MODELO DE SEGURIDAD PARA SISTEMAS E-GOBIERNO MEDIANTE SATISFACIBILIDAD BOOLEANA

MÓNICA MARLENE BAQUERIZO ANASTACIO

MÁSTER EN INVESTIGACIÓN EN INFORMÁTICA, FACULTAD DE INFORMÁTICA,

UNIVERSIDAD COMPLUTENSE DE MADRID

Trabajo de Fin de Máster en Ingeniería Informática para la Industria

Curso académico: 2013/2014

Director:

José Antonio Martín Hernández

Autorización de difusión y utilización

La abajo firmante, matriculada en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: "***Modelo de Seguridad para sistemas de e-gobierno mediante satisfacibilidad booleana***", realizado durante el curso académico 2013-2014 bajo la dirección de José Antonio Martín Hernández en el Departamento de Arquitectura de Computadores, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

_____

Mónica Marlene Baquerizo Anastacio

Alumna

Curso Académico 2013/2014

Abstract

New technologies have transformed the way people interact. Goverments as part of their technology innovation have been making changes in the way they interact with the society. Currently, security in e-government systems is important because of their political, economic and social significance. This investigation summarizes the importance of the e-government systems, its benefits, disadvantages, and risks. Additionally, it has been analyzed the reason why this kind of systems must be considered part of a critical infrastructure such as government and inter-continental infrastructure. This investigation shows the trend for cloud infrastructure in government systems; security as a fundamental part in these systems; IT governance and management as strategical management of state resources. Based on the analysis made, it has been established five frameworks for evaluation, which are fundamentals for building a security model for e-government systems using boolean satisfiability. This model has been implemented and provided with the security indicators investigated in order to offer to the managers a tool that facilitate the process of analyzing the crucial factors for the security of their systems. This application will show the most important indicators for getting a satisfiable security system based on international frameworks and protocols. The purpose of the model is providing assistance during the decision-making process when a security factor needs to be added or removed.

Keywords

E-governmet, frameworks security, cloud security, governance TI, critical infrastructure, SAT, satisfiability problem.

Resumen

Las nuevas tecnologías han transformado la forma de interactuar de las personas. Los gobiernos como parte de su innovación tecnológica, también han realizado cambios en la forma que interactúan con la sociedad. Actualmente, los sistemas e-gobierno poseen transcendencia política, económica y social y es por estos motivos que la seguridad en estas aplicaciones es importante. Este trabajo resume la importancia de los sistemas e-gobierno, sus beneficios, desventajas y riesgos. Adicionalmente, se analiza porque este tipo de sistemas tienen que ser considerados dentro de las infraestructuras críticas, tales como gubernamentales e incluso inter-continentales y ser tratados como tal. Esta investigación expone, la tendencia del cloud en los sistemas gubernamentales; la seguridad como base para estos sistemas; el gobierno y la gestión TI como administración estratégica de los recursos estatales. En base a este análisis, se han construido 5 marcos de evaluación, que son fundamentales para la construcción de un modelo de seguridad para sistemas de e-gobierno mediante satisfactibilidad booleana. El modelo ha sido implementado y alimentado con los indicadores de seguridad investigados, con el fin de poner a disposición de los administradores, una herramienta que facilite el proceso de análisis de los factores que son cruciales para la seguridad de sus sistemas. Esta aplicación, revela los indicadores imperantes para que la seguridad sea satisfacible en sus sistemas, basándose en normas y protocolos internacionales. Con este modelo, se pretende ayudar a la toma de decisiones al momento de añadir o remover factores de seguridad.

Palabras clave

e-gobierno, marcos de evaluación de seguridad, seguridad en el cloud, gobierno y gestión TI, seguridad informática, SAT, satisfacibilidad booleana.

Agradecimientos

A Dios, roca fuerte y fortaleza eterna. Al Padre, por traerme a España no solo a estudiar, sino también a conocerte. A Jesús, por amarme, autor y consumador de mi fe, ejemplo a mi vida. Al Espíritu Santo, por guiarme y enseñarme, por llenarme de fuerza y poder.

A mis padres Vinicio y Gladys, por su apoyo incondicional. A mis hermanas Belén y Daniela por ser inspiración. A mi tío Leonidas y mi abuelita Flora.

A Wendy, Vero, Duval, Jessica, César, Huguito, Jocelín, Maricela, Nathali, Alina, Tomás, Pamela, por ser amigos. A Óscar por estar siempre presente.

A mi familia, iglesia y amigos, por sus oraciones constantes. A los Pastores Óscar Azambuja, Teresa Reis y su familia; Rafael Cano, Tamara y familia.

A mi director de tesis José Antonio Martín Hernández, por su tiempo, dedicación, guía y conocimiento, que se reflejan en este trabajo.

A Javier García y José Antonio Rubio, por darme la oportunidad de conocer este tema, porque sus conocimientos también están plasmados en este escrito y en el artículo publicado. A Narciso Martí Oliet, por su apoyo.

A la Dra. María Del Pilar Cornejo, por el empuje y el apoyo incondicional.

A SENESCYT, por el financiamiento, por creer en la juventud.

A la Universidad Complutense de Madrid por brindar conocimiento.

A mí, por tener las ganas de cumplir un sueño que se vio hecho realidad, por la valentía, por querer crecer, por caminar en un mundo desconocido pero con fe, constancia y perseverancia. Gracias a todos por la educación que me han brindado, y por estar conmigo en el camino. Porque al educarse no solo ganas conocimiento, sino valores de vida, crecimiento humano y académico.

Este logro no es mío, sino es producto de mi fe. Tuve fe para venir a estudiar, necesité fe en el proceso y fe para ver la victoria.

Lista de acrónimos

ISO	Organización Internacional de Estandarización
IEC	Comisión Electrotécnica Internacional
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y comunicación
ITIL	Information Technology Infrastructure Library
COBIT	Control Objectives for Information and related Technology
SaaS	Software as a service
PaaS	Platform as a service
IaaS	Infraestructure as a service
ORVE-SIR	Oficina de Registro Virtual de Entidades
TI	Tecnologías de la Información
SAT	Boolean satisfiability problem

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Con el avance de la tecnología, los gobiernos innovaron la manera de brindar atención al público, creando portales que brindan diferentes tipos de servicios a las instituciones y ciudadanos en general. Esta transformación de relaciones del sector público internas y externas a través de las tecnologías de la información, aumentando la eficiencia, eficacia de la gestión administrativa y la participación ciudadana se la denomina gobierno electrónico[1].

Como ejemplos de un sistema de gobierno electrónico, tenemos los sistemas: de la policía nacional que entregan los certificados de récord policial; el portal de la institución que cobra impuestos, que da la opción de declararlos por Internet, el registro civil que vía online entrega certificados de nacimiento, estado civil; el pago de impuestos prediales a cargo del municipio local, etc.

Éstos, no son los únicos tipos de servicios que se han derivado de la evolución tecnológica. Actualmente, los nuevos paradigmas de "voto electrónico" y "democracia electrónica", están teniendo mucha acogida entre las sociedades. Si el usuario tiene una buena experiencia utilizando un sistema e-gobierno, habría una predisposición para utilizar un sistema de democracia electrónica o de voto electrónico.

La información que el gobierno tiene de la sociedad es de diferente índole y proviene de diferentes instituciones. Debido a que el gobierno se relaciona con todos en una sociedad, éste tiene información pública, privada y clasificada de cada uno de ellos.

Sin duda alguna, la evolución e innovación de sistemas está dada por muchos factores como la tecnología, efectividad en los servicios brindados,

satisfacción del usuario, etc., y esta se ha dado gradualmente. A partir de que los datos están expuestos a Internet, la vulnerabilidad de éstos crece, ya que podrían sufrir ataques cibernéticos. Cualquiera que fuera la tecnología usada, los sistemas e-gobierno tienen que ser seguros debido a la sensibilidad de los datos que manipulan.

Ahora, cómo realizar un análisis de seguridad?. Una manera es construyendo un modelo que nos permite analizar una gran cantidad de indicadores, pudiendo utilizar el problema SAT, que, dada las variables, las analizan e indican si las cláusulas relacionadas, son satisfacibles o no. En nuestro caso, se analizará según las variables que elijan los administradores de un sistema, qué variables de seguridad son decisivas y tienen que ser reforzadas.

1.1. Objeto de la investigación

Debido a la naturaleza de los sistemas de gobierno electrónico, éstos, están expuestos a ciberataques permanentemente, siendo blanco atractivo para los terroristas electrónicos debido a la información que se manipula. A partir de que los datos están expuestos a Internet, la vulnerabilidad de éstos crece.

Sin duda alguna, la seguridad es un factor crucial al momento de tener online un sistema de gobierno electrónico, y el Estado tiene que garantizar seguridad a los datos que están expuestos en Internet debido a la sensibilidad de estos.

Hablar de seguridad informática, es enfocarse en la protección de toda la infraestructura computacional, tanto física como lógica. Un sistema de gobierno electrónico debería de tener un alto grado de seguridad, porque los datos de toda una nación están albergados en los servidores gubernamentales, siendo crítica toda su infraestructura.

Actualmente existen un sin número de marcos de seguridad, cada uno desde su óptica y su alcance; planteados por diferentes organizaciones. Estándares por países que hablan de lo que debería de tener todo sistema para que sea seguro, guardando la confidencialidad, integridad y disponibilidad. Cada uno asegura que si cumplen con sus normas, podrán alcanzar la seguridad requerida en los sistemas computacionales.

Es por este motivo, que se propone realizar 5 marcos de seguridad integrales para este tipo de sistemas, que contemple todos los factores de seguridad, que han sido identificados a lo largo de toda esta investigación proporcionado por los diferentes marcos e ISOS existentes. Los marcos serán de seguridad integral, cloud computing, gobierno y gestión TI, web e infraestructuras críticas. Con los indicadores obtenidos, se realizará un sistema, que indique la satisfacibilidad con las variables ingresadas por el usuario, y analizar de qué manera se puede ayudar a la seguridad de los sistemas gubernamentales, analizados con esta herramienta.

1.2. Trabajos relacionados

Actualmente, existen estándares relacionados con la administración de las tecnologías de la información orientados a la entrega y soporte de servicios de calidad, reducción de vulnerabilidades, mitigación de riesgos, etc. que tienen como objeto estandarizar los diversos procesos adaptándose a las mejores prácticas.

Las normas ISO las realizan los organismos internacionales miembros de ISO e IEC que participan en el desarrollo de estándares internacionales a través de los comités establecidos para lidiar con áreas particulares de una actividad técnica [3]. Las normas internacionales dan el estado de las especificaciones del arte de productos, servicios y buenas prácticas, ayudando a hacer que la

industria sea más eficiente y eficaz. Existen varias ISO para tratar diferentes temáticas.

Así también hay empresas que han desarrollado marcos de referencias para la administración de recursos y generación de valor. El marco más reconocido en ese sentido es COBIT [4]. Otro marco que se ha preocupado por establecer normas de calidad de servicio es ITIL [5]. A continuación se menciona el propósito de algunas ISOS y marcos de referencia aplicables a los sistemas de gobierno electrónico:

Actualmente, manejar la seguridad de todo un sistema integralmente no es fácil. Si bien es cierto se lo puede controlar a través de firewalls, enrutadores, IDS, implementando la última tecnología, etc. no significa que nuestro sistema sea seguro. En los últimos años se ha desarrollado la cultura de la administración de sistemas, que se ha comprobado que teniendo una buena cultura de administración de cualquier servicio que brindemos, se tendrá mejores resultados y una institución mejor organizada, en caso de que se implemente algún control de este tipo.

Muchas de las empresas que a nivel mundial, e incluso a nivel intercontinental, país, ciudad, e institucional [6] [7] [8] [9] se realizan normas para poder administrar de una mejor manera las TICs con los procesos que existen en el negocio.

También hay que tener en consideración que, debido a la información que un sistema gubernamental maneja, hace que ésta sea una infraestructura crítica, ya que la alteración o eliminación de datos sería entrar en una catástrofe de seguridad informática a nivel país.

Otro aspecto importante es la tendencia que tiene cloud computing en la actualidad. Empresas públicas y privadas están migrando sus datos al cloud,

debido a los beneficios económicos y cómodos que representa a la institución, y los sistemas de gobierno electrónico, también están optando por la implementación del cloud. Un ejemplo es la red SARA que es un proyecto de interés prioritario para construir el cloud privado de la administración pública española.

Se trata por lo tanto de encontrar un consenso de marcos de seguridad existentes, es decir, factores de seguridad de todos los estándares y marcos existentes considerando también que este sistema es una infraestructura crítica y que podría estar en el cloud.

Con los marcos evaluadores, se implementará una aplicación que ayude a los administradores a analizar mediante el problema de la satisfacibilidad booleana, qué factores afectan crucialmente a la seguridad según los indicadores que ellos elijan. Este sistema permitirá tener una visión global si la seguridad sigue siendo satisfacible según los indicadores que ellos elijan.

1.3. Estructura del trabajo

La investigación está organizada en 4 capítulos con la estructura que se comenta a continuación.

El Capítulo 2 realiza un estado del arte de la administración y gobierno electrónico que incluye la manera de administrar antes los recursos gubernamentales y el desarrollo del gobierno electrónico, beneficios, desventajas y riesgos. También se aborda el tema de infraestructuras críticas, sus antecedentes, definición y porqué consideramos que los sistemas e-gobierno son críticos y la importancia de que los sistemas gubernamentales sean tratados como tal. Así mismo se centra en explicar la importancia del cloud, y del por qué los gobiernos están migrando hacia esta nueva tendencia. Una parte

importante es el tema de seguridad informática, bases de la seguridad de la información y la relación de éstas con los sistemas gubernamentales. También abarca la importancia de la implementación de gobierno y gestión TI en el estado y los marcos actuales. Seguido, se habla del problema de la satisfacibilidad, sus inicios, planteamiento, y sat solvers.

El Capítulo 3, contiene la propuesta de este trabajo Fin de Máster: los marcos de evaluación de seguridad, y el sistema que ayuda a los administradores a conocer las variables que influyen en la seguridad de sistemas e-gobierno, según los indicadores elegidos.

El Capítulo 4 muestra las conclusiones extraídas de este trabajo.

2. MARCO TEÓRICO

2.1. Administración y Gobierno Electrónico

2.1.1. Administración

La administración se trata de suministrar, proporcionar o distribuir servicios a las partes interesadas, en este caso entre el estado y la sociedad. Para esto, el estado tiene que identificar qué bienes tiene que administrar y limitar el alcance de la administración.

El gobierno como tal, tiene un sin número de servicios que administrar, como médicos, policiales, prediales, agrícolas, militares, etc. Todos los servicios a administrar tienen que organizarlos, velar por sus intereses, estimularlos y vigilar la coordinación entre los entes relacionados sin perder su enfoque principal [10].

El gobierno había manejado la administración de manera tradicional hasta finales de la década de los 70 y medios de los 80, en la que se empiezan a realizar inversiones en computadores para automatizar procesos de gestión. Con el avance de la tecnología, Estados Unidos en 1993 inició el programa "National Performance Review" (NPR), con el fin de mejorar la calidad de los servicios a la sociedad; al igual que Japón con el proyecto "Plan de Promoción en Administración e Informatización" (1993); la Unión Europea (1995) con "Programa de Intercambio de Datos entre Administraciones", y América Latina a finales de los 90 [11].

A partir de que los servicios se digitalizaron, la administración en ellos también sufriría un cambio, debido a la interacción entre las TIC, el gobierno y

la sociedad. A causa de que las TIC llegan a ser estratégicas para brindar un servicio eficiente y eficaz, es importante la administración correcta de las mismas.

Es por este motivo, que surgieron marcos de referencias como ITIL, en la década de los 80, el cual tiene como objetivo proporcionar prácticas para la Gestión de Servicios de TI de alta calidad. En 1996 aparece COBIT, que proporciona una estructura para comprender, implantar y evaluar capacidades, rendimiento y riesgos de TI, separando la parte administrativa con la ejecutora en una institución. Buscando estandarizar los procesos, aparece la ISO 27001, que tiene como propósito reducir la vulnerabilidad en la seguridad de la información; así como la ISO 20000 en el 2005, que busca garantizar la entrega de servicios bien gestionados. [12]. Así también la ISO 38500 en el 2008, que proporciona principios para la administración al evaluar, dirigir y supervisar el uso de la tecnología de la información (TI) [13].

Como se puede observar tener una buena administración relacionando las TI al modelo de servicios que el gobierno brinda, a los procesos que se están ejecutando, a la calidad del servicio, a la seguridad implantada, es de fundamental importancia. En la actualidad, hay algunos países que han desarrollado sus propios marcos referenciales apoyados en los estándares ISO, en leyes que se han creado para soportar este nuevo modelo de interacción entre el gobierno y la sociedad denominado gobierno electrónico.

2.1.2. Gobierno Electrónico

Con el avance de la tecnología, los gobiernos innovaron la manera de interactuar con las instituciones y ciudadanos en general, creando portales que brindan diferentes tipos de servicios a las instituciones y ciudadanos en general. Un sistema de gobierno electrónico podría definirse como "*La innovación de los servicios públicos a través de las TICs, que permite una relación directa entre el gobierno estatal y la sociedad, aumentando la eficiencia, eficacia de la gestión administrativa y la participación ciudadana*" [14].

Durante años, el gobierno había atendido a sus ciudadanos de una manera tradicional: de persona a persona. Los ciudadanos tenían que trasladarse a las oficinas gubernamentales, esperar para ser atendidos, y finalmente (si ese trámite no dependía de otro), el proceso estaba completo. Actualmente los gobiernos han transformado la manera de brindar servicios a los individuos que requieren algún tipo de trámite, pasando del trato personal a brindar un servicio online [14].

Como parte de la innovación tecnológica, se han implementado portales que brindan servicios a través de Internet. El ciudadano puede realizar el trámite desde cualquier dispositivo que tenga acceso a la red: laptop, móviles, tablets, etc. Ésta es la corriente a nivel mundial, no sólo de los gobiernos, sino de todas las sociedades que tienen acceso a la red, brindar servicios en donde el punto focal siempre va a ser la satisfacción de los individuos.

La información que el gobierno tiene de la sociedad es de diferente índole y proviene de diferentes instituciones. Algunos estudios han analizado los entes con quienes el gobierno tiene relación, que se resumen en [2]:

- Gobierno a gobierno

- Gobierno a ciudadanos

- Gobierno a Empresas, privadas y mixtas

- Gobierno a otras instituciones, internacionales, sin fines de lucro.

Como se puede observar, el gobierno se relaciona con todos en una sociedad, y éste tiene información pública, privada y clasificada de cada uno de ellos.

Los sistemas de gobierno electrónico han sido el inicio de otras maneras de interactuar con la sociedad, entre los cuales tenemos voto electrónico, democracia electrónica, participación electrónica, parlamento electrónico, ciudad digital, que tienen acogida entre las sociedades [11]. Este es un punto a favor del gobierno, porque así tiene una sociedad dispuesta a cambiar la manera de interactuar usando las TICs teniendo al ciudadano como punto focal para poder brindar un sin número de servicios.

2.1.2.1. Beneficios

Tener una herramienta que potencia la administración pública, ya es un beneficio tanto para el gobierno como para el ciudadano, y no tan solo eso, sino que al utilizar este tipo de sistemas se gestiona la democracia y genera valor [11].

Los beneficios identificados al tener un sistema e-gobierno, tanto para el gobierno como para el ciudadano son los siguientes [15] [16]:

Beneficios para el gobierno:

- Incrementa la calidad de servicios públicos
- Promueven una mayor participación ciudadana
- Transición hacia la sociedad de la información

- Reduce costos operacionales y administrativos
- Agilidad y capacidad de ejecución de trámites, relacionando información entre dos o más instituciones.
- Coordinación de instituciones relacionadas como policía, hospitales, cruz roja, tránsito, etc.
- Incrementa la satisfacción del ciudadano
- Buena imagen y reputación

Beneficios para el ciudadano

- Reduce costos y tiempo
- Menos Corrupción
- Incrementa la transparencia
- Atención al ciudadano
- Reduce el tiempo del trámite
- Acceso desde cualquier parte del mundo

Beneficios para el gobierno

Al tener un sistema de gobierno electrónico, el estado brinda los servicios por Internet, haciendo que los trámites puedan realizarse con eficacia y eficiencia. Esto aumenta la calidad del servicio, ya que el gobierno no solo brinda atención en sus oficinas, sino que pone a disposición de la sociedad, todo un catálogo de servicios on-line.

Al ofrecer el gobierno una gama de servicios por Internet, éstos se proliferan fácilmente a través de la red, haciendo que haya una mayor participación ciudadana [17]. Consecuentemente, los ciudadanos comienzan a utilizar los diferentes servicios, no solo de e-gobierno, sino también de voto por Internet, parlamento electrónico, etc. Como resultado, el gobierno no solo tendrá presencia física como tal, sino presencia virtual a través de sus servicios o de

redes sociales como Facebook, Twitter, Flickr, etc., comentando las bondades de sus sistemas, afianzándose en el mundo virtual.

Esta nueva manera de interactuar de las sociedades, predisponen a los ciudadanos a utilizar las tecnologías, aprovechándolas al máximo, creando el concepto de poder tener a una institución y sus servicios virtualmente. Sabiendo administrar la información recolectada de los diferentes sistemas gubernamentales, el gobierno puede llegar a construir un "país virtual", creando un nuevo concepto.

Tener sistemas autónomos que realicen operaciones, reduce costos operacionales y administrativos, ya que el portal realiza las peticiones de los ciudadanos. Esto influye en el costo antes requerido de infraestructura como oficinas, servicios básicos: luz eléctrica, agua, teléfono, suministros de oficina, seguridad, etc. Este costo es reducido a una oficina, ambiental y técnicamente equipado con un servidor con la capacidad suficiente para dar servicio a los ciudadanos.

El personal administrativo también se ve reducido, ya que el portal sería como tener un empleado gubernamental atendiendo a cada ciudadano que se conecta para realizar una transacción, con la diferencia que el portal no cobra sueldo, servicio social, horas extras, etc. Para ejemplificar, en el reporte que emite la Casa Blanca en el año 2007, el gobierno de Estados Unidos ahorró U.S $133 millones sólo en costos de software [18].

Antes, la atención al ciudadano de forma tradicional, podía depender de dos o más instituciones, dilatando el trámite, gastando recursos de personal, movilización, tiempo, entre otros, hasta tener listo el requerimiento. Un sistema de gobierno electrónico bien diseñado e implementado, coordina actividades internas entre sus instituciones, recolectando los datos necesarios para dar trámite a la petición solicitada. La respuesta coordinada de los sistemas permite

controlar de manera armónica a las instituciones involucradas, de forma inmediata para dar respuesta a la petición solicitada.

Al dar un servicio eficiente y eficaz al usuario que interactúa con el sistema e-gobierno, incrementa la satisfacción de éste, cumpliendo con la meta principal para lo cual fueron creados estos sistemas. Facilitar una buena atención al usuario, provee una buena imagen de la institución que lo brinda, así también su reputación se ve beneficiada.

Beneficios para el ciudadano

Un beneficio bastante práctico para el ciudadano, es que al estar el sistema en la web, puede ser accedido desde cualquier parte del mundo si el usuario tiene Internet, lo que facilita poder realizar el trámite a cualquier hora desde un dispositivo móvil, ordenador, tablet, etc. Si el sistema se promociona de esta manera, es indispensable la disponibilidad del mismo.

El sistema al estar online, no necesita de terceras personas para su correcto funcionamiento, evitando la corrupción. Esto trae beneficios tanto al ciudadano como para el gobierno. El ciudadano no es estafado por terceros y el gobierno sigue guardando su reputación e integridad en sus instituciones.

El tener un sistema que a través de éste, el gobierno pueda informar a sus mandantes de temas relevantes, mantiene a la sociedad informada acerca de las últimas políticas, manera de gobernar, decisiones gubernamentales, etc. [19].

Utilizar un sistema de gobierno electrónico, ahorra tiempo y dinero al usuario y al gobierno, así como también afianza el grado de confiabilidad del ciudadano en los sistemas gubernamentales. Un reporte de la Unión Europea indicó que sus ciudadanos ahorran siete millones de horas anuales al utilizar el sistema de pago de impuestos, y por declararlos online, los ciudadanos

ahorraron 10 € por transacción [16].

A continuación se resume los beneficios de un sistema de gobierno electrónico y lo que produce en el gobierno, como en el ciudadano.

Beneficios de gobierno electrónico	**Gobierno**	**Ciudadano**
Calidad de servicios públicos	Eficiente y eficaz	Satisfacción
Participación ciudadana	Involucra a todos	Involucrarse en decisiones
Reduce costos	Operacionales y administrativos	Movilidad y transaccionales
Capacidad de ejecución de trámites, entre dos o más instituciones.	Agilidad	Satisfacción
Buena imagen y reputación	Satisfacción	Satisfacción
Reducción de tiempo	Eficiente	Satisfacción
Menos Corrupción	Credibilidad	Satisfacción
Incrementa la transparencia	Credibilidad	Satisfacción
Atención al ciudadano	Satisfacción	Satisfacción
Acceso desde cualquier parte del mundo	Disponibilidad	Satisfacción
Resultados	**Competitividad y Capacidad**	**Mejora la calidad de vida**

Tabla. 2.1. Resumen de beneficios de un sistema de gobierno electrónico.

Los beneficios que e-gobierno conlleva son excelentes para una sociedad, pero así también hay que analizar las desventajas del mismo, que se detallan en la siguiente sección.

2.1.2.2. Desventajas

A continuación, se analizan las desventajas podría tener un sistema de gobierno electrónico [11]:

- Despliegue de redes y servicios para garantizar la conectividad digital
- Analfabetismo y no interacción con la tecnología
- Resistencia al cambio de parte de los trabajadores
- Condiciones organizacionales
- Marco Legal
- Financiamiento
- Transformación de la administración (Reformas sociales y normativas)
- Cambio de gobernantes

Las redes y telecomunicaciones son aquellas que permiten el acceso a los diversos servicios que se encuentran en la web. El gobierno solo puede llegar a los ciudadanos, si éstos tienen la cobertura y la calidad que se necesita para poder acceder a los servicios.

Sin duda alguna, los usuarios de Internet aumenta día a día. En 1995, los usuarios de Internet eran 16 millones de personas, lo cual correspondía al 0.4% de la población mundial. Al 2012, el número de usuarios de Internet ya son 2.439 millones, correspondiente al 34.8% de la población mundial. A continuación una tabla, en la que se observa el crecimiento de usuarios de Internet, y una gráfica de la distribución de la misma [20].

Date	**Número de Usuarios**	**% Población mundial**	**Fuente**
Diciembre, 1995	16 millones	0.4%	IDC
Diciembre, 2000	361 millones	5.8%	Internet World Stats

Diciembre, 2005	1,018 millones	15.7%	Internet World Stats
Septiembre, 2010	1971 millones	28.8%	Internet World Stats
Diciembre, 2011	2.267 millones	32.7%	Internet World Stats
Septiembre, 2012	2.439 millones	34.8 %	Internet World Stats

Tabla. 2.2. Cantidad de Usuarios de Internet por periodos desde 1995

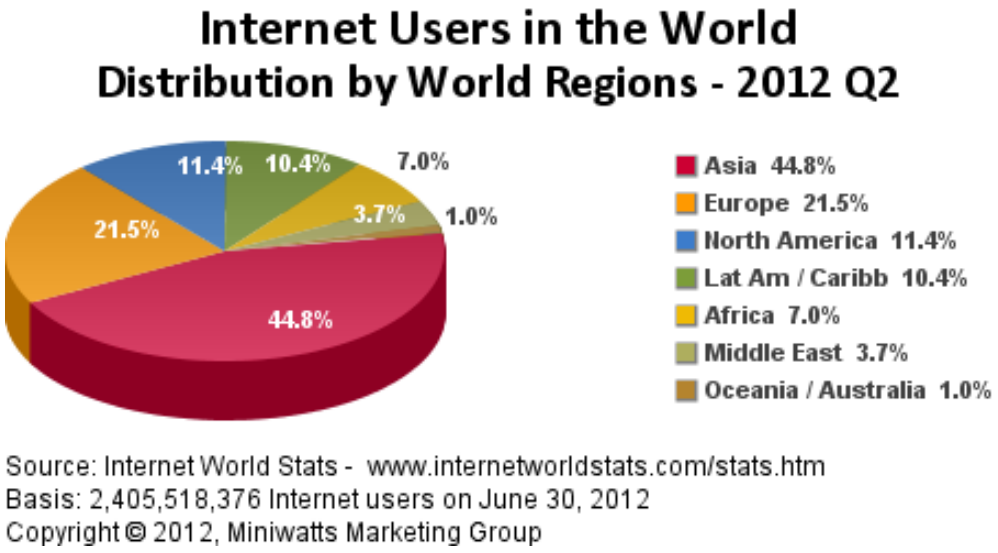


Fig. 2.1. Usuarios de Internet en el mundo

Estos resultados demuestran que no toda la población tiene acceso a Internet, lo cual es un punto débil de los sistemas de gobierno electrónico, ya que a pesar de que los sistemas funcionan 24 horas, 7 días a la semana, no todos tienen acceso.

Otra barrera es el analfabetismo existente. Según datos del Instituto de Estadística de la UNESCO, 793 millones de adultos son analfabetos. Otros 67 millones de niños en edad de asistir a la escuela primaria no lo hacen y 72

millones de adolescentes en edad de cursar el primer ciclo de la enseñanza secundaria tampoco están gozando de su derecho a la educación. Este problema está más acentuado en Asia, que alberga más del 50% de la población analfabeta del mundo. A continuación una tabla que ilustra la situación de analfabetismo a nivel mundial [21].

Región	Porcentaje
Sur y el oeste de Asia	51.8
África Subsahariana	21.4
Asia Oriental y el Pacífico	12.8
Estados Árabes	7.6
América Latina y el Caribe	4.6
América del Norte, Europa y Asia Central	2.0

Tabla. 2.3. Porcentaje de analfabetismo a nivel mundial

El analfabetismo es una barrera grande para la introducción de un sistema de gobierno electrónico para los continentes de Asia y África. El gobierno tendrá que seguir atendiendo de manera tradicional a sus ciudadanos, y el cambio en estas sociedades será a medida de que el grado de cultura aumente. Así también los individuos que no tienen relación con la tecnología, que básicamente serían los adultos mayores [22], y las personas que a pesar de que saben leer y escribir no tienen contacto con la tecnología y no saben cómo usarla.

El hecho de que la modernización llegue a los servicios públicos también afecta a los trabajadores, principalmente a las personas que tienen experiencia

limitada en el uso de sistemas informáticos. En este caso podría haber resistencia de los trabajadores a un cambio tecnológico. El gobierno debería de estar preparado y tener las condiciones organizaciones necesarias tanto en infraestructura de software, hardware, capacitaciones, y políticas que permitan dar la entrada a un sistema que va a aumentar la calidad del servicio, y no crear una resistencia al cambio para sus empleados.

Como cualquier producto o servicio existente en el mercado, los sistemas de gobierno electrónico, tienen que tener leyes y normativas a las cuales regirse. Los países tienen que contar con un marco legal referente a la protección de datos, el acceso compartido de las bases de información, riesgos asociados, derechos de propiedad intelectual, etc. Se tiene que estar consciente de que si un sistema va a brindar un servicio al ciudadano, tienen que existir políticas que tienen que cumplir tanto los ciudadanos como el gobierno. Este ámbito podría también ser un impedimento, ya que no todos los países tienen experiencia en leyes informáticas [11].

Contratar a los expertos en leyes, hardware, software, capacitación, personal capacitado, etc., trae consigo una gran inversión que tiene que realizar el estado. Primero que tiene que planificarlo bien, porque sería un desperdicio de dinero invertir millones en algo que va a quedar en el olvido o no va a cumplir con el objetivo. Este tipo de inversiones tienen un mantenimiento constante, por lo que el estado que decida implementar un sistema de gobierno electrónico, tiene que en su presupuesto anual tener en consideración la inversión que se va a realizar en TICs año a año.

Como una inversión tan importante no se puede perder, se tiene que asegurar que los próximos gobiernos tengan el compromiso de seguir apoyándose en las TICs, ya que si no se tiene el soporte del gobierno central, es muy difícil que los sistemas lleguen a proyectarse para lo que han sido desarrollados: dar servicio.

2.1.2.3. Riesgos

El riesgo es el posible impacto o resultado de un evento en los bienes de una organización, con sus respectivas consecuencias [23]. Por lo general se lo mide en términos monetarios, pero en este caso, "la modificación, destrucción, robo o falta de disponibilidad de los activos informáticos, tales como hardware, software, datos y servicios" tendría un valor más significativo. Un sistema de gobierno electrónico no está excepto a los riesgos que conlleva tener sistemas en Internet, ya que por la sensibilidad de los datos que se manipulan, el estado tiene que tratar sigilosamente la información. A continuación un listado de los riesgos a los que el sistema de gobierno electrónico está expuesto [16] [24] [25] [26] [27]:

- Penetración a los sistemas computacionales.
- Alteración de datos personales, confidenciales
- Fraudes, estafas a los ciudadanos.
- Entidades públicas fuera de Servicio, etc.
- Mala administración e implementación

Si un sistema de gobierno electrónico que fuera penetrado por intrusos, tendría un gran impacto social a nivel nacional, ya que dependiendo del ataque se podrían obtener, ingresar, modificar o eliminar datos de alto grado de sensibilidad. Los datos de empresas públicas, privadas, de ciudadanos, y otros quedarían al descubierto de terroristas con un fin desconocido. Como consecuencia de este ataque, se produciría un pánico social.

Otro riesgo es que tanto los empleados institucionales como personas externas, podrían modificar datos personales o confidenciales, por ejemplo, supongamos que hay una intrusión en los sistemas computaciones del registro civil, y logran ingresar datos de nacimiento de un grupo de ciudadanos, huellas digitales, etc. los cuales resultan ser narcotraficantes de alto mando que tienen

una nueva nacionalidad, nombre, estado, etc. Esto sería darle paso abierto a toda una red de mando narcotraficante "legal". O que a un empleado se le pague por ingresarlos. Como se ejemplifica, el ataque no solo puede provocarlo alguien externo, sino también empleados internos. En ambos casos, la seguridad institucional demuestra no ser la correcta.

Debido a que ciertos trámites tienen un costo, los ciudadanos están expuestos a fraudes informáticos, ya que si los sistemas no tienen la seguridad correspondiente, los ciudadanos están expuestos a "escuchas" en su comunicación, pudiendo captar los números de tarjetas de crédito y datos personales.

Actualmente, existen ciberterroristas que planean ataques a los portales que ellos definen como objetivos, de tal manera que los sistemas institucionales quedan fuera de servicio. Como ejemplos de ciberterrorismo, en el año 2000 un ex-empleado de una planta de aguas residuales australiana la ataca de forma inalámbrica. Tres años más tarde, el gusano Slammer provoca el apagado de la central nuclear de Davis-Besse. En enero de 2008 la CIA informa que un ciberataque causó la pérdida de electricidad en varias ciudades en una localización fuera de USA. Estos ciberataques aumentan año a año, por lo que las instituciones que brindan servicios, tienen que tomar medidas de seguridad para reducir el riesgo existente [28].

Todos estos riesgos a los que están expuestos los sistemas de gobierno electrónico traen consecuencias como pérdidas económicas, mala reputación, inseguridad en el gobierno, pánico social, protestas, entre otros.

Las consecuencias son de alto nivel. Las amenazas más comunes para los sistemas de gobierno electrónico son [23], [29], [30], [31]:

- Ataques DOS
- Acceso no autorizado a la red

- Robo de información
- Fraude financiero online
- Defacement del portal
- Ataques de aplicaciones web
- Penetración a los sistemas

Al administrar el riesgo, lo que se está haciendo es identificar todos los posibles escenarios que podrían afectar el rendimiento de los sistemas, ya sean físicos o lógicos y conocer la probabilidad de que estos ocurran y realizar los planes de mitigación. Mientras más vulnerables sean los sistemas, es más alto el riesgo.

De acuerdo con los informes anuales de investigación de SANS Institute, los tipos de vulnerabilidades que se explotan de un año a otro cambian. Debido a las amenazas cambian, las seguridades informáticas también tienen que renovarse desarrollando y adoptando nuevas medidas de seguridad [29]. Según la página web de SNAS, a Enero de 2013, estos veinte controles de seguridad críticos ya han comenzado a transformar la seguridad en las agencias gubernamentales y otras grandes empresas, centrándose su gasto en los controles claves que bloquean los ataques conocidos y encontrar los que reciben a través de [32]:

- Inventario de dispositivos autorizados y no autorizados
- Inventario de Software autorizado y no autorizado
- Configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores.
- Evaluación de la vulnerabilidad continua y Remediación
- Defensas malware
- Aplicación de Software de Seguridad
- Control de dispositivos Wireless
- Capacidad de recuperación de datos

- Seguridad de evaluación de habilidades y formación adecuadas
- Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches
- Limitación y Control de los puertos de red, protocolos y servicios
- Utilización controlada de privilegios administrativos
- Defensa de Fronteras
- Mantenimiento, Monitoreo y Análisis de registros de auditoría
- Acceso controlado
- Seguimiento y control de cuentas
- Prevención de Pérdida de Datos
- Respuesta a Incidentes y Gestión
- Garantizar la seguridad de la red
- Pruebas de penetración y red ejercicios de equipo

Estas 20 vulnerabilidades fueron acordadas por: NSA, CERT de EE. UU. JTFGNO, el Departamento de Energía Nuclear Laboratorios del Departamento de Estado, el Departamento de Defensa Centro de Delitos Cibernéticos, expertos forenses comerciales que sirven a las comunidades de las infraestructuras críticas y bancario [32]. Identificadas las vulnerabilidades de seguridad en Internet, las organizaciones saben en donde enfocarse para tomar medidas y prevenir ataques.

En base a estas vulnerabilidades identificadas, las organizaciones pueden mitigar y prevenir los riesgos existentes ante un posible ataque o debilidad que tenga la empresa y que ésta tenga controlado mediante acciones el evento. Es por este motivo que se debe de tener una administración del riesgo, para identificar mitigar y manejar el riesgo a un grado aceptable o tolerable para la institución. La gestión del riesgo no es una actividad defensiva, pero el proceso de desarrollo de una estrategia ajustada al riesgo, equilibra oportunidad con consecuencias de las acciones [23].

Los riesgos que pueden tener estos sistemas pueden ser de diferente índole. Si un sistema de gobierno electrónico tiene sus aplicaciones en el cloud, se debe de tener conocimiento a detalle de los riesgos a los que se está expuesto según el servicio que se ha contratado: IaaS, PaaS or SaaS. Para cada caso, se debería tener una estrategia de respuesta para mitigar el riesgo a los que se están expuestos tanto tangibles como servidores, infraestructura física, documental, personal, etc. e intangible, es decir, aplicaciones, sistemas, información, etc.

Sin duda alguna, la seguridad es un factor crucial al momento de tener online un sistema de gobierno electrónico, y el Gobierno tiene que garantizar seguridad a los datos que están expuestos en la web debido a la sensibilidad de estos.

Es por este motivo que es necesario conocer qué factores incluyen en la seguridad general de un sistema de gobierno electrónico, en su infraestructura y en sus aplicaciones web, para mitigar los riesgos y que se pueda brindar un servicio seguro a la sociedad.

2.2. INFRAESTRUCTURAS CRÍTICAS

2.2.1. Antecedentes

Las infraestructuras críticas siempre han existido, pero a lo largo del tiempo las formas de atacarlas han ido evolucionando conforme a los recursos existentes. Hace cincuenta años, las infraestructuras críticas eran atacadas mediante ejércitos con tanques, barcos, aviones, etc. [28]. Actualmente, los ataques han cambiado a formas más sofisticadas, usando la tecnología para estos fines.

En 1995, en un informe de la Casa Blanca, se mencionó ya la protección frente a ataques terroristas contra los EEUU y de la manifestación del gobierno de

tomar medidas para combatirlas mediante programas [33]. En 1998 la Casa Blanca, indica que mediante la tecnología, los terroristas pueden atacar las infraestructuras críticas de los Estados Unidos de Norteamérica afectando la economía de la nación y es por este motivo que se creó la Oficina de Coordinación Nacional para la Seguridad, Protección de Infraestructura contra el Terrorismo, siendo Estados Unidos el pionero en crear una oficina que supervise las políticas y programas para la protección de las infraestructuras. [34].

A pesar de tomar precauciones contra el terrorismo, en el 2001 Estados Unidos sufrió uno de los atentados más fuertes a nivel mundial: el ataque contra las Torres Gemelas World Trade Center en New York. Este acto terrorista puso al descubierto las fisuras de seguridad que tenía una potencia como Estados Unidos que fueron aprovechadas por terroristas que marcaron a toda una nación provocando pánico social, económico y político. El 8 de Octubre de 2011 el gobierno norteamericano constituyó la Office of Homeland Security, para que se encargue de la seguridad a nivel nacional [28]. Esto provocó que este país arme programas y estrategias para mitigar los riesgos existentes en las denominadas infraestructuras críticas.

Otro atentado terrorista, fue el ocurrido el 11 de Marzo de 2004, en España, que fue una serie de ataques en cuatro trenes de la red de Cercanías de Madrid, que dejaron 191 muertos y 1.858 heridos [35]. A raíz de este evento, la Comisión Europea (CE) quiso mejorar la seguridad en diferentes tipos de infraestructuras de la Unión Europea que considera "críticas".

2.2.2. Definición e importancia

Las instituciones interrelacionadas que brindan algún tipo de servicio vital, pueden generar un beneficio potencial, así como también producir un problema en casada, en caso de que el servicio que brindan se vea interrumpido. Estas

instituciones que son esenciales para el regular funcionamiento de una sociedad, son las infraestructuras críticas [36].

La Comisión Europea define como infraestructura crítica a aquellas instalaciones, redes, servicios, equipos físicos y tecnologías de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos [37].

Así como gozamos de los beneficios del avance de las TICs, debemos considerar que ésta también puede ser utilizada con fines maliciosos por terroristas. El uso de las tecnologías de información, comunicación, telecomunicaciones o afines que generan pánico entre la población se denomina ciberterrorismo o ciberataque, que es a lo que actualmente están expuestos los sistemas informáticos. Éstos podrían tener fines personales, económicos, religiosos, entre otros. Debido a los cyberataques, los países empiezan con la identificación, priorización y protección de las infraestructuras críticas [23].

Como ejemplo de infraestructuras críticas tenemos las hidráulicas, plantas nucleares, bancos, hospitales, transporte público, etc. Estas instituciones son importantes porque siempre deberían prestar servicio a la comunidad para que la sociedad se desarrolle con normalidad.

En la actualidad, las infraestructuras las han clasificado en sectores y subsectores según el ámbito de desempeño. Un país pudiera tener miles de infraestructuras críticas, pero por lo general, están clasificadas por afinidad como energética, nuclear, TIC, transporte, hidráulicas, salud, económico, químico, alimentación, judicial, etc. [36] [39].

Las infraestructuras críticas deben de tener un Plan Estratégico a incidentes en caso de que se presenten, coordinar y desplegar la ayuda que se necesite,

ante algún acto terrorista, natural o antrópico. Esta coordinación debe de ser acordada previamente, ya que las infraestructuras críticas son públicas y privadas, así como también el gobierno debe de dotar el marco legal para la operatividad de la misma. El realizar un Plan Estratégico se hace con el fin de aumentar, agilizar y estrechar lazos institucionales para superar un posible percance y tener un punto de vista común que permita mejorar las medidas de protección de las infraestructuras [28]. El objetivo es proteger los bienes, tanto lógicos como físicos ante un posible atentado mediante la colaboración mutua e interoperabilidad institucionales.

Este análisis no solo se hace a nivel país, sino también tiene que tener un alcance externo, para conocer si afecta a los países vecinos y el impacto generado. Un ejemplo de una red a nivel continental en la protección en este tipo de infraestructuras es la red European Programme for Critical Infrastructure Protection (EPCIP) [38], que es un programa de todos los países miembros de la Unión Europea para prevenir ataques a las infraestructuras críticas en toda esta región [38].

En la actualidad, los sistemas informáticos son de uso diario en las instituciones, es por este motivo que las redes de comunicaciones y los sistemas informáticos son esenciales para el desarrollo de la economía y la sociedad, por lo que la seguridad de las comunicaciones y los sistemas de información es considerada de especial interés y parte de la infraestructura crítica de servicio a los ciudadanos.

2.2.3. Relación entre las infraestructuras críticas y los sistemas de gobierno electrónico

Por lo general, los gobiernos dentro de su organigrama estatal, tienen identificados sus sectores estratégicos. Todo lo que es relacionado con comunicaciones y datos de las sociedades también forman parte de uno o varios

sectores y están expuestos a una serie de amenazas por lo que se necesita conservar su funcionamiento.

Para protegerlas, se tiene que catalogar el conjunto de instituciones que presten servicios esenciales, y diseñar un plan que contenga medidas de prevención y protección contra las posibles amenazas, tanto físicas como el de la seguridad de las tecnologías de la información y comunicaciones. Todos estos tienen que estar alineados a un Plan estratégico a nivel nacional y actuar conforme a normas establecidas.

La parte legal de una infraestructura crítica es importante, ya que esta iniciativa gubernamental contempla no solo instituciones públicas, sino también a las privadas, por lo que se necesita tener una base legal, para poder actuar y proteger los bienes que permiten el funcionamiento esencial de una sociedad. La base legal, permitirá actuar más allá de una protección material, sino también digital.

La dependencia de las infraestructuras de las tecnologías de la información cada vez es mayor, ya que para la interconexión de sistemas se realiza a través de medios de comunicación, sean de carácter público o privado. Es por este motivo que es necesaria la cooperación de todas las infraestructuras involucradas para analizar, planificar y mitigar posibles escenarios riesgosos.

Los sistemas e-gobierno al manipular datos privados de ciudadanos e instituciones de un país, es una infraestructura crítica, debido a la sensibilidad de datos que se albergan en los servidores gubernamentales. Un sistema de gobierno electrónico debe de tener la capacidad de estar preparado, para adaptarse a cambios inesperados en su plataforma, recuperarse rápidamente a interrupciones que pudiera tener el servicio ante ataques, accidentes naturales o antrópicos, incidentes o amenazas virtuales o físicas para garantizar el servicio a la comunidad [39]. Es por este motivo que es fundamental que la

infraestructura lógica y física de los sistemas de gobierno electrónico se considere dentro del Plan Estratégico de protección de infraestructuras críticas de un país.

2.3. CLOUD COMPUTING

2.3.1. Definición y clasificación

Cloud computing podría definirse como un modelo para permitir un acceso bajo demanda a un conjunto compartido de recursos informáticos configurables como redes, servidores, almacenamiento, aplicaciones y servicios de una manera escalable [40].

Cloud computing puede dar 3 diferentes tipos de servicios: software como servicio (SaaS), plataforma como Servicio (PaaS) e infraestructura como servicio (IaaS).

SaaS son aplicaciones ofrecidas por el proveedor, ejecutándose en la nube y accedidas por el usuario final mediante ordenadores, móviles, ipads, etc. El usuario no se preocupa de la instalación, mantenimiento, costos de operación, soporte técnico, almacenamiento. El usuario ingresa a la aplicación sin saber detalles técnicos y hace uso del servicio que se le está ofreciendo. Un ejemplo de este servicio es el correo electrónico de Google [41].

PaaS es la encapsulación de un ambiente de desarrollo o el empaquetamiento de una serie de módulos. Facilita la implementación de aplicaciones sin el costo y complejidad de comprar y administrar el hardware subyacente y sus capas de software. Un ejemplo es contratar en el cloud una plataforma Linux con entornos Java y Apache ya configurados o Windows Azure, de Microsoft, que permite el desarrollo y ejecución de aplicaciones codificadas en varios lenguajes

y tecnologías como .NET, Java y PHP. Básicamente el cliente utiliza los lenguajes de programación y herramientas facilitadas por el proveedor que le permiten al cliente desplegar sus aplicaciones programadas. Este servicio es flexible pero con restricciones limitadas por el proveedor de servicios [41] [42].

IaaS es un medio de entregar almacenamiento, procesamiento, redes y capacidades de cómputo como servicios estandarizados en la red en donde el cliente puede desplegar y ejecutar software y sistemas operativos. Esta es una infraestructura bajo demanda altamente escalable y el cliente tiene el control de los servicios contratados. Un ejemplo de esta infraestructura es Amazon Web Services servicios EC2 y S3 ofrecen cómputo y servicios de almacenamiento [41] [42].

El uso del cloud tiene algunos beneficios como el rápido procesamiento de datos, la reducción de costos en infraestructuras y personal, ahorro de tiempo en configuraciones, instalaciones, diferentes tipos de servicios listos para ser contratados, pago en función de demanda, acceso a recursos a través de internet, rápida implementación, energía eficiente, aumenta la eficiencia. Estos beneficios son atractivos para el gobierno, porque es más fácil contratar un servidor listo para su uso a tener que realizar la compra, configuraciones, pagar a un experto para que lo realice, y finalmente poder correr la aplicación necesitada. Así también si la aplicación necesita más ancho de banda, es muy fácil poder contratarla, o aumentarla según la demanda que se requiera. La velocidad a la que cloud computing ha calado en las actividades de Internet está aumentando de forma exponencial en los últimos años.

Sin duda alguna, uno de los beneficios más importante del cloud es que es escalable. Esta propiedad de poder añadir nuevos componentes o requerimientos de acceso según la demanda de usuarios que lo necesiten. Por medio del cloud, se tiene la facilidad y rapidez de poder contratarlo en caso de que los sistemas lo necesiten y de cancelar la contratación en caso de que la

demanda baje.

El cloud puede ser público, privado e híbrido. Un cloud público es mantenido y gestionado por el proveedor del servicio. En este tipo de cloud, los datos de varios clientes se almacenan en los servidores de proveedor. El proveedor de servicios es propietario de toda la infraestructura de su centro de datos y el acceso a los servicios es a través de internet.

Un cloud privado maneja los datos que alberga en los medios de almacenamiento como las bases de datos. El cliente controla sus aplicaciones, son propietarios de su infraestructura de red, almacenamiento, servicios, gestionar servicios. Puede gestionarla el cliente o una tercera parte y físicamente puede encontrarse externa o internamente en la organización [41].

Un cloud híbrido es la combinación del cloud público y privado. Este modelo tiene ciertas condiciones de tecnología propietaria en cuanto a la portabilidad de datos y aplicaciones.

El problema que conlleva el uso del cloud, es que la información está albergada en servidores externos y no institucionales. Al ejecutarse las aplicaciones en infraestructuras de un tercero, la seguridad es un factor a implementar por el proveedor cloud. El proveedor cloud manejaría datos confidenciales, y se tiene que analizar los riesgos de que éste manipule información clasificada o privada de todo un país. Otro problema es la carencia de control en caso de que no se firmen cláusulas en el contrato, así también la disponibilidad que ofrece el proveedor del servicio, ya que básicamente depende de la infraestructura y seguridades que el proveedor implemente en el cloud.

En un estudio realizado por KPMG, realiza la encuesta a 125 tomadores de decisiones y administradores de empresas en los Países Bajos (Netherlands),

como se puede observar en la figura 4.1 [65], la principal preocupación respecto al uso del cloud es la seguridad, seguido por las leyes, es el cumplimiento del servicio y la privacidad de datos. A ellos les preocupa la falta de transparencia de parte de los proveedores.

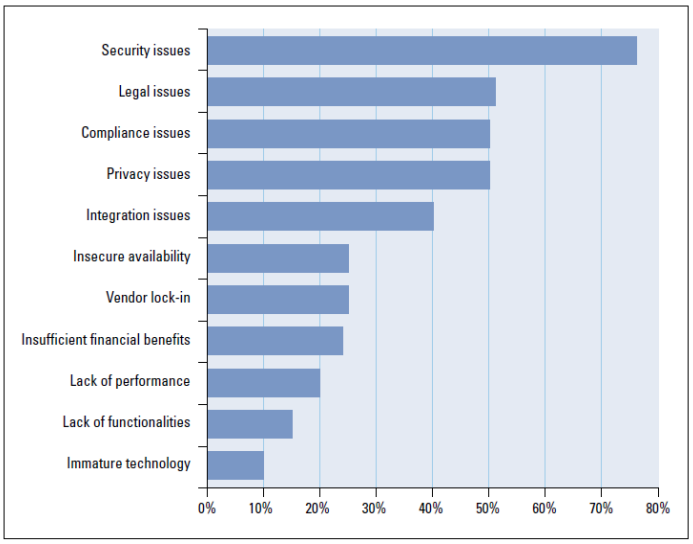


Fig. 2.2 Principales preocupaciones respecto al uso del cloud computing.

2.3.2. Los gobiernos y el cloud

Como se explicó en la sección anterior, una de las principales ventajas del cloud, es pagar solo por lo que se consume bajo demanda. Ésta característica puede ser explotada al máximo por los gobiernos en el mundo. Por ejemplo, Brasil a inicios del 2013 destinó USD 25 millones para la estrategia del cloud computing [63]; Australia, Italia, Dinamarca, Singapur y Estados Unidos, han indicado que tienen grandes avances en la implementación de la tecnología [64].Un ejemplo notable es el gobierno de los Estados Unidos, del cual hablaremos a continuación.

El gobierno de los Estados Unidos gasta más de $76 billones anualmente en 10.000 sistemas diferentes, siendo el de mayor inversión en TICS a nivel mundial [43].

En Septiembre 2009 el gobierno de los Estados Unidos anunció la iniciativa de llevar a cabo el proyecto del Cloud Computing en los servicios gubernamentales, debido a los beneficios que éste presta: reduce gastos, costos operativos y aumenta la eficiencia. En el cambio hacia el cloud, el gobierno buscó tres bases fundamentales: seguridad de la información gubernamental, proteger la privacidad de los ciudadanos, y garantizar los intereses de la seguridad nacional. El National Institute of Standards and Technology de Estados Unidos (NIST) desarrolló paulatinamente según los escenarios que se presentaban, sus propios estándares que tienen como prioridad la seguridad, interoperabilidad y portabilidad de requerimientos [43].

Como ejemplo de instituciones de Estados Unidos que migraron a un entorno cloud, tenemos a Recovery que con los ahorros obtenidos por el uso del cloud, en software y equipo de cómputo, prevé redirigir más de $1 millón para ayudar a identificar el fraude, despilfarro y abuso [44].

La ciudad de Los Ángeles tiene previsto ahorrar 5.5 millones en los próximos 5 años, como producto de mover su e-mail y herramientas de productividad al cloud de 34.000 empleados de la ciudad. Forge.mil y CollabNetto proveen de una plataforma de desarrollo de software para permitir a los usuarios reutilizar y colaborar en el código de software. La plataforma de código abierto permite evitar costos de proyectos al reutilizar software. Se estima que por proyecto se ahorrará entre 200.000 y 500.000 dólares norteamericanos [43]. Debido a la gran acogida del cloud, se planea eliminar un mínimo de 800 data center para el 2015, con lo cual el estado se ahorra dinero, pudiéndolo invertir en otras necesidades [44].

Otro claro ejemplo de administración electrónica es la red Sara, implementada por España y desplegada desde 2002. La red SARA es la red privada de las Administraciones públicas españolas. SARA interconecta a la Administración General del Estado a las Comunidades Autónomas y a los Entes Locales, y estos a su vez con la Unión Europea y a sus Estados miembros [45]. Con la tendencia de migrar los gobiernos al cloud, el 15 de enero de 2013, el Consejo Superior de la Administración Electrónica, declaró a SARA como proyecto de interés prioritario para construir el cloud privado de la administración pública española [46].

Actualmente, SARA da servicio SaaS y PaaS, por ejemplo el sistema de Oficina de Registro Virtual de Entidades (ORVE-SIR), que es un sistema de interconexión entre las oficinas de registro de las distintas administraciones públicas, sean estatales, autónomas o locales. ORVE hace instantánea la transmisión de solicitudes a la unidad administrativa solicitada con plena validez jurídica [47]. Este trámite reduce costos al ciudadano y al estado. Si un costo presencial aproximadamente tiene una media de 80 euros y el trámite electrónico 5 euros; y conociendo que 365 millones de trámites se realizaron en formato electrónico en el 2012, el estado se ahorraría 28500 millones de euros [48].

Para apoyar la gestión de SARA, se ha iniciado la reforma al Esquema Nacional de Interoperabilidad, que fomentará la adopción y desarrollo de SARA en las administraciones públicas. Así también se ha realizado la guía CCN-STIC 832, estableciendo requisitos de seguridad en plataformas cloud.

Cloud ahorra recursos en tiempo, monetarios, e incluso, crea valor a los sistemas e-gobierno, por lo que es necesaria la implementación de medidas de seguridad, para proteger ya no tan solo datos, sino toda una infraestructura virtual.

2.3.3. Relación entre cloud computing y los sistemas de gobierno electrónico

Si debido a los beneficios del cloud computing, el gobierno decide emplear los servicios de éstos, debe de tener en consideración ciertos parámetros antes de la contratación, ya que no puede ser tratado como un cliente más, porque la información que se maneja es confidencial. Tiene que realizar acuerdos especiales que le permitan tener el control de los datos que el proveedor manipularía. El gobierno debería constatar y evaluar los mecanismos de seguridad que se utilizan y el proveedor debería de pasar por auditorías externas para asegurar la seguridad íntegra de todo el sistema.

Los riesgos que pueden tener estos sistemas pueden ser de diferente índole. Si un sistema de gobierno electrónico tiene sus aplicaciones en el cloud, se debe de tener conocimiento a detalle de los riesgos a los que se está expuesto según el servicio que se ha contratado: IaaS, PaaS or SaaS. Para cada caso, se debería tener una estrategia de respuesta para mitigar el riesgo.

Lo recomendable sería que el gobierno contrate un cloud privado, ya que pueden ser gestionadas por el estado. La ventaja de contratar este tipo de servicios es que aportan una importante mejora de los niveles de seguridad y de privacidad porque solo el estado tendría el acceso y puede disponer del control de los recursos.

Es por este motivo que se considera necesario que los gobiernos tengan parámetros de estandarización en la implementación y seguridad del cloud para que los sistemas gubernamentales consideren tener implementados factores de seguridad identificados, y puedan asegurar seguridad en la infraestructura desplegada.

2.4. SEGURIDAD EN SISTEMAS E-GOVERNMET

2.4.1. Introducción

Los sistemas e-gobierno, usan la tecnología para brindar servicios y debido a su rápida expansión, se puede decir que se están construyendo gobiernos electrónicos virtuales y la seguridad de éstos es un factor crucial por lo que se requiere medidas fuertemente preventivas tecnológicas y administrativas [2].

Estudios han demostrado que los aspectos no técnicos son tan importantes como los técnicos al momento de salvaguardar una organización, y los aspectos no técnicos están relacionados con la administración de los recursos [50]. Es por este motivo, que la seguridad también tiene que ser administrada. La seguridad informática busca proteger la infraestructura computacional mediante un conjunto de estándares, protocolos, reglas, metodologías, leyes, marcos de referencia que minimicen los posibles riesgos a los bienes en una organización.

En los sistemas informáticos vamos a encontrar bienes tangibles como la infraestructura física, servidores, humanos, redes, etc. e intangibles como la información, servicios que se prestan, aplicaciones desplegadas, conocimiento organizacional, etc. La seguridad informática debe establecer normas que minimicen los riesgos a toda la infraestructura. Es por este motivo que se han creado protocolos, planes, normas, marcos de referencias, que encierran el control de: personal, accesos, servicios, instalaciones, y todo lo relacionado al bien computacional, siendo la información el principal activo.

Los sistemas de gobierno electrónico deben de proporcionar múltiples métodos de autenticación, autorización, emisión de credenciales, estar sometidos a auditorías, ser confiables, tener capacidad de respuesta, resolución de conflictos, estar disponibles, respeto a la privacidad, integridad de la

información, ser escalables, entre otras características [2].

Como se indicó en la sección 2.2.3, los sistemas de e-gobierno son infraestructuras críticas, por lo que es necesario que toda su infraestructura como tal, tenga las seguridades necesarias ante algún tipo de evento anormal. Los sistemas deberían de tener la capacidad para recuperarse en un corto tiempo, ya que los servicios que estos prestan, son imprescindibles a la sociedad; en este caso, el ciudadano también debe de tener la percepción de seguridad y confianza en este tipo de sistemas para que tengan continuidad en su uso.

2.4.2. Seguridad de la Información

Hay tres tipos de amenazas que afectan a la información que albergan los sistemas: el acceso no autorizado que afecta a la confidencialidad, el cambio o modificación no autorizada de la información que afecta la integridad y las amenazas que afectan la disponibilidad de información y servicios [51].

2.4.2.1. Confidencialidad

Un sistema e-gobierno tiene que ser confiable porque debe garantizar la protección, clasificación y seguridad de la información que alberga en sus servidores sea clasificada, pública, reservada, datos personales o institucionales; es decir que el acceso a la información la deberían de realizar los individuos que tengan la autorización.

En el caso de los sistemas e-gobierno la confidencialidad tiene que ser manejada muy sigilosamente debido a que la divulgación de la misma pone en riesgo o perjudica al ciudadano al revelarse información relativa al origen étnico, características físicas, morales, domicilio, teléfonos, creencias religiosas, estados de salud, físicos, mentales, patrimonio personal o familiares, intimidad

personal o propia de la imagen [52].

Un ejemplo es lo ocurrido en lo ocurrido a inicios del 2013 con el virus "Octubre rojo". El virus fue utilizado para robar información de instituciones gubernamentales e instituciones de investigación, el cual había estado activo por lo menos 5 años [66].

El estado debe de garantizar la confidencialidad tomando las medidas necesarias para que la información no pueda ser accedida incluso a personal administrativo gubernamental, al menos que el ciudadano lo autorice.

Debido a que los sistemas e-gobierno pueden ser accedidos a través del navegador, éstos están a disposición del público en general, pudiendo los ciberterroristas tener la probabilidad de mediante ataques dirigidos tomar información de los diferentes webs gubernamentales. Es por este motivo que el gobierno debe de proteger la información cuidando la confidencialidad de los mismos.

2.4.2.2. Integridad

La integridad se refiere a asegurar que la información que fue generada y guardada en los repositorios, se encuentre exactamente igual, sin ser manipulada o alterada por usuarios o procesos no autorizados.

Si la integridad de datos se viese alterada, afecta al ciudadano puesto que los datos que él ingreso no son los auténticos y al gobierno directamente en credibilidad y confianza [53].

Para ejemplificar, podemos ver lo ocurrido en Estados Unidos, en la clínica Surgeons of Lake Country, que accedieron a la base de datos, se robaron historias clínicas de los pacientes, las cifraron y solicitaban rescate por

devolverlas descifradas. Si al devolver las historias clínicas, los datos hubiesen sido modificados y entregados al hospital, pudo haber causado hasta muertes masivas de los pacientes. Desafortunadamente, la clínica decidió no pagar y se perdieron las historias clínicas [68].

Los sistemas e-gobierno tienen la responsabilidad de guardar la integridad de todos los datos que se albergan en sus bases de datos, sistemas y plataformas.

2.4.2.3. Disponibilidad

La disponibilidad es la condición de la información de encontrarse a disposición de personas, procesos o aplicaciones en el momento que así lo requieran.

Un ejemplo de esto es lo ocurrido el 15 de junio 2013, que se produjo una bajada brusca de la disponibilidad de cuatro de los dominios más visitados de Internet, tales como Google, Apple, Yahoo! y Microsoft. El ataque fue contra Akamai, responsable del mantenimiento de estos dominios [67].

Los sistemas de e-gobierno deben de tener una disponibilidad alta, indiferentemente si existen fallos eléctricos, hardware o mantenimientos de sistemas, debido a que el objetivo de estos sistemas es dar un servicio 24 horas al día, 7 días de la semana, indiferentemente si la información reside en servidores locales o en el cloud con un proveedor de servicios.

2.4.3. Problemática de e-gobierno respecto a la seguridad

Mientras día a día se crean nuevas tecnologías, las redes se expanden, en Internet se ejecutan millones de aplicaciones, existe mucho crecimiento de nuevos data centers, información, etc. todos ellos necesitan seguridad para

proteger los datos, redes, infraestructuras y todos los bienes relacionados a ellas.

Debido a que las TI, son bastantes amplias, manejar la seguridad en todos los bienes informáticos involucrados, es una tarea compleja. Se quiere identificar los parámetros que debería de tener los sistemas gubernamentales para considerarse que cumplan con normas y disciplinas de seguridad que prevengan y mitiguen posibles riesgos altamente costosos en las instituciones estatales.

Para tener una visión macro de lo que la seguridad implica, se necesita conocer: los requerimientos, las políticas, los mecanismos, las garantías y .los componentes de seguridad que se necesitarán en lo que se requiera proteger [49].

Alrededor del mundo existen normas, marcos, estándares que ayudan a la implantación de reglas en una organización, cada una desde su perspectiva. Pero la seguridad necesita ser integral, formándose como cultura desde la directiva principal hasta los empleados operativos, en los dispositivos que se utilizan y en las comunicaciones que se emplean, en las aplicaciones que se utilizan y en la infraestructura que la rodea.

En los sistemas gubernamentales, hay 5 aspectos principales que tienen que ser considerados para que haya una cultura de seguridad institucional:

- Seguridad integral

- Seguridad en las aplicaciones web

- Seguridad en Cloud

- Seguridad en los sistemas e-gobierno como infraestructuras críticas

- Gobierno y Gestión TI

Considerando estos aspectos principales, centralizaremos este trabajo investigativo en la seguridad que debería de haber en cada uno de ellos desde el punto de vista administrativo, creando marcos de evaluación que nos darán a conocer las falencias de nuestro sistema.

2.5. GOBIERNO Y GESTIÓN TI

Los gobiernos como parte de su innovación tecnológica, también se ha unido a la red de servicios por internet, haciendo uso de las tecnologías de la información (TI). Las TI son los recursos necesarios para adquirir, procesar, almacenar y difundir información. Debido al uso de las TI y la facilidad de su expansión, en empresas grandes, ha sido necesaria la reformulación de todo el proceso de gestión que se tenía sobre ellas. El Estado al ser un órgano que tiene ministerios, oficinas, secretarías, entre otros, las TI son un apoyo importante a las gestiones gubernamentales y el Estado las tiene en gran cantidad, ya sea en equipos, servicios o productos que brindan a la sociedad.

El estado también innova en los productos y servicios que brinda a la ciudadanía. Un ejemplo de ello es e-gobierno, e-voting, e-democracy, que han cambiado la forma de interactuar tradicional del Estado hacia los ciudadanos e instituciones. Todo esto lo ha llevado a cabo con el apoyo de la tecnología y la comunicación hace ya parte importante de la participación ciudadana. Definitivamente las TI ayudan a la gestión estatal y el Estado cuenta con ellas, pero ¿es éste consiente de la infraestructura que tiene desplegado en todo el territorio nacional y de todo su potencial? Así como la tecnología ha evolucionado, también la gestión administrativa de ésta ha sufrido cambios relevantes. Debido a la importancia de las TI porque son un instrumento de apoyo, deben ser consideradas con un enfoque estratégico para que el estado

cumpla sus objetivos [54].

La información que maneja el estado es de toda una sociedad y es éste el responsable del buen uso, almacenamiento, procesamiento y eliminación de ella. Ésta al igual que todos los recursos de las TI necesita de procesos planificados desde que es creada hasta cuando es destruida. El Estado Central como tal, tiene demasiados activos informáticos que incluyen servicios, productos, equipos, personal, infraestructura, arquitectura, entre otros. El crecimiento o limitantes que tengan las TI, depende principalmente de las decisiones que realicen sus gobernantes. Pero cómo saber si estas decisiones beneficiarán en poca o gran manera, a corto o largo plazo, y si la sociedad estaba o no preparada para el cambio. Todas las inversiones tienen que ser planificadas, proyectables y medibles para que al final la relación costo-inversión-valor sea positiva. Debido a que las TI son un apoyo fundamental en el estado y se expanden para ayudar a cumplir los objetivos institucionales, se propone que se siga un marco de trabajo integral y organizado basado en los marcos y estándares existentes [55].

El marco de trabajo para el Gobierno y la Gestión de las TI, ayudaría al estado a que los recursos TI se utilicen de una manera eficiente, a establecer y monitorizar procesos que ayudarán a tener un mejor control del riesgo, identificar beneficios, monitorizar si se están cumpliendo con las metas en los plazos establecidos y a reconocer el valor que tiene la institución en cada servicio o producto que ofrece.

Actualmente existen un sin número de reglamentos según el país de cómo se debería de mantener, procesar, eliminar la información; leyes y marcos legales que tienen como objetivo dar lineamientos que tienen que ver con confidencialidad, seguridad e integridad de datos; estándares internacionales propuestos para la gobernanza y gestión de las TI, marcos referenciales como COBIT, Calder-Moir, etc. cada uno desde su punto de vista. En este capítulo se

hablará de qué es el Gobierno y gestión TI, cómo está relacionado con el estado, los marcos existentes y de nuestra propuesta.

2.5.1. Generalidades

La organización interna estatal, definitivamente influye en la efectividad y eficacia de procesos y servicios que se brindan al exterior de ésta. Como parte de la evolución de la gestión administrativa de TI, es la propuesta de separar la "gobernanza o gobierno" de la "gestión". La propuesta de separar estas "gobernanzas", básicamente es para tener bien definida la parte ejecutiva de la parte operativa de quienes estén relacionados con el uso de las TI, así como sus responsabilidades y obligaciones.

Una propuesta de cómo separar éstas dos partes de una institución, fue realizada por [56], quienes separaron el gobierno (gobernanza corporativa) y gestión (Gobernanza del Negocio). El gobierno TI son los que evalúan, dirigen y monitorean el cumplimiento de los metas institucionales. Éstos son los que toman decisiones y controlan el cumplimiento de todos los procesos. La gestión, tiene que ver con la ejecución correcta de procesos alineados a las metas institucionales [54].

Se tiene que estar consciente de que implementar un marco TI es compromiso de toda la institución, desde los altos directivos hasta la parte operacional de la misma que estén involucrados con activos TI.

Al tener un control de gestión administrativo de las TI, mejora el rendimiento en los servicios y productos que el Estado brinda. Es por este motivo que es viable que el estado, como órgano rector de la sociedad, implementara un gobierno y gestión de IT, de esta manera, organiza efectiva y eficazmente los servicios IT que presta a la sociedad, promueve una mayor participación ciudadana y trata de cubrir a nivel nacional el acceso a las TI.

2.5.2. Relacionando Gobierno y Gestión TI con el estado

Como ya vimos anteriormente, el gobierno y la gestión son diferentes. Para cada uno hay que definir procesos distintos porque tienen objetivos que no son iguales.

Los procesos de Gobierno tratan de los objetivos de gobierno de las partes interesadas como entregar valor, optimización del riesgo y de recursos, realizando prácticas y actividades de evaluación, orientación y monitorización [57].

Los procesos de Gestión tratan de las prácticas y actividades de los procesos de ejecución con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar y tiene la responsabilidad de velar de proporcionar cobertura extremo a extremo de las TI [57].

Para poder tener una buena gobernanza TI, es necesario tener el total apoyo del jefe institucional para garantizar la implementación de todo el proceso. El liderazgo de funcionarios de alto rango es primordial para incentivar los planes, procesos, políticas y reglamentos a implementar. Así también el compromiso de los altos mandos para que se pueda cumplir una evaluación, orientación y monitorización del gobierno y gestión de TI. Se deberá conformar una Dirección General, que básicamente la conformarán los altos mandos institucionales.

Lo primero que hay que definir es en qué metas organizacionales, las TI dan soporte. La Dirección General tendrá que llegar a un consenso de la priorización de las metas y del alcance de cada una de ellas. Como compromiso, la Dirección General, tendrá que definir los roles de la gestión ejecutiva, con responsabilidades claramente definidas para las decisiones de TI, así como la frecuencia con que se reúnen y la documentación respectiva de las reuniones.

En el caso estatal, el ministro, gerente general o máximo representante institucional es quien debe de llevar el liderazgo de gobierno TI.

Para cada meta, se tendrán que definir los procesos para poder alcanzarla. Actualmente existen algunos marcos para poder establecer un gobierno en una institución. Todos tienen puntos comunes pero distintos enfoques. Entre los puntos comunes que tienen los marcos más usados, tenemos que en una buena gobernanza de TI, el gobierno tiene que tener evaluar, orientar y monitorizar [58] [59]:

- Alineamiento estratégico
- Creación de Valor
- Controlar el riesgo
- Optimizar Recursos
- Asegurar la transparencia interna y externa
- Medición de Resultados y retroalimentación

Alineamiento Estratégico

Toda institución tiene metas que persigue y para toda meta, tiene que haber una estrategia. Las TI no deben de estar fuera de las estrategias institucionales, es más, tienen que estar alineadas a ellas. La institución como tal tiene que tener bien claro los objetivos y comprender hacia dónde quiere ir. Dependiendo de esto, se tiene que evaluar el entorno, capacidades y rendimientos actuales institucionales. Reconocer las capacidades actuales de IT, y trazar una hoja de ruta según las capacidades disponibles, llegar a un consenso y comunicar la estrategia y la dirección de TI a seguir [57] [58] [59].

En el caso estatal, debido a que los ministerios tienen diferente temática, las estrategias que se planteen para cada institución tienen que ser distintas. Los objetivos que tenga el ministerio del ambiente, es totalmente diferente al ministerio de educación. Por lo que las TI apoyarán de diferentes maneras a

cada una según su necesidad.

La estrategia tiene que contemplar que los productos y servicios que se liberen a la sociedad, tienen que dar valor a la ciudadanía y mostrarle sus beneficios. La institución estatal, tiene que verse optimizada en costos, funcionalidades, recursos humanos y técnicos [57].

Creación de Valor

Este ítem tiene dos puntos de vista: la creación del valor para la institución gubernamental y para la sociedad.

1. **Para la institución estatal**

Los valores que van a crearse en la institución estatal son [56]:

- Optimización de los recursos financieros que se utilizaron
- Optimización de la inversión realizada
- Integración de los sistemas, servicios e información
- Uso eficiente de las TI
- Reputación
- Satisfacción del usuario
- Participación ciudadana

2. **Para el ciudadano o institución externa**

Los beneficios o valores que se crearán son:

- Ahorro de tiempo
- Ahorro de dinero
- Satisfacción hacia sus gobernantes
- Seguridad

Se tiene que optimizar el valor de los servicios TI resultado de la inversión realizada a costos congruentes. Cada proyecto tiene que tener en claro el valor que tiene, y la inversión realizada. En el caso estatal, éste tiene que tener un valor extra: seguridad. Todos los proyectos gubernamentales tienen que dar confianza a los entes que lo entregan debido a la información que manipulan. Se tendrá que evaluar, orientar y monitorizar continuamente esta fase para que se pueda obtener la optimización del valor para ambas partes [57] [58].

Institución estatal

- Evaluar
  - Inversiones
  - Servicios brindados
  - Retorno de la inversión
- Orientar
  - Principios y prácticas para que se dé el valor deseado
- Monitorizar
  - Indicadores y métricas del rendimiento del servicio

Ciudadano o institución externa

- Evaluar

- Servicio prestado cumple con su objetivo

- Orientar
  - Al uso del servicio

- Monitorizar
  - Satisfacción del usuario (Se podría realizar encuestas)

Controlar el riesgo

El riesgo del que hablamos aquí, no es solamente acerca de la mitigación de riesgos en la información que se maneja o de las plataformas que brindan el servicio, sino que es de todos los activos relacionados con TI, es decir desde un computador dañado hasta la información más sensible que pudiese existir en la institución. El riesgo tiene que ser tolerable, o en el caso de sistemas críticos mínimos, según el grado de criticidad.

La intención es crear una cultura de gestión de riesgos, de tal manera de que el fallo de incumplimiento se reduce al mínimo. Se tienen que reconocer procesos, equipos, servicios IT críticos y relacionarlos con la pérdida de valor en caso de que estos fallen, así como el valor que generan en caso de que ocurra un desastre y que el proceso se recupere correctamente en un tiempo apropiado.

Se tiene que evaluar el efecto del riesgo sobre el uso actual y futuro de las TI en la institución. El riesgo de gobierno TI sobre el valor de la institución tiene que ser identificado y gestionado. El gobierno tiene que orientar las buenas prácticas para que no se sobrepase el límite del riesgo que se esté dispuesto a tolerar y monitorizar los procesos de gestión de riesgos. Se tiene que hacer énfasis en los procesos, servicios e información crítica, ya que de ellos se tiene que cuidar la confidencialidad, disponibilidad e integridad. La mitigación del riesgo en los sistemas críticos tiene que ser reducida al mínimo.

Un ejemplo es Nebula, la plataforma cloud computing de la NASA de los Estados Unidos de Norteamérica, que muestra al público imágenes de alta resolución de la luna y Marte. La NASA exige medidas de seguridad, por lo que Nebula ofrece una manera segura que sus datos sean accesibles, evitando la necesidad de garantizar el acceso a las redes internas. La arquitectura de Nebula se ha diseñado de modo que exista interoperabilidad con los proveedores de servicios cloud comerciales, ofreciendo a los investigadores de la NASA el código para ejecutarse en el cloud. Así también la NASA se ahorró de cuatro a cinco meses de tiempo y aproximadamente 800 horas de trabajo, lo que permite a la agencia para centrarse en ampliar el contenido accesible al público en lugar de la construcción de la infraestructura de TI [43].

En caso de que existan aplicaciones corriendo en un proveedor cloud, se deberá analizar los riesgos de que los sistemas queden fuera de servicio, ya sean por razones internas o externas al proveedor. El estado tendrá que garantizar siempre seguridad. Si bien es cierto, los sistemas corren fuera del dominio estatal, no implica que no tenga responsabilidad. De hecho, quien tiene que velar por la seguridad de los mismos, es el estado. Lo recomendable sería que el estado tenga derecho a auditar los servicios que corren externamente y se aplique los mismos principios del gobierno TI al proveedor (previamente acordados).

Optimizar Recursos

Se refiere a todo tipo de recursos con que cuente la institución: financieros, humanos, infraestructura, etc. Los recursos relacionados con IT, tienen que estar disponibles para que se puedan cumplir los objetivos institucionales a un costo óptimo. Se tiene que evaluar y examinar la necesidad actual y futura de los recursos relacionados con IT. Se tiene que analizar las alternativas de aprovisionamiento, incluyendo personal o servicios externos que se necesiten en una condición de funcionamiento normal o de riesgos tolerables. Cuando se

esté analizando la opción de comprar algún tipo de recurso, también tienen que estar presentes las opciones de alquilar o reutilizar recursos. Se tiene que orientar el uso óptimo de recursos TI en la institución, así como la monitorización para verificar la asignación y eficacia de capacidades, así como las acciones correctivas [60].

Asegurar la transparencia interna y externa

Se tiene que asegurar que la medición y elaboración de informes en cuanto al desempeño de TI en la institución sean transparentes. La transparencia tiene que ser interna y externa. Internamente tiene que haber comunicación entre todos los agentes relacionados de TI acerca de las decisiones que se tomen, costos, beneficios y riesgos. La transparencia externa es de presentar información fiable a los ciudadanos en el portal. Para medirla, podría realizarse encuestas al usuario quien utiliza el servicio. Esto da al gobierno otro valor agregado, confianza.

El gobierno tiene que examinar continuamente que la comunicación en la institución sea efectiva y transparente creando mecanismos y estrategia de comunicación. Orientar a que los mecanismos se cumplan y monitorear que sea efectiva.

Retroalimentación

Como se puede observar, en todos los puntos anteriores se evalúa, orienta y monitoriza. Esta es un buen aporte que nos da la norma 38500. La retroalimentación es necesaria tanto para el gobierno como para los usuarios que usan el servicio.

Para el gobierno en el sentido de que corroboran si todos los procesos, procedimientos y guías que se han realizado, están efectivamente siendo usadas, por este motivo se monitoriza, en caso de que no se den los resultados

esperados, se tomarán las correcciones pertinentes. El proceso se vuelve a repetir: evaluar, orientar, monitorizar. En el caso de los ciudadanos, es fundamental que ellos indiquen alguna anomalía en el sistema.

2.5.3. Análisis de Marcos Actuales

Para el gobierno y gestión TI, existen algunos marcos, entre los más relevantes COBIT, Calder Moir, ITIL cada uno desde su punto de vista. A continuación un resumen de cada uno de ellos.

2.5.3.1. COBIT

COBIT es un framework, que se enfoca en el desarrollo de las políticas y buenas prácticas para el control de TI y se basa en cinco principios:

1. Satisfacer las necesidades de las partes interesadas
2. Cubrir la empresa de extremo a extremo
3. Aplicar un marco referencial integrado
4. Hacer posible un enfoque holístico
5. Separar el gobierno de la gestión

COBIT busca siempre satisfacer las necesidades de las personas involucradas en la institución, ya sean clientes, acreedores, mesa directiva, socios, directores ejecutivos. Esta parte trata de crear valor a todos los involucrados. Para COBIT crear valor involucra tomar las necesidades de los interesados y tratar de crear valor al concretar beneficios, optimizando el riesgo y los recursos.

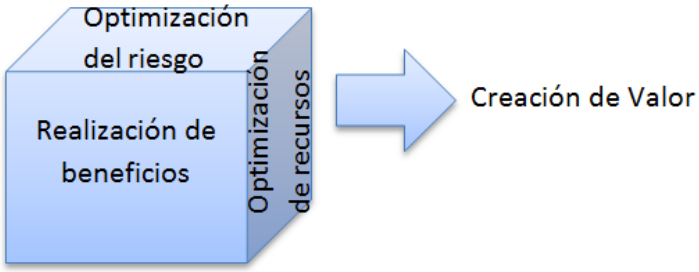


Fig. 2.3 Creación de Valor

Para lograr valor, COBIT ha identificado metas corporativas, de TI y facilitadoras que por lo general las empresas utilizan estos criterios para crear valor. Han identificado una serie de preguntas y factores que ayudan a la empresa a identificar qué es lo que podría generar valor a la empresa según sus intereses.

La ventaja de COBIT es que cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos. Esto implica que todos los procesos que se quieran realizar, tienen que involucrar funcionarios internos, externos, proveedores, e incluso a los ciudadanos que interactúan con las aplicaciones que están a su servicio. Para alcanzar a cubrir la empresa de extremo a extremo COBIT mediante un esquema define bien los roles, actividades y relaciones claves.

COBIT está alineado con otros estándares corporativos: COSO, ISO/IEC 9000, ISO/IEC 31000, y relacionado con TI: ISO/IEC 38500, ITIL, ISO/IEC 27000, TOGAF.

COBIT define un conjunto de facilitadores para el gobierno y la gestión de IT. Los facilitadores son puntos clave que ellos han identificado que pueden

ayudar a alcanzar los objetivos de la empresa.

El gobierno y la gestión son dos conceptos distintos y engloban diferentes tipos de actividades, tienen estructuras organizativas diferentes y tienen diferentes propósitos. COBIT tiene 5 procesos de gobierno de TI, en el cual evalúa orienta y supervisa a 27 procesos de gestión.

2.5.3.2. CALDER MOIR

Calder Moir se basa en los 6 principios de la ISO 38500:

- Responsabilidad
- Estrategia
- Adquisición
- Rendimiento
- Conformidad
- Comportamiento Humano

El marco de trabajo Calder-Moir para el gobierno de TI organiza los asuntos del gobierno y proporcionar herramientas para apoyar a la compañía, los ejecutivos y los profesionales.

El marco consiste en 6 segmentos. Cada segmento está dividido en 3 capas. La capa interna será utilizada por la dirección general. En la capa interna encontramos: estrategia TI, cambios, balance con TI, operaciones, estrategia del negocio y los riesgos, tendrán que ser bien estructurados para asegurar la entrega de valor, cumplimiento y control de riesgos. La capa intermedia la utilizarán los directores departamentales (responsables de administrar las actividades y procesos). Ellos utilizarán la capa realizando la pregunta ¿Cuál es la estrategia?, inmediatamente, la capa intermedia responderá la pregunta. La capa externa representa a los ejecutores TI, quienes usan las herramientas, metodologías para planear, diseñar, valorar, controlar y liberar las TI para la

institución. La capa exterior enumera una serie de soluciones que muchas organizaciones ya utilizan para regular, controlar y administrar como se visualiza en la fig. 6.3 [61] [54]

A continuación, se ilustra la manera de operar del marco Calder Moir:

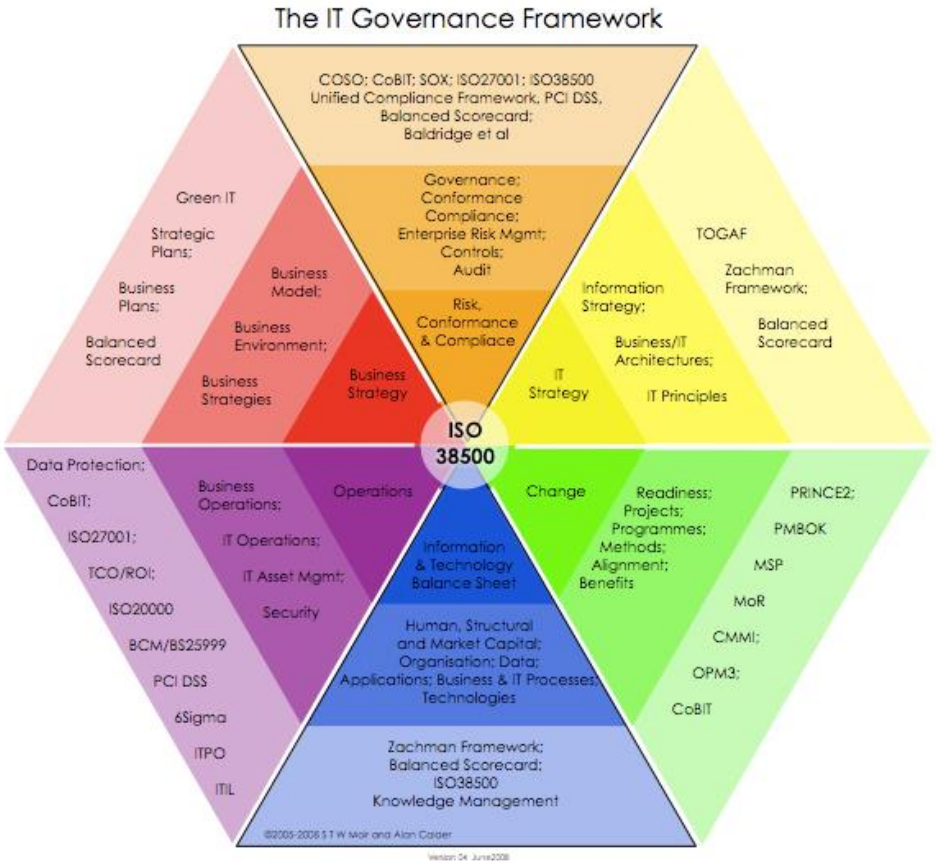


Fig. 2.4 Modelo Calder Moir

2.5.3.3. ITIL

ITIL es la abreviatura de Biblioteca de Infraestructura de Tecnologías de Información, y es un conjunto de conceptos y prácticas para la gestión de servicios de informáticos y fue desarrollado al ver que las organizaciones dependen de la informática para alcanzar los objetivos institucionales. Este conjunto de buenas prácticas, ayuda a las organizaciones a lograr calidad y eficiencia de las operaciones de TI. ITIL se basa la administración del servicio,

que lo ha dividido básicamente en soporte y prestación del servicio como se observa en la Fig. 6.5 [62].

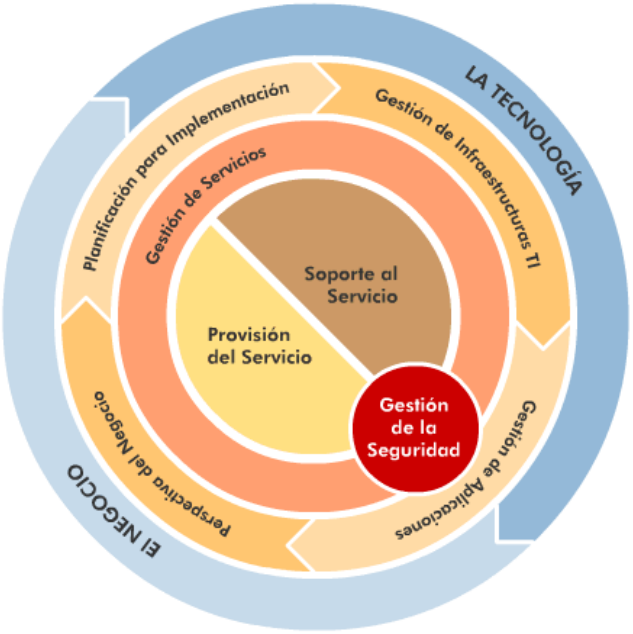


Fig. 2.5. Modelo ITIL

2.5.4. Riesgos de Gobierno y Gestión TI en el estado

Si bien es cierto, se han mencionado un sin número de beneficios que aporta el gobierno y gestión de IT al estado, hay que considerar los siguientes riesgos:

- Falta de compromiso de sus directores y ejecutivos
- Mala implementación o implementación a medias
- Mal enfoque

Falta de compromiso de sus directores, ejecutivos y parte operacional

Para que un gobierno y gestión TI tenga éxito, es necesario que toda la institución se involucre al 100 %. No es suficiente que la parte operativa o el departamento de TICs se comprometan a considerar todos los controles y políticas impuestas para el mejoramiento de procesos, si los altos mandos no dan seguimiento a los mismos para verificar los resultados esperados. O por el

contrario, que la parte operacional ponga poco interés en implementar las normas para un buen gobierno. El compromiso tiene que ser integral, ya que si alguna de las partes no cumple con sus responsabilidades, el tratar de ejecutar un gobierno TI será pérdida de tiempo. El incentivo lo pueden poner los directores mostrando todos los beneficios que pueden tener si la institución empieza a implementar un buen gobierno

Mala implementación o implementación a medias

Se tiene que considerar que si por algún motivo fracasa la implementación del gobierno y gestión de TI, será un alto costo que habrá corrido la institución. La pérdida no es tan solo económica, puesto que seguramente se contratará a expertos en leyes, tics, auditores, etc. para que se procedan a realizar los procedimientos, marcos, análisis de riesgos, y todo lo que implica llevar a cabo un gobierno y gestión TI, sino de pérdida de recursos institucionales, ya que seguramente se habrán asistido a reuniones, y se habrá sacado tiempo a altos y medios directivos para las capacitaciones y todo lo que gobierno TI involucraba.

Mal enfoque

Si la institución decide implementar el gobierno y gestión TI, es responsabilidad de todos la planeación e implementación bien hecha. Si por algún motivo las estrategias no están bien enfocadas o no es la deseada, la institución puede dar un giro total porque esas no eran las metas que se querían alcanzar. Esto es exclusivamente responsabilidad de los directores, ya que ellos conocen la esencia de la institución con sus metas y objetivos claros, por lo que deberían de saberlo plantear y organizar para la buena implementación del gobierno y gestión de TI.

2.6. PROBLEMA DE LA SATISFACIBILIDAD

2.6.1. Antecedentes

Desde muchos años atrás, había la inquietud de que los métodos matemáticos utilizados en la investigación de la lógica formal se los llevara a métodos computacionales para la obtención de teoremas matemáticos. Hilbert en 1920 notó que todas las matemáticas clásicas podrían formalizarse dentro de la lógica de predicados. El afirmó que la búsqueda de un algoritmo de decisión para la teoría de la cuantificación era el problema fundamental de la lógica matemática [72].

"La Teoría de la Complejidad Computacional es la parte de la teoría de la computación que estudia los recursos requeridos durante el cálculo para resolver un problema. Entonces, se puede definir la complejidad de cálculo como la cantidad de recursos necesarios para efectuar un cálculo". Los recursos estudiados son tiempo, es decir el número de pasos que se necesitan para resolver un problema y espacio, que es la cantidad de memoria, procesadores, discos duros, etc. que se utilizan para resolver dicho problema. De los procesos computacionales se derivan los problemas con solución y sin solución. Los problemas que se resuelven en un tiempo linealmente a su tamaño, son problemas con una solución de orden de complejidad lineal [78].

Actualmente la mayoría de algoritmos tienen una complejidad o costo computacional polinómico. Estos son los problemas que están en la clase P. Los problemas con costo no polinomial están en la clase NP, es decir que no tienen solución algorítmica [78]. El problema de la satisfacibilidad booleana (SAT), fue el primer problema identificado que pertenecía a la clase de complejidad NP-completo. Los problemas NP-completos, son los problemas más difíciles de NP. El problema de SAT, básicamente busca conocer si una cierta fórmula de lógica

proposicional puede ser verdadera, dados valores booleanos para las variables proposicionales.

Las investigaciones dieron como resultado de que, si bien no existe un procedimiento de decisión para la teoría de la cuantificación, hay procedimientos que hacen que una fórmula de cuantificación sea válida, pero que implican una búsqueda en los valores de las variables que intervienen, y que esta búsqueda si puede realizarse de una manera computacional [72].

En la actualidad, se han desarrollado diversas aplicaciones para la lógica proposicional, como la demostración de teoremas, modelación análisis y optimización de problemas, planificación y scheduling, sistemas a la ayuda de decisión, etc., con la ayuda de diferentes SAT algoritmos que se han desarrollado a lo largo del tiempo.

La utilización de las fórmulas booleanas proposicionales para solucionar problemas NP-completos, es un área de investigación en la Inteligencia Artificial. Este método consiste en reducir un determinado problema al problema de la satisfactibilidad (SAT), solucionar la instancia obtenida y a partir de la solución encontrada, generar una solución para el problema original [69]. El problema de la satisfacibilidad booleana fue el primer problema identificado que pertenece a la clase NP-completo y fue demostrado por Stephen Cook en 1971.

Actualmente SAT es propuesto para solucionar problemas de consumo de energía en la integración del diseño de los circuitos a alta escala. Un ejemplo está en [70] que propone un marco pseudo-booleano basado en SAT que tiene como objetivo la búsqueda de los patrones de entrada que provocan picos de potencia dinámica. Otro ejemplo práctico de la utilización de SAT es el descrito en [73] para resolver los problemas que tiene Linux al momento de realizar actualizaciones de paquetes.

El problema de satisfacibilidad tiene como objetivo evaluar toda una fórmula formada por conectores lógicos puede ser verdadera dando a sus variables booleanas valores de verdadero/falso. Procedimientos como SAT27 pueden comprobar fórmulas con cientos de miles de variables debido a las innovaciones de los algoritmos básicos, estructura de datos y el uso de los modernos microprocesadores. El progreso de los SMT solvers, ha permitido que se utilicen para demostrar teoremas, análisis de programas en desarrollo, estáticos y en ejecución, planeación y programación de trabajos en el microprocesador [71].

2.7. Planteamiento del problema SAT

2.7.1. Lógica proposicional y definiciones

La lógica proposicional es una formalización matemática que estudia las proposiciones, sus valores de verdad, su nivel absoluto de verdad a partir de los operadores lógicos.

Operadores Lógicos: son: disyunción ($\vee$), conjunción ($\wedge$), negación ($\neg$), entre otros. Para resolver problemas SAT, se utilizan los tres operadores lógicos arriba mencionados.

Valores de Verdad.- Los valores de verdad pueden ser: verdadero o falso {0,1}, pero nunca una variable puede tomar los dos valores a la vez. Hay 2^n diferentes asignaciones que puede ser definida sobre el conjunto de variables proposicionales.

Variables Proposicionales (VP).- es el conjunto de variables proposicionales X = {$X_1, X_2, X_3 \ldots\ldots X_n$}. Las variables proposicionales pueden tomar el valor de verdadero y falso, en caso de que esté precedida por el símbolo de negación, por ejemplo $\neg X_3$.

Literal es una variable proposicional o la negación de la misma.

Cláusula.- Es una disyunción de literales ($X_1 \vee X_2$). Una cláusula puede ser

unitaria, es decir que contiene un solo literal.

Fórmula: Está dada por la conjunción de las cláusulas $(X_1 \vee X_3) \wedge (\neg X1 \vee X_2) \wedge (X_1 \vee \neg X_3)$.

Una fórmula proposicional está en forma normal conjuntiva si es una conjunción de cláusulas, es decir si es una conjunción de disyunción de literales.

Una valoración σ, es relevante para una fórmula proposicional, φ, si y sólo si σ es una función booleana cuyo dominio contienen a Var (φ), siendo Var (φ) el conjunto de las variables proposicionales de φ. El número de valoraciones relevantes, σ, para la fórmula proposicional φ tal que σ(x)=0 para cada x Ɛ VP – Var (φ), es $2^{|Var(\varphi)|}$. De esta manera, sólo nos preocupamos de los valores que se le asignan a cada una de sus variables [79].

El problema SAT consiste en asignar valores a un conjunto de n variables booleanas x =(x1; x2; …… xn) de forma que satisfagan un conjunto dado de cláusulas c1(x);….; cm(x), donde ci(x) es una disyunción de literales, y un literal es una variable o su negación. Por tanto, podemos definir SAT como una función f: B^n -> B, siendo B = {0,1} tal que:

$$\text{fsat(x)} = C_1(\text{x}) \wedge C_2(\text{x}) \ldots\ldots \wedge C_n(\text{x}).$$

Una solución al problema SAT, x, se dice que es satisfacible si f_{SAT} (x) = 1, e insatisfacible en otro caso.

Un solucionador SAT determina si existe una asignación de las variables de tal manera que la fórmula se evalúa como verdadera o demuestra que no existe tal asignación.

Una interpretación I satisface una variable proposicional positiva x si I(x) = 1.

Una interpretación I satisface una variable proposicional negativa x si I(x) = 0. Una interpretación satisface una cláusula si satisface al menos un literal de la cláusula. Una interpretación satisface una fórmula si satisface todas las cláusulas que ocurren en la fórmula. SAT es el problema de decidir si una fórmula es satisfacible o no [69].

2.7.2. La satisfactibilidad de una fórmula proposicional

Para determinar si un problema es satisfacible dada una fórmula proposicional, consiste en conocer si existe un conjunto de valores tal que al evaluar la fórmula sea 1, es decir si $\exists f(v_1, v_2, v_3 .....v_n) = 1$. Si existiesen tales asignaciones a las variables proposicionales entonces podemos concluir que la fórmula es satisfacible. Los valores asignados, podemos decir que es un modelo que satisface la fórmula. Así también debemos saber de qué posiblemente no sea la única solución, sino que podrían existir otras alternativas de asignación de valor para las variables que satisfagan la fórmula. Si no existe un modelo que haga verdadera la fórmula, entonces decimos que ésta es insatisfactible.

El problema de determinar si una fórmula proposicional dada es satisfactible o insatisfactible, pertenece a la clase de problemas NP-Completo [74], "lo que significa que no se conoce un algoritmo cuya complejidad temporal sea polinomial que puede determinar si una fórmula es satisfactible o no" [75].

2.7.3. SAT Solvers

Los SAT solvers son aquellos algoritmos que nos permitirán determinar si una fórmula es satisfactible o no.

Los solucionadores SAT más exitosos se basan en "búsquedas sistemáticas". La búsqueda se la realiza en un árbol. Cada vértice representa una variable booleana y los bordes hacia fuera que representan las dos opciones (verdaderas

y falsas) para esta variable. Una fórmula que contiene n variables booleanas, el árbol tiene 2n hojas. Cada camino desde la raíz a una hoja corresponde a una asignación de verdad. Un modelo es una asignación de verdad que hace que la fórmula sea verdadera o satisfacible [77].

Entre los algoritmos más populares tenemos el de Davis-Putnam, que fue desarrollado para comprobar la satisfacibilidad de las fórmulas de la lógica proposicional en un conjunto de cláusulas. En este método para cada variable de la fórmula y para cláusula que contenga dicha variable (ya sea positiva o negativa), la resuelve y la agrega a la resolución de la fórmula. Luego se elimina todas las cláusulas que contengan la variable o su negación [72].

Una mejora a este algoritmo es el DPLL, desarrollado por Martin Davis, Hilary Putnam, George Logeman y Donald Loveland. Este método es uno de los más eficaces de solucionadores SAT y trata de construir un modelo con tres operaciones principales: decidir, propagar y dar marcha atrás. Este algoritmo consiste en elegir una variable proposicional y **decide** asignarle un valor de verdad, simplifica la fórmula y seguido a esto recursivamente (propagar) comprueba si la fórmula simplificada es satisfacible. Si la fórmula simplificada es satisfacible, entonces la original también, sino, la recursividad asume el valor de verdad contrario (marcha atrás). Básicamente la simplificación elimina las cláusulas que tienen valor de verdadero, de esta manera, el espacio de búsqueda se reduce. Si la cláusula contiene una sola variable, automáticamente es verdadera. Surge insatisfabilidad parcial si una cláusula se vacía, es decir, si todas las variables que han sido asignadas en una cláusula hacen las variables proposicionales falsas. La insatisfabilidad de la fórmula completa sólo puede detectarse después de una búsqueda exhaustiva.

3. DESARROLLO DE PROPUESTAS

Nuestra propuesta consiste en utilizar el problema de la satisfacibilidad booleana para modelar el conocimiento de los estándares internacionales, marcos referenciales, guías de seguridad y conocer si los requerimientos propuestos por los administradores cumplen con requerimientos de seguridad basados en normas internacionales, caso contrario el sistema propuesto no es viable.

Esta propuesta se ha desarrollado en dos partes:

- La Construcción de los marcos de seguridad basados en normas internacionales.

- La Implementación de un software basado en indicadores de seguridad.

El desarrollo de los marcos de seguridad, la basaremos en 5 aspectos fundamentales:

1) Marco de seguridad de infraestructuras críticas

2) Marco de seguridad considerando cloud computing

3) Marco de seguridad integral

4) Marco de seguridad para una aplicación web

5) Marco integral de gobierno y gestión TI

3.1. Marco de Seguridad Integral

3.1.1. Objetivo

Construir un marco integral de seguridad que abarque todos los aspectos a seguridad relacionados, para poder identificar aspectos importantes en un sistema e-gobierno.

3.1.2. Descripción

Este marco de evaluación fue construido en base a los estándares ISO 27000, 27001, 27002, los frameworks de seguridad GUÍA DE SEGURIDAD (CCN-STIC-804), SANS, e-gobierno Strategy Framework Policy and Guidelines, entre otros.

Se ha reconocido como pilares de la seguridad en un sistema e-gobierno es tener un Marco Administrativo, Marco Operacional y Medidas de Protección.

El Marco Administrativo básicamente es el Gobierno y la Gestión TI, que debe tener todo el sistema gubernamental, liderado por los ministros de estado de las instituciones que lideran. Al tener organizado los ministerios, agencias, y demás organizaciones estatales, el gobierno tendrá un mejor control de todos los activos que tiene y podrá sacar un mejor provecho, apoyándose en las TICs de una manera organizada.

El Marco Operacional tiene las secciones de:

- Control de Acceso
- Control de Activos intangibles
- Control a Incidencias

- Servicios Externos (Cloud Computing)

- Continuidad del Servicio

- Monitorización.

Debido a que la sección del Cloud es extensa, se ha realizado un marco de evaluación separado, el cual se detalla en las secciones posteriores.

La sección de Medidas de Protección está conformada por

- Infraestructura

- Gestión de Personal

- Gestión de Equipos

- Comunicaciones

- Aplicaciones informáticas e información

El marco referencial es el Anexo A. A continuación un esquema del mismo.

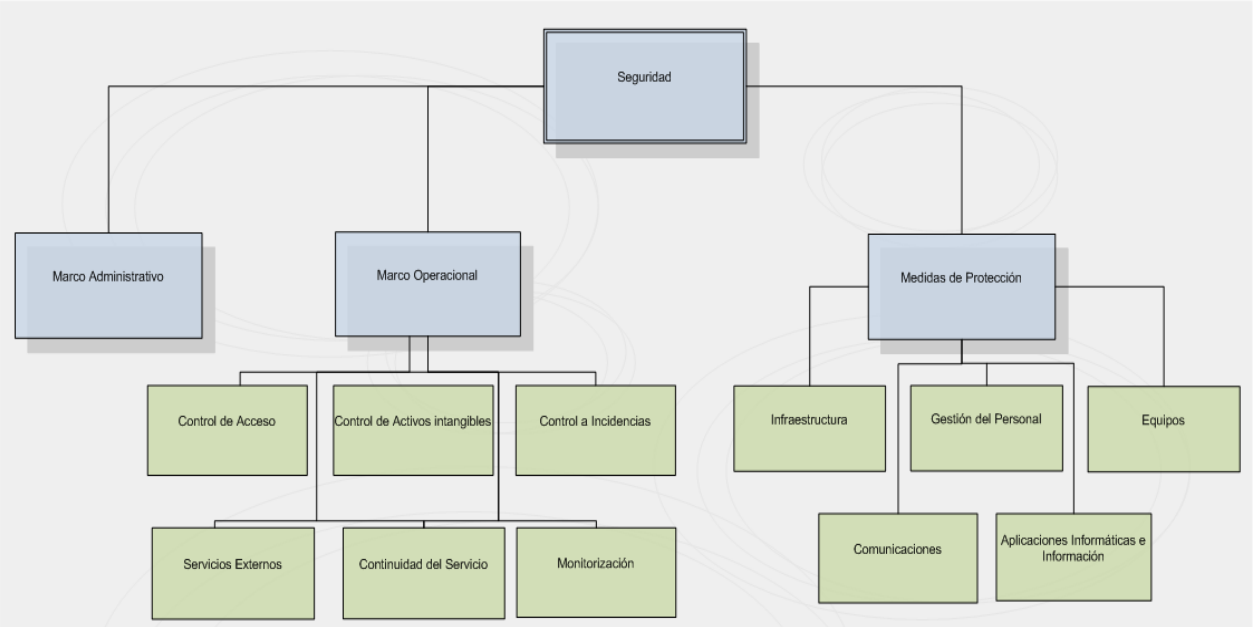


Fig. 3.1. Estructura Framework de Seguridad Integral.

3.2. Marco de gobierno y gestión TI

3.2.1. Objetivo

Construir un marco integral de gobierno y gestión TI, para conocer la potencia de la administración de los recursos informáticos que tenga el estado a nivel nacional, así como también sus falencias mediante indicadores estratégicos.

3.2.2. Descripción

Este marco fue construido en base a los estándares internacionales ISO 38500 para Gobierno TI; ISO 20000 para Gestión TI y los frameworks COBIT 5 y Calder Moir para el marco en general. Se escogió a los indicadores fundamentales para tener una base bastante sólida en Gobierno y Gestión TI.

Se reunió lo mejor de todos estos marcos, de tal manera que se acapare todo lo que un buen Gobierno y Gestión TI necesita para ser integral. Producto de

todo este análisis, podemos decir que un Gobierno y Gestión TI está conformado de la siguiente manera:

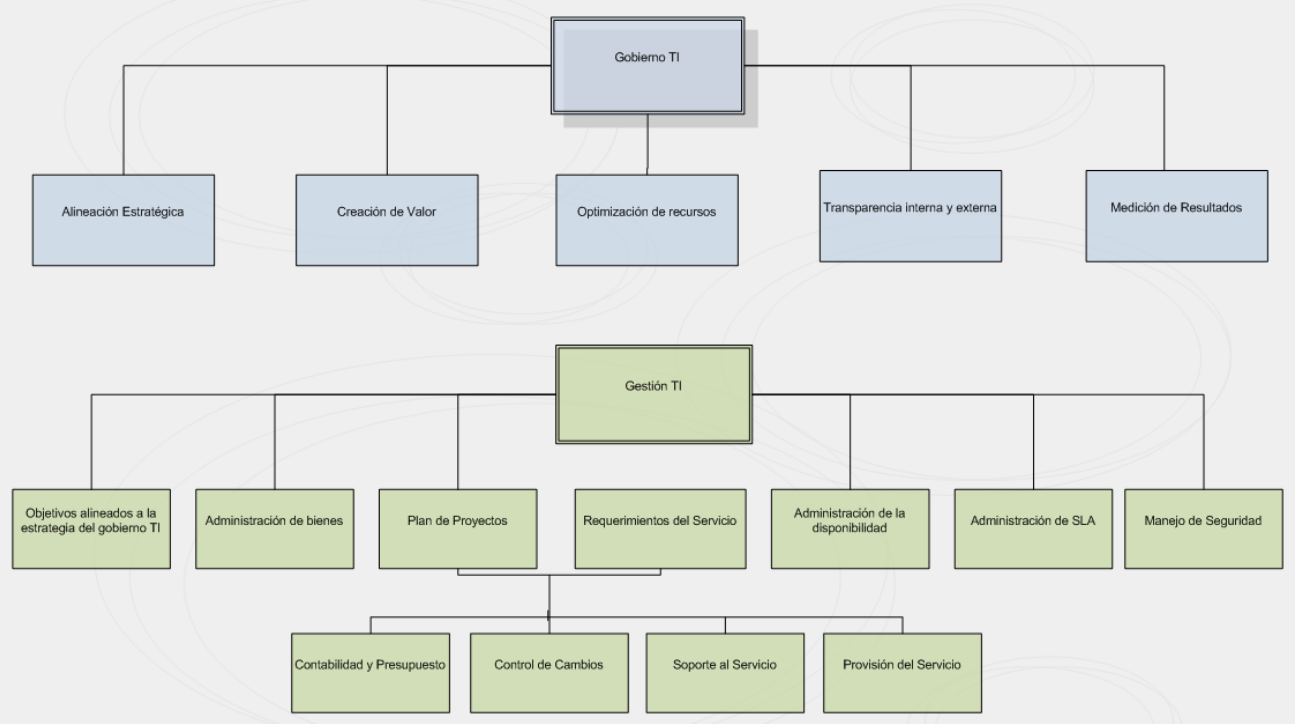


Fig. 3.2. Estructura Framework de Gobierno y Gestión TI

Este marco está dividido en dos partes. La primera, corresponde a los indicadores de Gobierno TI, y la segunda en la Gestión TI.

Basados en los diferentes estándares y macos existentes, se ha identificado que para que exista un buen gobierno TI, se tiene que basar en seis pilares:

- Alineamiento Estratégico
- Creación de Valor
- Optimización de Recursos

- Optimización del Riesgo
- Asegurar la transparencia
- Medición de resultados

La responsabilidad de éstos, depende exclusivamente de la Dirección General, y cada una de ellas tiene que ser: evaluada, orientada y monitorizada.

Así también, la gestión TI tiene que llevar controles en las siguientes secciones:

- Objetivos alineados a la estrategia del Gobierno TI
- Administración de Bienes
- Plan de Proyectos
- Requerimientos del Servicio
- Administración de la disponibilidad
- Administración de SLA
- Manejo de Seguridad
- Contabilidad y Presupuesto
- Control de Cambios

Todos estos son responsabilidad directa de la gestión TI institucional. El marco referencial es el Anexo B.

3.3. Marco de Evaluación Aplicación Web

3.3.1. Objetivo

Construir un marco de evaluación en donde se contemplen parámetros estratégicos para la seguridad de una aplicación online.

3.3.2. Descripción

Este marco fue construido en base a los estándares GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-812), ISO 27000, 27001, SANS, guías OWASP, entre otros.

Se reconoció los parámetros claves de evaluación para poder identificar qué aspectos tendría que tener un sistema web para que brinde seguridad al sistema. Se ha identificado los siguientes puntos claves:

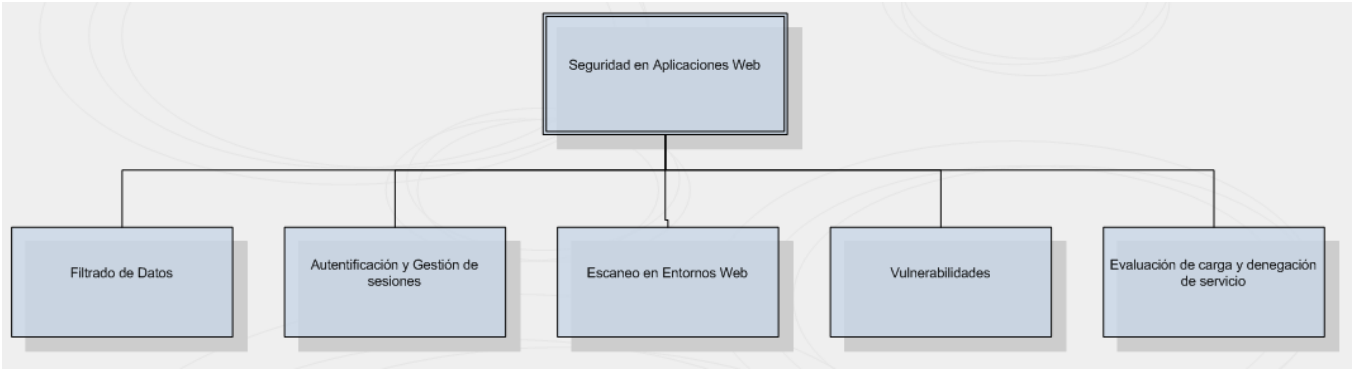


Fig. 3.3. Estructura Framework de Seguridad en Aplicaciones Web.

Se ha identificado las siguientes secciones que deberían ser evaluados los sistemas gubernamentales:

- Filtrado de Datos

- Autentificación y Gestión de Sesiones

- Escaneo de Entornos Web

- Vulnerabilidades

- Evaluación de carga y denegación de servicio

El marco referencial es el Anexo C.

3.4. Marco de Evaluación Cloud Computing

3.4.1. Objetivo

Construir un marco de evaluación que identifique los puntos fundamentales que debe de tener un sistema gubernamental en caso de que este quiera contratar o ya esté corriendo sus aplicaciones en la nube

3.4.2. Descripción

Este marco de evaluación fue construido en base a las ISO 27001, 27002, GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-823), SANS.

Se ha identificado los siguientes pilares para la evaluación de un entorno cloud:

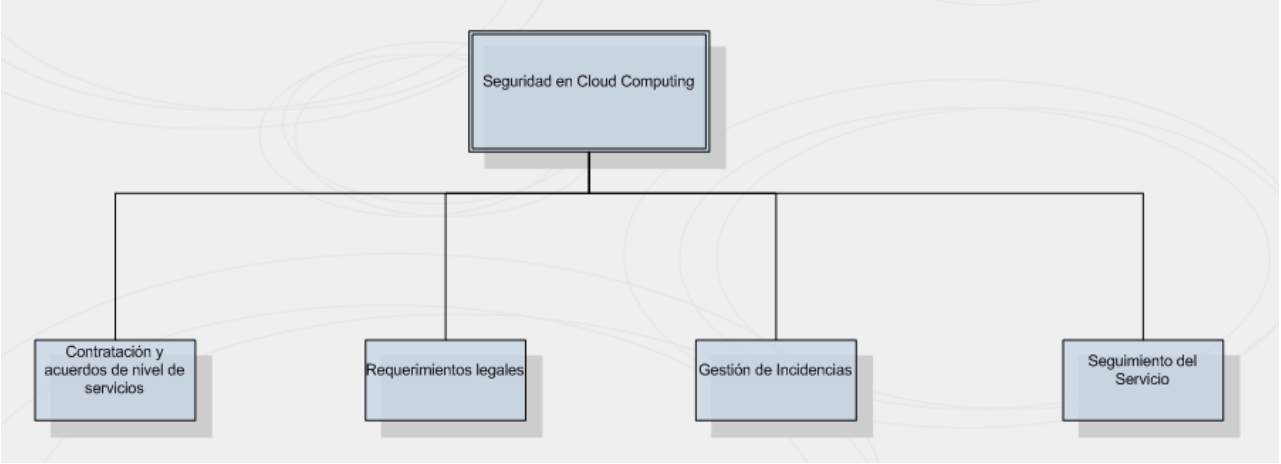


Fig. 3.4. Estructura Framework de Cloud Computing.

El marco referencial es el Anexo D.

3.5. Marco de Evaluación Infraestructuras Críticas

3.5.1. Objetivo

Construir un marco para evaluar el sistema total para que incluya los requerimientos mínimos para estar considerado dentro de las infraestructuras críticas que tiene identificado el estado.

3.5.2. Descripción

Este marco fue construido en base a los siguientes documentos: Estrategia de Seguridad Nacional, Ley 8/2011, de 28 de abril del gobierno de España, Department of Homeland Security Strategic Plan Fiscal Years 2012-2016, del Gobierno de Estados Unidos.

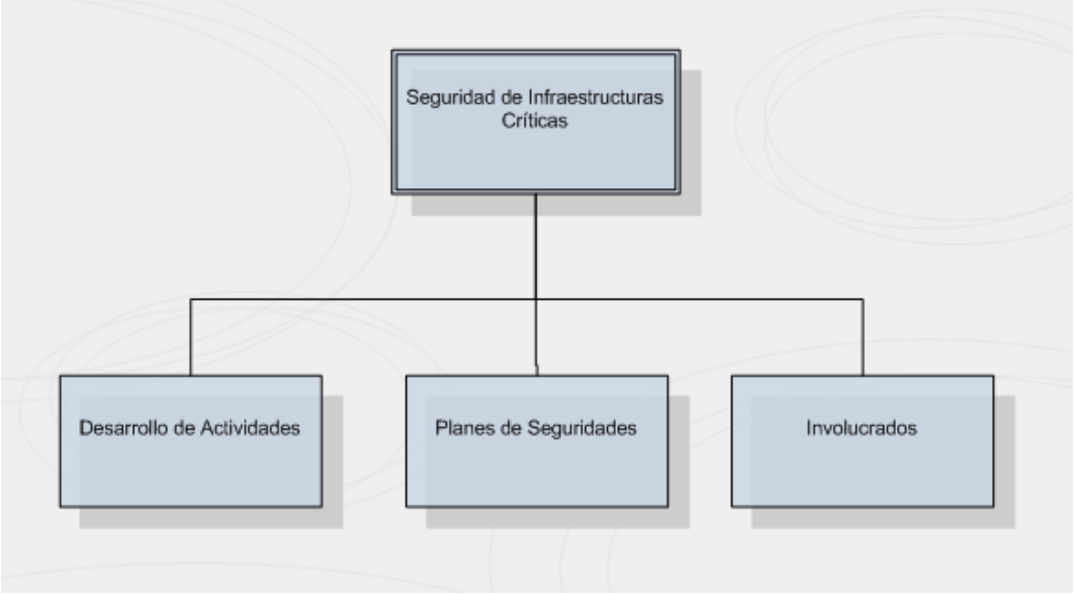


Fig. 3.5. Estructura Framework de Seguridad de Infraestructuras Críticas.

Este marco está basado en tres pilares de evaluación:

- Desarrollo de actividades
- Planes de seguridad
- Involucrados

A cada uno se lo evalúa según ciertos parámetros para conocer si la infraestructura como tal, está colaborando y pertenece a este grupo tan importante y estratégico a nivel nacional. El marco referencial es el anexo E.

3.6. SAT y el sistema para evaluar un sistema E-gobierno

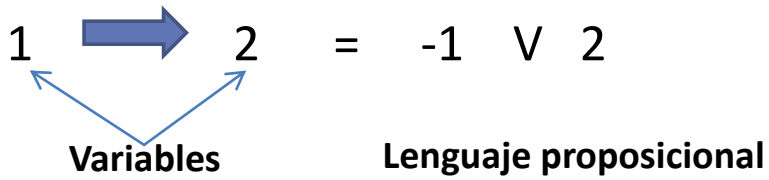
A lo largo de esta investigación, se han identificado aspectos importantes de la seguridad basados en diferentes ISOS, marcos de evaluación conocidos, guías internacionales, entre otros. Pero cómo saber qué aspectos son más cruciales que otros. Cómo saber qué variables de seguridad intervienen directamente en

la elección de los administradores en los sistemas e-gobierno, que son tan delicados, a tal punto de tratarlos como infraestructuras críticas debido a la información que almacenan. Todo este conocimiento recolectado, lo modelaremos de la siguiente manera:

Cada marco de seguridad tiene secciones y cada sección indicadores. Los indicadores (variables proposicionales) son los identificados a lo largo de esta investigación y están plasmados en los anexos. Ahora, para poder verificar la satisfacibilidad de la seguridad en un sistema e-government, se tuvo que crear cláusulas. Un indicador puede estar relacionado con una o muchas cláusulas de diferentes secciones de un marco de seguridad. Las cláusulas fueron construidas en base al conocimiento de los marcos construidos. A continuación un ejemplo de la construcción de las cláusulas:

Cláusula:

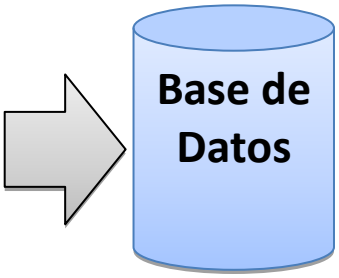
Si existe una Dirección General **entonces** todos los procedimientos, normas, protocolos de seguridad DEBEN estar aprobados y firmados por el Comité o Dirección General.



En lenguaje natural podemos crear la cláusula anterior basada en normas y estándares, pero el problema de satisfacibilidad necesita una fórmula en lenguaje proposicional. En lógica proposicional básica sabemos que p-> q = -p v q, por consecuencia la fórmula 1 -> 2 es equivalente a -1 V 2. Una variable de una sección, puede estar relacionada con cualquier otra de secciones diferentes. Una cláusula puede estar formada por una o muchas variables. Así empezamos a formar cláusulas con cada variable que está en el marco de seguridad creado.

Cada variable tiene su signo y pertenece a una cláusula. Finalizada las cláusulas basadas en conocimiento, las almacenamos en una base de datos.

n_clausula	id_relacionado	componente	signo
6	81	p	-
6	72	c	+
7	93	p	+
7	92	p	+
7	91	p	+
7	90	p	+
7	89	p	+
7	87	p	+
7	84	c	+
8	107	p	-
8	108	p	-
8	106	c	+
8	110	c	+



El esquema de la base de datos es el siguiente:

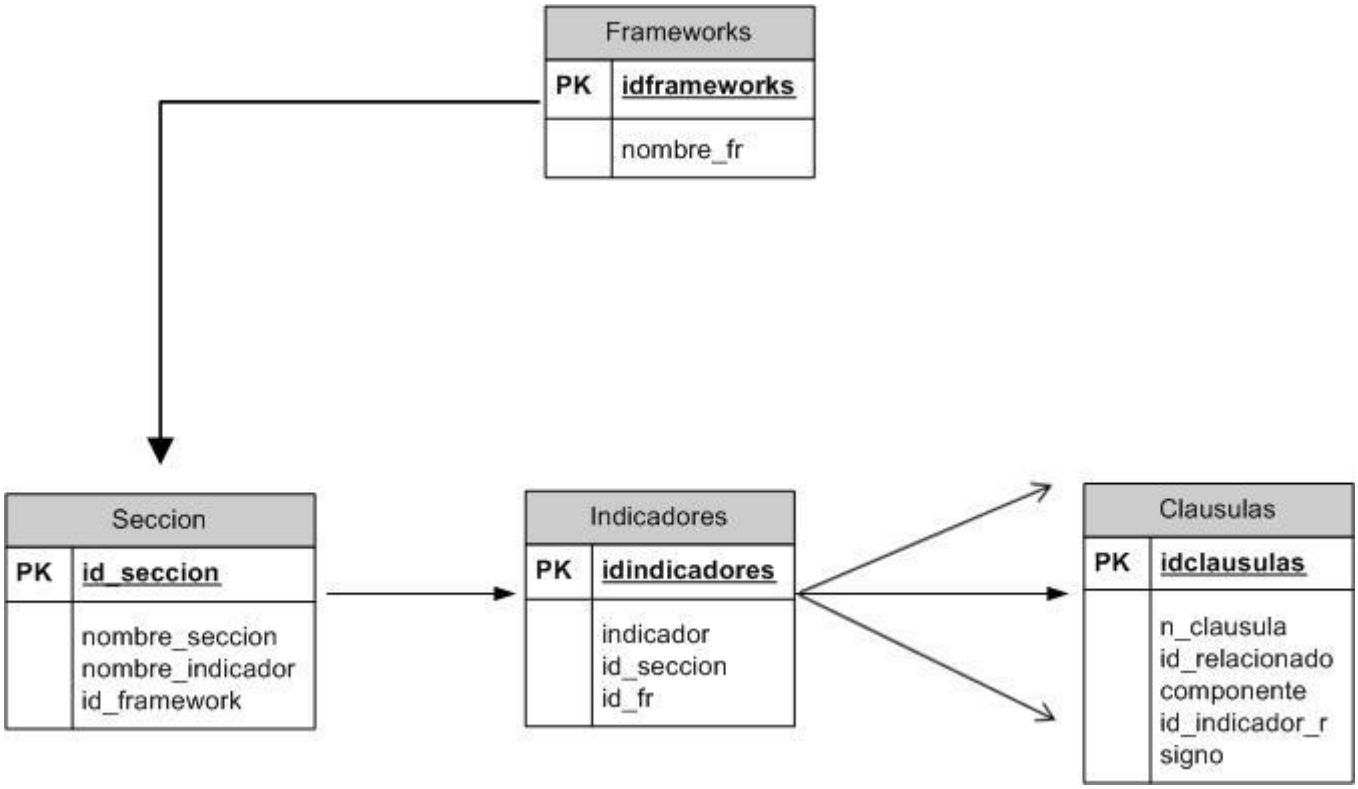


Fig. 3.6. Esquema de las tablas

La base de datos que alberga los indicadores recolectados es mysql. Los datos han sido categorizados en 5, debido a que hay 5 marcos de seguridad diferentes.

Hasta aquí la modelación del conocimiento basado en estándares y guías internacionales.

3.6.1. Herramientas utilizadas y el sistema evaluador

Con los indicadores de seguridad recolectados a lo largo de esta investigación y con la ayuda de los beneficios de SAT se realizó un sistema que evalúe la propuesta de seguridad del administrador de sistemas e-gobierno y conocer si ésta es viable, es decir si es satisfacible a la seguridad según el conocimiento modelado basado en estándares.

El sistema se implementó en lenguaje java, y se ha usado la librería Sat4j: SAT tooltit in java, que implementa solvers para la solución de problemas SAT [76].

La implementación de este sistema, tiene como fin conocer qué variables de seguridad impactan según la elección de los administradores, ya sea que ellos elijan las variables porque así está implementado en la institución, o quizás se quiera implementar tan solo ciertas aspectos, y el administrador no sabe cuál elegir.

Para ejemplificar supongamos que un administrador quiera implementar soluciones de seguridad según las limitaciones del presupuesto asignado. Elige las variables que él considere pertinente, y manda a analizar al sistema. En caso de que los indicadores den como resultado una respuesta satisfacible, él podrá observar las variables que impactan en su decisión; y en caso de que no sea así, dará como resultado que según los indicadores elegidos, no satisfacen la fórmula. El fin es ayudar al administrador a conocer qué variables influyen en

su decisión, y hacen que el sistema sea satisfactible.

En el sistema se presentan las 5 opciones de marcos referenciales de seguridad investigados: Seguridad, Cloud Computing, Gobierno y Gestión TI, Aplicaciones Web, e Infraestructuras Críticas. El usuario tiene que elegir qué tipo de evaluación va a realizar.

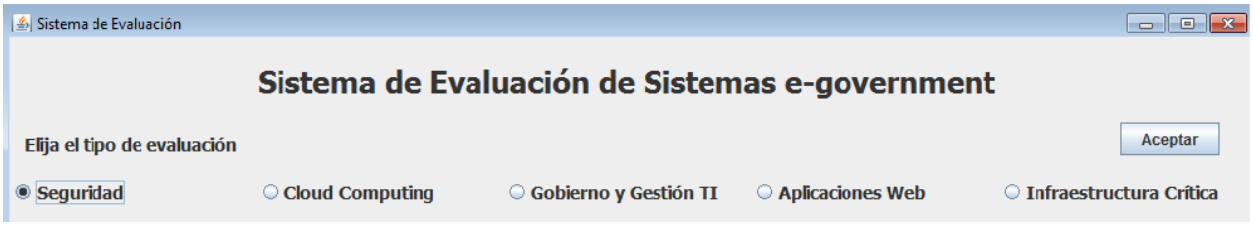


Fig. 3.7. Elección del marco a evaluar

Una vez que se ha elegido el marco a evaluar, aparecen las secciones pertenecientes a ese marco para que el administrador elija las variables a evaluar.

Fig. 3.8. Indicadores de seguridad según el marco elegido

Una vez que el usuario ha elegido las variables que le interesa, el sistema con todas las variables escogidas, entra en todo un proceso de conocer si con todas

las variables escogidas y relacionadas, según las cláusulas que se encuentran en la base de datos, pueden hacer que la fórmula sea satisfacible o no.

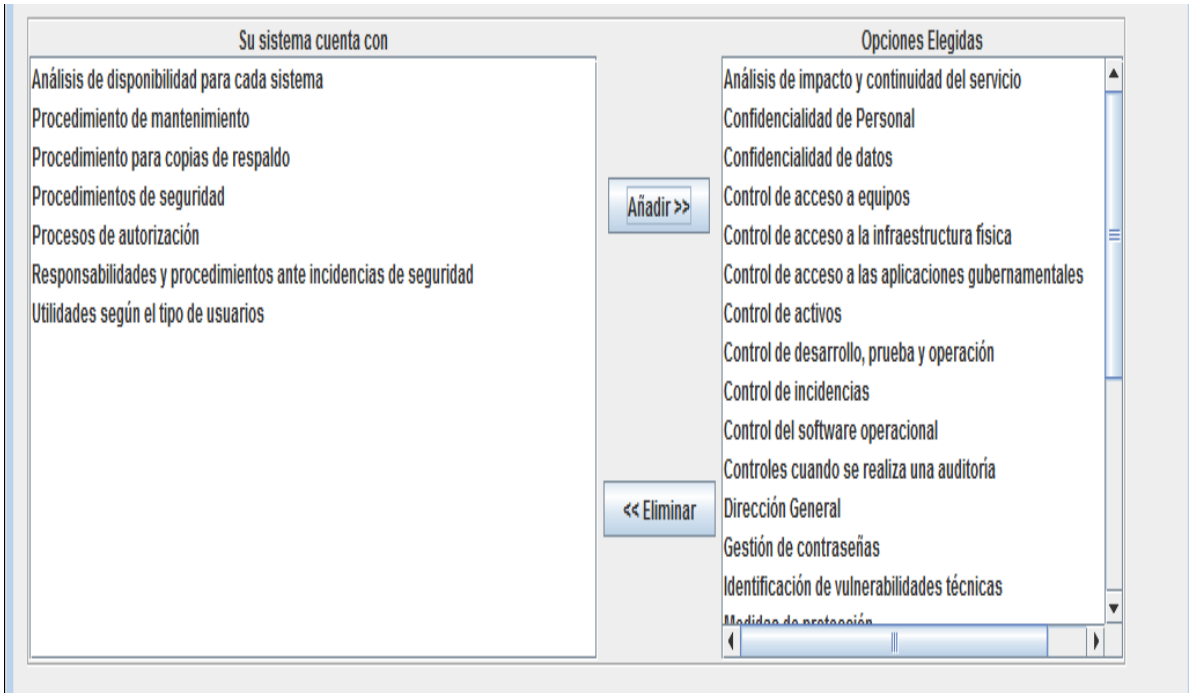
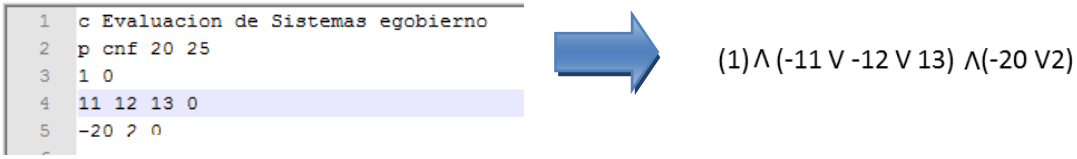


Fig. 3.9. Indicadores de seguridad elegidas por el usuario

Lo que realiza el sistema internamente el sistema, es coger todas las variables y con ella generar una fórmula, la cual está en formato de archivo CNF. Se guarda el archivo .cnf con todas las variables involucradas y creamos un objeto de tipo Solver, mandando a resolver nuestra fórmula con un solver de la librería SAT4j de java.

El archivo cnf es aquel que tiene ya las cláusulas listas para ser enviadas al sat solver y tiene que tener un formato específico; formándose de la siguiente manera:



Formato CNF Lenguaje Proposicional

Fig. 3.10. Formato de archivo cnf.

Observemos que la primera línea empieza con c debido a que es un comentario. Para indicar los parámetros de tipo de archivo, número de variables y cláusulas, se tiene que poner al inicio la letra "p". A partir de esta línea, se ponen las cláusulas, finalizándola cada línea con cero. Si se desea indicar que la variable es negativa, se antecede con el signo "-".

La cláusula está formada por las variables relacionadas, y se puede interpretar de la siguiente manera: a->b. Como el formato del archivo CNF es interpretar las variables de la manera disyuntiva, y se conoce que (a -> b) ≡ (¬a v b). Bajo esta equivalencia se ha procedido a construir cada cláusula.

Las cláusulas son obtenidas de la base de datos. Cada cláusula está formada por un indicador, que es una variable proposicional. La variable proposicional puede ser positiva o negativa. Las cláusulas en el archivo CNF, dependen de las secciones que elija el usuario, e internamente consulta la base de datos tomando las cláusulas relacionadas.

Para ejemplificar la construcción de las cláusulas en nuestro sistema, supongamos que el usuario elige a evaluar la sección de las Bases de la Directiva General del marco de infraestructuras críticas. Esta sección consta de 3 variables relacionadas. Según el conocimiento aprendido, se procede a formar las cláusulas de la siguiente manera:

c Evaluación de Sistemas egobierno // comentario

p cnf 3 4 // archivo cnf de 3 variables y 4 cláusulas

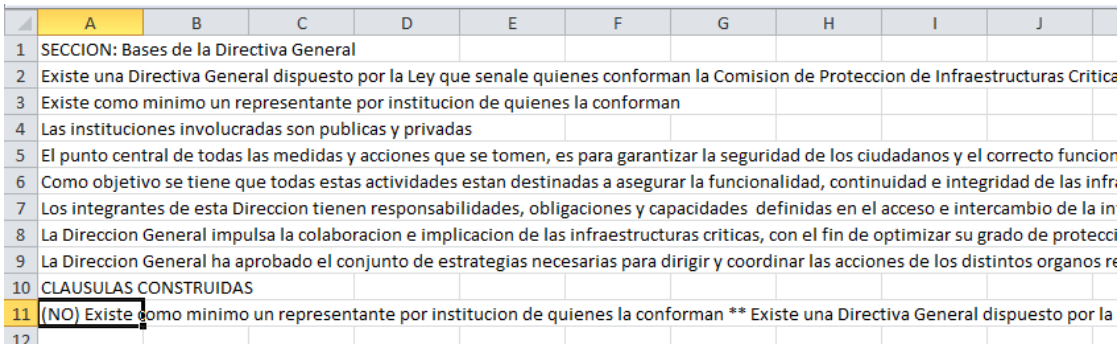
1 0

2 0

3 0

-2 1 0 // Equivalente a 2->1, es decir que para los indicadores: Si existe como mínimo un representante por institución de las infraestructuras críticas **ENTONCES** Existe una Directiva General dispuesta por la Ley que señale quienes conforman la Comisión de Protección de Infraestructuras Criticas.

Así también para que el administrador tenga una mejor interpretación del archivo cnf, se crea un archivo csv, en el que están las variables relacionadas en lenguaje natural.



	A	B	C	D	E	F	G	H	I	J
1	SECCION: Bases de la Directiva General									
2	Existe una Directiva General dispuesto por la Ley que senale quienes conforman la Comision de Proteccion de Infraestructuras Critica									
3	Existe como minimo un representante por institucion de quienes la conforman									
4	Las instituciones involucradas son publicas y privadas									
5	El punto central de todas las medidas y acciones que se tomen, es para garantizar la seguridad de los ciudadanos y el correcto funcion									
6	Como objetivo se tiene que todas estas actividades estan destinadas a asegurar la funcionalidad, continuidad e integridad de las infr									
7	Los integrantes de esta Direccion tienen responsabilidades, obligaciones y capacidades definidas en el acceso e intercambio de la in									
8	La Direccion General impulsa la colaboracion e implicacion de las infraestructuras criticas, con el fin de optimizar su grado de protecci									
9	La Direccion General ha aprobado el conjunto de estrategias necesarias para dirigir y coordinar las acciones de los distintos organos re									
10	CLAUSULAS CONSTRUIDAS									
11	(NO) Existe como minimo un representante por institucion de quienes la conforman ** Existe una Directiva General dispuesto por la									
12										

Fig. 3.11. Archivo csv

Una vez que se ha construido las cláusulas, se procede a escribirlas en el archivo CNF, para luego ser evaluadas por un SAT Solver de java.

ISolver solver = SolverFactory.newDefault();

El Solver va a buscar si según la fórmula dada, el problema tiene solución, es decir si las variables todas pueden dar una solución tal que la conjunción de todas las cláusulas sea igual a 1. El solver nos entrega una solución, es decir un conjunto de variables que hacen que el modelo sea satisfacible.

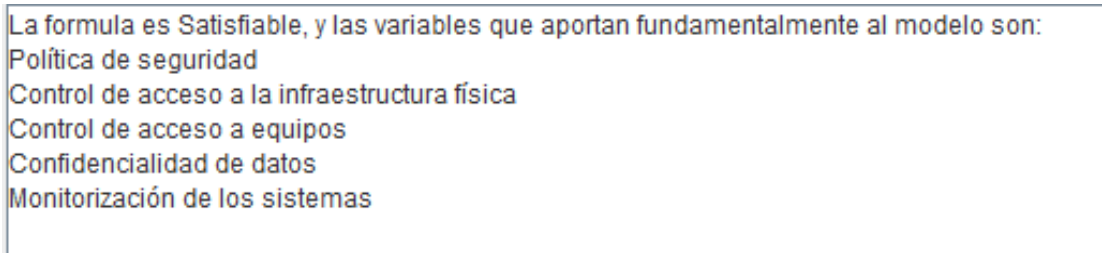


Fig. 3.12. Resultado de la ejecución del sistema

En este caso, con las variables escogidas, tenemos 5 variables que hacen que la fórmula sea satisfacible. Estas variables aportan fundamentalmente al modelo propuesto por el administrador, enfocando la seguridad en estos aspectos, que según las normas y estándares son esenciales.

4. CONCLUSIONES

Se han construido 5 marcos de evaluación de seguridad: seguridad integral, cloud computing, infraestructuras críticas, aplicaciones web y gobierno y gestión TI. Cada marco evalúa a los sistemas e-gobierno según su índole con el fin de conocer sus puntos débiles para fortalecerlos.

Realizar un estándar es de gran importancia para la administración de la seguridad, pero los marcos existentes están desarrollados según su enfoque. Los marcos de evaluación que se han construido, son en base a estándares a nivel mundial, de normas de países punteros en tecnología, de marcos de referencia líderes en gobierno y administración TI y encierran una recopilación de puntos fundamentales y críticos en la seguridad informática.

El marco de evaluación integral evalúa factores administrativos, operacionales y medidas de protección para poder mitigar el riesgo. Al evaluar un sistema de gobierno electrónico con este marco, se puede conocer si se ha considerado índices de seguridad que todo sistema computacional debería de tener con las características de un sistema crítico.

El marco de evaluación de Gobierno y Gestión TI, evalúa si el gobierno TI alinea las estrategias institucionales para que la parte operacional gestione los servicios según la estrategia gubernamental. Es importante que el gobierno conozca cómo administrar los recursos públicos, puesto que todos en la sociedad los pagamos mediante nuestros impuestos. Este marco permite evaluar si antes de empezar un proyecto, éste es analizado, genera valor, tiene el seguimiento correspondiente, si los recursos son bien administrados.

El marco de evaluación de aplicaciones web evalúa si los sistemas han sido

expuestos a pruebas, y siguen estándares de software. Al evaluar un sistema e-gobierno con este marco, se conocerá qué tipo de falencias tiene en cuanto a programación y ciberataques que podría enfrentar.

El marco de cloud computing evalúa si se ha tomado en consideración acuerdos pre-contratos y normas básicas a seguir. Básicamente se ha considerado la confidencialidad, disponibilidad e integridad de la información como un eje fundamental del marco referencial debido a que la información es albergada en los servidores del proveedor y las preguntas evaluadoras son esencialmente a qué acuerdos y cómo maneja la información el proveedor del servicio.

El marco de infraestructuras críticas, evalúa básicamente si los sistemas gubernamentales están considerados en los planes estatales para tratarlos como críticos, el desarrollo de actividades y si se están involucrando adecuadamente. Al evaluar el sistema e-gobierno con este marco, se conoce si se está relacionando adecuadamente con las otras instituciones y guarda la seguridad de la información.

Los marcos de evaluación son integrales y son producto de la investigación de marcos de países líderes en TICs, ISOS, marcos referenciales actuales punteros en el mercado.

Así también se presentó un modelo de un sistema que ayuda a la toma de decisiones respecto a los indicadores de seguridad de un marco en específico elegido por el usuario. Los administradores de los sistemas e-gobierno, se pueden apoyar en esta herramienta que analiza las variables y da una respuesta de tal manera que la seguridad es evaluada en términos proposicionales dando como resultado si la seguridad es satisfacible o no. La aplicación ha sido alimentada con indicadores basados con normas internacionales, que han sido los marcos evaluadores construidos .El sistema determina qué variables son

relevantes en el modelo que el administrador del sistema está construyendo o quiere implementar. Al tener una noción de qué variables influyen en la seguridad de sus sistemas, se puede tener una mejor proyección de seguridad en los sistemas gubernamentales, así como fundamentar la decisión sobre cumplimientos de seguridades apoyadas en cláusulas construidas bajo normas, marcos y protocolos internacionales.

El modelo propuesto proporciona un análisis del que se puede expresar conocimiento indispensable usando SAT. El análisis por medio de SAT, permite realizar inferencias interesantes a partir del conocimiento disponible.

El modelo construido aporta a los administradores de los sistemas e-gobierno los indicadores indispensables a la seguridad propuesta, aportando al conocimiento factores basados de normas internacionales.

Permite plantear problemas de planificación cuyas soluciones pueden aplicarse a problemas concretos basados en factores influyentes como presupuesto, tiempo entre otros.

REFERENCIAS

[1] Baum, C., Di Maio, A. Caldwell, F: "What is eGovernment". Gartner's definitions. *Research Note (TU-11-6474) 2000*.

[2] Wang Jing-Fu: "E-gobierno Security Management: Key Factors and Countermeasure". *Proceedings of IEEE Information Assurance and Security. IAS '09. Fifth International. ISBN: 978-0-7695-3744-3, Conference Location: Xi'an,* (Volume:2), Aug 2009.

[3] Official Web Page ISO.
http://www.iso.org.

[4] Official Web Page ISACA.
http://www.isaca.org.

[5] Official Web Page ITIL.
http://www.itil-officialsite.com

[6] Official Web Page Australian Government.
http://www.nationalsecurity.gov.au/

[7] Official Web British Security.
http://www.britishsecurity.com/

[8] Official Web Page The European Institute, homeland security.
http://www.europeaninstitute.org/

[9] Corporación Autónoma Regional Del César.
http://www.corpocesar.gov.co/files/POLITICA%20DE%20SEGURIDAD.pdf

[10] Eric Bravo, “Diferencias entre Gobierno y Administración”, *Internet Draft*, enero 2010.

[11] Red GEALC SEDI-OEA ICA/IDRC: "Cómo implementar con éxito el gobierno electrónico". *Internet Draft*, Octubre 2008.

[12] Jan van Bon: “ISO/IEC 20000 Una introducción”, ISBN: 9789087532932, marzo 2008.

[13] ISO/IEC International Standar 2008.

[14] José Esteves Rhoda C. Joseph: “A comprehensive framework for the assessment of e-gobierno projects”, Government Information Quarterly 25 (2008) 118-132.

[15] François-Xavier Chevallerau: “The impact of e-gobierno on competitiveness, growth, and jobs”. *Proceedings of Cisco*, February 2005.

[16] Jensen J. Zhao, Sherry Y. Zhao: “Opportunities and threats: A security assessment of state e-gobierno websites”. Government Information Quarterly, Volume 27, Issue 1, January 2010, Pages 49–56.

[17] Eduardo Rodal: “Programa para el establecimiento del gobierno electrónico en América Latina y el Caribe”, Diálogo Regional y Brecha Digital: Promoviendo el Gobierno Electrónico para el Desarrollo Regional.

[18] Evans, K. S. “Expanding e-gobierno: Achieving results for the American people”. Retrieved July 8, 2008,

[19] Promoting e-governance: The Smart Way Forward, Government of India, Eleventh report. December 2008.

[20] Internet World Stats, August 2013.

http://www.internetworldstats.com

[21] Página oficial de UNESCO, 2011

http://www.unesco.org/

[22] Sofia Elena Colesca: "Understanding Trust in e-government", ISSN 1392–2785 Inzinerine Ekonomika-Engineering Economics (3). 2009.

[23] Scott Paquette, Paul T. Jaeger, Susan C. Wilson: "Identifying the security risk associated with governmental use of cloud computing", Government Information Quarterly, Volume 27, Issue 3, 245-253, July 2010.

[24] Symantec:. "Symantec internet Security Threat Report". Symantec Enterprise Security, 12, 1-30. January 30, 2008, http://www.symantec.com

[25] Moen, V., Klingsheim, A. N., Simonsen, K. F., & Hole, K. J : "Vulnerabilities in e-gobiernos". International Journal of Electronic Security and Digital Forensics, Vol 1, No 1, pp 89-100. Proceedings, October, 2007.

[26] Halcnin, L. E. "Electronic government: Government capability and terrorist resources". Government Information Quarterly, Vol 21, No 4, pp 406−419, 2004.

[27] Barbara McNurlin, Ralph Sprague, "Information Systems Management in Practice", 7th ed. ISBN-10: 0131854712, Pearson Prentice Hall, 2006.

[28] S2 Grupo, Antonio Villalón, José Miguel Holguín, Nelo Belda, José Vila: "Protección de Infraestructuras críticas", Reporte, Diciembre 2011.

[29] World Bank. Retrieved March 27 2009.

http://go.worldbank.org/M1JHE0Z280.

[30] Kaspersky Lab Expert: “The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies” January, 2013.

http://www.securelist.com/

[31] Kevin J. O’Brien: “New European Guidelines to address Cloud Computing” The New York Times, July 2012.

http://www.nytimes.com

[32] SANS Institute: “Critical Security Controls”. January, 2013, http://www.sans.org/critical-security-controls/.

[33] The White House: “U.S. Policy on Counterterrorism”, Memorandum 39, June 1995.

[34] The White House: “Combating Terrorism: Presidential Decision Directive 62”, Presidential Decision Directive, May 1998.

[35] Sonia Aparicio: “El mayor atentado de la Historia de España”, El Mundo, Marzo 2004.

[36] Manuel Sánchez Gómez Merelo: "Protección de Infraestructuras Críticas. Un nuevo reto para la convergencia de las seguridades". Internet Draft. Mayo 2012.

http://manuelsanchez.com/.

[37] European Commission:” on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection”, Brussels, December 2008.

[38] European Commission: "Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector", Final Report, September 2009.

[39] Homeland Security: Official Page.
http://www.dhs.gov/

[40] Piers Wilson: "Positive perspectives on cloud security", Information Security Technical Report, Volume 16, Issues 3–4, Pages 97–101, September 2011.

[41] Luis Fernando Espino Barrios: "Cloud Computing como una red de servicios", noviembre 2009.

[42] Javier Areitio: "Protección del Cloud Computing en seguridad y privacidad". Página 42-48, Revista Electrónica, Mayo 2010.

[43] Federal Chief Information Officer: "State of Public Sector Cloud Computing", May, 2010

[44] The White House: "Federal Cloud Computing Strategy", February 2011.

[45] Gobierno de España: "La Conversión de Red SARA como el cloud de la Administración, proyecto de interés prioritario", 2013.

[46] Aleida Alcaide: "La hora del Cloud Computing". *Asociación Profesional del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. Abril 2013*.
http://tools.ietf.org/html/rfc3561.

[47] Portal del ciudadano, Comunidad de Madrid.

[48] Lexdiario: "Plan de Administración Electrónica 2013-2015", Enero 2013.

[49] Matt Bishop "What is Computer Security". IEEE Journals & Magazines, Vol. 1 Issue: 1, pp. 67 - 69, 2003.

[50] Dhillon, G. and Torkzadeh: "Value-focused assessment of information system security in organizations". Information Systems Journal, 2006.16, 293-314.

[51] Walid Al-Ahmad, Reem Al-Kaabi, NYiT Amman, AABFS Amman – Jordan: "An Extended Security Framework for e-gobierno". *Procedins of IEEE International Conference, Intelligence and Security Informatics,* 2008.

[52] Gobierno de Honduras: "Ley de transparencia y acceso a la información pública", 2008.

[53] Observatorio Tecnológico.

http://recursostic.educacion.es

[54] Ingrid Muñoz, Gonzalo Ulloa: "Gobierno de TI". Revista S&T, 9(17), 23-53. Cali: Universidad Icesi, 2011.

[55] Carlos Manuel Fernández Sánchez, Mario Piattini Velthuis: "Modelo para el gobierno de las TIC basado en las normas ISO", 2012.

[56] Weill Peter, Jeanne Ross: "IT Governance: How top performers manage IT decision", Book, Harvard Business School Press, 2004.

[57] ISACA: COBIT: "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa", 2012.

[58] International Standard ISO/IEC 38500, January 2008.

[59] José Antonio Ojeda: "Un marco integrado para el gobierno de TI".

[60] Antoni Bosch Pujol: "Herramientas para la implantación del gobierno de las TI: ISO 38500", Universidad Autónoma de Barcelona.

[61] IT Governance. http://www.itgovernance.co.uk

[62] Osiatis: "ITIL-Gestión de Sesrvicios TI". http://itil.osiatis.es/

[63] Comunicar.inf: "Brasil destina USD25M para estrategia de cloud computing", 2013.

http://www.comunicar.info/

[64] Pcworld: "El sector público comienza a adoptar cloud computing". http://www.pcworld.com.mx/

[65] KPMG: "From Hype to Future: KPMG's 2010 Cloud Computing Survey", 2010.

[66] Secure List, January 2013, http://www.securelist.com/

[67] Seguridad Internautas: http://seguridad.internautas.org

[68] Nicolás Rueda, "Cuatro ciberataques que nos pusieron los pelos de punta", Enter Co, marzo 2013, http://www.enter.co/

[69] Carlos Ansótegui, Felip Manyá "Una introducción a los algoritmos de satisfactibilidad", Revista Iberoamericana de Inteligencia Artificial, vol7, num20, 2003.

[70] Hratch Mangassarian, Andreas Veneris , Farid N. Najm "Maximum Circuit Activity Estimation Using Pseudo-Boolean Satisfiability", IEEE Transactions on computer-aided design of integrated circuits and systems, vol. 31, no. 2, february 2012.

[71] Nicolás Rueda, "Cuatro ciberataques que nos pusieron los pelos de punta", Enter Co, marzo 2013, http://www.enter.co/

[72] Martin Davis and Hilary Putnam. A computing procedure for quantication theory. J. ACM, 7(3):201-215, July 1960.

[73] Argelich, J., Berre, D. L., Lynce, I., Marques-Silva, J., & Rapicault, P. "Solving Linux upgradeability problems using boolean optimization", 2010.

[74] Stephen A. Cook. The complexity of theorem-proving procedures. In Proceedings of the third annual ACM symposium on Theory of computing, STOC '71, pages 151- 158, New York, NY, USA, 1971. ACM.

[75] Ignacio Vissani, Un sat-solver paralelo y distribuido con herencia de cláusulas aprendidas, Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, 2013.

[76] The boolean satisfaction and optimization library in Java, http://www.sat4j.org/

[77] Leonardo de Moura, Nikolaj Bjørner "Checking the satisfiability of logical formulas, SMT solvers scale orders of magnitude beyond custom ad hoc solvers.", communications of the acm, Vol 54, n 9, Septiembre 2011.

[78] Augusto Cortéz, "Teoría de la Complejidad Computacional", RISI 1(1), Revista de Investigación en Informática, páginas 102-105, 2004.

[79] Mario de J. Pérez Jiménez, Fernando Sancho Caparrini, Máquinas moleculares basadas en ADN, Secretariado de la Universidad de Sevilla, Colección de divulgación científica, número2, ISBN 84-472-0777-3, 2003

ANEXO A: MARCO DE EVALUACIÓN DE SEGURIDAD INTEGRAL

Marco Administrativo

Estructura General

Categoría	**Criterio a ser evaluado**
	Existe un Comité o Dirección General que apruebe las políticas, reglamentos, marcos legales, normativas, protocolos, procedimientos, manuales.
Responsabilidades de la Dirección General	Todos los procedimientos, normas, protocolos de seguridad están aprobados y firmados por el Comité o Dirección General
	Existe una política de seguridad escrita aprobada por la Dirección General
	Se tiene planes y programas para mantener la conciencia de la seguridad de la información, del sistema y del servicio
	Cuando se realiza cambios que afecten a la seguridad del sistema en general, se informa a cada responsable de seguridad
	Se realizan evaluaciones periódicas y análisis de la respuesta a los incidentes
	Según los análisis a incidentes, se corrigen defectos o debilidades
	Cada cierto periodo se revisan todos los documentos relacionados con la seguridad
	Se tiene registrado los cambios en los documentos con fechas de modificación y quienes aprobaron y modificaron los documentos
	Existe una Política de Seguridad que está aprobada y firmada por la Dirección o Comité general
	Política de seguridad
	La política de seguridad se basa en los resultados del análisis y gestión de riesgos.
La Política de Seguridad especifica	Una definición de seguridad de información
	Los objetivos y la importancia de la seguridad de la información
	Qué información y cómo se recopila
	Con qué propósito se recolecta esa información
	Cómo se protege la información
	Qué información es pública y privada
	El uso de cookies
	Si esa información se comparte, vende, alquila o se transfiere a otros websites.
La página web tiene	Un link a condiciones y términos de uso

	Un Contacto
	Una sección en la que se le da a conocer al usuario esta información
Los empleados de la organización	Conocen la política de seguridad
	Normativa de Seguridad
	Existe un procedimiento de revisión regular
	Existen reglas para la utilización del correo electrónico e Internet
	Existen reglas para el uso de dispositivos móviles, portátiles, PDAs, etc.
	Existen protocolos que clasifiquen la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización
	Existe una política que indique el control de acceso a la información según su clasificación
La Normativa de seguridad:	Fue escrita por personas expertas en base a la postura de la Organización
	Fue revisada por el departamento de asesoría legal
	Es realista, viable, concisa y sin ambigüedades.
	Es motivadora, descriptiva y define puntos de contacto para su interpretación correcta.
	La conocen los empleados y contratistas que usan o tienen acceso a los activos de la organización
	Son de carácter obligatorio y todos en la organización conocen de las consecuencias en caso de incumplimiento
La Normativa de seguridad en la web especifica:	Qué metodología se está utilizando para encriptar la información transaccional
	Qué metodología de encriptación se utiliza para encriptar los datos sensibles y almacenamiento de datos.
	El certificado de autenticación que se está utilizando
	Si son evaluados por empresas auditoras de seguridad y cada qué tiempo
	El manejo de la seguridad interna
	Cómo la organización se recuperaría ante un eventual desastre
	Lo que se considera uso correcto, así como lo que se considera uso incorrecto.
	Procedimientos de seguridad
	Los procedimientos operacionales están documentados
	Existe un procedimiento para la revisión y aprobación regular de los procedimientos
	Los procedimientos son aprobados por el Comité o Dirección General

	Cuando los procedimientos se actualizan, los empleados son informados de los cambios.
	Los empleados pueden acceder a las versiones recientes de los procedimientos fácilmente
El procedimiento de seguridad detalla	Para cada empleado: rol, responsabilidades y actividades que desempeña
	Quién lo lleva a cabo qué función y cuándo
	Procedimientos de copia de seguridad o respaldos
	Cómo identificar situaciones anómalas y cuál es mecanismo para escalar la situación
	Un proceso para que los usuarios puedan reportar errores, inexactitudes o carencias en los procedimientos.
	Contactos de soporte en el evento de dificultades inesperadas
	Procedimientos para operaciones especiales
	Procedimientos de reinicio y recuperación del sistema en caso de falla del sistema
	Proceso de autorización
	Existe una solicitud que describa el elemento y la actividad para que se solicita autorización
	Si el nuevo componente introduce posibles vulnerabilidades, anexa un análisis de riesgos y las medidas que se toman para gestionarlo según su categoría
	Se contempla el uso de autorizaciones temporales
	La autorización tiene la firma del gerente responsable por el ambiente del sistema de seguridad de información
	El sistema no admite elementos no autorizados
	No se puede acceder al sistema o equipos hasta que el proceso de autorización este completo
El sistema requiere autorización previa para:	La entrada de equipos en producción.
	La entrada de aplicaciones en producción.
	Establecimiento de enlaces de comunicaciones con otros sistemas.
	La utilización de soportes de información.
	La utilización de equipos móviles (móviles ordenadores, portátiles, PDA, entre otros).
Sección Marco Operacional	
	Planificación de seguridad
	Existe documentación del proceso de planificación de la seguridad
	El plan de seguridad está aprobado por el Comité o Dirección Gerencial
	El plan de seguridad contempla las proyecciones de los requerimientos de la capacidad futura

	Los componentes nuevos especifican los requerimientos de los controles de seguridad
	Existen procedimientos para recuperación tras errores
	Existen planes de contingencia
	Se consideran los riesgos del nuevo componente y los controles asociados
Los requerimientos y los controles de seguridad reflejan	El valor comercial de los activos de información involucrados
	El daño comercial potencial que podría resultar de una falla o ausencia de seguridad
	Dimensionamiento / Gestión de capacidades
	La compra del equipo está aprobado por el Comité o Dirección General
	Se tiene en consideración el costo, tendencias de uso y el tiempo en que el recurso será obsoleto según su tecnología
	Se analiza la compatibilidad con el sistema ya en producción
En cuanto a la gestión de capacidades	Están identificados los requerimientos de capacidad de todas las actividades y en proceso de producción
	Se consideran los negocios y sistemas nuevos y las tendencias actuales y proyectadas en las capacidades de procesamiento de la información de la organización
	Se monitorea el rendimiento del sistema de tal manera que se pueda conocer en qué momento se considere el mejoramiento de disponibilidad y eficiencia de los sistemas
Control de Acceso	
	Registro de usuarios
La creación de un nuevo usuario ó o procesos que acceden al sistema	Tiene un procedimiento de autorización
	Tiene asignado un identificador único
	Tiene definido derechos de acceso, así como un conjunto de atributos de seguridad para cada uno
	Conocen de todos sus derechos de acceso por escrito, y han aceptado las condiciones de acceso firmando un documento.
	Identificación y autenticación del usuario
Para todos los usuarios	Existe un procedimiento formalizado de registro de altas y bajas de acceso de usuarios a todos los servicios de la aplicación y del sistema
	Las cuentas de usuario son inhabilitadas cuando el usuario deja la organización
	Las cuentas de usuario son inhabilitadas cuando un funcionario cesa en la función que se desempeñaba

	No se permite el uso de claves compartidas o multiusuario al menos que la Dirección General lo autorice
	El registro de acceso se lo revisa de forma periódica
	Las medidas de identificación y autenticación se aplican en base a la naturaleza de la información
	Las contraseñas están encriptadas
	Las contraseñas se cambian cada periodo de tiempo
	La longitud de la contraseña mínima es 6 caracteres
	El sistema almacena las últimas contraseñas para impedir que los usuarios la vuelvan a usar
	Las contraseñas temporales sólo tienen un tiempo fijo de vigencia
	Las contraseñas se transmiten de forma cifrada
	No se imprimen en pantalla contraseñas
	Para la contraseña se tiene un mínimo de letras y números
	No se permiten caracteres especiales para las contraseñas, códigos ascci.
	En caso de generar una contraseña temporal, sólo valen una vez y en un tiempo determinado y superior a 6 caracteres
	El período mínimo de conservación de los datos registrados será de dos años.
	No se permiten contraseñas deducibles como el nombre del usuario, fechas de nacimiento, etc.
	El sistema permite que los usuarios seleccionen sus contraseñas.
	Los intentos de autenticación son registrados
	Se registran las solicitudes de cambio de contraseñas
	Se envía notificaciones a quien corresponda cuando la cuenta ha sido bloqueda debido a los inicio de sesión fallidos
	Cuando se cambia una contraseña, se verifica el cambio solicitando la contraseña actual
	Cuando las contraseñas se cambian con éxito, se envía un mensaje a la dirección de correo electrónico del titular informando el cambio
	Cuando se cambia una contraseña, el usuario se vuelve a autenticarse obligatoriamente
	Cuando un usuario se olvida una contraseña, la contraseña se cambia en vez de ser recuperada
	Las contraseñas son almacenadas de tal manera de que no permitan la recuperación de la misma
	En las comunicaciones, todos las contraseñas son encriptadas usando SSL

El nivel de acceso asignado al usuario	Corresponde a necesidades de funcionamiento de la Organización
	Es consistente con la normativa de seguridad de la Organización
	No se contradice con el principio de segregación de funciones.
	Se puede saber qué y quién ha realizado acciones en el sistema
Dispositivos de generación de contraseñas dinámicas (si aplica)	El PIN debe ser distinto al identificador de usuario
	Después de 3 números de intentos fallidos, se bloqueará el dispositivo
	Existe una lista actualizada de los usuarios que lo utilizan
	Cuando un usuario no requiere acceso al sistema, tiene que devolver el dispositivo
La autenticación basada en identificador de usuario y contraseña dinámica o de un solo uso	Las contraseñas generadas de forma aleatoria deben valer sólo para una vez.
	La contraseña generada de forma dinámica debe ser superior a 6 caracteres.
	Requisitos de acceso
	Para tener acceso al sistema, todos los usuarios se identifican y autentican
	Se limita el número de intentos de acceso al sistema
	Las medidas de identificación y autenticación se aplican en base a la naturaleza de la información
	Se tiene una lista de usuarios autorizados
	Tiene definido derechos de acceso, así como un conjunto de atributos de seguridad para cada uno
	El usuario tiene un identificador único
	Si la autenticación se realiza mediante claves complementarias, (pública y privada), son generadas con algoritmos de cifrado asimétrico RSA-1024 o equivalente, acompañadas del correspondiente certificado reconocido de autenticidad que cumplirá las especificaciones x.509 v3 o superiores.
	Identificación de equipos en la red
	Existe un mecanismo de identificación automática de equipos en la red
	Con el identificador del equipo, se puede conocer si ese equipo está autorizado a conectarse a la red y a qué red.
	El equipo queda registrado si ingresa al sistema
	Existe una política de control de acceso para dispositivos móviles
	Política de Control de Acceso
	Control de privilegios
	Están identificados los usuarios que tienen privilegios sobre las aplicaciones del sistema

	Existe un proceso de autorización y un registro de todos los privilegios asignados.
	Los privilegios son asignados una vez que se complete el proceso de autorización.
	Se promueve el desarrollo y uso de rutinas del sistema para evitar otorgar privilegios a usuarios
	Los privilegios se asignan con un ID diferente al resto de usuarios
	Uso de las utilidades del sistema
	Se restringe y controla el uso de los programas de utilidad
	Existe un registro de todo uso de las utilidades del sistema;
	Está definido y documentado los niveles de autorización de las utilidades del sistema
	Se limita el uso de las utilidades del sistema a un número práctico mínimo de usuarios autorizados y confiables
	Se limita la disponibilidad de las utilidades del sistema; según la actividad que se realice
	Se eliminaron todas las utilidades innecesarias
	Restricción del acceso a la información
	Se proporcionan menús para contralar el acceso a las funciones del sistema
	Se controla los derechos de acceso de los usuarios: lectura, escritura, eliminación y ejecución
	Se controla los derechos de acceso de otras aplicaciones
	Los outputs de los sistemas de aplicación sólo contienen la información relevante
	Los outputs del sistema se revisan periódicamente
	Control de Activos
	Segregación de funciones y tareas
	Las tareas y áreas de responsabilidad están segregados
	Separación de los medios de desarrollo, prueba y operación
	Los ambientes de desarrollo, prueba y operación están separados
	Está definido y documentado las reglas para la transferencia de software del estado de desarrollo al operacional;
	Los software de desarrollo y operacional corren en sistemas o procesadores de cómputo, y en diferentes dominios o directorios;
	los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no son accesibles desde los sistemas operacionales cuando no se requieren;

	El ambiente del sistema de prueba emula el ambiente del sistema operacional lo más estrechamente posible;
	los usuarios utilizan perfiles de usuario diferentes para los sistemas operacionales y de prueba
	Los menús de los sistemas operaciones y de prueba muestran los mensajes de identificación apropiados para reducir el riesgo de error
	Los datos confidenciales no pueden copiados en el ambiente del sistema de prueba
	Controles de auditoría de los sistemas de información
	Antes de realizar una auditoría, la Dirección General aprobó los requerimientos de la auditoría
	Se acuerdan y controlan el alcance de la auditoría
	Los auditores están limitados a un acceso sólo-de-lectura al software y data
	Mientas la auditoría esté en proceso, tanto los datos como el software tienen la protección apropiada
	Sólo cuando se realizan copias de seguridad, es permitido cambiar el acceso a escritura.
	Se identificaron explícitamente los recursos y su disponibilidad para realizar los chequeos
	Se identificaron y acordaron los requerimientos de procesamiento especial o adicional
	Se monitorearon y registraron todos los accesos a los sistemas incluyendo los sistemas críticos
	Están documentados todos los procedimientos, requerimientos y responsabilidades de la auditoría
	Las personas que llevan a cabo la auditoría son independientes a las actividades auditadas
	Protección de las herramientas de auditoría de los sistemas de información
	El acceso a las herramientas de auditoría de los sistemas de información están protegidas
	Las herramientas de auditoría de los sistemas de información; están separadas de los sistemas de desarrollo y operacionales
	Una vez terminada la auditoría, se han dado de baja las claves secretas otorgadas a los auditores
	Las herramientas que se utilizaron en la auditoría fueron dadas de baja
	Proceso de gestión de derechos de acceso

	Se tiene documentado a qué usuarios se autoriza el acceso según el tipo de información y los atributos relacionados con el referido acceso
	Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, datos recabados para fines policiales, tienen medidas fuertes de seguridad para poder acceder a éstos
	Se contempla el Control de Acceso
	Se contempla el Registro de Usuarios
	Se contempla la Gestión de Privilegios
	Se contempla la política de control de acceso
	Cancelación de los derechos de acceso
	Cuando se termina un contrato, ya sea de un empleado, contratista o terceras personas que tenían derecho al acceso de la información, aplicación o red del sistema, se retiran todos los derechos de acceso
	En caso de que se cambie de funcionalidades un usuario, se revisan todos los derechos accesos actuales, con el nuevo puesto, para de esa manera determinar qué accesos se cancelan y cuáles son los nuevos a los que tiene derecho
	Los derechos de acceso que se retiran o adaptar incluyen el acceso físico y lógico, llaves, tarjetas de identificación, medios de procesamiento de información, suscripciones; y el retiro de carnet de identificación institucional
	Si un usuario que está dejando la organización conoce las claves secretas para las cuentas aún activas, éstas se cambian inmediatamente.
	Las personas que se van, son retiradas de las listas de acceso
	Se comunica a todos los otros usuarios empleados, contratistas y terceros involucrados para que ya no compartan información con la persona que se va.
	Revisión de los derechos de acceso del usuario
	Existe un proceso formal para la revisión de derechos de acceso
	La revisión se realiza periódicamente y cuando un usuario deja la institución
	Los derechos de acceso del usuario se re-asignar cuando se traslada de un empleado a otro dentro de la misma organización
	Los cambios en las cuentas privilegiadas se registran
	En cuanto a los derechos de acceso se tiene en cuenta las necesidades de cada persona según su función en la organización y las tareas que tiene encomendadas

	La necesidad de acceso está acreditada por escrito por parte del responsable de la información o proceso al que va a concedérsele acceso
	El reconocimiento de la necesidad de acceso está reasegurado periódicamente, extinguiéndose cuando no se demuestre positivamente que la necesidad perdura
	Mecanismo de autenticación
	Se tiene en consideración los requisitos de acceso
	Se tiene en consideración el control de acceso
	Se tiene en consideración la Identificación y autenticación del usuario
	Gestión de las contraseñas secretas de los usuarios
	En los términos y condiciones de empleo, está estipulado que los usuarios deben mantener confidenciales las claves secretas
	Si un usuario tiene sus propias claves secretas, inicialmente se le proporciona una clave secreta temporal segura
	Hay procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta nueva, sustituta o temporal
	Las claves secretas temporales son únicas y no son fáciles de adivinar
	Las claves secretas tienen una fuerte seguridad
	Las claves secretas predeterminadas por el proveedor son cambiadas inmediatamente después de la instalación de sistemas o software.
	Uso de contraseñas secretas
Todos los usuarios tienen que	Mantener confidenciales las contraseñas secretas
	Evitar un registro en papel o dispositivos de las contraseñas
	Cambiar las claves secretas cuando haya el menor indicio de inseguridad de la contraseña
	Seleccionar claves mínimo suficiente que sean fáciles de recordar
	Seleccionar contraseñas que no sean vulnerables a los ataques de diccionarios
	Seleccionar contraseñas libre de caracteres consecutivos idénticos
	Deben de cambiar la clave secreta temporal en el primer registro de ingreso
	Está prohibido compartir las claves secretas individuales
	Acceso a través de redes
	Acceso remoto (remote login)

	Existe un tratamiento específico que regula las actividades que pueden realizarse remotamente
	Se tiene medidas de protección en las conexiones respecto al trabajo que se realiza fuera de la organización
	Acceso a través de redes
	Para terceras partes (si aplica)
	Se tiene un análisis de riesgos del acceso por usuarios externos a la organización
	Se tiene un procedimiento de protección de activos
	Se tiene un procedimiento de medidas de protección física, contra la introducción y propagación de virus o código dañino
	Está fijado el método de acceso permitido
	Existe una lista actualizada de los usuarios externos autorizados a recursos o activos específicos
	Están estipuladas las horas y fechas de disponibilidad del servicio
	Está contemplado en el contrato el derecho de auditoría
	Está contemplado en el contrato las restricciones en cuanto a la protección de datos de carácter personal
	Está contemplado en el contrato las restricciones contra la copia y la revelación no autorizada
	Está contemplado en el contrato la devolución de documentación y activos de información al finalizar el contrato
	Control de Activos Intangibles
	Inventario de Activos
	Existe el inventario
	Existe un inventario de los componentes desmantelados
	existen de procedimientos formales de mantenimiento del inventario
	Identificación y clasificación de activos a proteger
	Se debe realizar y mantener un inventario de los activos a proteger
	Para cada activo se tiene identificado su valor e importancia en términos cuantitativos o cualitativos
	Inventario de los activos
	El inventario de los activos incluye toda la información necesaria para poder recuperarse de un desastre.
	El inventario de activos considera los niveles de protección según la importancia de los activos
	Se ha considerado todos los tipos de activos: información, software, físicos, servicios, personas e intangibles
	Propiedad de los activos

	El encargado del activo asegura que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente
	El encargado del activo define y revisa periódicamente las restricciones y clasificaciones de acceso
	Fortificación o bastionado (proceso en el marco de cualquier proyecto que contemple la aplicación de controles de seguridad sobre los sistemas de información.)
	Existe un procedimiento de eliminación de cuentas o contraseñas estándar
	Existen perfiles avalados por una autoridad reconocida
	Existen procedimientos de configuración que garanticen la aplicación de dichos perfiles
	Existe un procedimiento de revisión periódica de los perfiles
	Existe un procedimiento de revisión de perfiles atendiendo a la publicación de vulnerabilidades de los sistemas
	Gestión de la configuración
	Existe un procedimiento para modificar la configuración del sistema que exige la aprobación del responsable
	Se han realizado las pruebas de la seguridad del sistema bajo la nueva configuración
	Se realizan copias de seguridad de la configuración cubriendo al menos la configuración actual y la inmediata anterior
	Copias de Respaldo
	Existen los procedimientos de realización, recuperación y pruebas de las copias de respaldo
	Está definida la periodicidad de respaldo y el número de las copias
	Está definido las versiones que se conservan de las copias
	Los procedimientos de realización de copias son automáticos
	Cuando se realiza un cambio en el sistema, se realiza la respectiva copia de respaldo
	Está definido el procedimiento de las versiones que se conservan de las copias
	Los procedimientos de realización de copias son automáticos
Para el mantenimiento del sistema, se ha considerado	Se sigue el procedimiento de respaldo, recuperación y pruebas de las copias de respaldo
	Las versiones de las copias
	Los procedimientos de realización de copias son automáticos
	Desarrollo y explotación
	Los cambios y modificaciones en el sistema no reducen la efectividad ni la seguridad del mismo

	En caso de requerir nuevos cambios, se informa al departamento correspondiente para que sea considerado en el Plan de Contingencias
	Se realizan mantenimientos preventivos
	Ante una eventualidad en el sistema, no se reduce la efectividad ni la seguridad del mismo
	Ante una incidencia, se informa al departamento correspondiente para que sea analizado conforme a la seguridad
	Control del software operacional
Actualización del software operacional	La actualización del software operacional, aplicaciones y bibliotecas de programas sólo es realizada por administradores capacitados con la apropiada autorización gerencial
	Los sistemas operacionales sólo tienen códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;
	Antes de lanzar la aplicación, ésta fue sujeta a pruebas extensas y satisfactorias que incluyan pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario
	Se ha establecido un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema;
	Se ha establecido una estrategia de rollback antes de implementar los cambios
	Se tiene una metodología de versiones previas del software de la aplicación
	Se archivan las versiones antiguas del software, junto con parámetros, procedimientos, configuración y software de soporte durante todo el tiempo que se mantengan la data en archivo.
	La organización ha analizado los riesgos de trabajar con software que no cuenta con soporte
	Para actualizar a una versión nueva, se considera la severidad de los problemas de seguridad que afectan esta versión.
	Las actividades del proveedor se monitorean
	A los proveedores se les da acceso físico o lógico para propósitos de soporte, y con aprobación de la gerencia
Mantenimiento de Software Operacional	El mantenimiento del software operacional, sólo es realizada por administradores capacitados con la apropiada autorización gerencial
	El mantenimiento en el software operacional ha sido aprobado por la Dirección de la Gerencia
	El mantenimiento sigue un procedimiento y está documentado en qué ha consistido

	Se ha establecido una estrategia de rollback antes de implementar el mantenimiento
	Se ha realizado el backup correspondiente antes del mantenimiento
	El backup nuevo se archiva con sus respectivas configuraciones
	El mantenimiento se monitorea
	Se da acceso físico o lógico dependiendo del mantenimiento
Cambio en Software Operacional	Los cambios en el software operacional, sólo es realizada por administradores capacitados
	Antes de realizar el cambio, la versión nueva fue sujeta a pruebas extensas y satisfactorias que incluyan pruebas de utilidad, seguridad, sobre los sistemas
	Se ha establecido una estrategia de rollback ante cualquier eventualidad
	Para realizar un cambio, se considera la severidad de los problemas de seguridad que afectan esta versión.
	El cambio es monitoreado
	Control de las vulnerabilidades técnicas
Se ha analizado y documentado	Información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando
	La exposición de la organización a las vulnerabilidades evaluadas
	Las medidas apropiadas tomadas para tratar los riesgos asociados.
En el proceso de gestión de vulnerabilidades técnicas, se ha considerado	Definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica
	Monitorear la vulnerabilidad
	Evaluación del riesgo de la vulnerabilidad
	Monitorear los activos y cualquier responsabilidad de coordinación requerida
	Están identificados los recursos de información que se utilizan para identificar las vulnerabilidades técnicas relevantes
	Está definida una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;
	Identificada la vulnerabilidad técnica potencial, la organización analiza los riesgos asociados y las acciones a tomarse
Antes de instalar un parche	Se han realizado pruebas exhaustivas
	Se ha realizado una evaluación de los riesgos que éste conlleva
Si el parche no está disponible, se considera cualquiera de las	Desconectar los servicios o capacidades relacionadas con la vulnerabilidad

siguientes acciones	Adaptar o agregar controles de acceso
	Mayor monitoreo para detectar o evitar ataques reales
	Elevar la conciencia acerca de la vulnerabilidad
	Mantener un registro de auditoría de todos los procedimientos realizados
	El proceso de gestión de vulnerabilidad técnica debiera ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia
En etapa de mantenimiento	Se ha planificado el mantenimiento y dado a conocer a los empleados
	Mientras se realiza el mantenimiento, se está monitoreando el sistema
	En caso de un fallo, existe un procedimiento para actuar ante alguna eventualidad
Antes de realizar el cambio, se tiene conocimiento de	Las medidas apropiadas en cuanto a la seguridad
	La exposición de la organización a las vulnerabilidades evaluadas
	Las medidas apropiadas tomadas para tratar los riesgos asociados.
	Está definida una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;
Antes de instalar un parche	Se han realizado pruebas exhaustivas
	Se ha realizado una evaluación de los riesgos que éste conlleva
Si el parche no está disponible, se considera cualquiera de las siguientes acciones	Desconectar los servicios o capacidades relacionadas con la vulnerabilidad
	Adaptar o agregar controles de acceso
	Mayor monitoreo para detectar o evitar ataques reales
	Elevar la conciencia acerca de la vulnerabilidad
	Mantener un registro de auditoría de todos los procedimientos realizados
	El proceso de gestión de vulnerabilidad técnica debiera ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia
Mantenimiento	
	Existen procedimientos para llevar a cabo las especificaciones del fabricante en cuanto a mantenimiento
Disponibilidad	
En la instalación	Existen medidas de protección física del cableado.
	Al instalar un software, se tienen identificadas las vulnerabilidades del software instalado, consultando las fuentes apropiadas
	Periódicamente se actualiza el software usado
	Se deben diseñar de forma adecuada las redes

En el cambio	Existen medidas de protección física del cableado.
	Mientras se realiza el cambio se está monitoreando el sistema
	Mantenimiento de equipos
	El equipo se mantiene en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor;
	Sólo el personal de mantenimiento autorizado lleva a cabo las reparaciones y da servicio al equipo;
	Se mantiene registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo
	Se han implementado los controles apropiados cuando se programa el equipo para mantenimiento
	Se revisa la información confidencial del equipo
	Se cumplen con todos los requerimientos impuestos por las pólizas de seguros.
	Gestión de cambios
	Existe un procedimiento para cambiar componentes del sistema
	El cambio ha sido aprobada por la Dirección General
	Existe una documentación del cambio
	Se realizan copias de seguridad de los componentes software, cubriendo al menos la versión actual y la inmediata anterior
	Se actualiza el inventario de activos
	Se actualizan los procedimientos operativos relacionados con el componente actualizado
	Se actualiza el plan de continuidad
	Protección frente a código dañino
	Integridad
	Se han instalado exploradores del software, con actualización periódica.
	Existen procedimientos para evitar la instalación de software no autorizado por la organización
	Los programas de protección, están activados y actualizados de forma automática
	La cobertura de los programas de protección alcanza a todos los equipos: servidores y puestos de trabajo
	El correo entrante y saliente se analiza para detectar y eliminar contenidos activos indeseables
	Los puestos de usuario se configuran para bloquear código dañino
	Gestión de incidencias
	Todos los sistemas disponen de un procedimiento de respuesta que debe estar automatizado

	Se cubren todos los procesos internos a la organización
	Se incluye la forma de recibir notificaciones de servicios prestados por terceras partes
	Se incluye la notificación a terceras partes que pudieran verse afectadas
	Gestión y registro de incidencias
	Existe un procedimiento de recuperación de los datos
	Se tiene registrado el usuario que ejecutó el proceso
	Los datos restaurados y, de ser el caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación
	Para la ejecución de los procedimientos de recuperación de los datos, existe una previa autorización
	Responsabilidades y procedimientos
	Se han establecido las responsabilidades y los procedimientos ante los incidentes de la seguridad de la información.
	Se reportan los eventos y debilidades en la seguridad de la información
Se han establecido procedimientos para manejar los diferentes tipos de incidentes en la seguridad de la información, como	fallas del sistema de información y pérdida del servicio
	código malicioso
	negación del servicio
	errores resultantes de data comercial incompleta o inexacta
	violaciones de la confidencialidad e integridad
	mal uso de los sistemas de información
Los planes de contingencia incluyen	Análisis e identificación de la causa del incidente
	Contención
	Planeación e implementación de la acción correctiva para evitar la recurrencia
	Comunicaciones con aquellos afectados por o involucrados con la Recuperación ante incidentes
	Reportar la acción a la autoridad apropiada
	Aprender de los incidentes en la seguridad de la información
	Se han establecido mecanismos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información
	La información obtenida de la evaluación de los incidentes en la seguridad de la información es utilizada para identificar los incidentes recurrentes o de alto impacto
	Se han incrementado los controles adicionales para limitar la frecuencia, daño y costo de ocurrencias futuras

	Monitoreo y revisión de los servicios de terceros
	Los servicios, reportes y registros provistos por terceros son monitoreados y revisados regularmente
Existe una relación y proceso de gestión de servicio entre la organización y la tercera persona para	Monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos
	Revisar los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme los acuerdos
	Proporcionar información sobre incidentes de seguridad de la información
	Revisar los rastros de auditoría de terceros y los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado
	Resolver y manejar cualquier problema identificado
	De parte de la organización se ha asignado a una persona o grupo de personas para manejar la relación con terceros
	Se ha puesto a disposición las capacidades y recursos técnicos para monitorear los requerimientos de seguridad de la información
	Se toman acciones apropiadas cuando se observan deficiencias en la entrega del servicio
	La organización tiene el control y la visibilidad general con relación a toda la información que es manejada por terceros
	Registro de la actividad de los usuarios
	Existen registros para todas las actividades realizadas en el sistema
	Existe un proceso formal para determinar el nivel de detalle de los registros basado en el análisis de riesgos
	Existen mecanismos que garanticen la hora a la que se realiza el registro, en prevención de manipulaciones de los relojes
	Se realiza una inspección regular de los registros para identificar anomalías en el uso de los sistemas (uso irregular o no previsto)
	Se utilizan herramientas automáticas para analizar los registros en busca de actividades fuera de lo normal
	Control de la seguridad
	La aplicación tiene un registro de eventos que registre al identificador de usuario, fecha, hora, y proceso realizado

	El registro se revisa periódicamente para asegurar que se cumpla con la política de acceso
	Se registran las fallas para asegurar que se identifiquen los problemas en los sistemas de información
Los registros para controlar la seguridad tienen como mínimo	Ids de usuarios
	Fecha y hora de entrada y salida
	Registros de intentos de acceso fallidos y rechazados al sistema;
	Registros de intentos de acceso fallidos y rechazados a la data y otros recursos
	Violaciones a la política de acceso y notificaciones para los 'gateways' y 'firewalls' de la red
	Alertas de los sistemas de detección de intrusiones
	Cambios en la configuración del sistema
	Uso de privilegios
	Uso de las utilidades y aplicaciones del sistema
	Archivos a los cuales se tuvo acceso y los tipos de acceso
	Direcciones y protocolos de la red
	Alarmas activadas por el sistema de control de acceso
	Activación y desactivación de los sistemas de protección
	Los administradores del sistema no tienen permisos para borrar o desactivar los registros de sus propias actividades
	Uso del sistema de monitoreo
Para usuarios con privilegios se tiene registrado	inicio y apagado del sistema;
	dispositivo I/O para adjuntar y eliminar lo adjuntado;
	El uso que le da a las cuentas privilegiadas (administrador, root, etc)
Alertas o fallas del sistema como	Alertas o mensajes en la consola;
	Excepciones del registro del sistema;
	Alarmas de la gestión de la red
	Alarmas activadas por el sistema de control de acceso
	Cambios o intentos de cambio en los marcos y controles del sistema de seguridad
	Los resultados de las actividades de monitoreo son insumos para considerar factores de riesgo
Los factores de riesgos que se han considerado son	Grado crítico de los procesos de aplicación
	Valor, sensibilidad y grado crítico de la información involucrada
	Antecedentes de infiltración y mal uso del sistema, y la frecuencia con la que se explotan las vulnerabilidades
	Desactivación del medio de registro

	Registros del administrador y operador
Los registros incluyen	La hora en la cual ocurre un evento (éxito o falla);
	Información relativa al evento
	Cuál cuenta y cuál operador o administrador está involucrado
	Cuáles procesos están involucrados.
	Sincronización de relojes
	Los relojs del sistema y dispositivos están coordinados y tienen una hora estándar
	Existe un procedimiento que chequee y corrija cualquier variación significativa
	Registro de la gestión de incidencias
Al ocurrir una incidencia, en el registro, se tiene constancia de	Existe un procedimiento formal para determinar las evidencias requeridas de cara a un proceso judicial
	Tipo de incidencia
	Hora exacta
	Persona que realiza la notificación
	A quién lo notifica
	Los efectos de la misma
	Las incidencias se notifican al encargado de seguridad
	Se toman acciones apropiadas relacionadas al acceso y control de usuarios
	Gestión de los incidentes y mejoras en la seguridad de la información
	Existen procedimientos y asignación de responsabilidades para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados.
	Existe un proceso de mejoramiento continuo para la respuesta, monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información.
	Protección de los registros
	Existe un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política
	Existe un procedimiento formal para la retención de evidencias tras un incidente
	Existen mecanismos para prevenir el acceso a los registros de personas no autorizadas
	Existe un procedimiento para la eliminación de los registros tras un periodo estipulado
	Los registros están contemplados en los procesos de copias de seguridad
	Se protegen los ficheros de recogida de eventos
	Monitoreo

	Se monitorean los sistemas y se reportan eventos de seguridad de la información
	Se registran las fallas para identificar los problemas en los sistemas de información
	Protección del registro de información
Los registros incluyen	Las alteraciones registradas a los tipos de mensajes
	Los archivos de registro que se editan o borran
	Control en la capacidad de almacenamiento de los registros
	Gestión de claves criptográficas
	Existe una política sobre el uso de controles criptográficos
	Existen procedimientos y medios para cada una de las fases del ciclo de vida de las claves criptográficas
	Existe evidencia de que se aplican los procedimientos establecidos
	Existe un registro que indica las actuaciones realizadas sobre cada clave en el sistema, a lo largo de su ciclo de vida
	Los medios de generación están aislados
	Cuando se destruyen las claves criptográficas, se elimina el original y la copia
Se protegen las claves criptográficas	Durante la generación con programas evaluados o dispositivos criptográficos certificados
	Durante su transporte en el uso de contenedores criptográficos
	Durante su transporte en doble canal: clave y datos de activación por separado
	Durante la custodia en la tarjeta inteligente protegida por contraseña
	Durante la custodia en dispositivo criptográfico certificado con control de acceso
	Durante copias de seguridad de claves activas y retención de claves retiradas de explotación activa en contenedores físicos seguros (por ejemplo, caja fuerte), en contenedores criptográficos, en medios alternativos aislados de los medios de explotación
	Política sobre el uso de controles criptográficos
	Existe una política sobre el uso de controles criptográficos
La política criptográfica contiene	El enfoque gerencial sobre el uso de los controles criptográficos a través de la organización
	El nivel de protección
	Uso de codificación para la protección de la información confidencial transportada por los medios y dispositivos móviles, removibles, o a través de las líneas de comunicación

	Métodos para lidiar con la protección de las claves criptográficas y la recuperación de la información codificada en el caso de claves perdidas, comprometidas o dañadas;
	Está escrito quién es el responsable de la implementación de la política
	Los estándares a adoptarse para la implementación efectiva en toda la organización
	El impacto de utilizar información codificada sobre los controles que se basan en la inspección del contenido (antivirus)
	Se han considerado las regulaciones y las restricciones nacionales que se podrían aplicar al uso de técnicas criptográficas
Gestión de claves	
	Existe un procedimiento de gestión de claves para dar soporte al uso de técnicas criptográficas en la organización
	Todas las claves criptográficas están protegidas contra una modificación, pérdida o destrucción.
	El equipo utilizado para generar, almacenar y archivar las claves, está protegido físicamente
El sistema de gestión de claves considera procedimientos y métodos seguros para	Generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones;
	Generar y obtener certificados de claves públicas
	Distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas
	Almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves
	Cambiar o actualizar las claves incluyendo las reglas sobre cuándo se debieran cambiar las claves y cómo se realiza esto
	Lidiar con las claves comprometidas
	Revocar las claves incluyendo cómo se debieran retirar o desactivar las claves
	Si un usuario deja la organización, las claves se archivan
	Recuperar las claves cuando han sido perdidas o corrompidas como parte de la continuidad y gestión del funcionamiento institucional
	Archivar las claves
	Destruir las claves
	Registrar y auditar las actividades relacionadas con la gestión de claves
Confidencialidad	

	Las personas que tienen algún tipo de contacto con claves criptográficas, en su contrato tienen un artículo específico de guardar confidencialidad en cuanto a metodología, almacenamiento, generación, uso y eliminación de ellas, durante su contrato y después de finalizar las relaciones laborales
	Servicios externos
	Contratos y acuerdos de nivel de servicio
	Existe un análisis de riesgos que identifica los riesgos asociados al proveedor externo
	Existe un esquema formal, aprobado por ambas partes y actualizado periódicamente
	Existen funciones o roles de ambas partes
	Existen obligaciones de cada parte
	Existen responsabilidades de cada parte
	Existen mecanismos y procedimientos para la sincronización de las actividades de gestión de incidencias
	Personal
	El personal que tiene contratos temporales ó personal que pertenece a empresas subcontratadas conoce y firmó una cláusula de confidencialidad
	Se tiene un análisis de riesgos del acceso por usuarios externos a la organización
	Se tiene un procedimiento de protección de activos
	Se tiene un procedimiento de medidas de protección física, contra la introducción y propagación de virus o código dañino
	Está fijado el método de acceso permitido
	Existe una lista actualizada de los usuarios externos autorizados a recursos o activos específicos
	Están estipuladas las horas y fechas de disponibilidad del servicio
En el contrato está contemplado	El derecho de auditoría
	Las restricciones en cuanto a la protección de datos de carácter personal
	Las restricciones contra la copia y la revelación no autorizada
	La devolución de documentación y activos de información al finalizar el contrato
	Identificación de los riesgos relacionados con los grupos externos
	Se ha llevado a cabo una evaluación de riesgos de que personal externo a la organización manipule información de la organización

En la evaluación de riesgos, se ha considerado los siguientes puntos	Los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo
	el tipo de acceso que tendrá el grupo externo a la información y los medios de procesamiento de la información; como accesos físicos, lógicos, conexiones externas o internas.
	El valor y sensibilidad de la información involucrada
	Los controles necesarios para proteger la información que no está destinada a ser accesible para los grupos externos
	El personal del grupo externo involucrado en el manejo de la información de la organización
	Cómo se puede identificar al personal de la organización y externo, cómo verificar la autorización, y el tiempo de prestación de servicios
	Los diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información
	El impacto del acceso no disponible para el grupo externo cuando lo requiere
	Prácticas y procedimientos para lidiar con los incidentes en la seguridad de la información provocados por el grupo externo
	Daños potenciales, generados por el grupo externo a incidentes
	Términos y condiciones para la continuación del acceso del grupo externo en caso de un incidente en la seguridad de la información
	Regulaciones y obligaciones contractuales relevantes que se debieran tomar en cuenta para el grupo externo
	Antes de otorgar acceso a los grupos externos a la información de la organización, se han implementado los controles apropiados
	Se ha aplicado controles para administrar el acceso del grupo externo a los medios de procesamiento de la información
	Tratamiento de la seguridad en acuerdos con terceros
	Existen acuerdos de indemnización entre las partes
En el acuerdo firmado entre las partes, están considerados los siguientes términos	La política de seguridad de la información
	Capacitación del usuario y administrador en métodos, procedimientos y seguridad
	Asegurar la conciencia del usuario para las responsabilidades y problemas de la seguridad de la información
	Provisión para la transferencia de personal, cuando sea apropiado
	Responsabilidades relacionadas con la instalación y mantenimiento de hardware y software

	Una estructura de reporte clara y formatos de reporte acordados
	Un proceso claro y especificado de gestión de cambio
	Una descripción de cada servicio que debiera estar disponible
	El nivel objetivo del servicio y los niveles inaceptables del servicio
	Una definición del criterio del desempeño verificable, su monitoreo y reporte
	El derecho a monitorear, y revocar, cualquier actividad relacionada con los activos de la organización
	El derecho de auditar las responsabilidades definidas en el acuerdo, el derecho que un tercero lleve a cabo la auditoria, y enumerar los derechos estatutarios de los auditores
	El establecimiento de un proceso escalonado para la solución de problemas
	Requerimientos de continuidad del servicio, incluyendo las medidas de disponibilidad y confiabilidad, en concordancia con las prioridades comerciales de la organización
	Las obligaciones respectivas de la organización y el cliente
	Responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales
	Derechos de propiedad intelectual
	Asignación de derechos de autor
	Protección de cualquier trabajo cooperativo
	Participación de terceros con subcontratistas, y los controles de seguridad que estos subcontratistas necesitan implementar
	Se ha implementado un plan de contingencia en caso que alguna de las partes desee terminar la relación antes del fin del acuerdo
	renegociación de acuerdos si los requerimientos de seguridad de la organización cambian
	Documentación actual de las listas de activos, licencias, acuerdos y derechos relacionados a ellos.
	Una Política de Control de acceso que abarque
	Las diferentes razones, requerimientos y beneficios que hacen que sea necesario el acceso de terceros
	Métodos de acceso permitidos, control y uso de identificadores singulares como IDs del usuario y claves secretas
	Proceso de autorización para el acceso y privilegios del usuario

	Un requerimiento para mantener una lista de personas autorizadas a utilizar los servicios que se están poniendo a disposición, y los derechos y privilegios con respecto a este uso
	Un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado
	Un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas
	Acuerdos para el reporte, notificación e investigación de las inexactitudes de la información, incidentes y fallas de seguridad de información
	Controles y procedimientos para asegurar la protección de los activos como
	Información, software y hardware
	Cualquier control y mecanismo de protección física requerido;
	Controles para asegurar la protección contra software malicioso
	Procedimientos para determinar si algún activo está comprometido
	Controles para asegurar el retorno o destrucción de información y los activos al final de, o en un punto de tiempo acordado durante el acuerdo
	Confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante
	Restricciones sobre el copiado y divulgación de información
	Utilización de acuerdos de confidencialidad
	Entrega del servicio
	Existen controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros
	En caso de transferirse información, medios de procesamiento, se ha identificado la forma de realizar la transferencia en el período de transición
	Se han realizado planes de trabajo de tal manera que se dé la continuidad del servicio después de fallas importantes o desastres
	Gestión diaria
	Hay evidencias que demuestren que todos los procedimientos ejecutados por terceras personas se siguen de forma rutinaria y en caso de incidentes
	Monitoreo y revisión de los servicios de terceros

	Los servicios, reportes y registros provistos por terceros son monitoreados y revisados regularmente
Existe una relación y proceso de gestión de servicio entre la organización y la tercera persona para	Monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos
	Revisar de los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme los acuerdos
	Proporcionar información sobre incidentes de seguridad revisados por los terceros y la organización
	Revisar los rastros de auditoría de terceros, los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado
	Resolver y manejar cualquier problema identificado
	De parte de la organización se ha asignado a una persona o grupo de personas para manejar la relación con terceros
	Se ha puesto a disposición las capacidades y recursos técnicos para monitorear los requerimientos de seguridad de la información
	Se toman acciones apropiadas cuando se observan deficiencias en la entrega del servicio
	La organización tiene el control y la visibilidad general con relación a toda la información que es manejada por terceros
	Manejo de cambios en los servicios de terceros
El proceso de manejar los cambios en el servicio de terceros necesita tomar en cuenta:	Desarrollo de cualquier aplicación y sistema nuevo
	Modificaciones o actualizaciones de las políticas y procedimientos de la organización
	Controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad
	Uso de tecnologías nuevas;
	Adopción de productos nuevos o versiones más modernas;
	Desarrollo de herramientas y ambientes nuevos
	Cambios en la ubicación física de los medios del servicio
	Medios alternativos
	Existe un plan para reemplazar el servicio por una alternativa
	El plan de reemplazamiento de servicios se vertebra dentro del plan de continuidad de la organización.
	Disponibilidad
	Continuidad del servicio
	Plan de contingencias
	El plan de contingencias se desarrolló en base al análisis y gestión de riesgos
El Plan de Contingencias contiene	Personal de contacto

	Acciones concretas
	Todas las posibilidades y escenarios que podrían ocurrir, con el fin de limitar al máximo la necesidad de tomar decisiones durante el período de recuperación
	Se han realizado pruebas con el fin de comprobar que el Plan de Contingencias funciona correctamente
	El Plan de contingencias se lo prueba y actualiza periódicamente
El plan de Contingencias tiene desarrollado y documentado	Sustitución de elementos
	Servicio degradado
	Sin servicio
	Definir procesos manuales
Análisis de impacto	
	El análisis de impacto está aprobado por la Dirección y sometido a un proceso de revisión periódica.
	El análisis de impacto incluye las necesidades derivadas sobre proveedores
Continuidad del servicio y evaluación del riesgo	
	Están identificados los eventos que pueden causar interrupciones, la probabilidad, impacto y consecuencias para la seguridad de la información.
	La continuidad del servicio se basan en la identificación de eventos que pueden causar las interrupciones en los procesos.
	Se desarrolló una estrategia de continuidad del servicio para determinar el enfoque general para la continuidad del mismo.
	La estrategia fue aprobada por la Dirección General, e implementada
Plan de continuidad	
Se han definido	Las funciones, responsabilidades y actividades a realizar en caso de desastre que impida prestar el servicio en las condiciones habituales
	Quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y avaluar las consecuencias
	Quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis
	Quiénes se encargan de reconstruir el sistema de información (recuperación de desastre)
Se ha previsto	Instalaciones alternativas
	Comunicaciones alternativas
	Equipamiento alternativo
	Personal alternativo

	Recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto
	Todos los medios alternativos están planificados y materializados en acuerdos o contratos con los proveedores correspondientes
	El plan debe determinar la coordinación de todos los elementos para alcanzar la restauración de los servicios en los plazos estipulados.
	Las personas afectadas por el plan han recibido formación específica relativa a su papel en dicho plan.
	El plan de continuidad es parte integral y armónica con los planes de continuidad de la organización en otras materias ajenas a la seguridad.
	Existe un documento formal donde se definen las funciones y se asignan a personas, de forma permanente o rotatoria
	Existen documentos formales para establecer puntos de contacto, obligaciones y canales de comunicación para la sincronización de la recuperación de un desastre en la medida en que se vean involucradas terceras partes (proveedores)
	Existe un procedimiento para sincronizar el plan de continuidad con las actualizaciones del sistema en lo referente a arquitectura, elementos componentes y servicios y calidad de los servicios prestados
	En cuanto al Plan
	En el Plan de Continuidad del servicio, está descrito el plan de intensificación y las condiciones para la activación
El plan está compuesto por	Personas responsables de ejecutar cada componente del plan
	Personas alternativas para la ejecución del Plan
	Los procedimientos de emergencia que describen las acciones a realizarse después del incidente
	Procedimientos de contingencia que describen cuándo y cómo involucrar los servicios temporales alternativos
	Procedimientos operacionales temporales hasta la culminación de la recuperación y restauración
	Procedimientos de reanudación que describen las acciones a tomarse para regresar a las operaciones comerciales normales;
	Un programa de mantenimiento que especifica cómo y cuándo se va a probar el plan, y el proceso para mantener el plan;
	Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información

	Se debieran desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos
El proceso de planeación de la continuidad del servicio debiera considerar lo siguiente:	Responsabilidades y los procedimientos de continuidad del servicio
	Identificar la pérdida aceptable de la información y los servicios
	Implementación de los procedimientos para permitir la recuperación y restauración del sistema, disponibilidad de la información
	Procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración
	Documentación de los procesos y procedimientos acordados
	Educación apropiada del personal en los procedimientos y procesos, incluyendo la gestión de crisis
	Prueba y actualización de los planes
	En el proceso de planeación están identificados los servicios que tienen que recuperarse con un tiempo definido, según la criticidad de los mismos.
	Están identificados los recursos que necesita la recuperación, incluyendo personal, recursos de procesamiento, arreglos de contingencia, etc.
	En los planes de continuidad del servicio se contemplan las vulnerabilidades organizacionales
	Debido a que los planes de continuidad manejan información confidencial, están protegidos apropiadamente
	El plan de continuidad del servicio estén actualizadas y protegidas
	Pruebas periódicas
	Existe un plan de pruebas
	Todas las pruebas que se realizan están documentadas, y se puede apreciar los datos de entrada, resultados y recomendaciones
	El personal en funcionamiento participa de las pruebas
	Las pruebas se realizan periódicamente de forma aleatoria
	Prueba, mantenimiento y re-evaluación de los planes de continuidad institucionales

	Los planes de continuidad institucionales son probados y actualizados regularmente para asegurar que sean actuales y efectivos.
	Todos los miembros del equipo de recuperación y otro personal relevante están al tanto de los planes y su responsabilidad con la continuidad del servicio y la seguridad de la información
	Cada elemento del plan es probado frecuentemente
Se han realizado pruebas con el objeto de	Conocer qué tan preparadas están las personas en sus papeles en la gestión post-incidente/crisis
	Conocer que tan efectiva es la recuperación técnica
	Recuperación en una sucursal
	Los medios y servicios del proveedor para conocer el tiempo de respuesta de los proveedores ante una eventualidad
	Ensayos completos (probando que la organización, personal, equipo, medios y procesos puedan lidiar con las interrupciones).
	Los resultados de las pruebas están registrados y en caso de ser necesario, tomar acciones para mejorar los planes
	Existen responsables para las revisiones del plan de continuidad
Los planes de continuidad se tienen que actualizar cuando existen cambios de	Adquisición de equipo nuevo
	Actualización de los sistemas
	Personal
	Direcciones o números de teléfonos
	Estrategia comercial
	Local, medios y recursos
	Legislación
	Contratistas, proveedores
	Procesos, los nuevos o los eliminados
	Riesgo (operacional y funcional)
	Monitorización del sistema
	Detección de intrusión
	Existe una herramienta de detección de intrusión
	Se atienden las alarmas
	Se analizan los registros
	Acceso a través de redes
Los dispositivos del cortafuegos permiten	la autenticación de la conexión
	Control de acceso
	Ocultación de la estructura interna de la red (direcciones)
	Inspección del tráfico
	Registro de eventos.

Los cortafuegos incluyen	Mecanismos de detección de intrusión, así como de análisis de vulnerabilidades.
	Empleo de intermediarios o apoderados de aplicaciones o protocolos, en la medida de lo posible.
	El cortafuegos es totalmente independiente de las computadoras en donde se ejecutan las aplicaciones o residen datos
	Medidas de Protección
	Protección de las instalaciones e infraestructuras
	Áreas separadas y con control de acceso
	Los equipos se encuentran en áreas separadas
	Existe un control de acceso a las áreas
	Seguridad física
	El equipamiento que soporta a la aplicación, así como los soportes de información están en áreas seguras y protegidas adecuadamente.
	Hay barreras físicas del suelo al techo para prevenir entradas no autorizadas o contaminación del entorno.
	Las ventanas y puertas de las áreas seguras están cerradas y se controlan periódicamente.
	Las ventanas están protegidas externamente
	Las terminales que manejan información y datos sensibles están ubicadas en lugares donde se reduzca el riesgo
	Está controlada la entrada en exclusiva al personal autorizado a las áreas que se hayan definido como áreas a ser protegidas
	Al entrar a una área protegida se registran los datos y tiempos de entrada y salida.
	Todo el personal lleva una identificación visible dentro del área segura
	Si se observa la presencia de personal extraño en el área, se informa
	La puerta externa al área restringida está cerrada mientras la interna está abierta
	Está restringido el acceso a las áreas seguras a los proveedores o mantenimiento a excepción de que sea requerido y autorizado.
	Si se autoriza el acceso a personal externo a la institución, se controlan sus actividades
	Áreas seguras
	Hay perímetros de seguridad definidos
	Hay barreras de seguridad
	Existen controles de entrada apropiados
	Perímetro de seguridad física

	Cuando sea apropiado, se debieran considerar e implementar los siguientes lineamientos para los perímetros de seguridad físicos:
	Los perímetros de seguridad debieran estar claramente definidos, dependiendo de los resultados de la evaluación del riesgo;
	Las puertas externas debieran están adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control
	Existe un área de recepción con una recepcionista u otros medios para controlar el acceso físico al local o edificio
	El acceso a los locales y edificios está restringido solamente al personal autorizado
	Las puertas de emergencia en un perímetro de seguridad tienen alarma
	Las puertas son monitoreadas
	Hay implementado sistemas de detección de intrusos en puertas, ventanas accesibles
	Las áreas no ocupadas tienen alarma
	Los medios de procesamiento de información manejados por la organización están físicamente separados de aquellas manejadas por terceros.
	Controles de ingreso físico
Están considerados los siguientes lineamientos	Se registra la fecha y la hora de entrada y salida de los visitantes
	Todos los visitantes son supervisados
	Está permitido el acceso con propósitos específicos y autorizados
	El acceso a áreas donde se procesa o almacena información está controlado y restringido sólo a personas autorizadas;
	Se utilizan controles de autenticación
	Todos los empleados y visitantes llevan una identificación visible
	Todas las personas ajenas a la institución tienen acceso restringido a las áreas restringidas al menos que hayan sido autorizados
	Los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario
	Asegurar las oficinas, habitaciones y medios
	Se debiera diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios

Se consideran los siguientes lineamientos	Estándares y regulaciones de sanidad y seguridad relevantes
	El edificio en donde se encuentra procesando la información es discreto, sin carteles que llamen la atención
	Los directorios y teléfonos internos que identifiquen la ubicación de los medios de procesamiento de la información no son accesibles al público.
	Áreas de acceso público, entrega y carga
Se consideran los siguientes lineamientos	El acceso al área de entrega y carga desde fuera del edificio está restringido al personal identificado y autorizado
	Está definida el área de entrega y carga de tal manera que no se tenga acceso a otras áreas
	Las puertas externas del área de entrega y carga están aseguradas cuando se abren las puertas internas;
	Se inspecciona el material que ingresa para evitar amenazas potenciales, antes que el material sea trasladado del área de entrega y carga al punto de uso;
	El material que ingresa se registra
	Equipo de seguridad
	Se debiera proteger el equipo de amenazas físicas y ambientales
	Ubicación y protección del equipo
	Se proteger el equipo para reducir las amenazas y peligros ambientales y de las oportunidades para acceso no-autorizado
Se consideran los siguientes lineamientos para la protección del equipo	El equipo está ubicado de manera que se minimice el acceso innecesario a las áreas de trabajo;
	Están aislados los ítems que requieren protección especial para reducir el nivel general de la protección requerida
	Se han implementado controles para minimizar el riesgo de amenazas potenciales; como robo, explosivos, humo, agua, etc.
	Se han establecido lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información
	Se monitorean las condiciones ambientales como temperatura y humedad

	Hay protección contra rayos y se han adaptado filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones
	Acondicionamiento de los locales
	Los locales garantizan que la temperatura se encuentra en el margen especificado por los fabricantes de los equipos
	La humedad se encuentra dentro del margen especificado por los fabricantes de los equipos
	El local está protegido frente a las amenazas identificadas en el análisis de riesgos, tanto de índole natural, como derivadas del entorno o con origen humano, accidental o deliberado
	Se puede identificar cada cable físico y su correspondencia a los planos de la instalación
	El cableado está protegido frente a accidentes
	Existe un sistema de acondicionamiento de temperatura y humedad dimensionado para cubrir con holgura los requisitos de los equipos
	Existe equipamiento de acondicionamiento redundante para el caso de fallo de los equipos principales
	No existen cables fuera de uso
	Existe un plano del cableado que incluye el etiquetado de los cables
	Existe un procedimiento para mantener al día el etiquetado de los cables
	No existe material innecesario dentro de la sala de equipos
	Seguridad física
	Existe un Plan de evacuación en caso de incendios, inundación o cualquier evento de carácter natural o antrópico
	Según el estándar nacional o internacional, se tiene las señalizaciones correspondientes de emergencia
	Se tiene las señalizaciones de las vías de escape en caso de evacuación
	Se ha capacitado al personal conforme al Plan de Evacuación
	Se han realizado simulacros para los diferentes eventos
	Electricidad
	Existe un sistema de alimentación ininterrumpida para todos los servidores
	Existe generador eléctrico propio con capacidad para mantener activos el conjunto de dispositivos en donde se procesa, almacenan datos, así como donde se ejecutan las aplicaciones
	Existe un contrato con un proveedor alternativo (doble acometida)

	Los requisitos de suministro de potencia pueden conjugarse complementándose con los medios alternativos
	Incendios
	Según el área, se tiene señalización de prohibido fumar, no acumulación de papel y la no ocupación de las vías de emergencias
	Se ha instalado sistemas de detección, alarma, y extintores de incendios
	Se realiza una revisión periódica. De los sistemas de alarma, extintores y planes de evacuación en caso de cambios en la infraestructura física
	Hay armarios ignífugos para el almacenamiento de las copias de respaldo
	Clima
	Se han instalado sistemas de control de la temperatura y de la humedad conforme a las necesidades de los equipos
	Se ha considerado las recomendaciones de los proveedores de los equipos computacionales, red, etc.
	Agua
	Se han instalado sistemas de detección y evacuación de agua
	Interferencias
	Se ha implementado algún tipo de mecanismo para evitar interferencias electromagnéticas
	Consideraciones
	Los procedimientos de emergencia son revisados regularmente
	Se han implantado medidas para proteger los cables de líneas de datos contra escuchas no autorizadas
	Se ha implementado la norma nacional para el almacenamiento de materiales peligrosos y/o combustibles
	Protección contra amenazas externas e internas
	En el plan de eventos o antrópicos se ha considerado el hecho de que agentes externos también puedan ocasionar daños a las instalaciones gubernamentales. Ejemplo: incendios en los lugares adyacentes
	El equipo de reemplazo y los medios de respaldo están ubicados a una distancia segura para evitar el daño de un desastre que afecte el local principal
	El equipo contra-incendios está ubicado adecuada y estratégicamente según la organización física de las instalaciones.
	Servicios públicos de soporte
	Las computadoras tienen UPS

	Los servicios públicos como electricidad, agua, desagüe, son revisados regularmente
	Se tiene un generador de emergencia para el funcionamiento posterior a un corte de energía largo
	Se dispone de un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado.
	El equipo UPS y los generados se debieran chequear regularmente para asegurar que tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante
	Existe iluminación de emergencia en caso de una falla en la fuente de energía principal
	El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas
	Seguridad del cableado
	El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información están protegidos contra la intercepción o daño.
	Las líneas de energía y telecomunicaciones son subterráneas
	Los cables de energía están separados de los cables de comunicaciones para evitar la interferencia
	Toda el cableado de red está documentado
En los puntos más sensibles de la red se ha implementado	El uso de rutas alternativas y/o medios de transmisión
	El uso de un escudo electromagnético para proteger los cables
	La iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves;
	Acceso controlado para empalmar los paneles y los cuartos de cableado.
	Registro de entrada y salida de equipamiento
	Existe un procedimiento formal aprobado por la dirección del registro de entrada y salida de equipamiento
	Todas las entradas y salidas de equipos quedan registradas, así como la persona quien lo manipuló
El registro debe tener	Fecha y hora
	Nombre de quien entra o recibe el equipamiento
	Nombre de quien lo entrega
	Tipo de soporte que recibirá el equipo
	Información que contiene
	Características del equipo
	Condiciones que se entrega el equipo
	Autorización del jefe, que especifica que el equipo sea retirado

	Tiempo que el equipo permanecerá fuera de las instalaciones
	Instalaciones alternativas
	Existen acuerdos informales para continuar trabajando en otras instalaciones, indicando el tiempo estimado de entrada en operación
	En caso de utilizar las instalaciones alternativas, el personal fue capacitado previamente
	El equipamiento alternativo y copias de respaldo están en sitios diferentes y a una distancia conveniente de seguridad.
	Capacitación al personal
	Gestión del personal
	Caracterización del puesto de trabajo
	Están definidas las responsabilidades relacionadas con cada puesto de trabajo
	Se capacita al personal en las funciones que realizará, así como también se le entrega por escrito los procesos que están a su cargo
	Las responsabilidades están aprobadas por la Dirección General
	Están defindos los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad.
	Se verificó los requisitos en la selección de la persona de sus antecedentes laborales, formación y otras referencias dentro del marco de la ley
	Deberes y obligaciones
	Las personas que tienen relación con el sistema están concientes de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad
	Tienen firmado acuerdos de confidencialidad
	Como parte de sus deberes, tienen conocimiento del procedimiento de resolución de incidentes
	Acuerdos de confidencialidad
Se ha considerado los siguientes elementos en el acuerdo de confidencialidad	Una definición de la información a protegerse
	Duración del acuerdo
	Acciones requeridas cuando se termina un acuerdo
	Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada
	Propiedad de la información, propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial;

	Derechos del firmante para utilizar la información confidencial
	Proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial
	Acciones esperadas a realizarse en caso de incumplimiento de este acuerdo
	Responsabilidades de la Dirección General
La Dirección ha informado a todos los empleados sobre	Sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información;
	Lineamientos para establecer las expectativas de seguridad de su rol dentro de la organización
	Nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades dentro de la organización
	Términos y condiciones de empleo, los cuales incluyen la política de seguridad de la información de la organización y los métodos de trabajo apropiados
	Capacitaciones apropiadas según su rol
	Concienciación
	Se concientiza regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.
	Periódicamente se recuerda al personal la normativa de seguridad relativa al buen uso de los sistemas
	Periódicamente se recuerda al personal la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado
	Periódicamente se recuerda al personal el procedimiento de reporte de incidencias de seguridad, seas reales o falsas alarmas
	Existe un plan para que regularmente todo el personal reciba información de los diferentes protocolos, manuales, etc respecto a seguridad
	Existe constancia de que cada persona ha seguido el plan establecido en cada periodo temporal
	Formación
	Se ha capacitado regularmente a las personas en aquellas técnicas que requieran para el desempeño de sus funciones
	Se los ha capacitado en la configuración de sistemas
	Se los ha capacitado en gestión de incidencias
	Se los ha capacitado en procedimientos relativos a sus funciones

	Existe un plan de formación que determina qué personas deben recibir qué entrenamiento, así como la frecuencia con la que deben actualizar su formación
	El departamento de Recursos Humanos tiene un registro de las capacitaciones que ha recibido el personal
	Se ha formado al empleado con el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes
	Equipos
	Protección de Equipos Portátiles
	Está establecido un mecanismo adecuado de autenticación
	Un equipo portátil hereda la categoría de la máxima información que contiene.
	La información sensible que reside en equipos portátiles está encriptada
	Se lleva un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo
	Se tiene disponible un canal de comunicación para reportar pérdidas o sustracciones al servicio de gestión de incidencias.
	Existe un inventario de equipos con su contenido
	Seguridad del equipo fuera del local
	Durante un viaje, las computadoras portátiles son llevadas como equipaje de mano
	Existen controles para el trabajo en casa
	Los portátiles están asegurados
	Computación y comunicaciones móviles
La política de computación móvil incluye lo siguiente	Requerimientos de protección física
	Controles de acceso
	Técnicas criptográficas
	Respaldos (back-up).
	Protección contra virus
	Reglas y consejos para la conexión de medios móviles con las redes
	Lineamientos para el uso de estos medios en lugares públicos.
	Los respaldos (back-up) son realizados con regularidad.
	Los móviles están protegidos contra robo
	El personal que utiliza computación móvil ha sido capacitado para elevar el nivel de conciencia y de los controles que se debieran implementar.
	Comunicaciones
	Segregación de redes
	Se tiene control (de entrada) de los usuarios que llegan a cada segmento

	Se tiene control (de salida) de la información disponible en cada segmento
	Se tiene control (de entrada) de las aplicaciones utilizables en cada segmento
	Las redes se pueden segmentar por dispositivos físicos o lógicos.
	El punto de interconexión debe estar particularmente asegurado, mantenido y monitorizado.
	Las redes lógicas o virtuales están identificadas en la arquitectura del sistema
	Existe una normativa para determinar el tratamiento debido para operar en cada segmento
	Se controla rutinariamente el paso de información y el acceso de los usuarios a través del punto de interconexión
	Los dominios fueron definidos en base a una evaluación del riesgo y los requerimientos de seguridad diferentes dentro de cada uno de los dominios.
Segregando redes	En caso de utilizar un gateway o firewall para separar las redes, filtra el tráfico entre los dominios y bloquea el acceso no autorizado según la política de seguridad gubernamental.
	En caso de utilizar redes privadas o IP switching, para segregar dominios lógicos se ha implementado listas de control de acceso para controlar los flujos de data a la red
	En el caso de las redes inalámbricas, se ha realizado una evaluación del riesgo para identificar los controles como autenticación sólida, métodos criptográficos, y selección de frecuencia
	Seguridad de los servicios de la red
	Se monitorea regularmente la capacidad del proveedor
	Se tiene el derecho de auditoría sobre el proveedor
	Se tiene un plano esquemático de la red con todos sus componentes, físicos y lógicos
	La red está dividida en dominios de red lógicos separados
	Se ha aplicado un conjunto de controles graduados en dominios de red lógicos diferentes para segregar aún más los ambientes de seguridad de la red; (redes internas y activos críticos)
	Protección de los soportes de información
Son considerados soportes de información	Discos de los servidores y equipos de usuario final, con especial consideración a equipos portátiles y discos removibles
	Disquetes, cintas, CD, DVD,
	Discos USB
	Material impreso
	Criptografía

	Existe un criterio para saber qué tipo de protección criptográfica debe aplicarse a cada tipo de información
	Se aplica a los soportes el criterio asociado a la información de mayor nivel de clasificación
	Para datos confidenciales, la información se encripta tanto para transacciones, comunicación y almacenamiento.
	La información sensible almacenada en servidores, está almacenada
	Las transacciones electrónicas, están encriptadas
	Los ordenadores con información sensible, están encriptados
	Borrado y destrucción de soportes de información
Aplicado a	Discos de equipos portátiles
	Discos removibles
	Discos duros de todo tipo de equipos
	CDs
	Existe un procedimiento de borrado seguro a los soportes que vayan a ser reutilizados
	El mecanismo de destrucción será proporcionado a la clasificación de la información contenida.
	Los mecanismos de borrado y destrucción respetan la normativa de protección medioambiental o certificados de calidad medioambiental
	Los dispositivos que contienen información confidencial son físicamente destruidos o borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original
	Protección de las aplicaciones informáticas
	Revisar el marco de seguridad para aplicaciones informáticas
	Protección de los servicios
	Protección del correo electrónico (e-mail)
	Existen normas de uso del correo electrónico por parte del personal, determinando idoneidad (o no) de su uso en cada paso del proceso administrativo
	Se protege la información distribuida por medio de correo electrónico, tanto el cuerpo de los mensajes como los anexos
	Está protegida la Organización frente a problemas como correo no solicitado (spam)
	Está protegida la Organización frente a problemas como programas maliciosos: virus, troyanos, espías, etc.
	Existen mecanismos para analizar el contenido de los mensajes y procedimientos para reaccionar ante contenidos inadecuados
	Se protegen los mensajes del acceso no-autorizado, modificación o negación de servicio

USO DE CONTRASEÑAS	
	Gestión de las claves secretas
	Existe un proceso para la gestión de contraseñas
	Para empleados
	En el contrato existe un enunciado de confidencialidad en cuanto al uso de contraseñas otorgadas porla institución
	La contraseña temporal asignada a un nuevo usuario, le es obligación cambiarla inmediatamente
	Se han establecido procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta nueva, sustituta o temporal
	La contraseña temporal asignada al nuevo usuario, son únicas y no son fáciles de adivinar
	en las bases de datos del sistema
	Los empleados no utilizan las misma contraseña personal para propósitos comerciales y no-comerciales
	Por vendedores
	Las contraseñas secretas predeterminadas en las compras de equipos, son cambiadas inmediatamente después de su configuración
	Sistema de gestión de claves secretas
	Los ids de usuarios son únicos
	Los usuarios pueden cambiar su contraseña mediante un método seguro
	Se mantiene un registro de cambio de contraseñas para evitar el re-uso
	Bajo ningún caso se muestra la contraseña en la pantalla al momento de ingresarlas
	Las contraseñas no están en la misma base de datos de la aplicación
	El almacenamiento y transmisión de contraseñas está codificado o encriptado

ANEXO B: MARCO DE GOBIERNO Y GESTIÓN TI

	Gobierno TI en instituciones públicas
	Dirección General
	Se ha implantado un gobierno y gestión TI en la institución
	La Dirección General está conformada por los altos directivos incluyendo al máximo representante legal de la institución pública
	Todos los directivos tienen asignados sus roles y responsabilidades
	Tienen reuniones definidas cada cierto periodo de tiempo
	Todas las resoluciones y acuerdos llegados para el gobierno TI se encuentran documentadas y firmadas
	La evaluación, orientación y monitorización de procesos se realiza constantemente
	Existe un plan estratégico para alcanzar las metas institucionales
	Toda la institución conoce acerca de los procedimientos y normas generales que se tienen que seguir
	Está separado el gobierno de la gestión
	Se han establecido mecanismos de comunicación entre el gobierno y gestión de TI
	Alineamiento Estratégico
	Se han definido las metas institucionales
	Las metas institucionales están priorizadas
	Las TI están alineadas conforme a las metas institucionales
	Existe un plan estratégico para alcanzar cada meta institucional
Para cada plan estratégico se conoce	La capacidad actual de la empresa para poder ejecutarlo
	La cantidad de recursos humanos a necesitar
	La cantidad de recursos financieros a necesitar
	La cantidad de recursos tecnológicos a necesitar
	La cantidad de recursos de tiempo a necesitar
	La cantidad de recursos de capacitación a necesitar
	Se han reconocido los valores y beneficios que van a tener las partes interesadas (ciudadanos y estado)
	Se tiene una cultura de servicio enfocada al ciudadano
	En la estrategia, se ha contemplado los planes de contingencia para los servicios brindados
	Existen procedimientos para realizar toma estratégicas de decisiones basadas en información
	Se tiene un procedimiento para valorar la estrategia
	Después de la valoración que se ha dado a la estrategia, se llega a un consenso por todos los directivos
	Existe la retroalimentación proveniente de la gestión TI

	Se han definido las métricas de valoración para cada proyecto según los objetivos que se deseen alcanzar
	Los directivos evalúan
	Si los mecanismos que han implantado son eficaces
	Si los procedimientos que han implantado son eficaces
	Con los análisis realizados, si los proyectos son viables
Con los proyectos que se tienen en ejecución	Si están cumpliendo con los objetivos propuestos
	Si cambian la estrategia debido a cambios tecnológicos, económicos, sociales o políticos
	Si las necesidades o capacidades de la empresa siguen satisfaciendo la demanda
	Si hay un uso eficiente de las TI
	Los directivos orientan
	A que los mecanismos aprobados sean implantados
	A que los procedimientos aprobados sean implantados
	A que si un proyecto va a pasar a estado operativo, se tienen que seguir los procedimientos adecuados
	A incentivar las estrategias de gobierno TI
	A que se cumplan las responsabilidades y roles según la estrategia
	Los directivos monitorizan
	Si los mecanismos están siendo cumplidos
	Si los procedimientos implantados están siendo cumplidos
	El progreso de los proyectos implantados según la estrategia
	El uso de las TI y los beneficios causados para el logro de las metas
	Si las responsabilidades y roles asignados están siendo cumplidos
	El rendimiento en general de toda la estrategia implantada
	Creación del Valor **Valor para la institución gubernamental** **Optimización de los recursos**
	Para la realización del presupuesto del proyecto, se consideró las necesidades de todos los departamentos relacionados
	Se consideró que la implementación del proyecto la lleve a cabo la institución
	Se consideró que la implementación del proyecto la lleve a cabo una empresa externa
	Se consideró el alquiler del servicio
	Se consideró contratar el personal requerido
	Se consideró contratar una empresa para el personal requerido
	Se consideró el costo de tiempo y dinero en cuanto a las capacitaciones requeridas
	Se consideró el tiempo de análisis y el tiempo de desarrollo, así como la inversión en cada una de esas etapas

	Con los análisis realizados, se enviaron a la dirección opciones de posibles funcionamientos de los procesos
	Se envió el análisis de recursos a la Dirección General para la toma estratégica de decisiones
	Optimización del riesgo
	La gestión del riesgo está incluida en el análisis del proyecto
	Las gestiones que se realizan para mitigar el riesgo, están alineados con los procedimientos, políticas y reglamentos internas de la empresa
	El costo de mitigar el riesgo está incluido en el análisis estratégico del proyecto
	En la consideración del riesgo, se ha incluido al personal provisional en caso requerirlo
	Se ha considerado la compra de equipos o infraestructura para mitigar el riesgo
	Se ha considerado el alquiler de equipos o infraestructura para mitigar el riesgo
	Las gestiones que se realizan para mitigar el riesgo, están alineados con leyes y regulaciones externas
	Los procedimientos que se han considerado para la mitigación del riesgo, son acordes a lo que se quiere proteger
	El análisis de riesgos incluye ataques cibernéticos que podrían ocurrir a las plataformas
	El análisis de riesgos incluye la protección de datos
	El análisis de riesgos incluye la protección de infraestructura física tanto operacional de los sistemas como institucional
	El análisis del riesgo contempla la continuidad del servicio en los sistemas críticos
	Valor para el ciudadano o institución a quien se brinda el servicio
	Se realizan encuestas en la que se mida la satisfacción del ciudadano de los servicios ofrecidos
	Según la encuesta realizada, el ciudadano percibe ahorro de tiempo
	Según la encuesta realizada, el ciudadano percibe ahorro de dinero
	Según la encuesta realizada, el ciudadano está satisfecho con el servicio brindado
	Según la encuesta realizada, el ciudadano percibe seguridad al realizar sus transacciones en el portal
	Según la encuesta realizada, es indispensable la continuidad del servicio para el ciudadano
	Existe una sección de sugerencias y comentarios
	Los directivos evalúan
	Que las inversiones realizadas tengan un equilibrio entre los riesgos el valor invertido y el valor generado

	Que el valor esperado, sea el valor obtenido para la institución
	Que según el análisis, se escoja el valor óptimo para los recursos
	Que según el análisis, se escoja la opción óptima para mitigar los riesgos
	Si el servicio entregado al ciudadano cumple con su objetivo
	Si la inversión realizada es oportuna según los beneficios entregados
	La capacitación del personal en cuanto a las acciones que cada uno debería de tomar para mitigar un riesgo imprevisto
	El riesgo actual de las TI en la institución
	El riesgo futuro de las TI en la institución
	Las consecuencias en caso de no haber una buena gestión del riesgo en sus sistemas críticos
	El riesgo tolerable que la institución esté dispuesta a asumir
	El riesgo que se puede mitigar
	El riesgo inaceptable, debido a la inversión que se ha realizado
	El riesgo de dejar sin servicio a la ciudadanía
	El riesgo de tener las aplicaciones corriendo en un servidor cloud
	El riesgo de que un tercero tenga una información al ser considerada confidencial
	El riesgo de que el proveedor deje de brindar servicio
	Si el proveedor cloud cumple con leyes y reglamentos externos
	Si el proveedor cloud está alineado con las políticas y reglamentos institucionales
	Si las garantías del proveedor cloud se acoplan a la necesidad de la empresa
	Si el proveedor cloud cumple con garantías internacionales que garanticen la seguridad de los sistemas e información
	Si la disponibilidad de los sistemas que brindan servicio a la ciudadanía, es la deseada
	Si los indicadores de calidad del servicio son los esperados
	La satisfacción del usuario
	El aumento o disminución de la participación ciudadana
	Los directivos orientan
	Que se cumplan los principios y prácticas para garantizar que se dé el valor deseado
	Que el punto central es la atención al ciudadano
	A que se consideren todos los escenarios de riesgos existentes
	A que se consideren todos los recursos necesarios para la optimización de costos
	Para que haya una capacitación al personal en cuanto a la gestión del riesgo
	A crear una cultura de gestión de riesgos

	A priorizar procedimientos en caso de un riesgo a algún activo identificado como crítico
	A la calidad del servicio
	Los directivos monitorizan
	Que se cumplan los principios y prácticas garantizando el valor deseado
	Que los empleados responsables de acciones para mitigar el riesgo tengan conocimiento y cumplan sus responsabilidades
	La satisfacción del ciudadano con el servicio entregado
	Los recursos humanos estén rindiendo según sus responsabilidades
	Que el proveedor cloud esté cumpliendo con el contrato y acuerdos llegados
	Continuamente aspectos relevantes en cuanto a la disponibilidad, integridad y confidencialidad de datos
	El valor entregado sea el deseado
	Los resultados de las encuestas realizadas por los ciudadanos
	La motivación de los empleados sea constante
	La satisfacción del empleado en relación al entorno de trabajo
	La disponibilidad de los sistemas que brindan servicio a la ciudadanía
	La calidad de los procesos
	La acogida de los servicios brindados por los ciudadanos
	Asegurar la transparencia interna y externa
	Existe un mecanismo de comunicación entre el gobierno y la gestión TI
	El gobierno TI informa oportunamente a la gestión TI sobre los proyectos que han sido o no aprobados
	Si existen cambios en las políticas y marcos internos, se informa a la institución acerca del cambio
	Todas las reuniones que se realizan son debidamente documentadas y llevadas a un archivo
	Cuando existen cambios en los proyectos, se informa a los departamentos relacionados.
	Se ha informado al personal acerca de los costos, beneficios y riesgos de las TI
	Evaluar
	Si los mecanismos de comunicación son adecuados
	Si los empleados de la institución son informados de los cambios
	Si los empleados afectados por los cambios, se adaptan al cambio
	Orientar
	A que se apliquen los mecanismos de comunicación impuestos
	Cómo se pueden informar de cambios realizados a las políticas, normas, plataformas o servicios institucionales

	A los empleados que necesiten capacitación debido a los cambios realizados
Monitorizar	
	Que los mecanismos de comunicación se cumplan
	Que se cumplan los cambios
	Si hubo comunicación efectiva
	Si las capacitaciones en caso de requerirlas se dictaron a satisfacción
	Las nuevas habilidades de los empleados
Medición de Resultados y retroalimentación	
	Al iniciar un proyecto, se definen las métricas
	Los resultados son tomados en base a las métricas
	Existen métricas para medir el rendimiento del personal
	Existen criterios para la toma de decisiones según su tipo
	Los documentos de resultados están a la fecha acordada
	Los directivos de gestión TI informan al gobierno TI oportunamente anomalías que se presenten
	Si los resultados de un proyecto no fueron los esperados, según sus métricas, existe un procedimiento para darlo de baja, dejarlo en stand by, ponerlo en revisión, o cambiar de estrategia
Evaluar	
	A que las métricas escogidas sean las correctas
	Los criterios de la toma de decisiones
	Los procedimientos sean asertivos
Orientar	
	A los empleados a cumplir con objetivos planteados
	De que su labor correcta, permite tener resultados favorables
Monitorizar	
	Los resultados de los diferentes procesos
	Al personal que cumpla con sus responsabilidades
	Los resultados de procesos, procedimientos, normas políticas sean los esperados

Gestión TI

Gestión TI	
	Responsabilidades Administrativas
	Se ha integrado una Dirección de Gestión TI
La Dirección de Gestión TI	Ha establecido objetivos, planes y servicios de acuerdo con las estrategias del gobierno TI
	Se ha establecido un responsable de la coordinación y gestión de todos los servicios TI
	Para cada proyecto de TI existe un responsable de ese servicio TI
	Provee de los recursos para planear, implementar, monitorizar, revisar y mejorar el servicio
	Manejar los riesgos a que los servicios están expuestos
	Continuamente monitorizar todos los procesos
	Estructura Interna
Están definidas	Funciones internas y externas relativos a TI
	Niveles de autoridad asignados
	Roles internos y externos relativos a TI
	Quiénes toman las decisiones relativos a TI
	Mecanismo de toma de decisiones relativos a TI
	Actividades de TI realizadas por terceros relativos a TI
	Quiénes rinden cuentas
	Periódicamente se revisa la eficacia de la estructura organizativa
	Se ha implementado un sistema de gestión de seguridad de la información (SGSI)
	Se ha implementado un sistema de gestión de calidad (SGC)
	Toda la institución conoce las políticas y procedimientos de gestión, protocolos, marcos relativos a TI
	Procesos de Entrega de Servicios
	Capacidad de Administrar
	Están asignados todos los roles y responsabilidades según las competencias de quienes las ejecutan
	Las competencias y las necesidades de formación son revisadas periódicamente
	Se ha informado a los empleados la importancia de sus actividades y de cómo contribuye la función que desempeñan para alcanzar las metas institucionales
	Se coordinan los procesos de gestión de servicios
	Se consideran las observaciones y recomendaciones proveniente de los reportes
	La dirección de gestión TI consulta con las partes involucradas las recomendaciones realizadas en los procesos
	Se analiza con los involucrados las mejoras posibles a los procesos

	La dirección de gestión de TI mide reporta y comunica según sea pertinente a la Dirección General de Gobierno TI
	La dirección de Gestión de TI revisa continuamente las políticas, procesos, procedimientos y planes y corrige donde fuera necesario dentro de sus competencias
	Los reportes son entregados a tiempo, son precisos y concisos en su contenido
	Los reportes tienen un formato que contiene el propósito, desarrollo, análisis, comparación con los resultados esperados, satisfacción, recomendaciones y conclusiones
	La Dirección de gestión prevé algún cambio en requerimientos y capacidades
	Está atento a las nuevas tecnologías
	La Dirección de gestión prevé algún cambio en cambios internos o externos
	La dirección de gestión TI aprueba las políticas, objetivos y plan de servicio administrativos
	Se han creado políticas de calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual
	Los empleados tienen conocimiento que están bajo un régimen de gobierno y gestión TI, y que por lo tanto se tiene que cumplir con las políticas y reglamentos impuestos
	Están definidas la "propiedad" de información y los sistemas
	Se realiza una evaluación de los procesos como mínimo 1 vez al año
	Están definidas las métricas para los procesos
	Se han implementado las correcciones en los rendimientos no óptimos identificados
	Existen las mejoras priorizadas, según el proceso
	Existen planes rendimiento y capacidad
	Se revisan las propuestas de innovación
	Se ha definido una hoja de ruta estratégica
	Responsabilidades de la Dirección de Gestión TI
	Compromiso de la Dirección de Gestión TI
	Hay reuniones constantes del directorio. (mínimo cada 3 semanas)
	La Dirección de Gestión TI define el alcance de las políticas, objetivos y planes administrativos
	Aprueba los procesos y procedimientos según las políticas definidas por el Gobierno TI
	Tareas de Comunicación de la Dirección de Gestión TI
	Los procedimientos de comunicación están diseñados, gestionados, implementados y usados
	Los procedimientos de comunicaciones fueron aprobados por la Dirección de Gestión TI
	Los procedimientos de comunicación fomentan la motivación

Los procedimientos de comunicación incluyen	El método con que se comunica
	La frecuencia
	A quienes se comunica
	Contacto
	Lista de distribución
	Herramientas y acceso a la información
	Horarios y responsabilidades
La Dirección de Gestión TI informa:	Cambios organizacionales, políticas, estándares, misión, visión y objetivos
	Las necesidad de la institución gubernamental de tener un gobierno y gestión TI, la importancia y los resultados esperados
	Cómo la gestión TI está alineada con el gobierno TI, según sus objetivos, misión y visión
	Cómo la gestión TI aporta a la seguridad de la información y la continuidad de los servicios que se brindan a la sociedad
	Acuerdos y restricciones con los proveedores
	Limitaciones del personal tercerizado
	Horario de trabajo, seguro médico y seguridad de los sistemas críticos
	El rendimiento de los procesos
	Objetivos de la Gestión TI
	Los objetivos de Gestión TI están alineados a los objetivos del gobierno TI
	Los objetivos de Gestión TI pueden ser medidos
	El plan de Gestión TI contiene acciones para alcanzar los objetivos de Gestión TI
	Los objetivos de Gestión TI son revisados regularmente por la Dirección de Gestión TI
	Administrando los bienes
	Los activos como (licencias, dispositivos móviles, componentes de infraestructura, humanos, contratos y otros documentos son manejados por procedimientos efectivos
	Los activos como las bases de datos, son manejados y configurados por personal especializado
	Los activos como las bases de datos, son administradas según las políticas y reglamentaciones dependiendo de los tipos de datos que contengan
	Plan de proyectos
	El plan y las políticas están alineadas entre si
	El plan contiene ya los recursos y capacidades eficientes para su implementación
	El plan se comunica a todos los involucrados para su ejecución
	El plan contiene el plazo asignado, tareas y responsabilidades, así como la comunicación explícita y entendida los de cada una de las partes involucradas.
	El plan contiene las métricas para la revisión y medición

	Todos los cambios en el plan son documentados: sus motivos, los cambios realizados y recomendaciones
	El plan contiene los mecanismos de comunicación a los proveedores de servicio en caso de que se modifiquen o actualicen
Un plan contiene	Una introducción
	Una descripción de funciones
	Prioridades
	Resultados Esperados
	Medidas de rendimiento
	Servicio
	Planes del proyecto
	Tareas y dependencias
	Beneficios
	Plazos y personas responsables
	Riesgos y acciones para reducir el riesgo
	Recursos que apoyan a un Plan
Los siguientes recursos están considerados dentro del Plan	Los recursos humanos, que tengan la capacidad y experticia necesaria para la ejecución normal de actividades
	Técnicos, infraestructura
	Herramientas que soporten los procesos
	Facilidades de oficina apropiadas para los recursos humanos
	Información, requerimientos, los servicios ejecutados por terceros, políticas, métricas y otros reportes
	Recursos financieros
	Disponibilidad del personal con la cantidad de horas a trabajar
	Se tiene prácticas para medir el rendimiento del personal
	Requerimientos del servicio
	El servicio está diseñado de acuerdo a las necesidades del ciudadano o instituciones
	El servicio detalla el valor creado tanto para la institución gubernamental como para el ciudadano o institución
	Se detalla la demanda que va a tener el servicio
El servicio tiene definido	Documentado todas las funcionalidades que debería de tener
	La calidad del servicio
	Grado de criticidad
	Prioridad
	Requerimientos de disponibilidad
	Las leyes o marcos regulatorios a los que se rige
	Los requerimientos de seguridad
	Riesgos del servicio
	Los riesgos del servicio han sido identificados, documentados y valorados
	Se tiene varias opciones identificadas para la mitigación del riesgo

	La mejor opción de mitigación está implementada
	La institución ha sido capacitada para actuar ante algún evento de riesgo
	Se han realizado pruebas de escenarios de riesgo para determinar qué tan preparados están ante una eventualidad
	Los riesgos a los que están expuestos, son analizados como mínimo 1 vez al año
	Administración de la disponibilidad de la continuidad servicio
	Existe una política respecto a la continuidad del servicio
	La política fue aprobada por la dirección de gestión TI
	Se consideran las observaciones y recomendaciones proveniente de los reportes
	La dirección de gestión TI revisa las métricas de la continuidad del servicio al menos una vez al año
	Planear
	Una política respecto a la continuidad del servicio
	Un plan de contingencia según los riesgos identificados
	Cualquier cambio en las plataformas TI
	Métricas aceptables según el servicio
	Las herramientas con que se monitorizan los servicios
	Hacer
	La implementación de la política desarrollada
	Los cambios aprobados por la dirección de gestión TI
	Testear los servicios
	Supervisar
	Que los empleados cumplan la política
	La efectividad de la política
	Que los cambios realizados no influyan en la continuidad del servicio
	Los cambios que podrían afectar la disponibilidad del servicio
	Retroalimentar
	A la dirección de gestión TI la efectividad de la política implantada
	El comportamiento del cambio ya implementado, con el cambio planeado
	Los resultados de la disponibilidad verdadera del servicio
	Administración de SLA
	Planear
	Todos los puntos a acordar entre la institución y el proveedor cloud: alcance del servicio, características, carga de trabajo
	Los SLA por ambas partes
	Los procedimientos de cómo se brindará el servicio
	Cambios en el servicio
	La coordinación y comunicación entre ambas partes
	La auditoría y la monitorización del servicio
	Sanciones para el proveedor en caso de incumplimiento

	Hacer
	Recomendaciones de SLA para abarcar todos los posibles escenarios
	Supervisar
	El cumplimiento de las SLA
	Cualquier anomalía en el rendimiento que provoque una sanción según la SLA acordadas
	Retroalimentar
	Los resultados del cumplimiento o no de las SLA a la dirección de gestión TI
	Manejo del servicio otorgado por terceros
	Se tiene explícito y detalladamente los acuerdos entre la institución y el proveedor
	Se tienen políticas del servicio brindado
	Se tiene los SLA
	Se ha definido un responsable de parte del proveedor de servicios
	Se planea
	El alcance del servicio prestado por el proveedor
	Los objetivos y requerimientos que tienen que ser alcanzados por el proveedor
	Los procesos que tienen que ser ejecutados
	La coordinación entre la institución y el proveedor cloud
	Los entornos de prueba
	Los cambios en las plataformas y los riesgos que podrían ocasionar
	Cómo se medirá la calidad del servicio, la auditoría y las mejoras a tomar
	El flujo de comunicación entre las instituciones
	Una auditoría TI, en un periodo determinado, con un alcance definido
	Cambios solicitados en caso de requerirlo por la institución
	Cambios aprobados por la institución y el proveedor para el mejoramiento del servicio
	Se hace
	Asignación de presupuesto
	Asignación de roles y responsabilidades
	Políticas, planes y procedimientos para cada proceso
	Identificación de riesgos
	Asignación de personal
	Manejo eficiente de presupuesto
	Reportar el progreso vs el plan
	La auditoría planeada según el alcance, frecuencia y métodos definidos en el procedimiento
	Cambios solicitados
	Cambios aprobados entre las instituciones
	Se supervisa
	Que el proveedor cumpla según los SLA

	Que el proveedor cumpla según el contrato fijado
	Que las políticas, planes y procedimientos estén siendo aplicadas
	Continuamente a manera de auditoría que se cumpla las medidas identificadas en el plan de riesgo
	Que la auditoría se realice
	Los cambios se lleven a cabo según lo planeado
	Se retroalimenta
	A los directivos sobre el rendimiento del proveedor según los acuerdos llegados
	Los resultados de la auditoría realizada a los directivos
	De la efectividad de las políticas, planes y procedimientos
	El progreso del proyecto según lo planeado
	Algún incidente con respecto al riesgo
	A la institución los resultados de los cambios efectuados
	Manejo de la Seguridad
	Existe una política para la seguridad de la información
	Se maneja el riesgo asociado al acceso de la información
	Los controles de seguridad están documentados.
	En caso de que la documentación tenga carácter reservado, se toman las medidas del caso para la guardar la confidencialidad
	Los incidentes por falta de seguridad son reportados
	Existe un mecanismo de comunicación establecido
	Se planea
	Todo mantenimiento y cambio referente a los procesos y servicios críticos que tiene la institución
	Toda medida de seguridad en los sistemas e información crítica
	Se hace
	Todo mantenimiento y cambio aprobado por la dirección de gestión TI
	Todo mantenimiento y cambio siguiendo las recomendaciones, políticas y procedimientos establecidos
	La implementación de la medida de seguridad aprobada
	Se supervisa
	El comportamiento del cambio ya implementado, con el cambio planeado
	Que las políticas, planes y procedimientos estén siendo aplicadas
	Se retroalimenta
	A la dirección de gestión TI la efectividad de la política implantada
	A la dirección de gestión TI el comportamiento del cambio realizado
	Contabilidad y presupuesto de los servicios TI
	Existe una política y procedimientos acerca de cómo realizar el presupuesto de un proyecto TI que incluya los recursos a utilizar, riesgos, valor, licencias, etc.
	La política considera los costos directos e indirectos del proyecto
	Control y autorización del presupuesto para el proyecto

	Se monitoriza durante la ejecución que el presupuesto esté acorde con el planeado
	Se realizan las respectivas sugerencias en caso de que el presupuesto cambie
	Se toman las respectivas correcciones con la aprobación de la dirección de gestión y gobierno TI
	Controlando Cambios
Los cambios que se desean realizar consideran impactos	Costos
	Técnicos
	Al usuario final
	Mantenimientos requeridos
	Tiempo de planeación e implementación
	Los resultados de los análisis son pasados al Gobierno TI
Los planes del cambio incluyen	Los roles y responsabilidades afectados
	La comunicación entre los nuevos actores
	Las nuevas habilidades que debería de tener el personal
	Los procesos, medidas, métodos y herramientas usados en el nuevo servicio
	Los resultados producto del cambio planteado
	Administración de documentación
	Documentos de evidencia
Se tiene	Políticas, objetivos y planes definidos
	Procesos y procedimientos
	Catálogo de servicios
	Documentos que incluyan diseño, requerimientos, SLAs, de servicios
	Documentos contractuales
	Auditorías y reportes realizados
	Actividades planeadas
	Control de documentos
	Se tiene un estándar de los diferentes documentos que se elaboran
	Los documentos elaborados están definidos quienes lo elaboran y tienen responsabilidad sobre los mismos
	Se tiene control de los documentos restringidos
	Los documentos están enumerados y control de versión
	Responsable de la escritura, edición, aprobación, actualización, eliminación y archivo
	Cuando se cambia un documento, se conoce en donde fue el cambio, fecha y hora y quien realizó el cambio
	Control de acceso
	Un procedimiento para actualizarlo
	Un procedimiento para archivarlo
	Un procedimiento para aprobar su uso

	La dirección revisa
	El rendimiento de procesos ejecutados
	Las métricas de los procesos
	Los resultados de auditorías internas y externas
	Si los procesos están alineados a los objetivos institucionales
	La implementación de cambios
	Que se realicen las mejores prácticas
	La satisfacción del usuario final
	Los reportes ejecutivos enviarlos al gobierno TI
	Que el riesgo de los servicios se minimice
	Que el desarrollo de nuevos servicios sigan un formato, un orden
	Gestión del Servicio TI
	Soporte de Servicio
	Gestión de incidentes
	Existe un protocolo para reportar un incidente según el grado de criticidad
	Se monitoriza continuamente los incidentes reportados
	Se conoce de los mecanismos necesarios para realizar el reporte
	El reporte tiene un formato
	El reporte tiene una firma de responsabilidad
	El reporte tiene recomendaciones al incidente reportado
	El reporte solo finaliza cuando se ha dado una solución parcial o definitiva al mismo
	En caso de que el incidente sea crítico, el responsable del proceso informa a la Dirección de TI
	Post cambios
	Si el incidente que ha sido considerado como crítico, del cual tiene conocimiento la Dirección TI, mediante el informe presentado y los resultados obtenidos del cambio, es quien da por cerrada la solicitud de incidentes
	Gestión de problemas
	Los problemas son priorizados según el grado de criticidad
	Según el grado de criticidad es fijado el tiempo a demorar la solución
	Investiga las causas subyacentes a alteraciones reales y potenciales del servicio TI
	Plantea soluciones
	En caso de que la solución definitiva se demore más del tiempo tolerable, se plantea una solución temporal
	La solicitud de incidentes sigue abierta, pero se indica el estado en el que se encuentra
	Post cambios
	Realiza revisiones de implementación junto a la gestión de cambios
	Monitoriza el comportamiento del sistema

	Gestión de cambios
	Existe un procedimiento para gestión de cambios que se deseen realizar
	Se evalúa el impacto de los posibles cambios sobre la infraestructura TI
	Se informa a la dirección TI acerca de la necesidad de realizar los cambios respectivos mediante procesos estandarizados
	La dirección TI es la que aprueba el cambio
	La solicitud de incidentes sigue abierta, pero se indica el estado en el que se encuentra
	Post cambios
	Se monitoriza el sistema, para conocer su comportamiento (con la gestión de problemas)
	Gestión de versiones
	Existe un procedimiento de control de versiones
	Se conoce de los mecanismos necesarios para realizar el versionamiento correctamente
	Se realiza un reporte indicando el respaldo y con qué fin se lo realiza
	Implementa los cambios
	La solución implementada es testeada en el ambiente de pruebas
	Tiene desarrollado planes de "lanzamiento de nuevas versiones" y "recuperación de versiones antiguas"
	La solicitud de incidentes sigue abierta, pero se indica el estado en el que se encuentra
	Gestión de configuraciones
	Existe un procedimiento de control de configuraciones
	Lleva un control de todos los elementos de configuración de la infraestructura TI
	Realiza revisiones periódicas de configuración
	Proporciona información precisa sobre la configuración TI de todos los procesos de gestión
	Provisión del Servicio
	Gestión del Nivel del Servicio
	Define los servicios de TI que están prestando servicios a la ciudadanía
	Define los SLA (Service level agrement) con sus proveedores de servicios
	Realiza planes para mejorar la calidad en los servicios dados
	Emite informes sobre la calidad del servicio prestado a la dirección de TI
	Gestión de disponibilidad
	Vela que los servicios TI estén disponibles 24 horas, 7 días a la semana
	Vela que los servicios TI sean fiables y estén operativos
	Vela que los servicios TI tengan mantenimiento oportuno
	Vela que los cambios ante incidentes se realicen
	Vela por que se cumplan las políticas de seguridad implantadas
	Gestión de capacidad

	Elabora planes de capacidad
	Monitoriza el rendimiento de la infraestructura TI
	Realiza simulaciones de requisitos de capacidad en diferentes escenarios
	Prevé e informa a la Dirección General si el sistema tendrá sobrecarga
	Recomienda lo que hay que contratar para que el sistema pueda responder ante la demanda prevista
	Gestión Financiera
	Mide la relación calidad/coste de los servicios a implementar y actuales
	Toma medidas correctivas si la relación calidad/coste no es la esperada
	Vela que la inversión realizada dé servicios de calidad
	Gestión de Continuidad
	Evalúa los riesgos que acechan la continuidad del servicio
	Informa a la Dirección TI acerca de los riesgos y sus consecuencias
	Elabora planes de contingencia
	Todo cambio en la infraestructura TI es informado a la gestión de continuidad
	Vela por la recuperación del servicio ante catástrofes naturales o antrópicas
	Gestión de Configuración de Base de datos
	Existe un mapeo general de toda la base de datos
	SE tiene información detallada de cada elemento de configuración: físico y lógico
	Se tiene documentada las relaciones e interdependencias lógicas y físicas
	Se tiene configurada los respaldos de datos según la criticidad de los sistemas
	Se tiene un esquema de las bases de datos que interactúan entre ellas, así como la relación entre los RAID existentes
	Toda la información está documentada

ANEXO C: MARCO DE EVALUACIÓN DE APLICACIONES WEB

Seguridades Web	
Generalidades	En el plan de Seguridad se involucró a la parte administrativa y desarrolladores del sistema
	Se consultan periódicamente las bases de datos de vulnerabilidades (SANS, xssed, etc)
	Ante una petición, se conoce qué aplicaciones se ven afectadas por el cambio solicitado
	Para cada aplicación, se conoce quiénes son los usuarios del sistema
	Se conoce la ubicación física de los usuarios
	Se ha identificado las aplicaciones críticas
	Se ha identificado los procedimientos críticos de la aplicación
	Se ha identificado los datos críticos de la aplicación
	Se ha identificado qué procesos podrían alterar, modificar, eliminar o ingresar datos no deseados en la aplicación
	Se analizó en dónde la aplicación iba a ser localizada físicamente
	En cada uno de los análisis de riesgos, se encuentran cuantificado las pérdidas financieras en sus diferentes escenarios, en caso de verse comprometida la aplicación
	Se tiene un esquema de la base de datos en la que estén identificados las tablas críticas del sistema
	Se revisa continuamente las vulnerabilidades de la base de datos que se está utilizando en la página oficial del DBMA
	Las tablas que son críticas, se tiene bien documentado los campos, el diseño, descripciones, relaciones, longitud de datos y los permisos de acceso de cada una
	En cada uno de los análisis de riesgos, se encuentra cuantificada la reputación, en caso de verse comprometida la aplicación
	Se tiene un historial del sistema operativo utilizado respecto a la seguridad
	Se han identificado las motivaciones por las que alguien quisiera ingresar a la aplicación
	La aplicación está abierta al público en general
	En caso de que utilice cookies, el usuario está consciente del uso de estas
	Los esquemas de cifrado son desarrollados por una empresa comercial, no desarrollados internamente

	Arquitectura de un entorno Web
	El servidor Web, servidor de aplicación y servidor de base de datos están en sistemas independientes
	Disponen de dispositivos dedicados exclusivamente a la inspección y filtrado del tráfico web (HTTP o HTTPS)
	Los Web Application Firewall (WAF) están delante del servidor Web
	HTTPS utiliza SSL versión 3 (Secure Socket Layer) o TLS (Transport Layer Security) para cifrar las comunicaciones entre el navegador Web y el servidor Web
	Se protege todos los elementos de la infraestructura en la que reside la aplicación Web, como routers, switches, servidores de nombres (DNS), etc.
	Se ha considerado las guías oficiales de seguridad de Windows, Linux, Solaris, bases de datos, servidores web, equipos de comunicaciones, etc.
	Se han aplicado los últimos parches de seguridad en cada uno de los elementos que forman parte de la plataforma de la aplicación Web (dispositivos de red, sistemas operativos, web, aplicación, bases de datos, lenguajes de programación, etc)
	Se ha realizado un análisis detallado del usuario, grupo, permisos y derechos con los que ejecutarán cada uno de los componentes de la aplicación Web
	Se ha diseñado un sistema seguro de administración remota para conexiones al servidor
	DESARROLLO SEGURO DEL SOFTWARE DE APLICACIONES WEB
	Se tiene una metodología para el control de versiones de la aplicación
	Se ha incluido aspectos de seguridad de desarrollo de software durante el ciclo de vida de este
	El uso del método Get de HTTP sólo se lo utiliza para la consulta de información
	El uso del método POST de HTTP sólo se lo utiliza para el intercambio y envío de información
	Las cabeceras HTTP no se utilizan como método de validación o de envío de información.
	Los mecanismos de interacción entre los distintos componentes del entorno Web están cifrados y autenticados.
	El almacenamiento de información sensible, como la lógica de la aplicación y las credenciales de acceso, está almacenada de forma cifrada en todos los servidores
	FILTRADO DE DATOS DE ENTRADA DEL USUARIO

	Se aplican mecanismos de filtrado tanto en la entrada como en la salida de la aplicación
	Se permite sólo los caracteres válidos para cada entrada en la aplicación.
	En la librería de validación existen funciones sólo para letras, números, caracteres alfanuméricos, así como para datos más concretos como fechas, números de teléfono, número único de identificación del ciudadano, etc.
	Se comprueba la longitud de los datos de entrada
	Los filtros han sido aplicados mediante expresiones regulares
	Los datos de entrada del usuario son filtrados en el cliente y servidor
	Los datos de entrada se normalizan y luego se filtran
Funciones de filtrado frente a ataques de XSS	
Se filtra	Cualquier contenido recibido por el usuario que tenga validez en el lenguaje HTML (etiquetas o tags HTML), como por ejemplo: <script>, <img>, <a href=…>, <object>, <iframe>, etc.
	Caracteres para la creación de etiquetas HTML, "<" y ">", y sus múltiples representaciones: < y > , %60 y %62, < y >, junto a otros caracteres propios de código de scripts: = " ' ( ) ; &.
	Elementos para referenciar scripts remotos mediante etiquetas HTML qué permiten referenciar otras fuentes, "src=" (source).
	La salida de la aplicación, como por ejemplo scripts o iframes qué referencian sitios Web remotos.
Se ha reemplazado los datos según la siguiente tabla:	
Funciones de filtrado frente a ataques de inyección SQL (depende del motor de la base de datos)	
Se filtra	El envío de caracteres especiales para la base de datos y , caracteres comodín, concatenación u operadores SQL
	Todas las representaciones de los caracteres especiales. Por ejemplo, la "'" es igual a %27 o el "=" es %3D.
	Se aplican filtrados a la inyección de comandos en otros lenguajes de consulta,(AND (&), OR (|), NOT (!), <=, >=, = y ~= y el carácter comodín (*)).
	Se utilizan procedimientos almacenados y no dinámicos
	Se traducen las funciones propias de la base de datos, como la función CHAR(). Por ejemplo, CHAR(77) = 'M' (valor ASCII decimal: 77).
Funciones de filtrado frente al desplazamiento por directorios	

Se filtra	Referencias relativas a los directorios padre, como ".." y todas sus representaciones (Unicode: %c0%af, %c1%9c, %255c,, etc), o referencias absolutas a directorios mediante "/" o "\"
	Funciones de filtrado frente a referencias directas a ficheros (locales o remotas)
	Está limitado el acceso a ficheros o recursos en URLs (es decir, remotos) como si fueran ficheros o recursos locales.
	Funciones de filtrado frente a ejecución de comandos del sistema operativo:
	Está limitado el envío de caracteres especiales para el sistema operativo, como por ejemplo ";", ">", "<", "|", etc.
	Funciones de filtrado frente a HTTP Response Splitting:
Se filtra	Los caracteres de fin de línea que podrían permitir añadir cabeceras HTTP adicionales o inyectar datos en la cabecera, tales como "\r", "\n" o ambas.
	Mensajes de Error y Otros Contenidos
Los mensajes de Error	No muestran información relevante del software, versiones, sistema de ficheros o detalles en donde están ubicados los recursos utilizados por la aplicación web
	Son personalizados y muestran la mínima cantidad de información posible
	No envían información confidencial a los clientes web, como campos ocultos o claves de la aplicación
	No muestran errores generados por el servidor Web, el servidor de aplicaciones o la base de datos.
	No se informa acerca de sistemas de archivos o permisos
	Si se produce un error que hace fallar al sistema, el sistema se bloquea, registra el error en un log, bloquea al usuario temporalmente y envía una alerta grave al administrador del sistema
	La gestión de errores se aplica a accesos a contenidos estáticos como dinámicos, tras la ejecución de código y scripts.
	Si en algún caso es necesario enviar algún campo sensible hacia el cliente Web, el campo está cifrado, expira en un tiempo determinado y no es reutilizable
	Según la sensibilidad de datos que se presenten, se aplica el cifrado a partes específicas del sitio. Ej: páginas de autenticación
	Se ha identificado los errores que tienen que ser registrados

	Para los errores que tienen que ser registrados, el log está encriptado
	Para los errores críticos que son registrados, el log contienen, fecha y hora, id de usuarios y el código del error
	AUTENTIFICACIÓN Y GESTIÓN DE SESIONES
	En caso de que usuario o contraseña sean incorrectos, el mensaje de error no especifica qué campo está erróneo
Existe una política de acceso, donde esté definido	La longitud y complejidad de las claves
	Los mecanismos de acceso,
	El bloqueo temporal de cuentas en base al tiempo tras un número de intentos de acceso fallidos.
	La gestión de sesiones en la aplicación Web se realizan empleando identificadores de sesión o tokens y caducan tras cierto tiempo
	Se han implantado comprobaciones de integridad sobre el identificador de sesión, como hashes criptográficos como MD5 o SHA-1, y cifrados, no codificados (en por ejemplo, base64).
	Se han empleado mecanismos de gestión de sesiones existentes en el lenguaje o entorno de programación empleado.
	En el caso de haberse empleado mecanismos de seguridad más avanzados, se extendieron las capacidades del mecanismo existente
	Los ID de sesiones son generados aleatoriamente utilizando un mecanismo seguro
	Los ID de sesiones no contienen información personal
	Los ID de sesiones son protegida con SSL
	Están registrados todos los eventos de inicio de sesión, cierre de sesión, e inicios fallidos
	Los logs de autenticación incluyen fecha, hora de éxito, hora de fracaso, intentos fallidos, usuario que solicita autorización, dirección IP y ubicación
	CSRF (Cross-site request forgery)
	Se lleva a cabo este control mediante tokens dinámicos, creados por cada sesión, usuario y formulario crítico, suficientemente aleatorios, y que deben tener una fecha o tiempo de expiración.
	Se utilizan imágenes CAPTCHA
	Se han restringido la entrada de datos a los caracteres permitidos
	Los datos tienen definido: el tipo, longitud, formato y rango
	Los datos ingresados son enviados a una función que valide el tipo de caracteres ingresados
	Se validan los datos de entrada del lado del servidor

	Gestión de Logs
	Se ha realizado un análisis en donde se defina qué acciones van a generar eventos de logs y con qué nivel de detalle
En la gestión de logs, está considerado	El espacio necesario en disco
	Permisos
	Rendimiento
	Ubicación local y remota, centralización
	Correlación de logs
	Herramientas y soluciones para su análisis detallado (automático y manual)
	El log del administrador del sistema
	El log de cualquier dato que ha sido eliminado
	El log de cualquier dato que ha sido modificado
	El log de datos críticos debe estar en modo Write Once Read Many (WORM) y encriptado para logs de eliminación y modificación
	La aplicación de logs está aplicada en firewalls, IDS, WAF, servidores web, aplicación, base de datos y código de la aplicación web
	Se han empleado los mecanismos estándar del lenguaje o entorno de desarrollo web
	Las funciones de manipulación de logs están centralizadas en una librería
	ANÁLISIS DE SEGURIDAD DE APLICACIONES WEB
	METODOLOGÍA DE ANALISIS DE Caja Negra
En las pruebas realizadas	Se ha utilizado caracteres especiales en los campos de entrada en la aplicación web
	El sistema superó la vulnerabilidad de inyección SQL (pruebas con caracteres especiales)
	El sistema superó la vulnerabilidad de inyección XSS (pruebas con etiquetas html)
	Se han utilizado herramientas automáticas
	Se ha complementado con análisis manuales
	METODOLOGÍA DE ANALISIS DE CAJA BLANCA
	Se ha realizado un análisis exhaustivo del código de la aplicación en busca de funciones vulnerables o de la ausencia de métodos de validación
	Se han considerado las recomendaciones y soluciones disponibles para el lenguaje de programación empleado
Se ha analizado el códido en busca de estas posibles	Desbordamientos de memoria (buffer overruns y overflows)
	Inyección de comandos en el sistema operativo

vulnerabilidades:	Inyección de comandos SQL en la base de datos
	XSS (Cross-Site Scripting)
	CSRF, Cross Site Request Forgery
	Gestión de logs
	Autentificación
	Autorización
	Gestión de sesiones
	Cifrado, tanto en almacenamiento como en tránsito
	Condiciones de carrera (race conditions)
RECONOCIMIENTO	
	INFORMACIÓN DE REGISTRO DE DOMINIOS (DNS) Y DIRECCIONES
Se tiene un registro disponible de	Los servicios de registro de dominios y rangos de direcciones IP.
	La Seguridad de los DNS: versión, vulnerabilidades, tipos de registros, transferencias de zona (por dominio y por rango de direcciones IP), etc.
	Los registradores de dominios del nivel de nombres principal, y del proveedor del rango de direcciones IP en WHOIS
	Información administrativa contenida en el servicio de nombres (DNS): personas de contacto, servidores de nombres, dominios, etc.
SERVICIOS DE BÚSQUEDAS EN INTERNET	
	En técnicas de búsqueda avanzadas, conocidas como "Google Hacking"., no se visualizó información confidencial y sensible
UBICACIÓN EN LA RED	
Se tiene identificado	Información de la ubicación en la red del entorno Web objetivo y tráfico ICMP permitido.
	Los sistemas de comunicaciones y dispositivos de red: routers, balanceadores, etc.
	Los sistemas de protección de perímetro (firewalls, IDS, etc).
	Todos los servidores, firewalls y demás equipos sincronizados a una hora precisa entre ellos
ESCANEO	
	Se han escaneado exhaustivamente los puertos (TCP y UDP)
	Se han utilizado técnicas de fingerprinting sobre cada servicio/puerto (TCP y UDP) descubierto.
SERVICIOS WEB	

	Se tiene identificación e información sobre el tipo de servicios, aplicación y versión para el servidor Web, servidor de aplicación y base de datos.
	Existe soporte de los métodos HTTP. Algunos métodos, como TRACE, están asociados a ataques Web conocidos, como XST, Cross-Site Tracing.
	Existe Soporte SSL del servidor Web: versión de SSL o TLS, protocolos soportados, algoritmos de cifrado (incluyendo longitudes de clave de cifrado admitidas), certificados digitales y validez (expiración del certificado), Autoridad Certificadora (CA), etc.
	Antes de que los servicios web sean instalados, todos los ajustes predeterminados han sido revisados y los servicios innecesarios eliminados o desactivados
	Están deshabilitados los servicios que no están siendo utilizados por el web server o las aplicaciones
	Se han eliminado las cuentas y las contraseñas que vienen por defecto
	Se han eliminado todas las cuentas de invitados
	Se ha cambiado la cuenta y contraseña de la cuenta de administrador que viene por defecto
	CONTENIDOS WEB
Se han utilizado mecanismos para obtener información de	Recursos existentes en el entorno Web, tanto enlazados como adivinados/obtenidos por fuerza bruta o técnicas de diccionario
	Estructura de la Web de los dominios objetivo, diferenciando contenidos y recursos estáticos y dinámicos.
	Páginas dinámicas detectadas, sus parámetros de entrada, los tipos de los parámetros y el método de transferencia al servidor.
	Lenguaje(s) y entorno(s) de programación empleado(s).
	Las extensiones de ficheros empleadas en los recursos Web y la gestión de las diferentes extensiones de ficheros.
	Contenidos por defecto propios de las tecnologías empleadas en el entorno Web.
	Acceso público a páginas administrativas, de gestión, estadísticas, etc.
	Los recursos con control de accesos, es decir, que requieren autentificación (páginas de login).
	Las copias de seguridad/versiones anteriores de recursos accesibles, tanto enlazadas como adivinadas/obtenidas por fuerza bruta o técnicas de diccionario.

	Relaciones con otros entornos y aplicaciones Web, y análisis de seguridad en la invocación y referencias a servicios Web tanto internos y externos.
	Capacidades de la base de datos, contenidos y funcionalidad disponible por defecto.
Existen mecanismos de control de	Contenidos en cachés y dispositivos de red intermedios, tales como proxies.
	Publicación de contenidos en los servidores de búsqueda de Internet: Google, Yahoo, etc.
	En base a todos los puntos anteriores, las vulnerabilidades identificadas se han analizado y se han implementado mejoras para mitigarlas
	Existe documentación de cada vulnerabilidad y la medida tomada
	VULNERABILIDADES DE APLICACIONES WEB
Se ha realizado el filtrado mediante el chequeo de parámetros de entrada en los componentes dinámicos de la aplicación, comprobando la existencia de vulnerabilidades de los siguientes tipos:	Inyección SQL
	Inyección SQL ciega, incluyendo análisis de las diferencias en los tiempos de respuesta
	Inyección LDAP y XPath
	XSS, reflejado y persistente
	CSRF
	HTTP Response Splitting
	Inyección de comandos en el sistema operativo
	Desplazamiento por directorios
	Referencias directas a ficheros
	Parámetros y contenidos reflejados en la respuesta del servidor Web
	Métodos para evitar comprobaciones de tipo CAPTCHA
	Desbordamiento de buffers
	Se tiene una lista de los parámetros chequeados y sus resultados
Se ha realizado un análisis e identificado vulnerabilidades en los mecanismos de autentificación	Descripción de la seguridad de los métodos de autentificación
	Transporte de credenciales sobre canales de comunicación seguros
	Elementos de protección frente a ataques de enumeración y adivinación de credenciales: número máximo de intentos de acceso fallidos, limitaciones por tiempo, etc.
	Escenarios de denegación de servicio por bloqueo de cuentas tras un número determinado de intentos de acceso fallidos
	Análisis de la fortaleza de las claves y de los mecanismos de generación de claves por defecto

	Análisis de los certificados digitales, y de los procedimientos de gestión de los certificados (alta, verificación, revocación de certificados, etc.) (si aplica)
	Ataques de diccionario y fuerza bruta sobre las credenciales de acceso
	Métodos para evitar el sistema de autentificación
	Mecanismos de renovación de claves
Se ha realizado un análisis de seguridad en los mecanismos de control de sesiones:	Seguridad de las sesiones
	Duración y ámbito de las sesiones
	Elementos empleados para implementar el mantenimiento de sesiones
	Formato y contenido del identificador o token de las sesiones
	Uso de tokens (cookies, variables, cabeceras HTTP, etc) por parte de la aplicación Web
	Mecanismos de manipulación del token de sesión
	Ataques de fijación de sesión
	Escenarios Single Sign On (SSO)
	Mecanismo de cierre de sesiones y gestión de la información de sesión cacheada en los clientes Web
Se realizado un análisis de los mecanismos de control de acceso (ACLs):	Acceso a contenidos de usuarios conocidos o típicos (existentes por defecto)
	Acceso a ficheros de configuración del entorno Web
	Acceso a versiones renombradas (bakups) de archivos en producción
	Acceso a la información de otros usuarios con credenciales
	Trazabilidad de los accesos de usuario
	Métodos para evitar el sistema de autorización
	Escalada de privilegios
En las páginas en donde el usuario requiere autenticación, se ha realizado un análisis de seguridad	Mediante un usuario externo sin credenciales de acceso
	Mediante un usuario con credenciales de acceso
	Todos los ingresos al sistema están registrados con las debidas medidas de seguridad
	PRUEBAS DE CARGA Y DENEGACIÓN DE SERVICIO (DOS)
Se han realizado pruebas de	DoS simple o distribuida, según las capacidades del entorno web
	Bloqueo de cuentas mediante intentos de acceso fallidos
	Existencia de errores no recuperables en la aplicación, como desbordamiento de buffers

	Reserva de recursos en base a las peticiones de un usuario, y errores de liberación de recursos
	Existencia de bucles de proceso infinitos en función de los parámetros de entrada
	Consumo excesivo de recursos en los elementos de búsqueda
	Diferencias de demanda de recursos en los diferentes componentes del entorno Web: servidor Web, de aplicación o base de datos.
	Denegación de servicio por rellenado automático de formularios
	Consumo de recursos de almacenamiento (espacio en disco) en base a las peticiones de un usuario

ANEXO D: MARCO DE EVALUACIÓN DE CLOUD COMPUTING

	Generalidades
	Se entregó los requisitos previos al proveedor
	Se tiene una descripción detallada del servicio contratado
	Se dio a conocer al proveedor la categoría del sistema
	En el contrato firmado se reflejan acuerdos, especificaciones y nivel de servicio
	TIPO DE SERVICIO
	En el contrato está determinado el servicio que el proveedor va a prestar: Saas, Paas, Iaas.
	TIPO DE INFRAESTRUCTURA
	El servicio se ejecuta en una infraestructura privada
	CAPACIDAD DEL SERVICIO
En el acuerdo está determinado	La capacidad del servicio
	Las medidas de penalización en caso de que no se cumpla
	Las condiciones bajo las que se podrá modificar la capacidad contratada
	Las herramientas que miden la capacidad del servicio y su rendimiento
	La posibilidad de cambiar la capacidad en tiempo real según la demanda, de manera automática
	CONFIDENCIALIDAD DEL SERVICIO
En el contrato está estipulado, que el proveedor cloud se compromete a	Mantener la confidencialidad en el tratamiento de la información
	No divulgar o acceder indebidamente a la información sin la autorización expresa de su propietario
	ACUERDOS DE NIVEL DE SERVICIO
	Existen acuerdos detallados del nivel de servicio (Service Level Agreement - SLA)
Los SLA detallan	Desviaciones de carga que el proveedor deberá asumir
	Tiempos de notificación cuando se detecte insuficiencia de recursos.
	Porcentajes de disponibilidad del servicio en función de la criticidad del mismo
	El tiempo de recuperación para los sistemas de información en línea menor a cuatro horas
	El tiempo de respuesta y resolución, horario de atención a peticiones de cambio realizadas

De cada SLA está definido	El identificador, la descripción del cálculo para la obtención del SLA (fórmula), los valores correctos en la prestación del servicio (umbrales), y la fórmula para aplicar las penalizaciones por incumplimiento de SLA (penalización)
	La periodicidad de los informes de cumplimiento y penalizaciones de los SLA
	MODO DE ACCESO AL SERVICIO
Está definido	Los protocolos empleados así como el nivel de seguridad requerido en los mismos
	El acceso al servicio mediante protocolos de comunicación que incorporen cifrado de datos para la información en tránsito y almacenada
	RESPONSABILIDADES Y OBLIGACIONES
Proveedor	Cumple con las medidas de seguridad requeridas.
	Notifica todos los incidentes que pueden comprometer la seguridad del servicio o de la información de la organización cliente.
	Realiza la entrega de informes en la monitorización de servicios.
	Realiza auditorías que demuestren el adecuado cumplimiento normativo.
	Garantiza el correcto funcionamiento de los servicios contratados cumpliendo con los niveles de servicio fijados en los SLAs.
	Mantiene el principio de confidencialidad durante y tras la finalización de la relación contractual.
Cliente	Designa representantes del cliente con autoridad y capacitación para la toma de decisiones ante cambios.
	Notifica las incidencias y las peticiones de servicio al proveedor haciendo uso de los canales establecidos para tal fin.
	Revisa el cumplimiento de los niveles de servicio contratados
	Solicita las auditorías realizadas por el proveedor
	FINALIZACIÓN DEL SERVICIO
Al término del contrato	El proveedor eliminará o devolverá la información, según lo estipulado en el contrato
	Está definido el tiempo para la ejecución de la migración o destrucción de la información tras la rescisión del contrato
	REQUERIMIENTOS LEGALES
En el contrato y en los acuerdos pactados	Están considerados los riesgos legales en caso de incumplir con el incumplimiento de la legislación aplicable, el acuerdo de confidencialidad y SLAs.
	Consideraciones a tomar
El proveedor	Se ha sido sometido a algún tipo de auditoría en donde se verifique que tiene un marco organizativo, marco operacional y medidas de protección acorde a normas internacionales y locales.

	Dispone de certificaciones internacionales en cuanto a la gestión de la información y seguridad
En el contrato	Está reflejado el cumplimiento de las medidas del proveedor cloud
La organización gubernamental	Dispone de un determinado nivel control sobre los servicios que se ejecutan en el cloud
Se dispone del derecho de auditoría, sobre el proveedor de servicios o de	Una declaración de aplicabilidad de las medidas a aplicar.
	Una auditoría que certifique que el marco organizativo, operacional y medidas de protección están de acuerdo con el nivel del sistema o con normas internacionales que la validen.
La auditoría	Es realizada por un tercero independientemente que tenga experiencia y formación en auditoría de sistemas de información.
	Análisis de riesgos
El proveedor cloud	Dispone de un análisis de riesgos
	Entregó un plan de tratamiento de riesgos
	Un análisis de riesgos actualizado, así como de una correcta gestión de los riesgos resultantes.
El análisis de riesgos	Siguió una metodología reconocida internacional
	Incluyó los servicios objeto de la prestación
	Tiene revisiones periódicas
	Gestión de personal
Tanto el proveedor cloud como el gobierno	Han designado un Responsable de Seguridad.
En el contrato está especificado	De que todo el personal participante en la provisión del servicio, mantiene la confidencialidad de la información durante la prestación del servicio como a la finalización de éste.
	Autorización y control de acceso
Existe limitaciones	Al acceso a la información en el cloud sólo al personal autorizado
	A recursos según las funciones asignadas al usuario
	* En la certificación del marco organizativo y operacional está considerada esta sección
	Protección de las instalaciones
Está definido	Un control de acceso físico a las instalaciones donde está albergado el servicio contratado
	Un registro de todos los accesos, físicos o lógicos
Las medidas de seguridad implantadas en el Centro de Proceso de Datos	Son informadas al encargado de Seguridad Gubernamental
	Son acordes a las medidas de seguridad gubernamentales
	Seguridad por defecto
Está limitado	Las funcionalidades técnicas del sistema que no sean requeridas.

	El acceso a la administración y al registro de actividad únicamente al personal autorizado.
	El número de intentos de acceso fallidos.
Están inhabilitadas	Las cuentas de usuario innecesarias.
Se ha establecido	Bloqueos de sesión por tiempo de inactividad.
	Periódicamente al proveedor cloud un informe de los controles de seguridad
	Integridad y actualización del sistema
	Existe un procedimiento de gestión de parches y vulnerabilidades
	Éste procedimiento es implantado y auditado sobre el sistema e-gobierno
Los resultados de esta auditoría	Son entregados al encargado de la seguridad del sistema e-gobierno
	Gestión de cambios
	Se dispone de un procedimiento de gestión de cambios
El proveedor cloud deberá informar:	Los cambios que puedan afectar al servicio.
	Procedimiento de solicitud de cambios.
	Proceso de autorización de cambios.
	Asignación de responsabilidades referentes a cambios.
	Tareas de mantenimiento y actualización de recursos.
	Protección de la información almacenada y en tránsito
En cuanto al cifrado	Existen medidas por parte del proveedor cloud y del gobierno
	Está implementado en los sistemas de información donde transita y se ubica la información
Se encuentran encriptados	Los ficheros, directorios, discos virtuales y datos en base de datos, con un nivel de seguridad de al menos 128 bits
	Los respaldos con un nivel de seguridad e al menos 128 bits
Para las encriptaciones	Tipo simétrico TDEA y AES, el nivel de seguridad es de al menos 128 bits
	Basado en curvas elípticas, el nivel de seguridad es de al menos 256 bits
	Tipo simétrico RSA, clave pública, el nivel de seguridad es de al menos 2048 bits
Las comunicaciones encriptadas	Están implementadas en todos los tipos de servicio empleando protocolos estándar como IPSEC, SSL o TLS, con un nivel de seguridad de al menos 128 bits
	Prevención ante otros sistemas de información interconectados
Está definida	La arquitectura de seguridad o un esquema que resuma los dispositivos (cortafuegos, IPS, IDS, WAF, etc.) para proteger la infraestructura donde se hospedarán los datos del sistema
	Registro de actividad

El proveedor cloud entrega	Los registros de acceso que permitan monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.
	Periódicamente un registro de los accesos realizados a las plataformas puestas a disposición del cliente
	Gestión de incidencias
	El proveedor cloud dispone de un procedimiento de gestión de incidencias
Periódicamente el proveedor cloud entrega	Procedimiento de notificación de incidencias.
	Tipología de incidencias incluidas en el servicio.
	Procedimientos específicos ante incidentes de seguridad.
	Tiempos de respuesta y resolución de incidencias/incidentes.
	Mantenimiento y gestión del registro de incidencias.
	Procedimiento de borrado de información
El proveedor cloud dá a conocer	Los procedimientos de borrado seguro siempre que se realice una modificación sustancial o terminación contractual
	Las notificaciones y certificación de borrados acometidos.
	Respaldo y recuperación de datos
	Existe un procedimiento de copias de respaldo que garantice la restauración de la información
El proveedor cloud informa:	Alcance de los respaldos.
	Política de copias de seguridad.
	Medidas de cifrado de información en respaldo.
	Procedimiento de solicitud de restauraciones de respaldo.
	Realización de pruebas de restauración.
	Traslado de copias de seguridad (si aplica).
	Continuidad de la actividad
El proveedor cloud dio a conocer	El plan de continuidad de negocio donde garantiza la restauración de los servicios.
	Evidencia satisfactoria de la ejecución periódica de pruebas de continuidad.
	Análisis de impacto del servicio cloud computing.
Sección Seguimiento del Servicio	
Se realiza el monitoreo de	La medición del cumplimiento del servicio y el procedimiento para restaurar las desviaciones estipuladas contractualmente.
	El proceso de coordinación para el mantenimiento de los sistemas implicados.
	El proceso de coordinación ante incidencias o desastres.
El proveedor cloud entrega periódicamente los siguientes controles de seguridad y servicio	Niveles de calidad, disponibilidad y capacidad del servicio ofrecido, cumplimiento de las obligaciones de servicio acordadas y la respuesta ofrecida por el proveedor ante desviaciones significativas.

	Gestión de incidentes de seguridad, para determinar orígenes, objetivos, riesgos asociados a cualquier incidente relevante.
	Controles de acceso al entorno cloud, incluyendo listado actualizado de usuarios autorizados para utilizar los servicios disponibles, y los privilegios asociados en cada caso.
	Cumplimiento normativo y legislativo como auditorías: ISO, financieras, etc.
	Situación actualizada de las medidas de protección de la información, incluyendo aspectos de seguridad física, protección contra software malicioso, seguridad del personal, copias de seguridad, etc.
	Mecanismos de comprobación regular de los controles de seguridad por parte del proveedor y resultados de dichas comprobaciones.
	Anomalías o desviaciones significativas, así como las acciones ejecutadas en cada caso como respuesta a estas situaciones
	Herramientas de detección o prevención de intrusiones
	Análisis de las alertas más significativas y las medidas adoptadas para mitigar un posible impacto
	Los resultados de los indicadores que midan el desempeño de la seguridad del entorno cloud
Se han establecido	Procedimientos de coordinación en el mantenimiento de sistemas entre ambas partes
	Mecanismos y procedimientos para la coordinación ante incidencias o desastres
	Los flujos de información y las interacciones entre cliente y proveedor ante incidentes y desastres.
	Informes periódicos de los mantenimientos y actualizaciones realizados en los sistemas que albergan los sistemas del cliente.
	Cuando el mantenimiento o actualización implica un cambio mayor, el proveedor habilita previamente un entorno actualizado para que el cliente verifique el correcto funcionamiento de sus sistemas en preproducción.
	MEDIOS ALTERNATIVOS
El plan de continuidad de negocio	Incluye los servicios objeto de la prestación
	Ha sido verificado por el Responsable de la Seguridad
	Es sometido a pruebas periódicas

ANEXO E: MARCO DE EVALUACIÓN DE INFRAESTRUCTURAS CRÍTICAS

	Infraestructuras Críticas
Bases de la Directiva General	Existe una Directiva General dispuesto por la Ley que señale quienes conforman la Comisión de Protección de Infraestructuras Críticas
	Existe como mínimo un representante por institución de quienes la conforman
	Las instituciones involucradas son públicas y privadas
	El punto central de todas las medidas y acciones que se tomen, es para garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales.
	Como objetivo se tiene que todas estas actividades están destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas tanto físicas como lógicas
	Los integrantes de esta Dirección tienen responsabilidades, obligaciones y capacidades definidas en el acceso e intercambio de la información bajo cláusulas de confidencialidad
	La Dirección General impulsa la colaboración e implicación de las infraestructuras críticas, con el fin de optimizar su grado de protección y de contribuir a la seguridad de la población
	La Dirección General ha aprobado el conjunto de estrategias necesarias para dirigir y coordinar las acciones de los distintos órganos responsables.
-	
Aspectos Legales	Se tiene un Marco Legal que respalde la gestión de Protección de las Infraestructuras Críticas
	Existe un reglamento de Protección de las Infraestructuras Críticas
	Todas las acciones y acuerdos se alinean según el Reglamento Legal
	Existe un organigrama para conocer la estructura departamentales de toda la Comisión Crítica
	Existe un documento oficial en el que se detalla la responsabilidad en la protección de infraestructuras críticas por cada uno de los actores implicados.
-	
	Desarrollo de Actividades
Catálogo de Infraestructuras críticas	Existe un catálogo que contenga información completa de todas las infraestructuras críticas a nivel nacional, categorizándolas según el grado de criticidad y sectorización dada
	El catálogo contiene la ubicación, titularidad, servicios que prestan, contactos, nivel de seguridad que precisan según los riesgos evaluados
	El catálogo es secreto y confidencial
	El catálogo es actualizado según el periodo dispuesto en el reglamento

	En caso de que se produzca un evento crítico que sea de repercusión internacional, tener los contactos
-	Existe un órgano superior responsable del Sistema de Protección de las Infraestructuras Críticas
El órgano superior es el encargado ó ha definido organismos, instituciones, comisiones que se encarguen de la elaboración, evaluación y seguimiento de:	Diseñar y dirigir la estrategia nacional de protección de infraestructuras críticas
	Aprobar el Plan Nacional de Protección de las Infraestructuras críticas
	Aprobar planes de protección y seguridad
	Aprobar los planes de apoyo operativo, su supervisión y coordinación e implantación de los mismos
	Aprobar una zona como "zona crítica" según análisis previo
	Identificar las situaciones que podrían generar un estado crítico de una o más instituciones en cadena
	Analizar los mecanismos de prevención y respuesta previstos para cada uno de los actores implicados
	Emitir instrucciones y protocolos a las partes involucradas
	Dirigir y coordinar los análisis de riesgos que se realicen en organizaciones públicas o privadas
	Evaluar el cumplimiento de los protocolos
	Que todos los mecanismos permanentes de información, alerta y comunicación en todos los involucrados sean confidenciales
	Que los análisis de las diferentes índoles sean realizados por expertos
	Acuerdos por escrito de que ante un evento, las instituciones tienen que asignar y priorizar recursos humanos, materiales y económicos, según el plan definido
	Acuerdos acceso e intercambio de información
	Los parámetros para determinar la criticidad, gravedad y consecuencias ante un evento crítico están en función del número de personas afectadas, impacto económico, medioambiental público y social
	El aspecto comunicacional externo como prensa pública nacional e internacional
	Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico
-	
Según la responsabilidad detallada en el reglamento a las diferentes instituciones, se debe	Ejecutar y mantener actualizado el Plan de Seguridad
	Determinar la criticidad y consecuencias ante un evento crítico
	Analizar y evaluar los análisis de riesgos de los organismos privados y públicos de todos los escenarios posibles ante un evento crítico
	Analizar los mecanismos de prevención y respuesta previstos
	Analizar las repercusiones en las infraestructuras que dan apoyo a las infraestructuras principales
	Analizar las repercusiones en otras infraestructuras no necesariamente críticas a nivel local, nacional e internacional

	Realizar simulacros en el ámbito de la protección de las infraestructuras críticas.
	Enviar los resultados al órgano superior encargado
	Evaluar los planes de seguridad por expertos según los resultados de los simulacros
	Enviar al órgano rector para su aprobación
	Validar los planes de apoyo operativos para enviarlos al órgano rector para aprobación
	Realizar los planes por expertos en el campo a analizar
	Coordinar la participación de expertos en las reuniones
	Supervisar que los protocolos se estén cumplimiento
	Definir los parámetros homogéneos de protección de los activos de las instituciones involucradas
	Preservar, garantizar y promover la existencia de una cultura de seguridad de las infraestructuras críticas
El Plan de Seguridad Nacional tiene	Un enfoque integral
	Las infraestructuras críticas priorizadas
	Las infraestructuras críticas sectorizadas según sus afinidades
	Diferentes niveles de seguridad según el tipo de infraestructura crítica
	Identificadas y definidas todas las tareas, responsabilidades y recursos existentes para poder hacer frente a un evento crítico que se presente
	Políticas comunicacionales ante soluciones y aprobaciones a los incidentes presentados
	La comunicación que se establece entre infraestructuras críticas tiene canales y procedimientos seguros
	Actualizaciones según el reglamento
	Criterios y las directrices precisas para movilizar las capacidades operativas, articulando las medidas preventivas necesarias para asegurar la protección permanente, actualizada de las infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.
Los Planes Sectoriales	Dan a conocer los servicios esenciales proporcionados a la sociedad
	Funcionamiento General del sector
	Vulnerabilidades sectoriales
	Consecuencias potenciales de su inactividad
	Medidas estratégicas para su funcionamiento
	Fue acordado por la mesa sectorial
	Están basados en un análisis general de riesgos, vulnerabilidades y consecuencias
	Propuestas para prevenir, reaccionar las posibles consecuencias de los diferentes escenarios

	Propuestas de mantenimiento de planes operativos
	Medidas de coordinación con el Plan Nacional
	Actualización según el reglamento
	Identifica, evalúa, previene y mitiga riesgos de las instituciones involucradas
	Las metodologías para enfrentar algún evento de riesgo están homogeneizadas entre las instituciones
	Sistemas redundantes o aislados y la adecuada dotación de elementos de reposición.
	Metodologías para una adecuada coordinación operativa entre las organizaciones responsables en la gestión de riesgos y crisis
	Un Plan de protección estratégico por cada infraestructura crítica según su escenario considerando las otras infraestructuras críticas o no críticas que pudieran verse afectadas
	Todas las versiones generadas quedan registradas
	Se conoce la capacidad mínima imprescindible de cada infraestructura del sector
	Se conoce los requisitos y procedimientos de alerta de cada infraestructura del sector
	Se conoce las estrategias de respuesta
	Los procedimientos para la reconstitución de los servicios
	Los programas de capacitación a los involucrados
	Los presupuestos involucrados si se llegasen a ejecutar los planes
	Las leyes y marcos que aplican en eventos críticos
	Han identificado los factores para determinar un inicio de ataque hacia alguna de las infraestructuras críticas
	Las estrategias de prevención y mitigación de riesgos se innovan periódicamente
	Existen protocolos coordinados de comunicación entre todos
	Los protocolos están estandarizados entre los sectores
Planes de Seguridad del Operador	Están compuesto por las políticas generales de las instituciones, empresas u organizaciones que han sido identificadas como críticas
	Establecen una metodología de análisis de riesgos
	La metodología protege los bienes tanto físicos como lógicos
	El plan fue aprobado por el órgano superior
	Se encuentra especificado el orden de las medidas y procedimientos a adoptar
	El Plan aprobado ha sido difundido a las instituciones involucradas aprobadas
	El Plan es de carácter confidencial y secreto
	El Plan es actualizado según el marco
	Si este Plan cambiara, se revisan todos los planes de seguridad del operador

Planes de Protección Específicos	Contiene las medidas concretas a adoptar por las instituciones, empresas u organizaciones que han sido identificadas como críticas
	Las medidas contemplan la protección de bienes tanto físicos como lógicos
	El conjunto de planes fue aprobado por el órgano superior
	Las medidas que se contemplan en el plan han sido verificadas antes de sus institución para comprobar que funcionan
	Si ingresa una nueva infraestructura crítica, los planes son verificados
	Estas medidas contienen todos los riesgos asociados respecto amenazas, terrorismo o ataques informáticos
	Los planes tienen medidas permanentes, temporales y graduadas, y serán implementadas según lo que recomiendo el Plan Nacional de Protección
	Todo Plan de Protección por infraestructura contiene los requisitos de funcionamiento mínimo de la infraestructura crítica
	Se mantiene un registro de las instituciones y operación que realiza la institución crítica a reincorporarse con normalidad
	Si este Plan cambiara, se revisan todos los planes específicos
Proveedores	Se ha firmado un acuerdo con el proveedor de apoyo a las infraestructuras críticas en caso de que se soliciten
	Según acuerdo firmado con el proveedor está disponible las 24 horas del día, 7 días a la semana, 365 días al año
	Se tienen identificado los proveedores de servicios de las infraestructuras críticas e identificado los riesgos de que éstos no puedan dar servicio a la infraestructura crítica
	Los proveedores de servicios a la infraestructura crítica, tienen definido por escrito sus funciones, responsabilidades y obligaciones ante un evento
	Los proveedores de servicios a la infraestructura crítica han realizado los planes de seguridad y protección de ellos mismos
Reportes	Toda alerta genera un reporte
	Todo reporte generado digitalmente está encriptado
	Todo reporte impreso debe de tener un identificador único, así como su respectivo registro de quién lo generó, en dónde y fecha
	Todo reporte generado es estrictamente clasificado y confidencial
	La Dirección General aprueba los reportes que pueden ser mostrados o mantenerse confidenciales
	El órgano superior aprueba quienes tienen acceso a los reportes según su tipo
	La respuesta ante un incidente es inmediata según las soluciones definidas con anterioridad
	Existe un protocolo para comunicar el o los estados de las infraestructuras en caso de un ataque

	Se ha considerado proteger los activos tangibles e intangibles de las instituciones involucradas
	Ante una alerta de alguna infraestructura crítica, se levanta un consenso de seguridad inmediato
	A la alerta de alguna de las instituciones críticas existe una coordinación acordada previamente
	Existen protocolos de coordinación entre la empresa pública y privada
	Existe reuniones de Dirección General periódicas
	Existe una retroalimentación de parte de todas las infraestructura críticas
El grupo de infraestructuras críticas	Participan y colaboran para la protección de las infraestructuras críticas individual y en conjunto
	Verifican dentro de sus competencias el cumplimiento de los Planes de Seguridad acordados
	Colaboran activamente con el órgano superior
	Colaboran en la elaboración de indicadores críticos
	Proporcionan asesoramiento técnico dentro del sector de su competencia
	Comprometerse con la confidencialidad solicitada dentro del grupo
	Asigna un responsable de la seguridad de la institución con la facultad de voz y voto en las decisiones que se quieran tomar en las reuniones conjuntas
	Participar en el proceso de clasificación de una infraestructura como crítica