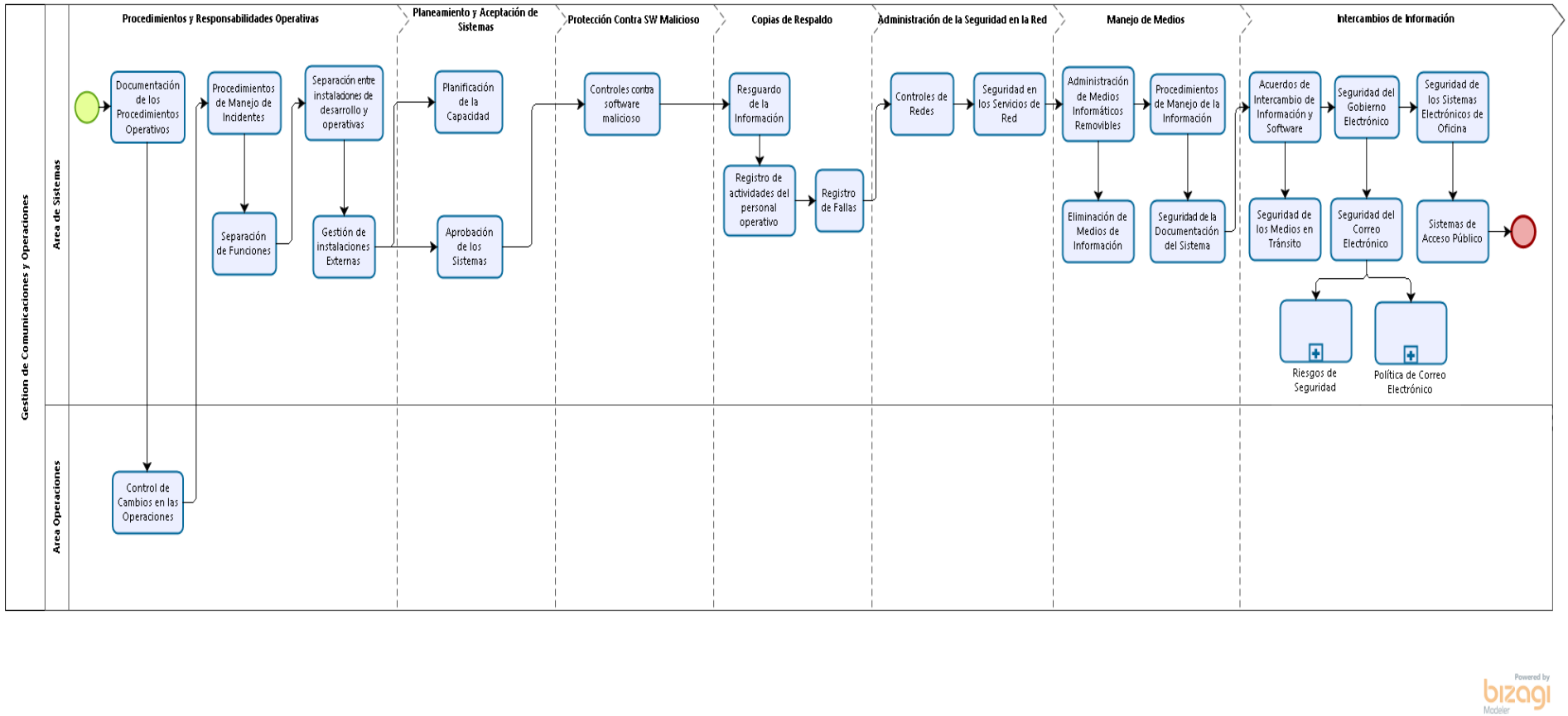


Imagen 13 Flujograma Gestión de Comunicaciones y Operaciones

Responsabilidad

"Se especifica encargados y asignaciones de tareas para la gestión de comunicaciones y operaciones."

El Responsable de Seguridad Informática junto con el Responsable del Área Informática y el Responsable del Área Legal del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posible segregar. Asimismo, revisará los registros de actividades del personal operativo.

6.2.1.6. Control de Accesos

Generalidades

"Información general de los controles de acceso que se tendrán para asegurar la seguridad de la información"

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento

Objetivo

"Objetivo para el cual se desarrolla los controles de acceso."

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Flujograma

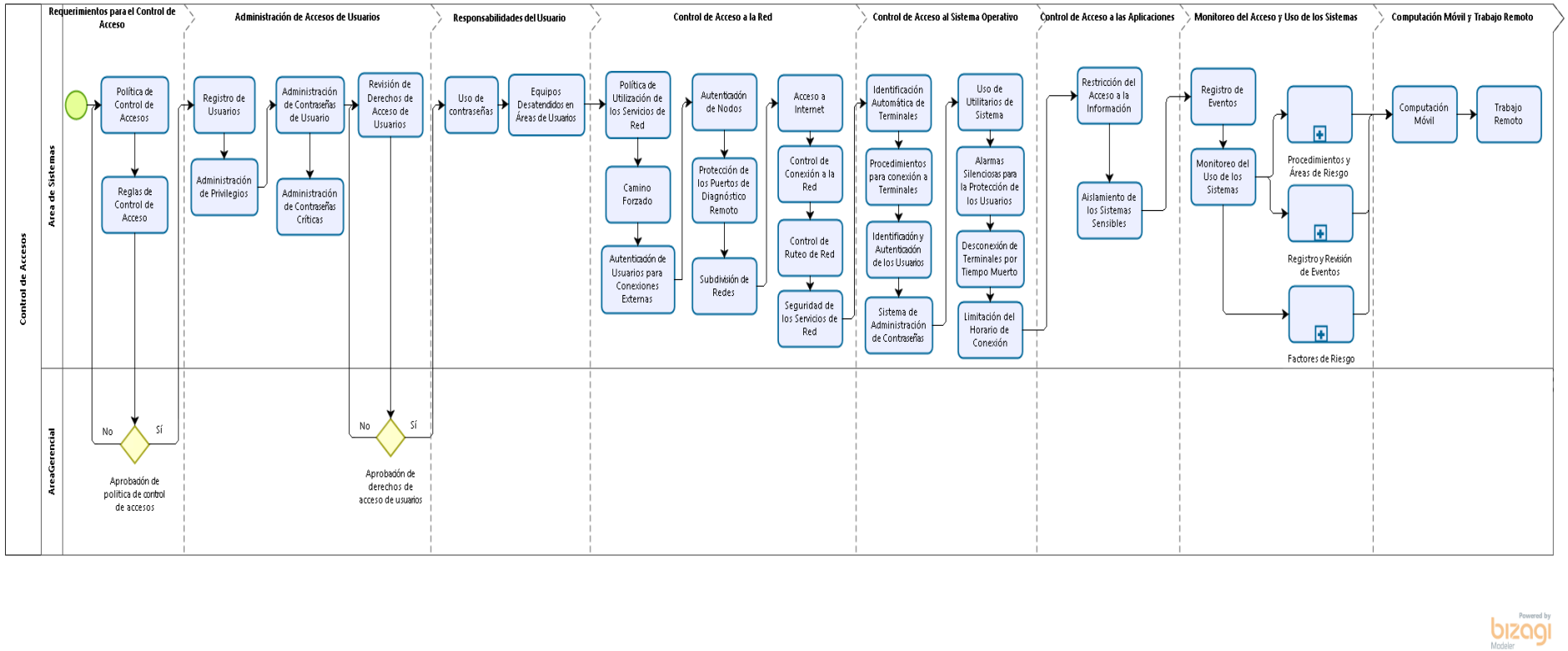


Imagen 14 Flujograma Gestión de Activos

Responsabilidad

"Se especifica encargados y asignaciones de tareas para el control de acceso"

El Responsable de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.

- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso y definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsable de las Unidades Organizativas, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Área Informática cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.

- Evaluar el costo y el impacto de la implementación de “enrutadores” o “gateways” adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados

6.2.1.7. Desarrollo y Mantenimiento de Sistemas

Generalidades

"Información general del desarrollo y mantenimiento de sistemas concerniente a la seguridad de la información."

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

"Objetivo para el cual se realiza el desarrollo y mantenimiento de sistemas."

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Flujograma

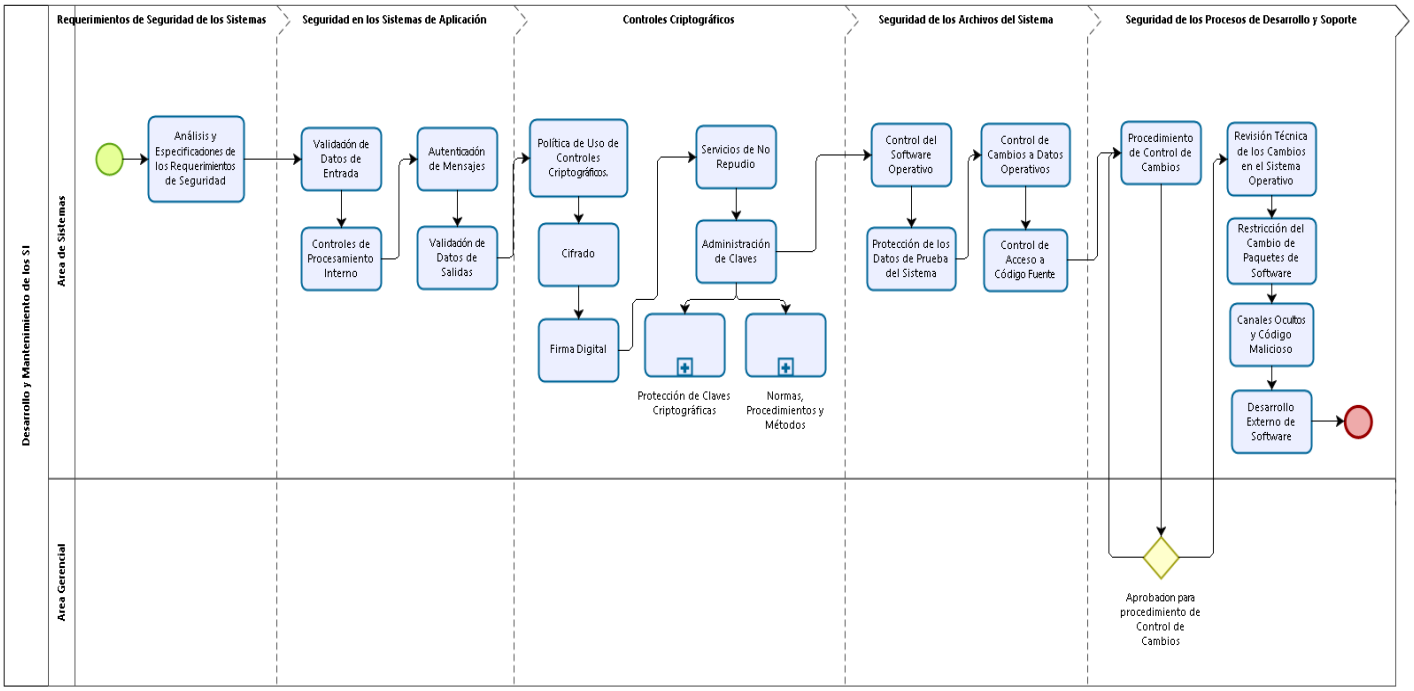


Imagen 15 Flujograma Desarrollo y Mantenimiento de los Sistemas

Responsabilidad

"Se especifica encargados y asignaciones para el cumplimiento del desarrollo y mantenimiento de sistemas"

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser

implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos, luego, el responsable de Seguridad Informática definirá junto con el Responsable del Área de Sistemas, los métodos de encriptograficos a ser utilizados.

Asimismo, el Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Sistemas propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

6.2.1.8. Gestión de Incidentes de Seguridad de Información

Generalidades

"Información general de la gestión de incidentes de la seguridad de la información."

La gestión de incidentes en la seguridad del a información se implementará por procedimientos formales para controlar la asignación de responsables para la comunicación y medidas correctivas para los mismos.

Los procedimientos comprenden todas las etapas de la gestión de incidentes de todos los niveles, desde el registro inicial desde la comunicación hasta la fase final de las medidas adoptadas para dicho incidente.

La cooperación de los usuarios es esencial para la esta política, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de la eficacia que tienen para la gestión de incidentes, en particular aquellos relacionados con el uso de los sistemas de información y la seguridad de la información.

Objetivo

"Objetivo para el cual se realiza el desarrollo y mantenimiento de sistemas."

Tener una gestión para los incidentes desde su comunicación hasta las medidas adoptadas para solución o minimizar riesgos que afecten a la seguridad de la información.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

La Política definida en este documento se aplica a todos los trabajadores de la empresa con el fin de que se detecte en primera instancia los incidentes o riesgos que afecten a la seguridad de la información en la empresa.

Flujograma

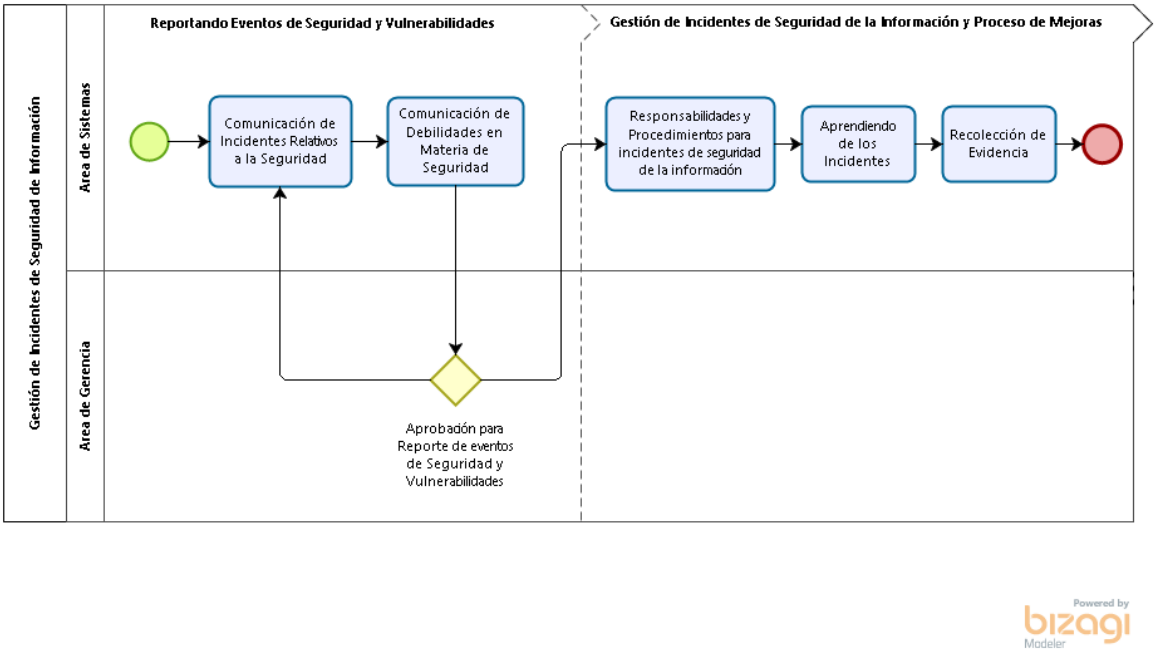


Imagen 16 Flujograma Gestión de Incidentes de Seguridad de la Información

Responsabilidad

"Se especifica encargados y asignaciones para el cumplimiento del desarrollo y mantenimiento de sistemas"

El Responsable de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para la gestión de incidentes a en todos los sistemas y servicios de información multiusuario.
- El monitoreo de la aplicación de la política de gestión contra incidentes para la seguridad de la información. la solicitud y aprobación de la administración de los incidentes suscitados.
- La respuesta a la identificación de incidentes reportados.
- La revisión de registros de incidentes y medidas adoptadas para cada una.
- Controlar que los incidentes reportados anteriormente no se vuelvan a suscitar.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de la gestión de incidencias.

Los Propietarios de la Información estarán encargados de:

- Comunicar a su superior los incidentes que se susciten con respecto a la seguridad de la información
- Los jefes de área comunicaran de forma oral y por correo los incidentes suscitados.
- Evaluar los riesgos a los cuales se expone la información con respecto a las incidencias reportadas
- Validar que las incidencias sean reportadas.
- Llevar a cabo un proceso formal y periódico de revisión de las incidencias reportadas.
- Corroborar y constatar medidas adoptadas para las incidencias reportadas.

6.2.1.9. Administración de la Continuidad de las Actividades de la Empresa

Generalidades

"Información general de la administración de la continuidad de las actividades del organismo."

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

"Objetivo para el cual se realiza la administración de la continuidad de las actividades del organismo."

Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

- Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
- Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la empresa y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a todos los procesos críticos identificados de la empresa.

Flujograma

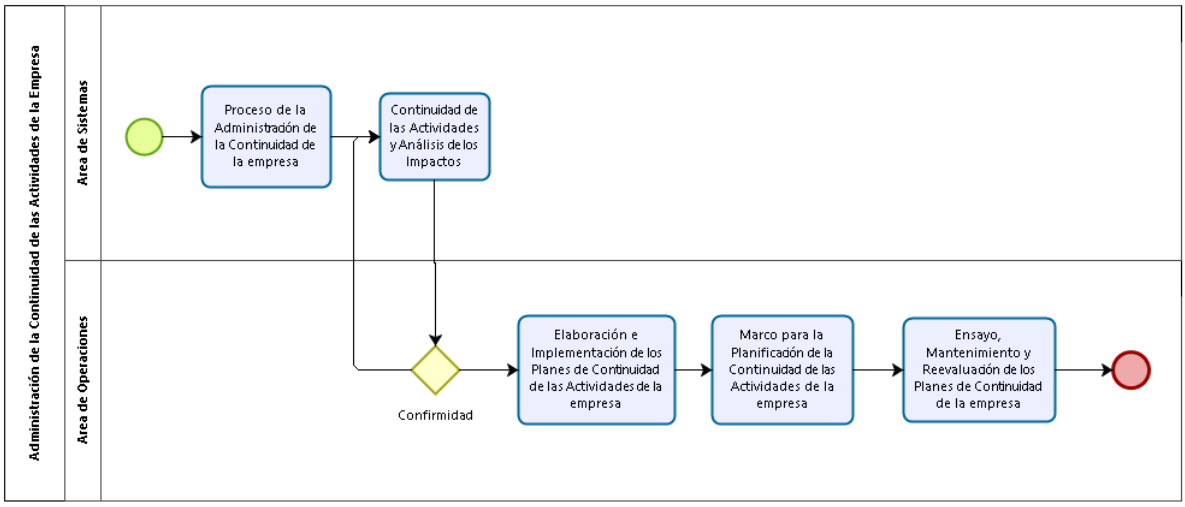


Imagen 17 Administración de la Continuidad de las Actividades de la Empresa

Responsabilidad

"Se especifica encargados y asignaciones para la administración de la continuidad de las actividades del organismo"

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones

relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades del Organismo.
- Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- Proponer las modificaciones a los planes de contingencia.

6.2.1.10. Cumplimiento

Generalidades

"Información general de la administración de la continuidad de las actividades del organismo concerniente a la seguridad de la información."

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Legal del Organismo, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivo

"Objetivo para el cual se realiza la administración de la continuidad de las actividades del organismo."

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

Alcance

"Se define el alcance de lo que aplica dicho documento y deben ser cumplidas por las áreas, operaciones o personal."

Esta Política se aplica a todo el personal de la empresa, cualquiera sea su situación de revista.

Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la empresa y a las auditorías efectuadas sobre los mismos.

Flujograma

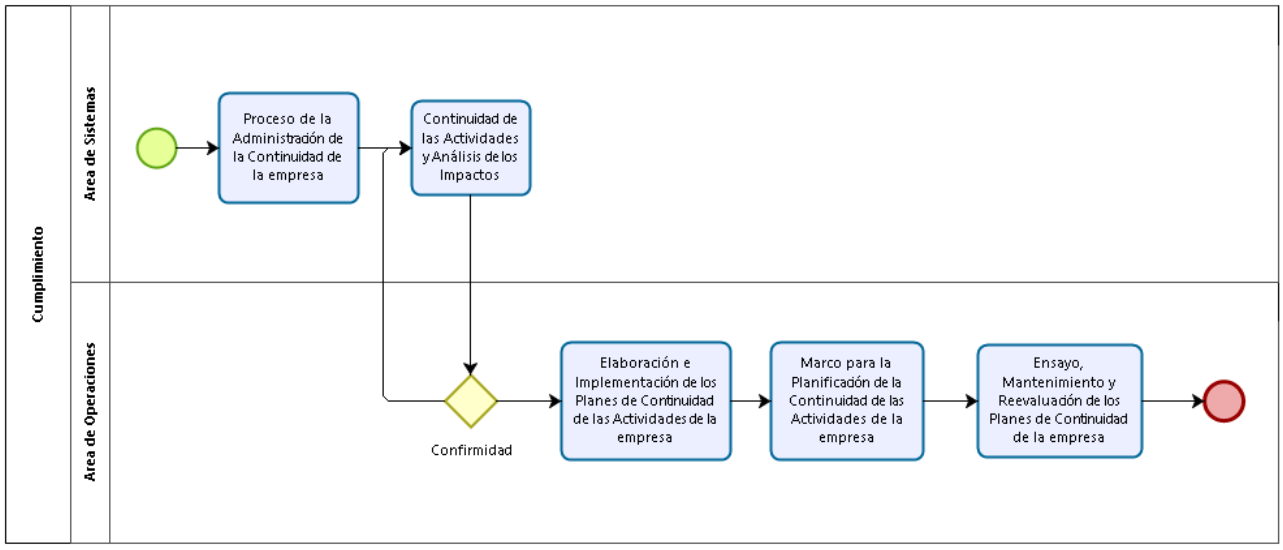


Imagen 18 Flujograma de Cumplimiento

Responsabilidad

"Se especifica encargados y asignaciones para la administración de la continuidad de las actividades del organismo"

El Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Legal del Organismo, con la asistencia del Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente

6.3. Funciones, responsabilidades y autoridad de la organización

"La gerencia asignará y comunicará las responsabilidades y funciones para los roles correspondientes con la seguridad de la información"

El Gerente general, asigna las funciones relativas a la Seguridad Informática del Organismo al Jefe de Sistemas, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

A continuación, se detallan los procesos de seguridad indicándose en cada caso el o los responsables del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Tabla 8 Funciones y Responsables designados

Proceso	Responsable
Manejo de Activos	Jefe de Operaciones y Sistemas
Seguridad de Recursos Humanos	Jefe de RRHH
Seguridad Física y Ambiental	Jefe de Operaciones
Gestión de Comunicaciones y Operaciones	Jefe de Operaciones
Control de Accesos	Jefe de Sistemas
Desarrollo y Mantenimiento de los SI	Jefe de Sistemas
Gestión de Incidentes de Seguridad de Información	Jefe de Sistemas
Administración de la Continuidad de las Actividades	Jefe de Operaciones
Cumplimiento	Gerencia

De igual forma se detallan los propietarios de la información, quienes serán los Responsables de las Unidades Organizativas a cargo del manejo de la misma:

Tabla 9 Detalle de propietario de recursos y procesos de la información

Información	Propietario	Recursos asociados	Procesos involucrados	Administrador
Contable	.....	Sistemas de información, equipamiento, bases de datos, comunicaciones,	.....	.....
Presupuesto	.....	.....	.....	.....
Inventario				
.....				
.....				

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

7. Planificación

7.1. Acciones para enfrentar los riesgos y las oportunidades

7.1.1. General

"Se detalla como determinar los riesgos y oportunidades que deban ser orientados a Garantizar que el sistema de gestión de seguridad de la información logre los resultados esperados, Evitar o reducir efectos indeseados y lograr la mejora continua."

Las acciones tomadas para enfrentar los riesgos y las oportunidades se darán en 2 etapas, la evaluación de riesgos y la administración de los riesgos. Se entiende por acciones para evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo. Así misma la administración de riesgos al proceso de identificación, control y minimización o eliminación a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Se llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta aspectos como:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del Organismo.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro del Organismo, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Las acciones tomadas para la evaluación y administración de riesgos deberán ser evaluada en periodos semestrales para identificar si estas son eficientes para la operación de la seguridad de la información de la empresa.

7.1.2. Evaluación de los riesgos de seguridad de la información

"Se detalla los procesos o plan a seguir para realizar la evaluación de los riesgos de la seguridad de la información."

Para la evaluación de riesgos de seguridad de la información se debe hacer llevar a cabo los siguientes pasos:

- Establecer un marco de evaluación de riesgos
- Identificar los riesgos
- Analizar y evaluar los riesgos
- Seleccione las opciones de gestión del riesgo
- Revisión, informe y mantenimiento

7.1.3. Tratamiento de los riesgos de la seguridad de la Información

"Se detalla los procesos o plan a seguir para realizar el tratamiento de los riesgos de la seguridad de la información."

Para el tratamiento de los riesgos de la seguridad de la información se aplicará los siguientes pasos:

- Definir una Metodología de evaluación del riesgo
- Implantación de la evaluación del riesgo
- Implementar el tratamiento del riesgo

7.2. Objetivos de Seguridad de la Información y la planificación para alcanzarlos

"Se detalla que procesos o medios se utilizarán para cumplir los objetivos de la seguridad de la información."

La organización deberá establecer los objetivos de seguridad de la información en relación a las funciones y niveles.

Los objetivos de seguridad de la información se realizarán mediante la clasificación de la información las cuales evalúa las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad

A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características

A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

- Confidencialidad:
  - Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la empresa o no.
  - Información que puede ser conocida y utilizada por todos los empleados de la empresa y algunas entidades externas debidamente autorizadas y cuya divulgación o uso no autorizados, podría ocasionar riesgos o pérdidas leves.
  - Información que sólo puede ser conocida y utilizada por un grupo de empleados que la necesiten para realizar su trabajo, cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la empresa
  - Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la empresa y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo a terceros.
- Integridad:
  - Información cuya modificación no autorizada puede repararse fácilmente o no afecta la operación de la empresa.
  - Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la empresa o terceros.
  - Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la empresa o terceros.

- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves para la empresa y a terceros.

- Disponibilidad:
  - Información cuya inaccesibilidad no afecta la operación.
  - Información cuya inaccesibilidad permanente durante 3 meses podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
  - Información cuya inaccesibilidad permanente durante 1 semana podría ocasionar pérdidas significativas a la empresa o a terceros.
  - Información cuya inaccesibilidad permanente durante 1 día podría ocasionar pérdidas significativas a la empresa o terceros.

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- **CRITICIDAD BAJA:** ninguno de los valores asignados supera a 1.
- **CRITICIDAD MEDIA:** alguno de los valores asignados es 2
- **CRITICIDAD ALTA:** alguno de los valores asignados es 3

8. Apoyo / Soporte

8.1. Recursos

"Se detalla los procesos o medida se adoptará para determinar el recurso que será para la implementación y mantenimiento de la SGSI"

La organización deberá determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información a través de los ingresos mensuales por recaudación estimando un ……. del porcentaje del mismo para el recurso en mención.

8.2. Competencia

"Se determina las competencias necesarias y detallará las acciones que permitan adquirir las competencias necesarias de las personas para realizaran la implementación y mantenimiento de la SGSI"

La Empresa Concesionaria Terrapuerto Trujillo determinará si sus empleados actuales en labor cumplen con las competencias necesarias en caso contrario deberá capacitar a los mismos con el fin de que cumplan con la implementación y mantenimiento de la seguridad de la información requerida por la empresa.

8.3. Concientización

"Se determina las medidas que se tomaran para tener en qué grado los trabajadores tienen concientización sobre la seguridad de la información."

Los trabajadores de la empresa deben tener en claro las políticas de seguridad de la información con fin de evitar riesgos, así como tener en claro su contribución a los cumplimientos, normas y beneficios de la seguridad de la información.

Se tomarán encuestas y evaluaciones para determinar el grado de concientización que tienen los trabajadores de forma semestral para cada área u unidad organizacional.

8.4. Comunicación

"Se establece los procedimientos y medios que se usaran para las comunicaciones como apoyo o soporte de la política."

Se establecerán las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia

Los sucesos de defectos, fallas o vulnerabilidades en la seguridad de la información serán comunicados automáticamente al encargado de seguridad de la información que se ha designado, además de corroborar dicha comunicación el responsable del área o unidad organizativa, por medio de correo con fotos como evidencia de los mismos.

Se deberán comunicar dichos sucesos en el mismo momento que se den estos, así como facilitar la información correspondiente para la solución o prevención de los mismos.

8.5. Documentación de la información

8.5.1. General

"Se indica de forma general el proceso de la documentación de la seguridad de la información"

Se debe tener todas las políticas correspondientes a la seguridad de la información debidamente documentadas, así como los controles que se deben tener para aplicar dichas medidas; toda información correspondiente a la seguridad de la información deberá ser documentada, foliada y registrada siguiendo el modelo de documentación anexado para la efectividad del sistema de seguridad de la información.

NOMBRE DE REGISTRO	QUIEN REGISTRA	TIEMPO DE CONSERVACION
Modelo de Implementación ISO 27001	Área de Sistemas	Indefinido
Políticas Generales de Seguridad de la Información	Área de Sistemas - Área Gerencial	Indefinido - Actualización Semestral
Mecanismos de Control Generales de Seguridad de la Información	Área de Sistemas	Indefinido hasta actualización.
Actas y Documentación de Seguridad de la Información	Áreas Competentes	Indefinido
Almacenamiento de documentación	Área Gerencial	Indefinido hasta actualización.

Tabla 10 Registro de Documentación

8.5.2. Creación y actualización

"Se indica el proceso para la creación y actualización de la documentación concerniente a la seguridad de la información"

Para la creación de documentación correspondiente a la seguridad de información se utilizará el formato anexo 2 el cual deberá ser revisado y aprobado por el encargado designado para la documentación.

Para actualizar un documento tendrá que tener la aprobación del encargado de seguridad de la información y responsable del área con el fin de tener un control para los cambios de los mismo, los cuales también tendrán que ser registrados en cada documento.

8.5.3. Control de la información documentada

"Se indica los controles para la información que es documentada concerniente a la seguridad de la información"

Los documentos en un lugar cerrado bajo llave, pero estarán disponibles para su uso en momento que sea necesario, el resguardo y protección de los documentos estarán bajo la responsabilidad del encargado de la seguridad de la información para su mayor control, encargándose también de la retención y disposición de los mismos.

9. Operación

9.1. Planificación y control operacional

"Se detalla la planificación y controles que se adaptaran para cumplir con los requisitos de la seguridad de la información e implementar acciones determinadas"

El Comité de Seguridad de la Información, coordinará el desarrollo de los procesos que garanticen la implementación de la seguridad de la información acorde con las actividades de la empresa, para lo cual aplicará los siguientes controles

- Identificar y priorizar los procesos críticos de las actividades de la empresa.
- Asegurar que todos los integrantes de la empresa comprendan los riesgos que

la misma enfrenta en términos de probabilidad de ocurrencia e impacto de posibles amenazas.

- Verificar que las políticas de control de seguridad de la información sean publicadas, validadas y aprobadas
- Verificar que los procesos de la implementación se cumplan en el orden de las etapas planificadas
- Elaborar y documentar una estrategia de continuidad de las actividades de la empresa consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.

Proponer las modificaciones a los planes de contingencia

9.2. Evaluación de los riesgos de seguridad de la información

"Se detalla el proceso de evaluación de riesgos que de adoptará para resguardar la seguridad de la información de la empresa."

La organización llevará a cabo evaluaciones de los riesgos de seguridad de la información a intervalos planificados para los cuales realizará en primera instancia los siguientes pasos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades de la empresa y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la empresa. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la gerencia y directores para su aprobación

9.3. Tratamiento de los riesgos de la seguridad de la Información

"Se detalla el tratamiento que se aplicara para los riesgos identificados que afectan a la seguridad de la información."

El marco para el tratamiento de los riesgos de seguridad de la información para la empresa, tendrá en cuenta los siguientes puntos:

- Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de

servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

- Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.
- Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

10. Evaluación del desempeño

10.1. Monitoreo, medición, análisis y evaluación

"Se indica cómo se aplicará los procesos de monitoreo, medición, análisis y evaluación correspondiente a la seguridad de la información en la empresa."

El Comité de Seguridad de la Información monitoreará periódicamente y complementará con herramienta de check list que se cumplan las políticas dadas correspondientes a la seguridad de la información, así mismo con los resultados de esta herramienta se analizara en qué grado se cumplen cada control dado por la empresa.

El comité de Seguridad de la información coordinará evaluaciones para los trabajadores de acuerdo a sus funciones para identificar si tienen claro la importancia de la seguridad de la información que se debe tener en la empresa.

10.2. Auditorías internas

"Se detalla el proceso de las auditorias que se realizarán para identificar en qué grado se están cumpliendo dichas políticas y controles dados por la empresa correspondiente a la seguridad de la información."

La empresa realizara auditorias anuales para el caso de seguridad de la información.

La empresa si no cuenta con personal idóneo para realizar las auditorías internas, se contratará auditores externos para identificar el grado de cumplimiento de las políticas y controles correspondientes a la seguridad de la información.

Los trabajadores y el comité de seguridad de igual forma deberá cumplir con las evaluaciones y controles dados para el cumplimiento de estas.

10.3. Revisión por parte de la Dirección

"Se detalla el proceso de revisión del sistema de gestión de seguridad de la información a intervalos establecidos para garantizar su continua disponibilidad, adecuación y efectividad"

La dirección o gerencia deberá revisar el estatus de las acciones de las anteriores revisiones por parte de la Gerencia o Dirección.

Se revisarán los cambios propuestos por el comité de seguridad de la información.

Retroalimentar sobre el desempeño e importancia de la seguridad de la información basándose en las no conformidades y las acciones correctivas que se puedan presentar, resultados del monitoreo y medición, Resultados de la auditoría, cumplimiento de los objetivos de seguridad de la información.

Se tomarán resultados de la evaluación de los riesgos y estatus del plan de tratamiento de los riesgos y oportunidades de mejora continua para tomar decisiones correspondientes para el mantenimiento del SGSI.

Estas revisiones y decisiones deberán conservarse, documentadamente como evidencia de los resultados de las revisiones por parte de la dirección

11. Mejora

11.1. No conformidad y acción correctiva

"Medidas a tomar antes inconformidad y acciones correctivas para evitar recurrencias."

La no conformidad por parte gerencial o responsable de seguridad de la información deberá ser comunicado y documentarán claramente indicando el motivo de tal acción, con el fin de que exista un registro y bajo esta se toma una acción inmediata para corregir los puntos citados por la cual fue negativa.

A fin de cumplir con estas normas, se tomarán las siguientes medidas:

- Elaborar y divulgar los lineamientos que se tomaran para comunicar la no conformidad y las acciones correctivas.
- Revisar los históricos de no conformidades y acciones correctivas que se dieron a las observaciones detalladas.
- Determinar las causas de no conformidad
- Implementación de acciones necesarias para evitar recurrencias.
- Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.
- Registrar resultados de las acciones correctivas dadas.

11.2. Mejora continua

"Se detalla procedimientos que serán tomados para una mejora continua correspondiente al SGSI"

La gerencia y el comité de seguridad de la información se reunirán periódicamente semestralmente para acordar mejoras considerando resultados de evaluaciones y de controles adaptados a la empresa, identificando procesos, normas, políticas que tengan que ser modificadas para asegurar la idoneidad, adecuación y efectividad del sistema de gestión de la seguridad de la información.

V. DISCUSIÓN DE RESULTADOS

5.1. Análisis de la hipótesis

La hipótesis planteada es la siguiente:

H0: “Un modelo de procesos construido con la Framework Spark implementará en un 90 por ciento la norma ISO 27001:2014 en la empresa Concesionaria Terrapuerto Trujillo S.A.”

VI: Modelo de procesos construido con la Framework Spark

VD: Implementación de la norma ISO 27001

DIMENSIONES	INDICADORES
X_1=Modelo de procesos	X_{11}: Nro de Etapas o fases X_{12}: Nro de entregables o resultados
X_2=Procesos	X_{21}: Nro de diagramas procesos X_{22}: Nro de descripciones de procesos X_{23}: Nro de indicadores por proceso

Tabla 11 Modelo de procesos construido con el framework Spark

DIMENSIONES	INDICADORES
Y_1=Procesos en cada área o criterio	Y_{11}:% de proceso implementados
Y_2=Criterios o áreas	Y_{21}:% de criterios o áreas implementadas

Tabla 12 Implementación de la norma ISO 27001

La hipótesis será contrastada a través del método pre-test y post-test, a través de la validez de los indicadores que operacionalizan las variables de la hipótesis.

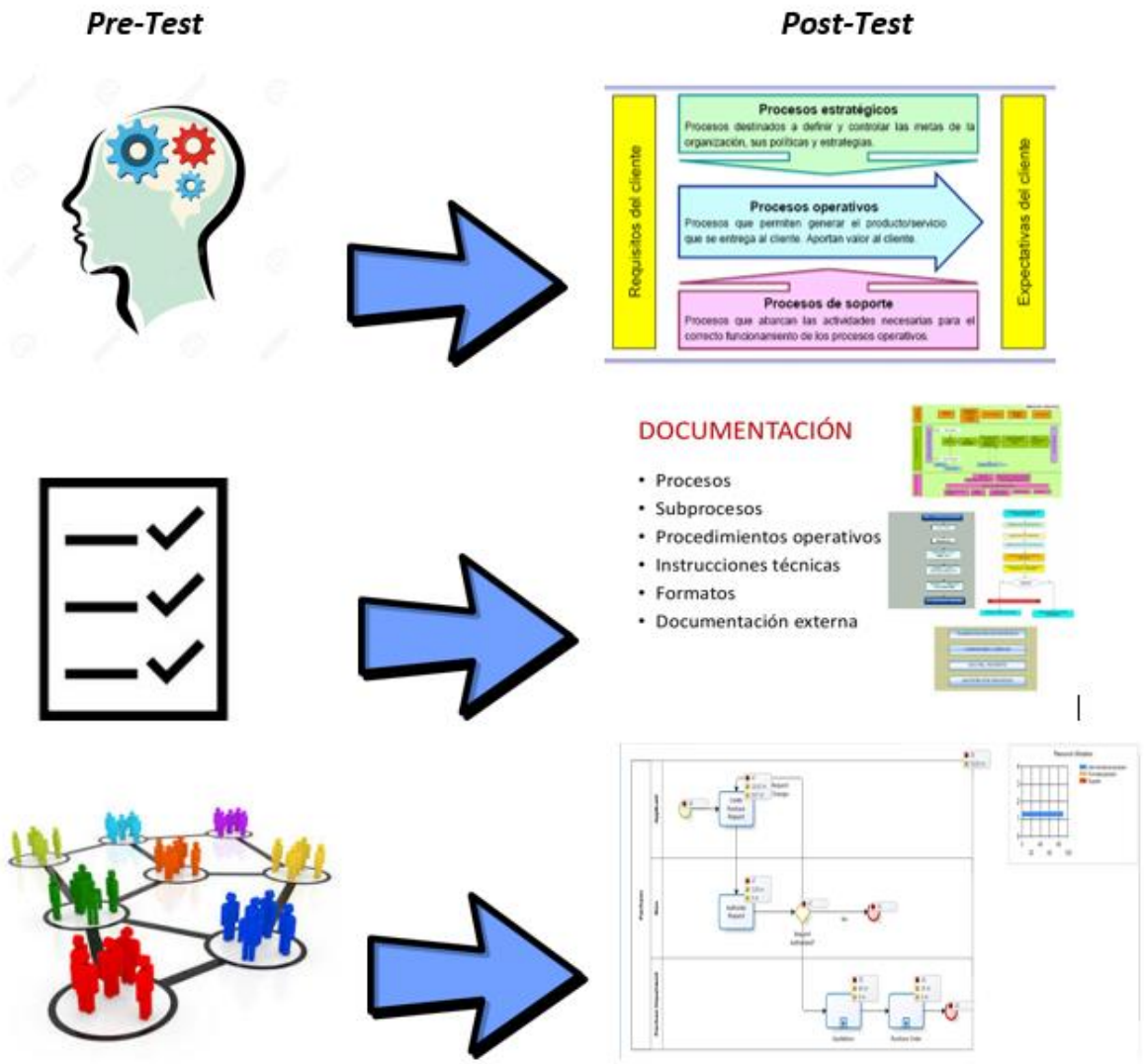
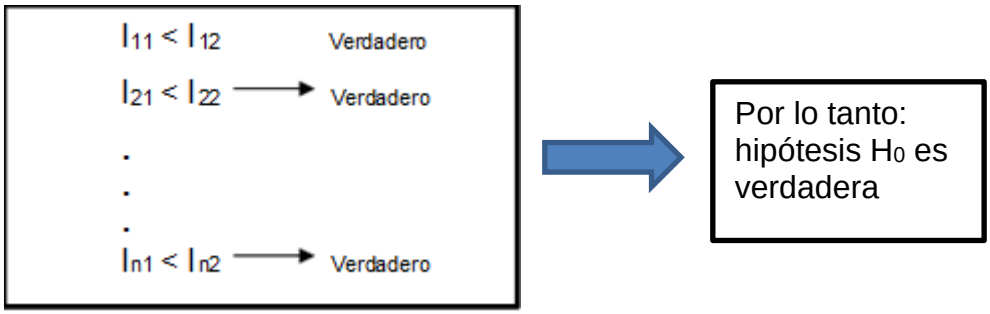


Imagen 19 Pre-Test, Post-Test

5.2. Regla de inferencia de validez de la hipótesis

Para efectos de contrastar la hipótesis se utilizará como regla de inferencia la validez de los indicadores que caracterizan a la hipótesis por ello para que la hipótesis sea verdadera todos los indicadores tienen que ser verdaderos.

Teniendo como hipótesis H0: Un modelo de procesos construido con el framework Spark implementa en un 90 por ciento la norma ISO 27001:2014 en la empresa Concesionaria Terrapuerto Trujillo S.A



5.3. Presentación de resultados

A continuación, se presentan los resultados de la observación utilizada para el pre-test y post-test, de la muestra, el mismo que estuvo conformado por los trabajadores del área de desarrollo de software

5.1.1 Número de etapas o fases del modelo de procesos(X11)

Descripción	PRE-TEST	POST-TEST
Número de etapas o fases del modelo de procesos	0	3

El número de etapas o fases en el POST-TEST se extrajo la cantidad de las etapas que se usan para realizar el modelo de procesos que tenemos que son 3: Analizar, Diseñar y Construir.

En el resultado del indicador X11 el resultado es el esperado con respecto a la hipótesis planteada.

5.1.2 Número de entregables o resultados (X12)

Descripción	PRE-TEST	POST-TEST
Número de entregables o resultados	0	1

El número de entregables en el POST-TEST se extrajo la cantidad de entregables que tenemos que se obtienen de la construcción del modelo de procesos para la implementación de la norma ISO 27001. En el resultado del indicador X12 el resultado es el esperado con respecto a la hipótesis planteada.

5.1.3 Número de diagramas de procesos (X21)

Descripción	PRE-TEST	POST-TEST
Número de diagramas de procesos	0	11

El número de entregables en el POST-TEST se extrajo la cantidad de diagramas de procesos que se obtienen de la construcción del modelo de procesos para la implementación de la norma ISO 27001.

En el resultado del indicador (X21) el resultado es el esperado.

5.1.4 Número de descripciones de procesos (X22)

Descripción	PRE-TEST	POST-TEST
Número de descripciones de procesos	0	11

El número de entregables en el POST-TEST se extrajo la cantidad de descripciones de los procesos que se obtienen de la construcción del modelo de procesos para la implementación de la norma ISO 27001.

En el resultado del indicador (X22) el resultado es el esperado.

5.1.5 Número de indicadores por proceso (X23)

Descripción	PRE-TEST	POST-TEST
Número de indicadores o controles por proceso	0	2

El número de indicadores o controles en el POST-TEST se extrajo la cantidad promedio de indicadores o controles para los procesos que se obtienen de la construcción del modelo de procesos para la implementación de la norma ISO 27001. En el resultado del indicador (X23) el resultado es el esperado.

En resumen se llaga a la conclusión de que todo lo antes expuesto son resultados esperados y verdaderos ante la hipótesis planteada en el presente trabajo de investigación.

VI. CONCLUSIONES

1. La creación del modelo de procesos con la guía de las fases del framework Spark, cumple para implementar la norma ISO 27001 en la empresa Concesionaria Terrapuerto Trujillo S.A.
2. El modelo de procesos para la implementación de la norma ISO 27001 ha obtenido complemente el alcance estimado, con apoyo de las etapas del framework Spark, en la empresa Concesionaria Terrapuerto Trujillo S.A.
3. El prototipo elaborado del modelo de procesos permitió la implementación de la norma iso 27001 a través de procesos de forma útil, fácil de usar y de forma confiable.
4. La aceptación del prototipo fue validado y aprobado por gerencia y directores de la empresa, concluyendo en su implementación basada en esta.
5. La hipótesis planteada es aceptada, ya que se comprueba que se cumple con los controles, políticas y procesos que indica la normativa ISO 27001.

VII. RECOMENDACIONES

1. A la empresa que brindo la información para este modelo (que aún continua con la fase de prueba para la implementación de la norma ISO 27001), debe tomar en cuenta los procesos y controles identificados en el modelo de procesos presentado en el presente trabajo de investigación.
2. Propiciar el uso del framework Spark como herramienta para guía de las etapas de implementación en la seguridad de la información de la empresa.
3. Modelar, Diseñar y Construir un sistema de Gestión de Seguridad de la información que integre las etapas y procesos para integrar y mantener una mayor seguridad de la información que se tenga en la empresa.
4. Elaborar o implementar un sistema de documentación que apoyara en registros de modificaciones de documentos de información.
5. Usar la plantilla en empresas con operaciones o en áreas similares de las empresas asociadas en el grupo empresarial al cual pertenece la empresa Concesionaria Terrapuerto Trujillo S.A.

VIII. BIBLIOGRAFÍA

Bizagi. (2013). *Página Oficial Bizagi*. Obtenido de http://www.bizagi.com/es/

Bizagi Spark. (29 de Abril de 2015). *Página Oficial Bizagi - Metodología Spark*. Obtenido de http://www.bizagi.com/es/que-hacemos/transformacion-digital/metodologia-spark

Castro, W. (2013 de Agosto de 11). *Trujillo ya cuenta con un moderno Terminal Terrestre de Pasajeros*. Obtenido de La Republica: http://larepublica.pe/11-08-2013/trujillo-ya-cuenta-con-un-moderno-terminal-terrestre-de-pasajeros

David Aguirre, M. (2014). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.* PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, Lima. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677

DefinicionMX. (2014). *Procesos*. Obtenido de Blog Definición: https://definicion.mx/proceso/

Euronews. (09 de Junio de 2013). *Infraestructuras y transporte*. Obtenido de http://es.euronews.com/2013/06/09/infraestructuras-y-transporte-problemas-brasilenos-a-un-ano-del-mundial/

Ferreiro, S. (Setiembre de 2006). *Historia del Transporte*. Obtenido de Transporte Internacional: http://transporteinternacional.blogspot.pe/2006/09/historia-del-transporte.html

hernandez, L. (1 de Junio de 2013). *UNIDAD 5: MODELO DE IMPLEMENTACIÓN*. Obtenido de http://ithleovi.blogspot.pe/2013/06/unidad-5-modelo-deimplementacion-el.html

Huamán Monzón, F. (2014). *DISEÑO DE PROCEDIMIENTOS DE AUDITORÍA DE CUMPLIMIENTO DE LA NORMA NTP-ISO/IEC 17799:2007 COMO PARTE DEL PROCESO DE IMPLANTACIÓN DE LA NORMA TÉCNICA NTP-ISO/IEC 27001:2008 EN INSTITUCIONES DEL ESTADO PERUANO.* Lima.

IsoTools. (28 de Mayo de 2017). *Cómo definir el alcance del Sistema de Seguridad de la Información*. Obtenido de https://www.isotools.org/2017/05/28/definir-alcance-del-sistema-seguridad-la-informacion-sgsi/

Jaén, U. d. (Julio de 2015). *Criterio 5: Procesos*. Obtenido de Universidad de Jaén: https://www10.ujaen.es/sites/default/files/users/archivo/Calidad/Criterio5.pdf

Kumar, V. (2014). *ISO-27001-Chequeo-de-Cumplimiento*. Obtenido de Scribd: https://es.scribd.com/document/161768494/102262732-ISO-27001-Chequeo-de-Cumplimiento#

López, A. (Febrero de 2014). *El portal de ISO 27001 en español*. Obtenido de http://www.iso27000.es/sgsi.html

Maciel, V. F. (2014). *Problemas y desafíos en transporte público urbano*. Obtenido de BRTBRASIL: http://www.brtbrasil.org.br/index.php/sala-de-imprensa/artigos/35-art-4#.VsaNCfLhDIW

Morales, I. (Abril de 2015). *Contexto de la Organización*. Obtenido de http://www.5consultores.com/contexto-de-la-organizacion/

OnTarget, B. (28 de Abril de 2015). *Bizagi Spark, Fortalecer*. Obtenido de http://download.bizagi.com/docs/OnTarget_es.pdf

Penagos, J. L. (08 de Julio de 2011). *Transporte Público en Lima, siglo XX: el microbús*. Obtenido de Blog PUCP: http://blog.pucp.edu.pe/blog/juanluisorrego/2011/07/08/el-transporte-publico-en-lima-siglo-xx-el-microbus/

Peña, F. (Marzo de 2015). *¿Qué son las normas ISO y cuál es su finalidad?* Obtenido de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Peruano, D. e. (2016). *Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Siste*. Obtenido de http://busquedas.elperuano.com.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

QuickStart, B. (28 de Abril de 2015). *Bizagi Spark - Impulsar*. Obtenido de http://download.bizagi.com/docs/QuickStart_es.pdf

School, H. D. (Junio de 2014). *Características y ejemplos del modelado de procesos*. Obtenido de Blog "Retos para ser Directivo: http://retos-directivos.eae.es/caracteristicas-y-ejemplos-del-modelado-de-procesos/

Seclén Arana, J. (2016). *actores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*. UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS, Lima. Obtenido de http://cybertesis.unmsm.edu.pe/bitstream/cybertesis/4884/1/Seclen_aj.pdf

SGSI Blog especializado. (30 de Julio de 2014). *ISO 27001:2013 Liderazgo y compromiso*. Obtenido de http://www.pmg-ssi.com/2014/07/iso-2700-12013-liderazgo-compromiso/

Tola Franco, D. (2015). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001*. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, Guayaquil. Obtenido de https://www.dspace.espol.edu.ec/retrieve/89073/D-84631.pdf

ANEXOS 01:

Referencia		Evaluacion Norma ISO 27001		Resultado	
Checklis	Estanda	Sección	Preguntas	Observaciones	Estado (%
Política de Seguridad					
1	**3**	**Políticas de Seguridad de Información**			
1.1	3.1	Aspectos Generales	Existe una Política de Seguridad de la Información, que es aprobada por la dirección, publicada y comunicada según proceda, a todos los empleados?		
			Establecen las políticas un compromiso de las Gerencias con relación al método de la organización para la gestión de la seguridad de la información?		
			Se Indica pautas e informacion para el cumplimiento de la Politica de Seguridad		
1.2	3.2	Sanciones Previstas por incumplimiento	Se indica medidas y normas previstas ante incumplimiento de dicho documento		
1.3	3.3	Revisión de la Política de Seguridad	Las políticas de seguridad son revisadas a intervalos regulares, o cuando hay cambios significativos para asegurar la adecuación y efectividad?		
			Las políticas de Seguridad de la Información tiene un propietario, que ha aprobado la responsabilidad de la gestión para el desarrollo, revisión y evaluación de la política de seguridad?		
			Existen procedimientos de revisión de las políticas de seguridad y estos incluyen requerimientos para el manejo de su revisión?	Revisión Anual o cada vez que haya cambios importantes	
			Los resultados del revisión de la gestión son tenidos en cuenta?		
			Se obtiene la aprobación de la alta gerencia con relació a las políticas revisadas?		
Organización de la Seguridad de la Información					
2	**4.1**	**Infraestructura de la Seguridad de la Información**			
2.1	4.1.1	Comité de Seguridad de la Información	Si la gerencia demuestra soporte activo a las medidas de seguridad dentro de la organización. Esto puede ser realizado por direcciones claras, compromiso demostrado, asignaciones explícitas y conocimiento de las responsabilidades de la seguridad de información.		
			Si las actividades de seguridad de información son coordinadas por representantes de distintas partes de la organización, con sus roles pertinentes y responsabilidades.		
2.2	4.1.2	Asignación de Responsabilidades de Seguridad de Información	Están establecidas las responsabilidades de protección de activos individuales y llevar a cabo procesos de seguridad específicos que estén claramente identificados y definidos?		

2.3	4.1.3	Proceso de autorizacion de instalaciones de Procesamiento de Información	Si el proceso de gestión de autorización está definido e implementado para cada nuevo equipo de procesamiento de información dentro de la organización.		
2.4	4.1.4	Asesoramiento Especializado en Materia de Seguridad de la Información	Existe algún procedimiento que describa cuando y quienes deben contactar a las autoridades competentes, departamento de bomberos, etc y cómo deben reportarse los incidentes?		
			Existe un plan o cronograma del asesoramiento con respecto de la seguridad de la información que se dará a los trabajadores		
2.5	4.1.5	Revisión Independiente de la Seguridad de la Información	Existen los contactos apropiados con grupos especiales de interés, foros de seguridad o asociaciones profesionales relacionadas con la seguridad?	Participación en colectividades o asociaciones de seguridad para estar actualizado	
			Tiene la organización un enfoque sobre la gestión de la seguridad de información, su implementación, revisión independiente a intervalos regulares o cuando ocurran cambios significativos?		
3	**4.2**	**Seguridad Frente al Acceso por Parte de Terceros**			
3.1	4.2.1	Identificación de Riesgos del Acceso de Terceras Partes	Los riesgos inherentes a equipos o sistemas de información de terceros son identificados y luego implementadas medidas de control apropiadas antes de permitir el acceso?		
3.2	4.2.3	Requerimientos de Seguridad en Contratos o Acuerdos con Terceros	Los acuerdos con terceros incluyen accesos, procesamiento, comunicaciones, manejo de la información o equipos que involucren almacenamiento de información que cumplan con todos los requerimientos de seguridad?		
4	**4.3**	**Tercerización**			
4.1	4.3.1	Requerimientos de Seguridad en Contratos de Tercerización	Son identificados todos los requerimientos de seguridad sean cumplidos antes de conceder acceso a los clientes a los activos de la organización?		
Administración de Activos					
5	**5.1**	**Inventario de Activos**			
5.1	5.1.1	Inventario de Activos	Son los activos debidamente identificados e inventariados o se mantiene un registro de los activos importantes?	Hardware, Software e Información (PO2.3 Cobit)	
5.2	5.1.2	Propiedad de Activos	Los activos tienen identificados a sus respectivos propietarios y definidas con ellos clasificaciones de datos y restricciones de acceso en base a la criticidad, y estas restricciones revisadas periodicamente?		
5.3	5.1.3	Uso aceptable de Activos	Son identificadas, documentadas e implementadas todas las regulaciones existentes con respecto al uso aceptable de información y activos asociados con el procesamiento de información?		

6	**5.2**	**Clasificación de la Información**			
6.1	5.2.1	Directrices de Clasificación	La información es clasificada en terminos de su valor, requerimientos legales, sensibilidad y criticidad para la organización?		
7	**5.3**	**Rotulado de la Información**			
7.1	5.3.1	Etiquetado y manejo de información	Son definidos conjuntos de procedimientos para etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización?		
Seguridad de Recursos Humanos					
8	**6.1**	**Previo al Empleo**			
8.1	6.1.1	Incorporación de la Seguridad en los Puestos de Trabajo	Están claramente definidos y documentados de acuerdo a las políticas de seguridad de información de la organización los roles y responsabilidades de los empleados, contratistas y terceros?		
8.2	6.1.2	Control y Política del Personal	Los controles de verificación de antecedentes para todos los candidatos a empleo, contratistas y terceros, son llevados a cabo de acuerdo a las regulaciones relevantes?		
			Incluye la verificación referencias sobre el carácter, confirmación de titulos académicos, cualidades profesionales y chequeos independientes de identidad?		
8.3	6.1.3	Compromiso de Confidencialidad	Son los roles y responsabilidades definidos previamente, comunicados claramente a los candidatos a empleo durante el proceso de pre empleo?		
8.4	6.1.4	Términos y condiciones de empleo	Son firmados con los empleados, contratistas y terceros, contratos de confidencialidad y acuerdos de no divulgación como parte inicial de los términos y condiciones de contratos de trabajo?		
			Estos acuerdos y contratos cubren las responsabilidades de seguridad de información de la organización, los empleados, contratistas y terceros?		
9	**6.2**	**Durante el Empleo**			
9.1	6.2.1	Formación y Capacitación en Materia de Seguridad de la Información	La gestión requiere a los empleados, contratistas y terceros a que apliquen la seguridad en concordancia con las Políticas y Procedimientos establecidos en la Organización?		
			Los empleados, contratistas y terceros reciben la apropiada sensibilización, educación y formación permanente sobre la Seguridad de Información con respecto a sus funciones laborales específicas?		
			Existe un proceso disciplinario para aquellos empleados que incumplen las políticas de seguridad?		
10	**6.3**	**Terminación o Cambio de Empleo**			
10.1	6.3.1	Responsabilidades de Terminación	Las responsabilidades de procedimiento determinación o cambio de empleo están claramente definidas y asignadas?		
10.2	6.3.2	Retorno de activos	Existe un procedimiento a seguir con respecto a asegurar que los empleados, contratistas y terceros devuelvan los activos de la organización que estén en su poder al terminar el contrato de empleo?		

10.3	6.3.3	Remoción de Derechos de Acceso Lógico	Son removidos los derechos de acceso de todos los empleados, contratistas y terceros a los sistemas de información al termino de empleo o adecuación en caso de que cambien de función?	Eliminar todos los usuarios al salir un empleado o cuando cambia de puesto.	
Seguridad Física y Ambiental					
11	**7**	**Seguridad Física y Ambiental**			
11.1	7.1	Perímetro de Seguridad Física	Existen mecanismos de control de acceso implementados con respecto al acceso a los sitios de procesamiento de información? Algunos ejemplos son controles biométricos, tarjetas de acceso, separación por muros, control de visitantes, etc.		
11.2	7.2	Controles Físicos de Entrada	Existen controles de acceso de tal modo a que solo las personas autorizadas puedan ingresar a las distintas areas de la organización?		
11.3	7.3	Protección de Oficinas, Recintos e Instalaciones	Las salas de servidores u otros equipos de procesamiento (routers, switches, etc.), están apropiadamente resguardadas bajo llave o en cabinas con llave?		
11.4	7.4	Trabajando en Areas Seguras	Se tienen procedimientos designados e implementados sobre como trabajar en las areas seguras?		
11.5	7.5	Aislamiento de las Áreas de Recepción y Distribución	Con respecto a las zonas de acceso público, entrega, descarga donde personas no autorizadas pueden acceder, las zonas de procesamiento de información y equipos delicados son aislados y asegurados para prevenir el acceso no autorizado?		
11.6	7.6	Ubicación y Protección del Equipamiento y Copias de Seguridad	Se tienen implementadas protecciones o resguardos contra fuego, inundaciones, temblores, explosiones, manifestaciones y otras formas de desastres naturales o provocadas por el hombre?		
			Existe alguna amenaza potencial en los locales vecinos del lugar donde se encuentran las instalaciones?	Verificar locales de posibles problemas en las cercanías en caso de conflictos.	
			Los equipos son protegidos para reducir los riesgos de daños ambientales y oportunidades de acceso no autorizado?		
11.7	7.7	Suministros de Energía	Los equipos son protegidos contra fallas eléctricas y otras fallas que pudieran tener (redundancia)?		
			Que mecanismos de protección eléctrica son utilizados? Alimentación multiple, UPS, generador de backup, etc?		
11.8	7.8	Seguridad del Cableado	Los cables de suministro eléctrico y comunicaciones son debidamente protegidos contra intercepción y/o daños?		
			Existen controles adicionales de seguridad con respecto al transporte de información crítica? Por ej. Encriptado en las comunicaciones.		

11.9	7.9	Mantenimiento de Equipos	Se realiza mantenimiento periódico de los equipos de modo a asegurar la continua disponibilidad e integridad?		
			En la realización de mantenimientos, son respetados los intervalos y recomendaciones de los fabricantes?		
			Los mantenimientos son realizados unicamente por personal capacitado y autorizado?		
			Los logs de alertas de los equipos, son revisados periodicamente para detectar y corregir posibles fallas en los mismos? (principalmente fallas en discos)		
			Se aplican los controles adecuados cuando se envían los equipos fuera de la organización?	No deben contener información confidencial.	
			Todos los equipos están cubiertos por pólizas de seguro y los requerimientos de la Compañía de Seguros están apropiadamente realizados?		
11.10	7.10	Seguridad de los Equipos Fuera de las Instalaciones.	Existen mecanismos de control y mitigación de riesgos implementados con relación a equipos utilizados fuera de la organización? (encripción de discos de las notebooks, seguro, etc.)	Utilizar encripción de los datos de las notebooks (Truecrypt es gratuito y muy bueno)	
			En caso de utilización de equipos fuera de la organización, estos cuentan con la autorización respectiva de las gerencias?		
11.11	7.11	Disposiciones de Seguridad de Reutilización de Equipos	Cuando se disponga la reutilización de equipos o cuando sean dados de baja, son verificados los medios de almacenamiento con respecto a datos y software licenciado y luego destruidos totalmente antes de su entrega?		
11.12	7.12	Política de Escritorio Limpio y Pantalla Limpia	La organización ha adoptado una política de escritorio limpio con relación a los papeles y dispositivos de almacenamiento removibles?		
			La organización ha adoptado una política de pantalla limpia con relación a los equipos de procesamiento de información?		
11.13	7.13	Retiro de los Bienes	Existen controles implementados con respecto a que ningún equipo, información y software sea sacado de la organización sin la autorización respectiva?		
Gestión de Comunicaciones y Operaciones					
12	**8.1**	**Procedimientos y Responsabilidades Operativas**			
12.1	8.1.1	Documentación de Procedimientos Operativos	Los procedimientos operativos son documentados, actualizados y están disponibles para todos los usuarios que puedan necesitarlos?		
			Dichos procedimientos son tratados como documentos formales y cualquier cambio en los mismos necesita la autorización pertinente?		
12.2	8.1.2	Control de Cambios en las Operaciones	Son controlados todos los cambios en los sistemas y equipos de procesamiento de información?		
12.3	8.1.3	Procedimientos de Manejo de Incidentes	Existen procesos para el manejo de incidentes suscitados en la empresa que afecten a la seguridad de la información?		

12.4	8.1.4	Separación de Funciones	Son separadas las tareas y responsabilidades de modo a reducir las oportunidades de modificación o mal uso de los sistemas de información?		
12.5	8.1.5	Separación de desarrollo e instalaciones operativas	Los equipos de desarrollo y pruebas están separados de los equipos operacionales? Por ejemplo desarrollo de software debe estar en un equipo separado del de producción. Cuando sea necesario, incluso deben estar en segmentos de red distintos unos del otro.	Separar ambientes y ponerlos en VLANes distintas que no se vean entre sí. Los datos de desarrollo deben ser ilegibles.	
12.6	8.1.6	Gestión de Instalaciones Externas	Existen procedimientos y controles para la administración de instalaciones externas		
13	**8.2**	**Planeamiento y Aceptación de Sistemas**			
13.1	8.2.1	Planificación de la Capacidad	La capacidad de procesamiento de los sistemas son monitoreados en base a la demanda y proyectados en base a requerimientos futuros, de modo a asegurar que la capacidad de proceso y almacenamiento estén disponibles? Ejemplo: Monitoreo de espacio en disco, Memoria RAM, CPU en los servidores críticos.		
13.2	8.2.2	Aprobación del Sistema	Son establecidos criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones? Son realizadas pruebas antes de la aceptación de los mismos?		
14	**8.3**	**Manejo de Entrega de Servicios Tercerizados**			
14.1	8.3.1	Entrega de Servicios	Existen medidas que son tomadas para asegurar que los controles de seguridad, niveles de servicio y entrega sean incluidos y verificados en los contratos de servicios con terceros, así como su revisión periódica de cumplimiento?		
14.2	8.3.2	Monitoreo y revisión de servicios tercerizados	Son los servicios, reportes y registros proveídos por teceros regularmente monitoreados y revisados?		
			Existen controles de auditoría que son realizados a intervalos regulares sobre los servicios, reportes y registros suministrados por terceros?		
14.3	8.3.3	Manejo de Cambios de servicios tercerizados	Se gestionan los cambios en la provisión de servicios, incluyendo mantenimiento y la mejora en las políticas de seguridad de información existentes, procedimientos y controles?		
			Se tienen en cuenta sistemas de negocio críticos, procesos involucrados y re-evaluación de riesgos?		
15	**8.4**	**Protección contra código malicioso**			
15.1	8.4.1	Controles contra código malicioso	Existen controles para detección, prevención y recuperado contra código malicioso y son desarrollados e implementados procedimientos apropiados de advertencia a los usuarios?		

16	**8.5**	**Copias de Respaldo**			
16.1	8.5.1	Resguardo de la Información	Se realizan copias de respaldo de la información y software y son testeados regularmente en conconrdancia con las políticas de backup?		
			Toda la información y el software esencial puede ser recuperado en caso de ocurrencia de un desastre o fallo de medios?	Ver donde se va a recuperar el backup en caso de desastre.	
16.2	8.5.2	Actividades del Personal Operativo	¿Existen controles para el registro de las actividades de personal en sus turno y accesos?		
16.3	8.5.3	Registro de Fallas	¿Existe un procedimiento de documentación para el registro de fallas de los sistemas de información?		
17	**8.6**	**Administración de la Red**			
17.1	8.6.1	Controles de Red	La red es adecuadamente administrada y controlada para protegerse de tretas y en orden a mantener la seguridad de los sistemas y aplicaciones en uso a traves de la red, incluyendo la información en transito?		
			Existen controles implementados para asegurar el transito de la información en la red y evitar que esta sea leída o accesada de forma no autorizada?		
17.2	8.6.2	Seguridad en los Servicios de Red	Las características de seguridad, niveles de servicio y requerimientos de administración de todos los servicios de red son identificados e incluidos en cualquier acuerdo de servicio de red?		
			La capacidad del proveedor de servicios de red de proporcionar los servicios de forma segura, es determinada y regularmente monitoreada y se tienen derechos de auditoría acordada para medir niveles de servicio?		
18	**8.7**	**Manejo de Medios**			
18.1	8.7.1	Manejo de medios removibles	Existen procedimientos para el manejo de medios removibles como cintas, diskettes, tarjetas de memoria, lectores de CD, pendrives, etc.?		
			Los procedimientos y niveles de autorización están claramente definidos y documentados?		
18.2	8.7.2	Eliminación de Medios de Información	En caso de que los medios ya no sean requeridos, estos son eliminados de forma segura bajo procedimientos formalmente establecidos?		
18.3	8.7.3	Procedimientos de manejo de la información	Existen procedimientos para el manejo del almacenamiento de la información?		
			Aborda este procedimiento temas como: protección de la información contra acceso no autorizado o mal uso?		
18.4	8.7.4	Seguridad en la Documentación de los Sistemas	La documentación de los sistemas está protegida contra acceso no autorizado?		

19	**8.8**	**Intercambio de Información**			
19.1	8.8.1	Acuerdos de Intercambio de Información y Software	Existe una política formal, procedimientos y/o controles aplicados para asegurar la protección a la información?		
			Estos procedimientos y controles cubren el uso de equipos de comunicación electrónica en el intercambio de información?		
			Existen acuerdos de intercambio de información y software entre la organización y partes externas?		
			El contenido de los acuerdos con respecto a la seguridad refleja la sensibilidad y criticidad de la información de negocio envuelta en el proceso?		
19.2	8.8.2	Seguridad de los Medios en Tránsito	Los medios físicos que contengan información es protegida contra acceso no autorizado, mal uso o corrupción de datos durante el transporte entre las organizaciones?		
19.3	8.8.3	Seguridad del Gobierno Electrónico	El uso de las TIC se aplica para una eficacia y entrega eficiente de los servicios brindados en la empresa?		
19.4	8.8.4	Seguridad del Correo Electrónico	La información que se envía por mensajería electrónica es bien protegida? (Mensajería Electrónica incluye pero no es restringida solamente a email, intercambio electrónico de datos, mensajería instantanea, etc.)	Correos importantes que van afuera deben ser encriptados GPG, y lo demás por VPNs.	
19.5	8.8.5	Seguridad de los Sistemas Electrónicos de Oficina	Existen controles de seguridad que se debe tener con los sistemas electrónicos de las oficinas?		
19.6	8.8.6	Sistemas de Acceso Público	Los sitemas de acceso publico tienen controles para evitar alteración o robo de información?		
Control de Accesos					
20	**9.1**	**Requerimientos para el Control de Acceso**			
20.1	9.1.1	Política de Control de Acceso	Las políticas de control de acceso son desarrolladas y revisadas basadas en los requerimientos de seguridad del negocio?		
			Los controles de acceso tanto físico como lógico son tenidos en cuenta en las políticas de control de acceso?		
20.2	9.1.2	Reglas de Control de Acceso	Tanto a los usuarios como a los proveedores de servicios se les dio una clara declaración de los requisitos de la empresa en cuanto a control de acceso?		
21	**9.2**	**Administración de Accesos de Usuarios**			
21.1	9.2.1	Registración de Usuarios	Existe algún procedimiento formal de altas/bajas de usuarios para acceder a los sistemas?		
21.2	9.2.2	Administracion de Privilegios	La asignación y uso de privilegios en los sistemas de información, es restringida y controlada en base a las necesidades de uso y dichos privilegios son solo otorgados bajo un esquema formal de autorización?		

21.3	9.2.3	Administración de Contraseñas de Usuarios	La asignación y reasignación de contraseñas debe controlarse a través de un proceso de gestión formal.		
			Se les solicita a los usuarios que firmen un acuerdo de confidencialidad del password?		
21.4	9.2.4	Administración de Contraseñas Críticas	¿Existe procedimiento para la administración de contraseñas de usuarios con funciones o actividades críticas?		
21.5	9.2.5	Revisión de Derechos de Acceso de Usuarios	Existe un proceso de revisión de privilegios y derechos de acceso a intervalos regulares. Por ejemplo: Privilegios especiales cada 3 meses, privilegios normales cada 6 meses?		
22	**9.3**	**Responsabilidades de Usuarios**			
22.1	9.3.1	Uso de Contraseñas	Existe alguna práctica de seguridad en el sitio para guiar a la selección y mantenimiento de contraseñas seguras?		
22.2	9.3.2	Equipos desatendidos de Usuarios	Los usuarios y terceros son concientes de los requisitos de seguridad y procedimientos para proteger los equipos desatendidos? Por ejemplo: Salir del sistema cuando las sesiones son terminadas o configurar terminación automática de sesiones por tiempo de inactividad, etc.		
23	**9.4**	**Control de Acceso a la Red**			
23.1	9.4.1	Políticas sobre Servicios de Red	Se le provee a los usuarios acceso unicamente a los servicios de red a los cuales han sido autorizados específicamente?		
			Existen políticas de seguridad relacionadas con la red y los servicios de red?		
23.2	9.4.2	Camino Forzado	¿Existe procedimiento para evitar alteraciones a la seguridad de la información y realizar caminos forzados de comunicación en las conexiones de red?		
23.3	9.4.3	Autenticaciones de Usuarios para conexiones externas	Son utilizados mecanismos apropiados de autenticación para controlar el acceso remoto de los usuarios?		
23.4	9.4.4	Autenticación de Nodos	Existen medios o se tiene sistemas para autenticar nodos con conexiones especificas?		
23.5	9.4.5	Protección de los Puertos de Diagnóstico Remoto	Los accesos físicos y lógicos a puertos de diagnóstico están apropiadamente controlados y protegidos por mecanismos de seguridad?		
23.6	9.4.6	Subdivisión de Redes	Los grupos de servicios de información, usuarios y sistemas de información son segregados en la red?		
			La red (desde donde asociados de negocios o terceros necesitan acceder a los sistemas de información) es segregada utilizando mecanismos de seguridad perimetral como firewalls?		
			En la segregación de la red son hechas las consideraciones para separar las redes wireles en internas y privadas?		
23.7	9.4.7	Acceso a Internet	¿Existen medidas adoptadas para el acceso a internet que tendrán los usuarios?		

23.8	9.4.8	Control de Conexión a la Red	Existe una política de control de acceso que verifique conexiones provenientes de redes compartidas, especialmente aquellas que se extienden mas allá de los límites de la organización?		
23.9	9.4.9	Control de Ruteo de Red	Existen políticas de control de acceso que establezcan los controles que deben ser realizados a los ruteos implementados en la red?		
			Los controles de ruteo, están basados en mecanismos de identificación positiva de origen y destino?		
23.10	9.4.10	Seguridad de los Servicios de Red	¿Existe procedimientos que garantice la seguridad de los servicios de red en la empresa?		
24	**9.5**	**Controles de Acceso a Sistemas Operativos**			
24.1	9.5.1	Identificación Automática de Terminales	Son considerados equipos de identificación automática para autenticar conexiones desde equipos y direcciones específicas?		
	9.5.2	Procedimientos de Conexión de Terminales	¿Existe procedimiento para las conexiones a los equipos informáticos?		
24.2	9.5.3	Identificación y Autenticación de Usuarios	Un único identificador de usuario (user ID) es proveído a cada usuario incluyendo operadores, administradores de sistemas y otros técnicos?		
			Se eligen adecuadas técnicas de autenticación para demostrar la identidad declarada de los usuarios?		
			El uso de cuentas de usuario genéricas son suministradas sólo en circunstancias especiales excepcionales, donde se especifícan los beneficios claros de su utilización. Controles adicionales pueden ser necesarios para mantener la seguridad.		
24.3	9.5.4	Sistema de Administración de Contraseñas	Existe un sistema de gestión de contraseñas que obliga al uso de controles como contraseña individual para auditoría, periodicidad de caducidad, complejidad mínima, almacenamiento encriptado, no despliegue de contraseñas por pantalla, etc.?		
24.4	9.5.5	Uso de Utilitarios de Sistema	En caso de existir programas utilitarios capaces de saltarse los controles de aplicaciones de los sistemas, estos están restringidos y bien controlados?		
24.5	9.5.6	Alarmas Silenciosas para la Protección de los Usuarios	¿Los sistemas tienen implementado alarmas silenciosas para la protección de los usuarios?		
24.6	9.5.7	Desconexión de Terminales por Tiempo Muerto	Las aplicaciones son cerradas luego de un periodo determinado de inactividad? (Un tiempo determinado de inactividad puede ser determinado por algunos sistemas, que limpian la pantalla para prevenir acceso no autorizado, pero no cierra la aplicación o las sesiones de red)		
24.7	9.5.8	Limitación del Horario de Conexión	Existen restricciones limitando el tiempo de conexión de aplicaciones de alto riesgo? Este tipo de configuraciones debe ser considerada para aplicaciones sensitivas cuyas terminales de acceso se encuentran en lugares de riesgo.		

25	**9.6**	**Control de Acceso a las Aplicaciones y a la Información**			
25.1	9.6.1	Restricción de Acceso a la Información	El acceso a la información y los sistemas de aplicaciones por parte los usuarios y personal de soporte, está restringido en concordancia con las políticas de control de acceso definidas?		
25.2	9.6.2	Aislamiento de Sistemas Sensibles	Aquellos sistemas considerados sensibles, están en ambientes aislados, en computadoras dedicadas para el efecto, con recursos compartidos con aplicaciones seguras y confiables, etc?		
26	**9.7**	**Monitoreo del Acceso y Uso de los Sistemas**			
26.1	9.7.1	Registro de Eventos	Las eventos suscitados son registrados en logs para luego ser analizadas y tomar acciones apropiadas realizadas en consecuencia?		
26.2	9.7.2	Monitoreo del Uso de los Sistemas	Son desarrollados procedimientos de monitoreo de equipos de procesamiento de datos?		
			El resultado de la actividad de monitoreo es revisada regularmente de forma periódica?		
			Los niveles de monitoreo requeridos por los equipos de procesamiento de información son determinados por un análisis de riesgos?		
27	**9.8**	**Computación Móvil y Trabajo Remoto**			
27.1	9.8.1	Computación Móvil	Existe una política formal y medidas apropiadas de seguridad adoptadas para protegerse contra riesgo de utilización de computación móvil y equipos de comunicación?	Encripción de discos en las notebooks	
			Algunos ejemplos de computación móvil y equipos de telecomunicación incluyen: notebooks, palmtops, laptops, smart cards, celulares.		
			Son tenidos en cuenta los riesgos tales como trabajar en ambientes no protegidos en cuanto a las políticas de computación móvil?		
27.2	9.8.2	Trabajo Remoto	Se desarrollan e implementan políticas, planes operativos y procedimientos con respecto a tareas de trabajos remotos?		
			Las actividades de trabajos remotos, son autorizadas y controladas por las gerencias y existen mecanismos adecuados de control para esta forma de trabajo?		
Desarrollo y Mantenimiento de Sistemas de Información					
28	**10.1**	**Requerimientos de Seguridad de los Sistemas de Información**			
28.1	10.1.1	Análisis y Especificaciones de Requerimientos de Seguridad	Los requerimientos de seguridad para nuevos sistemas de información y fortalecimiento de los sistemas existentes, especifican los requerimientos para los controles de seguridad?		
			Los requerimientos y controles identificados reflejan el valor económico de los activos de información envueltos y las consecuencias de un fallo de seguridad?		
			Los requerimientos para la seguridad de información de los sistemas y prcesos para implementar dicha seguridad, son integrados en las primeras etapas de los proyectos de sistemas?		

29	**10.2**	**Seguridad en los Sistemas de Aplicación**			
29.1	10.2.1	Validación de Datos de Entrada	Los datos introducidos a los sistemas, son validados para asegurar que son correctos y apropiados?		
			Los controles tales como: Diferentes tipos de mensajes de error para datos mal ingresados, Procedimientos para responder a los errores de validación, definición de responsabilidades para todo el personal envuelto en la carga de datos, etc. son considerados?		
29.2	10.2.2	Control de Procesamiento Interno	Son incorporadas validaciones en las aplicaciones para detectar/prevenir que puedan ser ingresados datos no válidos por error o deliberadamente?		
			Se tiene en cuenta en el diseño y la implementación de las aplicaciones que el riesgo de falllas en el procesamiento que conduzcan a perdida de integridad de datos sea minimizado?		
29.3	10.2.3	Autenticación de Mensajes	Los requerimientos para aseguramiento y protección de la integridad de los mensajes en las aplicaciones, son debidamente identificados e implementados los controles necesarios?		
			Si una evaluación de riesgos de seguridad se llevó a cabo para determinar si es necesaria la integridad del mensaje, y para determinar el método más apropiado de aplicación.		
29.4	10.2.4	Validación de Datos de Salida	Los sistemas de aplicaciones de salida de datos, son validados para asegurar que el procesamiento de información almacenada sea correcta y apropiada a las circustancias?		
30	**10.3**	**Controles Criptográficos**			
30.1	10.3.1	Políticas de Uso de Controles Criptográficos	La organización posee políticas de uso de controles criptográficos para protección de la información? Estas políticas son implementadas con éxito?		
			La política criptográfica considera el enfoque de gestión hacia el uso de controles criptográficos, los resultados de la evaluación de riesgo para identificar nivel requerido de protección, gestión de claves y métodos de diversas normas para la aplicación efectiva?		
30.2	10.3.2	Cifrado	¿Se usa cifrados en los sistemas de información usados en la empresa?		
30.3	10.3.3	Firma Digital	¿Las firmas digitales de los usuarios son resguardadas por cada usuario?		
30.4	10.3.4	Servicios de No Repudio	Existe procedimiento para identificar acciones o eventos no admitidos por los usuarios de haberlas realizado		
30.5	10.3.5	Administración de Claves	La administración de claves se utiliza efectivamente para apoyar el uso de técnicas criptográficas en la organización?		
			Las claves criptográficas están protegidas correctamente contra modificación, pérdida y/o destrucción?		
			Las claves públicas y privadas están protegidas contra divulgación no autorizada?		
			Los equipos utilizados para generar o almacenar claves, están físicamente protegidos?		
			Los sistemas de administración de claves, están basados en procedimientos estandarizados y seguros?		

31	**10.4**	**Seguridad de los Archivos de Sistemas**			
31.1	10.4.1	Revisión Técnica de los Cambios en el Sistema Operativo	Existen procedimientos para controlar la instalación de software en los sistemas operativos (Esto es para minimizar el riesgo de corrupción de los sistemas operativos)		
31.2	10.4.2	Protección de Datos de Prueba de Sistemas	Los sistemas de testeo de datos, están debidamente protegidos y controlados?		
31.3	10.4.3	Control de Cambios a Datos Operativos	Existen controles para la utilización de información y cambios de datos operativos?		
31.4	10.4.4	Control de Acceso a Código Fuente	Existen controles estrictos de modo a restringir el acceso al código fuente? (esto es para prevenir posibles cambios no autorizados)		
32	**10.5**	**Seguridad de los Procesos de Desarrollo y Soporte**			
32.1	10.5.1	Procedimientos de Control de Cambios	Existen procedimientos de control estricto con respecto a cambios en los sistemas de información? (Esto es para minimizar la posible corrupción de los sistemas de información)		
			Estos procedimientos aborda la necesidad de evaluación de riesgos, análisis de los impactos de los cambios?		
32.2	10.5.2	Revisión Técnica de los Cambios en el Sistema Operativo	Existen procesos a seguir o procedimientos para revisión y testeo de las aplicaciones críticas de negocio y seguridad, luego de cambios en el Sistema Operativo? Periódicamente, esto es necesario cada vez que haya que hacer un parcheo o upgrade del sistema operativo.		
32.3	10.5.3	Restricciones del Cambios de Paquetes de Software	Las modificaciones a los paquetes de software, son desalentadas o limitadas extrictamente a los cambios mínimos necesarios?		
			Todos los cambios son estrictamente controlados?		
32.4	10.5.4	Canales Ocultos y Código Malicioso	Existen controles para prevenir la fuga de información?		
			Controles tales como escaneo de dispositivos de salida, monitoreo regular del personal y actividades permitidas en los sistemas bajo regulaciones locales, monitoreo de recursos, son considerados?		
32.5	10.5.5	Desarrollo Externo de Software	¿El desarrollo de software tercerizado, es supervisado y monitoreado por la empresa?	Controlar aplicaciones y disclaimer contractual	
			¿Puntos como: Adquisición de licencias, acuerdos de garantía, requerimientos contractuales de calidad asegurada, testeo antes de su instalación definitiva, revisión de código para prevenir troyanos, son considerados?	Revisión de los contratos para tener en cuenta los Service Level Agreements (Acuerdos de Niveles de Servicio).	

Gestión de Incidentes de Seguridad de Información					
33	**11.1**	**Reportando Eventos de Seguridad y Vulnerabilidades**			
33.1	11.1.1	Comunicación de Incidentes Relativos a la Seguridad	Los eventos de seguridad de información, son reportados a través de los canales correspondientes lo más rápido posible?		
			Son desarrollados e implementados procedimientos formales de reporte, respuesta y escalación en incidentes de seguridad?		
33.2	11.1.2	Comunicación de Debilidades en Materia de Seguridad	Existen procedimientos que aseguren que todos los empleados deben reportar cualquier vulnerabilidad en la seguridad en los servicios o sistemas de información?		
34	**11.2**	**Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras**			
34.1	11.2.1	Responsabilidades y Procedimientos para incidentes de seguridad de la informacion	Están claramente establecidos los procedimientos y responsabilidades de gestión para asegurar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad de información?		
			Es utilizado el monitoreo de sistemas, alertas y vulnerabilidades para detectar incidentes de seguridad?		
			Los objetivos de la gestión de incidentes de seguridad de información, están acordados con las gerencias?		
34.2	11.2.2	Aprendiendo de los Incidentes	Existen mecanismos establecidos para identificar y cuantificar el tipo, volumen y costo de los incidentes de seguridad?		
			La información obtenida de la evaluación de incidentes de seguridad que ocurrieron en el pasado, es utilizada para determinar el impacto recurrente de incidencia y corregir errores?		
34.3	11.2.3	Recolección de Evidencia	Si las medidas de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica una acción legal (ya sea civil o penal)		
			Las evidencias relacionadas con incidentes, son recolectadas, retenidas y presentadas conforme las disposiciones legales vigentes en las jurisdicciones pertinentes?		
			Los procedimientos internos son desarrollados y seguidos al pié de la letra cuando se debe recolectar y presentar evidencia para propósitos disciplinarios dentro de la organización?		
Administración de la Continuidad de las Actividades de la Empresa					
35	**12.1**	**Aspectos de Seguridad en la Gestión de la Continuidad del Negocio**			
35.1	12.1.1	Proceso de la Administración de la Continuidad de la empresa	Existen procesos que direccionan los requerimientos de seguridad de información para el desarrollo y mantenimiento de la Continuidad del Negocio dentro de la Organización?		
			Estos procesos, entienden cuales son los riesgos que la organización enfrenta, identifican los activos críticos, los impactos de los incidentes, consideran la implementación de controles preventivos adicionales y la documentación de los Planes de Continuidad del Negocio direccionando los requerimientos de seguridad?		

35.2	12.1.2	Continuidad de las Actividades y Análisis de los Impactos	Los eventos que puedan causar interrupción al negocio, son identificados sobre la base de probabilidad, impacto y posibles consecuencias para la seguridad de información?		
35.3	12.1.3	Elaboración e Implementación de los Planes de Continuidad de las Actividades de la empresa	Son desarrollados planes para mantener y restaurar las operaciones de negocio, asegurar disponibilidad de información dentro de un nivel aceptable y en el rango de tiempo requerido siguiente a la interrupción o falla de los procesos de negocio?		
			Considera el Plan, la identificación y acuerdo de responsabilidades, identificación de pérdida aceptable, implementación de procedimientos de recuperación y restauración, documentación de procedimientos y testeo periódico realizado regularmente?		
35.4	12.1.4	Marco para la Planificación de la Continuidad de las Actividades de la empresa	Existe un marco único del Plan de Continuidad de Negocios?		
			Este marco, es mantenido regularmente para asegurarse que todos los planes son consistentes e identifican prioridades para testeo y mantenimiento?		
			El Plan de Continuidad del Negocio direccionan los requerimientos de seguridad de información identificados?		
35.5	12.1.5	Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la empresa	Los Planes de Continuidad del Negocio, son probados regularmente para asegurarse de que están actualizados y son efectivos?		
			Los tests de planes de continuidad de negocio, aseguran que todos los miembros del equipo de recuperación y otros equipos relevantes sean advertidos del contenido y sus responsabilidades para la continuidad del negocio y la seguridad de información, son concientes de sus roles y funciones dentro del plan cuando este se ejecuta?		
Cumplimiento					
36	**13.1**	**Cumplimiento con Requerimientos Legales**			
36.1	13.1.1	Identificación de Legislación Aplicable	Todas las leyes relevantes, regulaciones, requerimientos contractuales y organizacionales son tenidos en cuenta de modo a que estén documentados para cada sistema de información en la organización?		
			Los controles específicos y responsabilidades individuales de modo a cumplir con estos requerimientos, son debidamente definidos y documentados?		
36.2	13.1.2	Derechos de Propiedad Intelectual	Existen procedimientos para asegurar el cumplimiento de los requerimientos legales, regulatorios y contractuales sobre el uso de materiales y software que estén protegidos por derechos de propiedad intelectual?	Musica mp3, imágenes, libros, software, etc.	
			Estos procedimientos, están bien implementados?		
			Controles tales como: Política de Cumplimiento de Derechos de Propiedad Intelectual, Procedimientos de Adquisición de Software, Política de concientización, Mantenimiento de Prueba de la Propiedad, Cumplimiento con Términos y Condiciones, son consideradas?		

36.3	13.1.3	Protección de los Registros de la empresa	Los registros importantes de la organización están protegidos contra pérdida, destrucción y falsificación en concordancia con los requerimientos legales, regulatorios, contractuales y de negocio?	Backup y Auditoría	
			Están previstas las consideraciónes con respecto al posible deterioro de medios de almacenamiento utilizados para almacenar registros?	Unidades de Cintas que ya no tienen repuestos, Storage de Discos fallan y ya no hay.	
			Los sistemas de almacenamiento son elegidos de modo a que los datos requeridos puedan ser recuperados en un rango de tiempo aceptable y en el formato necesario, dependiendo de los requerimientos a ser cumplidos?		
36.4	13.1.4	Protección de Datos y Privacidad de la Información Personal	La protección de los datos y la privacidad, están asegurados por legislaciones relevantes, regulaciones y si son aplicables, por cláusulas contractuales?		
36.5	13.1.5	Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información	El uso de instalaciones de proceso de información para cualquier propósito no autorizado o que no sea del negocio, sin la aprobación pertinente, es tratada como utilización impropia de las instalaciones?		
			Los mensajes de alerta de ingreso, son desplegados antes de permitir el ingreso a la red o a los sistemas? El usuario tiene conocimiento de las alertas y reacciona apropiadamente al mensaje en pantalla?		
			Es realizado un asesoramiento jurídico, antes de aplicar cualquier procedimiento de monitoreo y control?		
36.6	13.1.6	Regulación de Controles para el Uso de Criptografía	Los controles criptográficos son usados en cumplimiento de los acuerdos contractuales establecidos, leyes y regulaciones?		
37	**13.2**	**Revisiones de la Política de Seguridad y la Compatibilidad Técnica**			
37.1	13.2.1	Cumplimiento de la Política de Seguridad	Los Administradores se aseguran que todos los procedimientos dentro de su area de responsabilidad, se llevan a cabo correctamente para lograrl el cumplimiento de las normas y políticas de seguridad?		
			Los Administradores, revisan regularmente el cumplimiento de las instalaciones de procesamiento de información dentro del area de su responsabilidad de modo a cumplir con los procedimientos y políticas de seguridad pertinentes?		
37.2	13.2.2	Verificación de la Compatibilidad Técnica	Los sistemas de información son regularmente revisados con respecto al cumplimiento de estándares de seguridad?		
			La verificación técnica es llevada a cabo por, o bajo la supervisión de, personal técnico competente y autorizado?		

38	**13.3**	**Consideraciones de Auditoría de Sistemas**			
38.1	13.3.1	Controles de Auditoría de Sistemas	Los requerimientos y actividades de auditoría, incluyen verificación de sistemas de información que fueron previamente planeados cuidadosamente de modo a minimizar los riesgos de interrupciones en el proceso de negocio?		
			Los requerimientos de auditoria son alcanzables y de acuerdo con una gestión adecuada?		
38.2	13.3.2	Protección de los Elementos Utilizados por la Auditoría de Sistemas	La información a la que se accede por medio de las herramientas de auditoría, ya sean software o archivos de datos, están protegidos para prevenir el mal uso o fuga no autorizada?		
			El ambiente de auditoría está separado de los ambientes operacionales y de desarrollo, a penos que haya un nivel apropiado de protección?	Servidores de auditoría (ACL, IDEA, etc.) separados de los ambientes de desarrollo y oltp.	
39	**13.4**	**Sanciones Previstas por Incumplimiento**			
39.1	13.4.1	Sanciones por Incumplimiento	¿Se tiene previsto sanciones por incumplimiento de medidas o procedimientos incumplidos para la seguridad de la Información?		