ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

ELABORACIÓN DE LA GUÍA DE IMPLANTACIÓN DE LAS NORMAS PRIORITARIAS DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN EGSI EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA CENTRAL

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

CAROLINA ELIZABETH CÁCERES TARCO
caroely0516@yahoo.com

CRISTINA ELIZABETH MENA GONZÁLEZ
cemg_845@hotmail.com

DIRECTOR: ING. RAÚL CÓRDOVA M.SC.
raul.cordova@epn.edu.ec

Quito, Mayo 2015

DECLARACIÓN

Nosotras, Carolina Elizabeth Cáceres Tarco y Cristina Elizabeth Mena González, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Carolina Elizabeth Cáceres Tarco	**Cristina Elizabeth Mena González**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Carolina Elizabeth Cáceres Tarco y Cristina Elizabeth Mena González, bajo mi supervisión.

Ing. Raúl Córdova M.SC.
DIRECTOR DE PROYECTO

DEDICATORIA

Para mis pequeños ángeles, por ser la inspiración de mi vida.

Carolina

DEDICATORIA

A mis padres Jorge y Laura, por haber forjado con su amor, ejemplo y apoyo la mujer que soy ahora. Ustedes son el pilar fundamental en la culminación de esta carrera. Sin ustedes, jamás hubiese alcanzado esta meta.

A Martín y Paula, mis hijos, que son el tesoro más valioso que Dios me ha regalado, quienes constituyen el centro de mi vida y quienes me han impulsado a superarme cada día. Mis hijos, que con su dulzura e inocencia son las vitaminas que llenan mi vida, me permiten continuar en esta lucha por ser mejor.

A Juan, mi esposo, mi compañero y amigo, quien me brindo su amor, su cariño, su estímulo y su apoyo constante.

A Jorge, mi ñaño, en la vida hemos estado siempre los dos para todo, aunque con desacuerdos e inconvenientes siempre juntos. A ti te dedico este esfuerzo. Nunca es tarde para lograr nuestros sueños y metas.

A mis dos ángeles, Papá Manuel y Papá Enrique, que desde el cielo siempre me han dado sabiduría. Aunque ya no están presentes en cuerpo siempre los llevo en mi corazón.

A mis abuelitas, que con sus enseñanzas he aprendido el valor de la familia.

Cristina Mena G.

AGRADECIMIENTOS

Al director de este proyecto, Ing. Raúl Córdova, por su apoyo y enseñanzas, que contribuyeron en gran medida para la finalización de mi carrera.

A mis amigos y compañeros, por toda su ayuda durante el tiempo que nos esforzamos juntos.

A mi familia, porque el trabajo invertido ha sido de todos nosotros.

Finalmente a mi compañera de tesis, por su voluntad para cumplir esta meta que nos la merecíamos desde hace mucho.

Carolina

AGRADECIMIENTOS

A mis padres, gracias por su apoyo, su dedicación, su sacrificio, sus palabras de aliento, por ser mi inspiración. Sé que siempre voy a contar con ustedes en las buenas y en las malas, espero poder recompensar todo lo que en la vida me han enseñado y brindado.

A mis hijos, gracias por ser la principal motivación para seguir adelante, gracias por hacerme sentir lo maravilloso y único que es ser madre y llenar mi vida con solo una sonrisa y un beso.

A mi esposo Juan, por apoyarme en todas las decisiones que he tomado, por haber llegado a mi vida y brindarme el regalo más valioso que es el formar una familia. Gracias por ser mi amigo, mi complemento, mi compañero, mi fuerza, mi alegría, mi amor.

A mi tutor, Ing. Raúl Córdova, por su apoyo y confianza en la realización de este proyecto, y sobre todo por su paciencia.

A mi compañera de Tesis, Caro, quien con su empuje y ganas siempre estuvo predispuesta a salir adelante con este proyecto.

A mi jefe y amigo Milton por su paciencia y apoyo para la culminación de esta meta.

A todos quienes formaron parte de mi carrera profesional y contribuyeron de alguna forma a la consecución de mis metas.

Cristina Mena G.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El proyecto de titulación que se presenta contiene una Guía para la implantación del Esquema Gubernamental de Seguridad de la Información EGSI en las entidades gubernamentales de la Administración Pública Central de Ecuador, que permite a los involucrados seguir un conjunto de pasos para realizar la implantación de esta norma. En el capítulo I, se detalla un análisis de la Seguridad de la Información en las entidades públicas del país, la normativa relacionada con el tema, el análisis de EGSI respecto al marco legal, métodos definidos para el control y seguimiento del proyecto; y finalmente, la revisión de los controles que tienen relación con Tecnologías de la Información.

En el capítulo II, se incluye la guía para la implantación de EGSI, con los pasos para definir el análisis de la situación actual de Seguridad de la Información en la entidad, la Política de Seguridad de la Información, y los procedimientos para la aplicación de los controles de EGSI en las unidades de TI de la entidad.

En el tercer capítulo, se valida la guía desarrollada mediante la aplicación de la Guía en la Agencia de Regulación y Control de Electricidad.

Finalmente, el capítulo IV contiene las conclusiones y recomendaciones obtenidas en el desarrollo de este proyecto de titulación.

PRESENTACIÓN

El presente proyecto es la propuesta de una “Guía de implantación del Esquema Gubernamental de Seguridad de la Información EGSI”, definida para las entidades del sector público que pertenecen a la Administración Pública Central del Ecuador.

El objetivo principal de la Guía es colaborar en el proyecto de implantación del Esquema Gubernamental de Seguridad de la Información EGSI, mediante la determinación del estado inicial de la seguridad de la información, la definición de la política general de seguridad de la información y la determinación de los procedimientos para la implantación del EGSI.

A continuación se elabora la guía, definiendo el objeto, alcance, base legal responsabilidades y políticas que se proponen para la implantación del EGSI en las entidades gubernamentales de la Administración Pública Central. En el mismo capítulo se elaboran los cuatro procedimientos del EGSI que tienen directa relación con TI.

Una vez que se elabora la Guía, se realiza una validación mediante la aplicación de la misma en la Agencia de Regulación y Control de Electricidad.

Finalmente se presentan las conclusiones y recomendaciones obtenidas a lo largo de la ejecución de este proyecto.

CAPÍTULO 1: SEGURIDAD DE LA INFORMACIÓN

1.1. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES PÚBLICAS

En la actualidad, las tecnologías de la información forman parte determinante de los procesos en todo el planeta, requiriendo para su protección una disciplina denominada Seguridad de la Información. A nivel nacional e internacional, se han determinado estándares o normas que permitan su gestión, y particularmente su control, más allá del giro del negocio donde se desee aplicarlas.

Se puede definir entonces a la Seguridad de la Información como todas aquellas medidas que se implementen para el resguardo de información; cumpliendo estrictamente los dominios de confidencialidad, integridad y disponibilidad. Bajo una política de Seguridad de la Información, cualquier tipo de información, ya sea en medios físicos o magnéticos, debe ser: entregada a quien le pertenece; debe ser verdadera respecto a su origen y debe estar accesible para quien vaya a revisarla. A continuación, se explican los dominios que forman parte de este concepto.

1.1.1. CONFIDENCIALIDAD

La Organización Internacional de Estandarización (ISO) expidió la norma ISO/IEC 27000, misma que define a la confidencialidad como "la propiedad [cualidad, NDLA] de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados" [1].

La importancia de la confidencialidad radica en la naturaleza de la información. Por esta razón, en los esquemas de seguridad se deben definir claramente los perfiles de acceso a la información. Muchos casos han demostrado que por fallas en la determinación de estos esquemas de seguridad, las entidades pueden perder grandes cantidades de dinero, o los usuarios pueden ver expuesta su información privada en manos de quienes no harán uso adecuado de la misma, e inclusive puedan emplear esta información para actividades ilegales. Por lo descrito, es fácil deducir que, a mayor criticidad de la información, mayores deben ser los cuidados para garantizar su confidencialidad.

Se observa el papel fundamental que juega en esta gestión el dueño de la información. Solamente él podría determinar con especificidad los niveles de acceso, clasificando la información de acuerdo al proceso que con ella se maneja. Entonces, las TI servirán para aplicar éstos niveles de acceso previamente definidos en los esquemas de seguridad.

La importancia de la confidencialidad se evidencia cuando se utilizan medios públicos de trasmisión de datos como el internet o se almacenan datos en repositorios de información poco confiables. Las medidas a implementarse en estos aspectos deben ser técnicamente definidas, de manera que se evite cualquier fuga no autorizada.

En el contexto legal ecuatoriano, la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), expedida mediante Registro Oficial 337 del 18 de mayo de 2004, define en su artículo 6 a la información confidencial como:

> *"aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.*
>
> *El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.*
>
> *No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República".[3]*

1.1.2. INTEGRIDAD

La norma ISO/IEC 27000 define a la integridad como "propiedad de proteger la precisión y completitud de los activos (se considera como activo cualquier cosa que tiene valor para la organización)" [1].

La confidencialidad y la integridad no son complementarias y, en consecuencia, se deben determinar diferentes controles de seguridad para proteger la información en ambos aspectos.

Las entidades públicas son objeto de ataques, especialmente de organizaciones que no están de acuerdo con las directrices gubernamentales, siendo sus principales intenciones no solo capturar información sino modificar datos y poner en evidencia bajos niveles de seguridad.

1.1.3. DISPONIBILIDAD

En la norma ISO/IEC 27000, se define a la disponibilidad como "propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada" [1].

De los tres dominios de la seguridad de la información expuestos, el de la disponibilidad es el que se encuentra más estrechamente ligado a la tecnología, y es posible su medición. De los fallos en los sistemas, se puede contabilizar el tiempo que la información ha estado disponible, entonces se pueden emplear medidas de hardware o software como se requieran para mejorar estos indicadores numéricos.

1.1.4. SITUACIÓN ACTUAL

De la 11ava Encuesta de Seguridad para la Industria Financiera realizada por Deloitte en mayo de 2014, se indica que el 45% de empresas ecuatorianas señaló que la falta de políticas de seguridad y evidencias de soporte representan la principal observación de auditoría interna o externa. Las participantes también indicaron que su objetivo en esta área es el cumplimiento regulatorio y legislativo de seguridad de la información. De esto, se desprende una visión general sobre la importancia de la seguridad de la información en nuestro país [2].

En el sector público, también existe el sentido de precautelar la información. Así, la LOTAIP, ya define ciertas características acerca de la información y su acceso.

Por ejemplo, en el artículo 1, que se refiere al principio de publicidad de la información, dictamina que “El acceso a la información pública es un derecho de las personas que garantiza el Estado” [3]. Siendo de aplicación en todas las entidades del sector público y aquellas que manejen fondos públicos, la información que se genera en éstas debe estar a disposición de cualquier ciudadano que exprese su necesidad de conocerla.

Adicionalmente, la LOTAIP determina tipos de acceso a la información en los siguientes artículos:

> "Art. 5.- Información Pública.- Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.
>
> Art. 6.- Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República."[3]

En este contexto, y al comparar esta definición de la Ley con el estándar internacional, el dominio de confidencialidad queda disminuido para las entidades del sector público. En este marco, se deben tomar en cuenta los siguientes aspectos.

En toda institución, independientemente de su giro de negocio, existe información que, por su naturaleza o antes de cumplir ciertas revisiones y/o validaciones, no puede ser expuesta como versión final o información aprobada. En el sector público, dado que se toman decisiones de aplicación nacional, la confidencialidad de información en estado de borrador es altamente requerida en función de evitar malas interpretaciones, o en el peor de los casos, un caos social.

La aplicación del principio de publicidad debe ser solicitada por vía escrita y dirigida al titular de la institución pública que administre el proceso que genera la información, tal como indica la LOTAIP en su artículo 19. Esta actividad genera un nivel de acceso público de la información para los ciudadanos de nuestro país con carácter de obligatorio en todas las entidades públicas.

La LOTAIP establece, en su artículo 9, para todas las entidades de sector público un período de diez días para la atención de solicitudes de información. Aquí juega un papel determinante la disponibilidad de la información, ya que las sanciones para

la no entrega de información pueden llegar hasta la remoción permanente del servidor público.

Sobre el dominio de la integridad, la LOTAIP en su artículo 10 acerca de la custodia de la información, expresa lo siguiente: “Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública.”[3]

Se pueden resumir entonces éstos conceptos respecto a la aplicación de la seguridad de la información en la Figura 1-1.

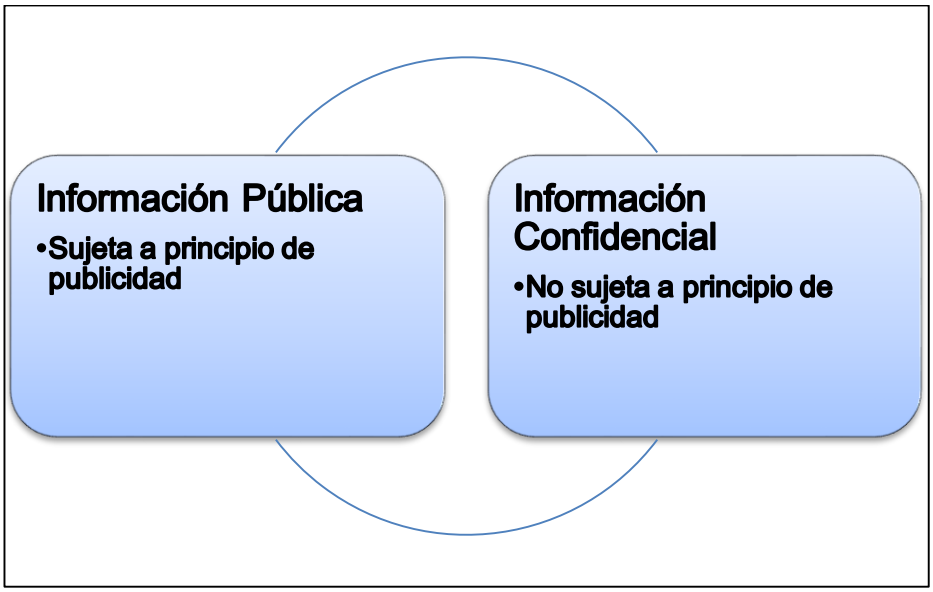


Figura 1-1: Ley de aplicación de la seguridad (Elaborado por los autores)

Con estos antecedentes, es de prioridad para las entidades del sector público implantar medidas para controlar los dominios de la seguridad de la información y atenderlos dentro de lo estipulado en la LOTAIP. El Esquema Gubernamental de Seguridad de la Información EGSI atiende este requerimiento del gobierno.

1.2. ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

1.2.1. MARCO LEGAL

1.2.1.1. Secretaría Nacional de la Administración Pública

La Secretaría Nacional de la Administración Pública (SNAP) tiene como misión "Mejorar la eficiencia de las instituciones del Estado Central a través de políticas y procesos que optimicen la calidad, la transparencia y la calidez del Servicio Público." [4]

Además, la SNAP impulsa proyectos de tecnologías de la información; y con este fin, creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, mismo que desarrollo el EGSI, elaborado en base a la norma NTE INEN-ISO/IEC 27002, expedidas por el Servicio Ecuatoriano de Normalización INEN.

1.2.1.2. Acuerdo Ministerial 166

Mediante el Acuerdo Ministerial 166, la SNAP dispone a las entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva, el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la información.

En el artículo 2 del acuerdo se indica que "La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información."[5]

1.2.1.3. Entidades que comprenden la Función Ejecutiva.

El Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva (ERJAFE), emitido mediante Decreto Ejecutivo 2428, publicado en el Registro Oficial No. 534 de 18 de marzo de 2002, establece:

"Para sus efectos la Función Ejecutiva comprende:

a) La Presidencia y la Vicepresidencia de la República y los órganos dependientes adscritos a ellas;
b) Los Ministerios de Estado y los órganos dependientes o adscritos a ellos;
c) Las personas jurídicas del sector público adscritas a la Presidencias de la República ; a la Vicepresidencia de la República o a los ministerios de estado;
d) Las personas jurídicas del sector público autónomas cuyos órganos de dirección estén integrados en la mitad o más por delegados o representantes de organismos, autoridades, funcionarios o servidores que integran la Administración Pública Central.

Los órganos comprendidos en los literales a) y b) conforman la *Administración Pública Central* y las personas jurídicas del sector público señaladas en los demás literales conforman la *Administración Pública Institucional* de la Funciona Ejecutiva."[6]

Esta organización gubernamental se describe en la Figura 1-2.

Este proyecto tomará en cuenta el ámbito de la Administración Pública Central con la finalidad de homogenizar el tipo de entidades a las que se encuentra dirigido. Esto debido a que las entidades de la Administración Pública Institucional difieren en gran medida en tamaño y en competencias, por lo que la generalización de esta guía se tornaría compleja y poco entendible.

1.2.2. CONTENIDO DEL EGSI

El EGSI establece un conjunto de directrices prioritarias para la gestión de la seguridad de la información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

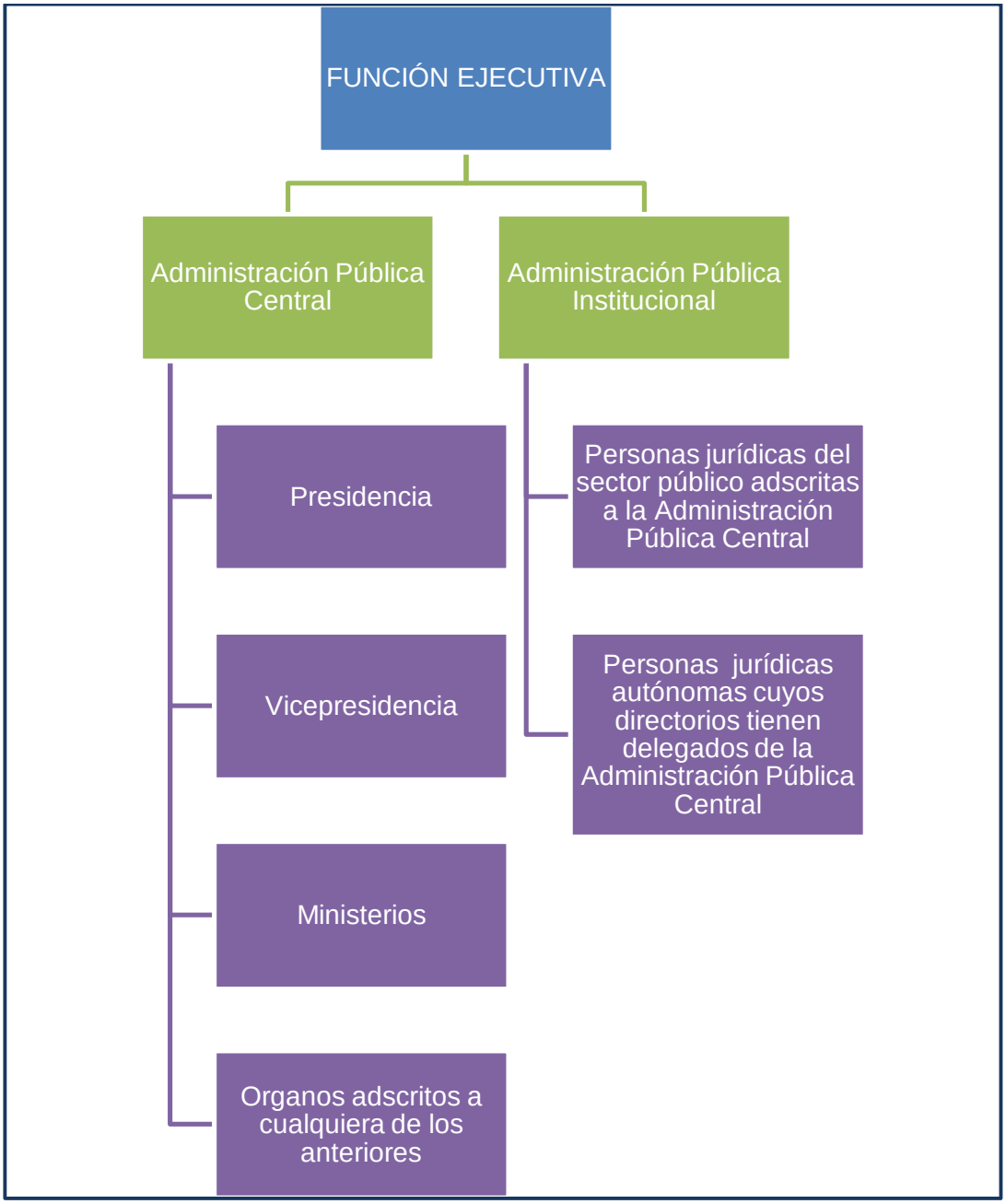


Figura 1-2: Ámbito de la Función Ejecutiva (Elaborado por los autores)

Su contenido es el siguiente: [5]

- Políticas de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de los Activos
- Seguridad de los Recursos Humanos
- Seguridad Física y del Entorno

- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de los Incidentes de la Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento

El EGSI está completamente basado en la norma ISO/IEC 27002 e implementa desde una perspectiva de gobierno los controles que en el estándar internacional se sugieren. Se definen más de 800 controles a lo largo de sus 11 capítulos, 125 de ellos son establecidos como prioritarios y solamente estos últimos serán objeto de este proyecto.

Para la determinación de los capítulos que deben ser abordados en este proyecto, se describen a continuación cada uno de ellos con una tipificación del ámbito en el que se aplican:

1.2.2.1. Política de seguridad de la información

Tipo: Gerencial.

Objetivos Principales:

- Emitir la política de seguridad de la información institucional.

Número total de ítems de control: 3

Números de ítems de control prioritarios: 2

1.2.2.2. Organización de la seguridad de la información

Tipo: Gerencial.

Objetivos Principales:

- Definir el Comité de Gestión de Seguridad de la Información institucional.
- Definir al Oficial de Seguridad.

- Definir al Responsable de Seguridad del área de TI.
- Definir el proceso de seguridad de la información.

Número total de ítems de control: 50

Números de ítems de control prioritarios: 10

1.2.2.3. Gestión de activos de información

Tipo: Administrativo y Gerencial.

Objetivos Principales:

- Inventariar los activos institucionales.
- Reglamentar el uso de correo electrónico, internet y video conferencia.
- Clasificar la información.

Número total de ítems de control: 47

Números de ítems de control prioritarios: 20

1.2.2.4. Seguridad de los recursos humanos

Tipo: Administrativo.

Objetivos Principales:

- Definición de aspectos sobre la seguridad de la información en el proceso de selección, reclutamiento, ingreso y salida de los funcionarios.

Número total de ítems de control: 25

Números de ítems de control prioritarios: 3

1.2.2.5. Seguridad física y del entorno

Tipo: Administrativo.

Objetivos Principales:

- Definición de aspectos sobre la seguridad de la información en el ambiente físico institucional.

Número total de ítems de control: 61

Números de ítems de control prioritarios: 12

1.2.2.6. Gestión de las comunicaciones y operaciones

Tipo: Tecnologías de la Información.

Objetivos Principales:

- Definición de aspectos sobre la seguridad de la información en las comunicaciones tecnológicas.

Número total de ítems de control: 173

Números de ítems de control prioritarios: 28

1.2.2.7. Control de accesos

Tipo: Tecnologías de la Información.

Objetivos Principales:

- Definición de aspectos sobre la seguridad de la información en los accesos a sistemas informáticos.

Número total de ítems de control: 105

Números de ítems de control prioritarios: 30

1.2.2.8. Adquisición, desarrollo y mantenimiento de sistemas de información

Tipo: Tecnologías de la Información.

Objetivos Principales:

- Definición de aspectos sobre la seguridad de la información para la adquisición, desarrollo y mantenimiento de sistemas informáticos.

Número total de ítems de control: 138

Números de ítems de control prioritarios: 2

1.2.2.9. Gestión de incidentes en la seguridad de la información

Tipo: Gerencial.

Objetivos Principales:

- Definición del procedimiento para la gestión de los incidentes de la seguridad de la información.

Número total de ítems de control: 20

Números de ítems de control prioritarios: 12

1.2.2.10. Gestión de continuidad del negocio

Tipo: Gerencial.

Objetivos Principales:

- Definición del plan de continuidad del negocio incluyendo aspectos de seguridad de la información.

Número total de ítems de control: 30

Números de ítems de control prioritarios: 0

1.2.2.11. Cumplimiento

Tipo: Gerencial.

Objetivos Principales:

- Revisión del cumplimiento de los controles de seguridad de la información.

Número total de ítems de control: 62

Números de ítems de control prioritarios: 0

Los capítulos 5. Seguridad física y del Entorno, 6. Gestión de comunicaciones y operaciones, 7. Control de acceso y 8. Adquisición, desarrollo y mantenimiento de sistemas de información, son los capítulos con mayor número de ítems de control, como se muestra en la Figura 1-3.

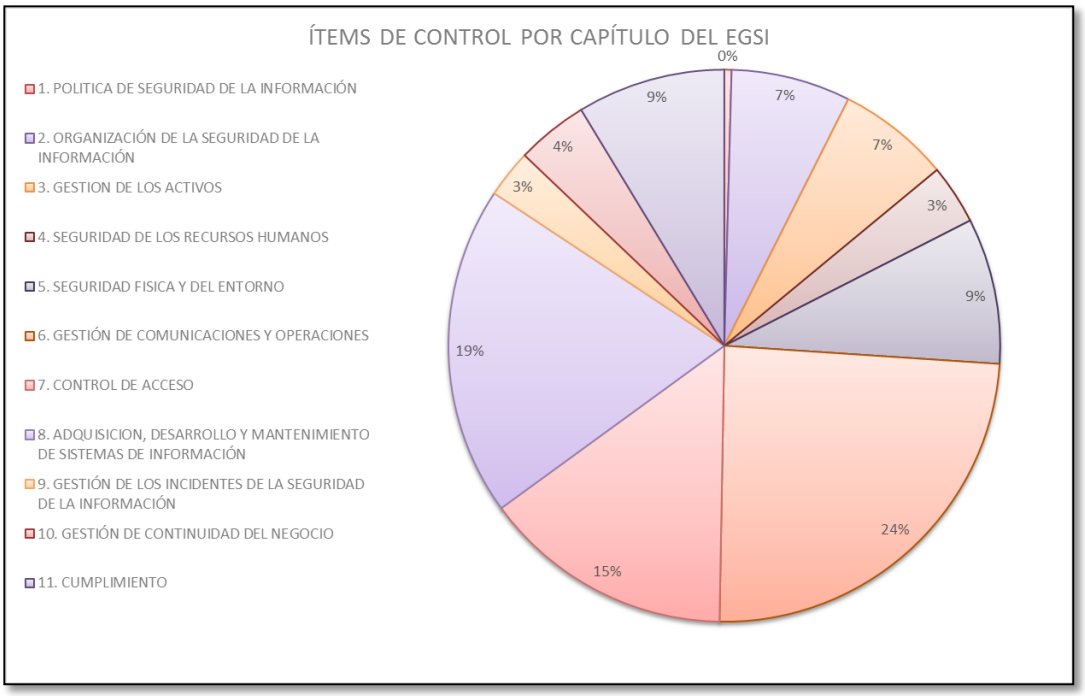


Figura 1-3: Porcentaje de ítems de control por capítulo de EGSI. (Elaborado por los autores)

Para el presente proyecto, se analizan los ítems de control priorizados, encontrando un total de 109 ítems prioritarios en EGSI, que se encuentran divididos por capítulo como se presenta en la Tabla 1-1.

CAPÍTULO	NÚMERO DE ITEMS DE CONTROL	NÚMERO DE ITEMS DE CONTROL PRIORITARIOS
1. POLITICA DE SEGURIDAD DE LA INFORMACIÓN	3	2
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50	10
3. GESTION DE LOS ACTIVOS	47	20
4. SEGURIDAD DE LOS RECURSOS HUMANOS	25	3
5. SEGURIDAD FISICA Y DEL ENTORNO	61	12
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	173	28
7. CONTROL DE ACCESO	105	30
8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	138	2
9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	20	2
10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO	30	0
11. CUMPLIMIENTO	62	0
Total	**714**	**109**

Tabla 1-1: Capítulos de EGSI con el número de ítems de control. (Elaborado por los autores)

Los capítulos 10. Gestión de Continuidad del Negocio y 11. Cumplimiento, no registran ítems de control prioritarios, por lo cual no se toman en cuenta en el desarrollo del proyecto.

De los capítulos tipificados como Tecnologías de la Información resultarán la mayoría de ítems para generar la guía, pero por motivos de validación se revisarán los ítems prioritarios del resto de capítulos, de forma que se tomen en cuenta correctamente los parámetros para la guía de implantación.

1.2.3. SEGUIMIENTO EN EL SISTEMA GOBIERNO POR RESULTADOS

El sistema Gobierno Por Resultados (GPR) del gobierno central sirve para registrar la ejecución de los planes estratégicos y operativos de las entidades del sector público, mismo que presenta indicadores a los niveles jerárquicos superiores para mejorar el seguimiento de los proyectos gubernamentales.

Por disposición transitoria del Acuerdo Ministerial 166 la SNAP crea, en el sistema GPR, un proyecto homogenizado para todas las instituciones que deben implantar EGSI, de modo que se reporte a través de dicho sistema los avances realizados.

En la Tabla 1-2 se muestran los datos generales del proyecto.

Datos Generales
Descripción
El presente proyecto tiene como objetivo implementar las directrices prioritarias establecidas en el esquema gubernamental de seguridad de la información (EGSI) conforme establece el Acuerdo Ministerial 166. El EGSI establece directrices prioritarias que han sido homologadas como hitos del proyecto cuyo plazo de ejecución es de 6 meses. La implementación del EGSI reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica, que procesa la institución. Así mismo, contribuirá a establecer un proceso de mejora continua de la gestión de la seguridad de la información e incrementar la cultura de los servidores públicos en cuanto al manejo de la información que utilizan para cumplir sus funciones sea institucional o de la ciudadanía.
Beneficios Cualitativos
- Identificar, cuantificar y priorizar los amenazas, riesgos y vulnerabilidades que puedan afectar la seguridad de la información de la entidad. - Proporcionar a autoridades de las entidades soporte para gestión de la seguridad de la información, en concordancia con la constitución, las leyes y demás normativa legal vigente. - Contar con estructuras de evaluación y gestión de riesgos de la organización, así como la definición de las responsabilidades individuales de cada miembro a nivel de seguridad con los respectivos acuerdos de confidencialidad. - Aplicar los estándares internacionales (ISO/IEC 27000) adoptados como normas técnicas ecuatorianas para gestión de la seguridad de la información. - Incrementar el conocimiento y cultura de los servidores públicos en cuanto a la gestión de la seguridad de la información que utilizan.

- Implementar medidas para evitar problemas y consecuencias no deseadas de una gestión no adecuada de la gestión de la seguridad de la información. - Compartir información y gestionar incidentes de seguridad de la información afecten a la entidad o al gobierno en su conjunto en coordinación con la SNAP.
Tipo de Beneficiario
- Entidades - Funcionarios/servidores públicas - Gobierno - Ciudadanía

Tabla 1-2: Datos generales del Proyecto EGSI en el GPR (Tomado del sistema GPR)

Para la ejecución del proyecto, se registran en GPR 126 hitos que abarcan los ítems de control registrados como prioritarios en el Acuerdo Ministerial 166.

El objetivo de que EGSI sea registrado como un proyecto en GPR es el de reportar los avances que se alcancen sobre cada uno de los hitos y el respectivo cumplimiento a la normativa dispuesta.

1.3. DETERMINACIÓN DE LOS ÍTEMS DE COMPETENCIA DE TI EN EL EGSI

Dentro del alcance del presente proyecto, se desarrollan las políticas y/o procedimientos solamente de los ítems de control definidos como *prioritarios* por la SNAP en el Acuerdo Ministerial 166, y que su ámbito de aplicación corresponda a Tecnologías de la Información TI.

En la Tabla 1-3, se detallan los 109 hitos prioritarios de EGSI de la siguiente manera:

- Hito GPR: Número del hito con el cual se ha definido el ítem de control en el sistema GPR.
- Capítulo: Nombre del capítulo del Acuerdo Ministerial 166 al que corresponde el ítem de control.

- Título: Nombre del título del Acuerdo Ministerial 166 al que corresponde el ítem de control.
- Ítem: Descripción del ítem de control del Acuerdo Ministerial 166.
- Ítem es competencia de TI (SI / No): se define al ítem de control como responsabilidad del área de Tecnologías de la Información debido al ámbito de aplicación del ítem; basado en la misión, atribuciones, productos y servicios de la Dirección de Tecnologías de la Información del Manual de Creación de la Coordinación General de Gestión Estratégica emitido por la SNAP en el año 2012. [18]

Hito GPR	CAPÍTULO	TÍTULO	ÍTEM	ÍTEM ES COMPETENCIA DE TI
1	1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	1.1. Documento de la Política de la Seguridad de la Información	a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad.	NO
2			b) Se difundirá la siguiente política de seguridad de la información como referencia: "Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el EGSI para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera". Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.	NO
3		1.2 Revisión de la Política	a) Para garantizar la vigencia de la política de seguridad de la información en la institución, ésta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológica, económico, entre otros.	NO
4	2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 Compromiso de la máxima autoridad de la institución con la Seguridad de la Información	a) Realizar el seguimiento de la puesta en marcha de las normas de este documento.	NO
5			b) Disponer la difusión, capacitación y sensibilización del contenido de este documento.	NO
6			c) Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución (CSI) y designar a los integrantes. El CSI involucrará la participación y cooperación de los cargos directivos de la institución. El comité deberá convocarse de forma periódica o cuando las circunstancias lo ameriten. Se deberán llevar registros y actas de las reuniones.	NO
7, 8		2.2 Coordinación de la Gestión de la Seguridad de la Información	a) La coordinación estará a cargo del Comité de Gestión de Seguridad de la Información el cual tendrá las siguientes funciones: - Designar formalmente a un funcionario como Oficial de Seguridad de la Información, quien actuará como coordinador del CSI. El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará a la máxima autoridad de la institución. - Designar formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el director o responsable del área de Tecnologías de la Información de la Institución.	NO
9		2.5. Acuerdos sobre Confidencialidad	a) Elaborar y aprobar los acuerdos de confidencialidad y de no divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información y el EGSI.	NO
10			b) Controlar con los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución, sin excepción.	NO

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
11	2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.5. Acuerdos sobre Confidencialidad	c) Gestionar la custodia de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción	NO
12			d) Controlar la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionario a la institución, sin excepción	NO
13			e) Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas, proveedores, pasantes, entre otros), que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de información.	NO
14, 15, 16, 17, 18, 19,20, 21	3. GESTIÓN DE LOS ACTIVOS	3.1 Inventario de Activos	Inventariar los activos de hardware: j) Equipos móviles: teléfono inteligente (Smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc. k) Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc. l) Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc. m) Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina fax, etc. n) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc. o) Periféricos de comunicaciones: Tarjeta USB para redes inalámbricas (Wi-Fi, bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbrica (Wi-Fi, bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc. p) Tableros: de transferencia (bypass), de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc. q) Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.	NO

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
22, 23, 24 25	**3. GESTIÓN DE LOS ACTIVOS**	**3.1 Inventario de Activos**	Inventariar los activos de soporte Software: r) Sistemas Operativos s) Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc. u) Aplicativos informáticos del negocio t) Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, video conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.	NO
26, 27, 28, 29	**3. GESTIÓN DE LOS ACTIVOS**	**3.1 Inventario de Activos**	Inventariar los activos de soporte de redes: v) Cables de comunicaciones (interfaces: RJ-45 oRJ-11, SC, ST o MT-RJ, interfaz V35, RS232,USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc. w) Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.) x) Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc. y) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.	NO

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
30	**3. GESTIÓN DE LOS ACTIVOS**	**3.3 Uso aceptable de los activos**	d) Reglamentar el uso de correo electrónico institucional: - Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin. - Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte. - Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución. - Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario. - La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo. - Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios. - Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error. - Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución. - Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria. - Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos. - Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.	SI

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
31	**3. GESTIÓN DE LOS ACTIVOS**	**3.3 Uso aceptable de los activos**	e) Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios: - Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin. - Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución. - Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral. - El Oficial de Seguridad de la Información debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas. - Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución. - El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad. - La institución podrá en cualquier momento bloquear o limitar el acceso y uso del internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico. - Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo!, Facebook, entre otros. - Se prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.	SI

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
32	3. GESTION DE LOS ACTIVOS	3.3 Uso aceptable de los activos	f) Reglamentar el uso de los sistemas de Vídeo-Conferencia: - Definir un responsable para administrar la vídeo-conferencia. - Definir y documentar el procedimiento de acceso a los ambientes de pruebas y producción. - Elaborar un documento tipo "lista de chequeo" (check-list) que contenga los parámetros de seguridad para el acceso a la red interministerial que soporta el servicio de video-conferencia. - Crear contraseña para el ingreso a la configuración de los equipos y para las salas virtuales de video-conferencia. - Deshabilitar la respuesta automática de los equipos de video-conferencia.	SI
33		3.4 Directrices de clasificación de la información	a) Clasificar la información como pública o confidencial.	NO
34	4. SEGURIDAD DE LOS RECURSOS HUMANOS	4.1 Funciones y responsabilidades	a) Verificar a los candidatos, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida.	NO
35			b) Entregar formalmente a los funcionarios sus funciones y responsabilidades.	NO
36		4.4 Responsabilidades de la dirección a cargo del funcionario	a) Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles.	NO
37	5. SEGURIDAD FÍSICA Y DEL ENTORNO	5.1 Perímetro de la seguridad física	b) Definir un área de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio.	NO
38		5.2 Controles de acceso físico	a) Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida.	NO
39			c) Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas.	NO
40		5.3 Seguridad de oficinas, recintos e instalaciones	b) Proteger las instalaciones claves de tal manera que se evite el acceso al público.	NO
41			d) Ubicar las impresoras, copiadoras, etc., en un área protegida.	NO

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
42		**5.4 Protección contra amenazas externas y ambientales.**	d) Realizar mantenimiento de las instalaciones eléctricas y UPS.	NO
43			e) Realizar mantenimientos en los sistemas de climatización y ductos de ventilación.	NO
44		**5.5 Trabajo en áreas seguras**	d) No permitir equipos de grabación, cámaras, equipos de video y audio, dispositivos móviles, etc., a menos de que estén autorizados.	NO
45		**5.6 Áreas de carga, despacho y acceso público**	a) Permitir el acceso al área de despacho y carga, únicamente al personal identificado y autorizado.	NO
46		**5.7 Ubicación y protección de los equipos**	c) Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información.	NO
47		**5.8 Servicios de suministro**	c) Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la institución.	NO
48		**5.9 Seguridad del Cableado**	e) Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales/remotas), voz, eléctricas polarizadas, etc.	NO
49	**6. GESTIÓN DE COMUNICACIONES Y OPERACIONES**	**6.1. Documentación de los procedimientos de Operación**	e) Documentar los contactos de soporte, necesarios en caso de incidentes.	SI
73		**6.6. Monitoreo y revisión de los servicios, por terceros**	b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos.	SI
74			c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos.	SI
75			d) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.	SI

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
76		**6.8. Gestión de la capacidad**	a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.	SI
50		**6.10. Controles contra código malicioso**	a) Prohibir el uso de software no autorizado por la institución. Elaborar un listado de software autorizado.	SI
51			c) Instalar y actualizar periódicamente software de antivirus contra código malicioso.	SI
52			d) Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.	SI
53		**6.12. Respaldo de la información**	a) Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.	SI
54			b) Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención.	SI
55			c) Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución.	SI
56		**6.14. Seguridad de los servicios de la red**	a) Incorporar tecnología para la seguridad de los servicios de red como autenticación, encriptación y controles de conexión de red.	SI
57			b) Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.	SI
58		**6.26. Registros de auditorías**	h) Registrar los accesos y tipos de acceso.	SI
59			i) Registrar las direcciones y protocolos de red.	SI
60			j) Definir alarmas originadas por el sistema de control de acceso.	SI
61			k) Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS).	SI
62		**6.27. Monitoreo del uso del sistema**	a) Registrar los accesos autorizados incluyendo: identificación del ID de usuario, fecha y hora de eventos clave, tipos de evento, archivos a los que se han tenido acceso, programas y utilitarios utilizados.	SI
63			b) Monitorear las operaciones privilegiadas como: uso de cuentas privilegiadas.	SI
64			c) Monitorear intentos de acceso no autorizados, como: Acciones de usuario fallidos o rechazadas, Violación de la política de acceso y notificaciones de firewalls y gateways; Alertas de los sistemas de detección de intrusos.	SI
65			d) Revisar alertas o fallas del sistema, como: alertas y/o mensajes de consola, excepciones de registro del sistema, alarmas de gestión de red, alarmas del sistema de control de acceso.	SI

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
66		**6.29. Registros del administrador y del operador**	a) Incluir el registro, la hora en la que ocurrió el evento.	SI
67			b) Incluir al registro la información sobre el evento.	SI
68			c) Incluir al registro a la cuenta de administrador y operador que estuvo involucrado.	SI
69			d) Añadir al registro los procesos que estuvieron implicados.	SI
70		**6.30. Registro de fallas**	a) Revisar los registros de fallas o errores del sistema.	SI
71			b) Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles.	SI
72			c) Asegurar que el registro de fallas esté habilitado.	SI
100	**7. CONTROL DE ACCESO**	**7.4. Gestión de contraseñas para usuarios**	a) Establecer un proceso formal para la asignación y cambio de contraseñas.	SI
101		**7.6. Uso de contraseñas**	a) Documentar en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignadas.	SI
102			b) Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir que cumplen una complejidad media y alta.	SI
103			c) Evitar contraseñas en blanco o que vienen por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables: por ejemplo, admin, administrador, user, usuario, entre otros.	SI
104			d) Controlar el cambio periódico de contraseñas de usuarios.	SI
105			e) Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.	SI
106		**7.7. Equipos de usuarios desatendido**	a) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, éste se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.	SI
107		**7.8. Política de puesto de trabajo despejado y pantalla limpia**	b) Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.	NO
108			c) Desconectar de la red, servicio o sistema, los computadores personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.	SI
109			e) Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas.	SI
110			f) Retirar información sensible una vez que ha sido impresa.	NO
111			g) Retirar información sensible, como las claves, de sus escritorios y pantallas.	NO
112			h) Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.	NO

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
77		**7.10. Autenticación de usuarios para conexiones externas**	a) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR).	SI
78		**7.11. Identificación de los equipos en las redes**	a) Identificar y documentar los equipos que se encuentran en las redes.	SI
79		**7.12. Protección de los puertos de configuración y diagnóstico remoto**	b) Los puertos, servicios (Ej. Ftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.	SI
80		**7.13. Separación en las redes**	a) Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución.	SI
81		**7.15. Control del enrutamiento en la red**	a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.	SI
82		**7.16. Procedimiento de registro de inicio seguro**	a) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución que deberá estar documentada, definida y socializada.	SI
83			b) Llevar un registro de definición para el uso de privilegios especiales del sistema.	SI
84			c) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.	SI
85			d) Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de accesos y directorios.	SI
86			e) Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución.	SI
87			f) Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente.	SI
88			i) Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos.	SI
89			j) Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica.	SI

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
90		7.17. Identificación y autenticación de usuarios	a) Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución.	SI
91			b) Usar como excepción y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado.	SI
92			d) Evitar el uso de usuarios genéricos.	SI
93			e) Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación.	SI
94		7.18. Sistema de gestión de contraseñas	a) Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible.	SI
95			b) Controlar el cambio de contraseña de los usuarios y del personal de tecnología, y de los administradores de tecnología en rangos de tiempo y complejidad.	SI
96			c) Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión.	SI
97		7.25. Computación y comunicaciones móviles	a) Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo.	SI
98		7.26. Trabajo remoto	d) No se permite el uso de equipo de propiedad privada que no esté bajo control y monitoreo de la institución.	SI
99			f) Deberá considerarse la protección de antivirus y reglas del firewall.	SI
113	8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	8.1. Análisis y especificaciones de los requerimientos de seguridad	a) Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones.	SI
114			b) Definir los controles apropiados, tanto automatizados como manuales. En esta definición, deben participar personal de requerimiento funcional y personal técnico que trabajarán en el sistema. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y el daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.	SI
115	9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	9.1. Reporte sobre los eventos de seguridad de la información	a) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidentes, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.	SI

Hito GPR	CAPÍTULO	TÍTULO	ITEM	ITEM ES COMPETENCIA DE TI
116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126	9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	9.1. Reporte sobre los eventos de seguridad de la información	c) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden: - Identificar el incidente. - Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente. - Notificar al Oficial de Seguridad de la Información de la institución. - Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad. - Asignar una prioridad de atención al incidente en el caso de que se produjeran varios de forma simultánea. - Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas. - Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado. - Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente. - Resolver y restaurar el servicio afectado por el incidente debido a la par de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes. - Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o sistema de que el incidente ha sido resuelto.	SI

Tabla 1-3: Listado de ítems de control prioritarios de EGSI. (Elaborado por los autores)

Del listado anterior, se desprenden algunas consideraciones que se deben tomar en cuenta en el desarrollo del proyecto:

- Los hitos del 7 al 8, 14 al 29 y del 116 al 126 constan en el EGSI en un solo ítem de control respectivamente, pero en el proyecto GPR fueron desagregados en varios hitos. Es importante destacar esta desagregación para corroborar la inclusión de todos los ítems de control y para reportar correctamente el cumplimiento de los hitos en el sistema GPR.
- De los 109 ítems de control registrados como prioritarios en EGSI, 67 ítems son competencia del área de TI de cualquier institución pública donde se implante la norma. Se encontraron algunos ítems de control que se pueden incluir en la guía a pesar de no constar en un capítulo tipificado como Tecnologías de la Información, pero por su contenido no se tomaron en cuenta ya que influyen en el alcance de otros ítems de control.

Como resultado de este análisis, se determina que los capítulos 1, 2, 3 , 4 y 5 del EGSI no son competencia de TI, a excepción de los hitos 30, 31 y 32 del capítulo 3, que serán considerados en la Política General de Seguridad de la Información como controles adicionales.

Para el presente proyecto se elaborarán los procedimientos de aquellos controles que son de competencia de TI de los capítulos 6, 7, 8, y 9 del EGSI.

1.4. METODOLOGÍA PARA LA ELABORACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se expone un análisis de dos metodologías para la elaboración de políticas de seguridad de la información:

1.4.1. METODOLOGÍA DE LA UNIVERSIDAD NACIONAL DE COLOMBIA [7]

1.4.1.1. Definiciones

Política: Una política se define como una “Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas

se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de las reglas y criterios más específicos que aborden situaciones concretas" [7]. Con esta definición queda claro que la política es la base de cualquier otro instrumento que se pueda presentar para la implantación de normas de seguridad de la información.

Procedimiento: "Los procedimientos definen específicamente cómo las políticas serán implementadas en una situación dada. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico" [7]. Por lo que los procedimientos entonces describen claramente el cómo se debe aplicar una política y son la base para implantar la seguridad de la información.

1.4.1.2. Etapas en el Desarrollo de una Política.

Para la definición de una política institucional, en la metodología escogida existen 11 etapas agrupadas en 4 fases, como se describe en la Figura 1-4.

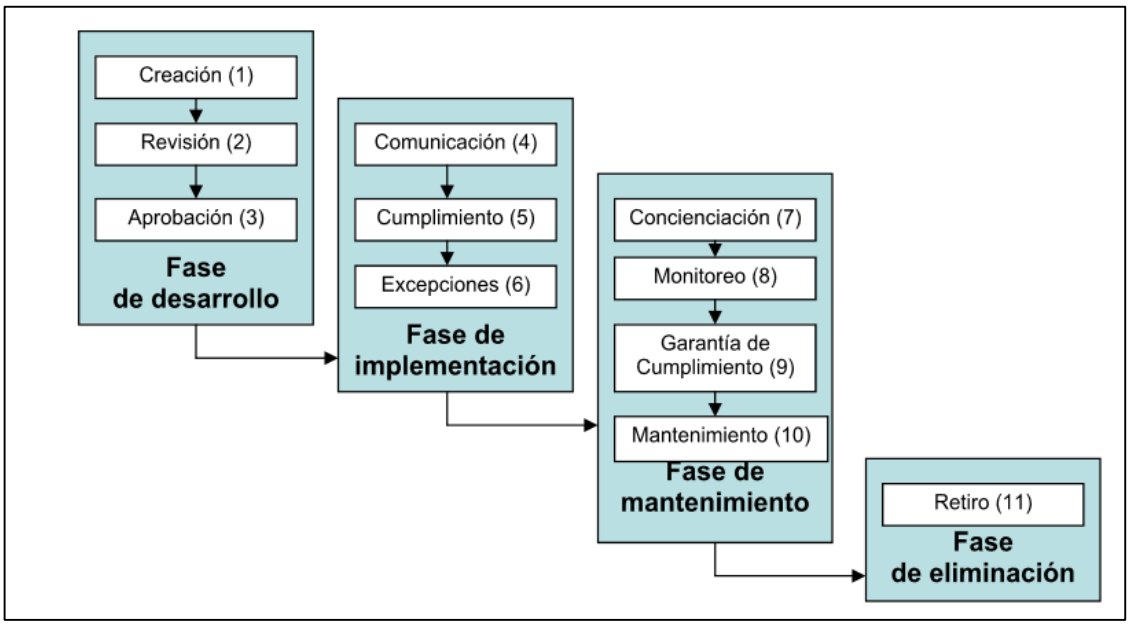


Figura 1-4: Etapas en el desarrollo de una Política [7]

- Fase de desarrollo: durante esta fase la política es creada, revisada y aprobada.
- Fase de implementación: en esta fase la política es comunicada y acatada (o no cumplida.

- Fase de mantenimiento: los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).
- Fase de eliminación: La política se retira cuando no se requiera más. [7]

1.4.1.3. Etapa de Creación

La creación de la política se realiza a través de la planificación, investigación, documentación y coordinación de la política, tal como se indica en la metodología; con los siguientes puntos:

- Necesidad de la política,
- Alcance,
- Aplicabilidad,
- Roles,
- Responsabilidades, y,
- Factibilidad.

1.4.1.4. Etapa de Revisión

Toda política debe ser revisada por el grupo involucrado en la implementación de la misma, de manera que se realice una validación independiente de las directrices desde una perspectiva distinta; así mismo, se puede conseguir mayor apoyo institucional mientras más áreas se encuentren involucradas en el proceso de elaboración. La retroalimentación es clave para el obtener una versión final de la política.

1.4.1.5. Etapa de Aprobación

En función del compromiso institucional con la implementación de las políticas, esta etapa puede involucrar un tiempo mínimo ya que solo se requiere la aprobación de una posición jerárquica de autoridad.

1.4.1.6. Etapa de Comunicación

Toda política debe ser siempre difundida en primera instancia a los miembros de la institución que son responsable del cumplimiento de los controles. Luego de una correcta difusión y capacitación, se puede iniciar el proceso de comunicación a todo el personal, con una correcta planificación y tomando en cuenta ubicación geográfica, idioma, cultura, etc.

1.4.1.7. Etapa de Cumplimiento

En esta etapa, se inicia la ejecución efectiva de la política. Se requiere trabajar con el personal para interpretar la mejor manera de implementar la política en las diversas situaciones actuales de la empresa. Se requiere medir el impacto de la implementación mediante informes del estado que se generen dentro de periodos regulares. De abstenerse de verificar el empuje inicial de la difusión, es posible que la política se pierda con el tiempo.

1.4.1.8. Etapa de Excepciones

Cómo es esperado, se presentan áreas o personal que por distintos motivos no pueden implementar ciertos controles. Estos casos deben ser debidamente documentados de manera que sean tomados en cuenta para un futuro proceso de actualización de las políticas.

1.4.1.9. Etapa de Concienciación

Se basa en la continuidad de la etapa de comunicación, mediante esfuerzos continuos de debe garantizar que el personal está consciente de lo que se requiere en términos de acciones de su parte para el acatamiento de la política y busca cumplir los controles especificados al ejecutar sus actividades.

1.4.1.10. Etapa de Monitoreo

Esta etapa se encuentra basada en la observación del personal y no requiere procesos formales, de modo que se compruebe deficiencias durante la ejecución.

1.4.1.11. Etapa de Garantía de Cumplimiento

Otro mecanismo de asegurar el cumplimiento son las sanciones que se prevean como resultado de las contravenciones a la política con el fin de prevenir que no ocurran. Cada contravención debe generar y aplicar la respectiva acción correctiva ya sea al proceso, a la tecnología o a las personas.

1.4.1.12. Etapa de Mantenimiento

De manera que el ciclo de vida de la política se mantenga con el tiempo, se debe hacer seguimiento a las tendencias de cambios que puedan afectar los controles de la política.

1.4.1.13. Etapa de Retiro

Transcurrido el tiempo, es posible que la política no sea requerida. Entonces, ésta debe ser retirada, archivada como referencia, y documentadas las causas del retiro.

1.4.2. METODOLOGÍA DEL INSTITUTO SANS

El instituto SANS es una empresa privada de los Estados Unidos, especializada en seguridad de la información y en entrenamiento en este ámbito.

El documento “Information Security Policy - A Development Guide for Large and Small Companies” [13] detalla los elementos que se deben tomar en cuenta al desarrollar y mantener Políticas de Seguridad de la Información y presenta un diseño que contempla varios documentos para las políticas con el proceso de desarrollo que las acompaña.

1.4.2.1. Tipos de Políticas

Esta metodología define tipos de políticas de acuerdo a la jerarquía de los documentos que se requiere generar en la institución. A continuación, se presenta una figura que ilustra los tipos de políticas de un proceso altamente desarrollado y maduro, alineado con una empresa de tamaño grande, y de preferencia con desarrollo de políticas institucionales de varios años.

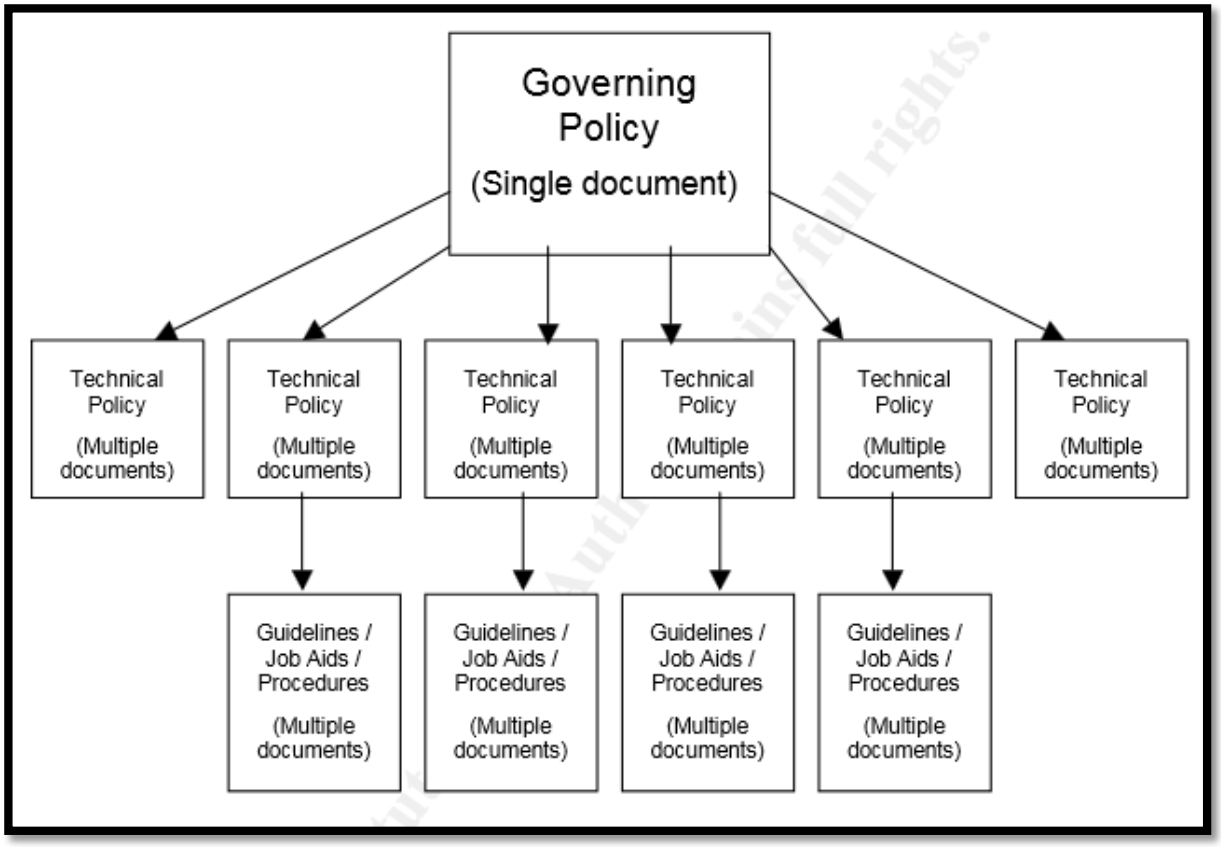


Figura 1-5: Jerarquización de los tipos de Políticas [13]

- Políticas Gobernante: Éste tipo de políticas contempla el QUÉ en relación a la seguridad de la información. “Abarca los conceptos de seguridad de información en un nivel alto, define cada uno de estos conceptos, describe por qué son importantes, y detalla que parte de la compañía se involucra en ellos.” [13].

  Las políticas de gobierno se desarrollan en un único documento que será soportado por una o varias políticas técnicas. Un ejemplo claro de la diferencia entre políticas de gobierno y técnicas puede ser el de las Políticas de Contraseñas. En una compañía de gran tamaño, se puede requerir una política general al respecto sobre la complejidad y uso de la contraseña, y adicionalmente políticas técnicas por cada sistema informático con las particularidades que se necesiten. Por otro lado, en una empresa pequeña con un número menor de sistemas informáticos puede ser suficiente un solo

documento de políticas técnicas al respecto, sin existir la necesidad de generar políticas gobernantes.

- Políticas Técnicas: Estas políticas contemplan el QUÉ (con mayor detalle), QUIÉN, CUÁNDO y DÓNDE en términos de seguridad de la información. Contienen mayor detalle que las anteriores y servirán para los responsables de implementar controles respecto a la Seguridad de la Información. Generalmente versan sobre un sistema o ítem específico, con una descripción de qué se debe hacer pero sin incluir el cómo hacerlo.

- Directrices: Estos documentos dan instrucciones paso a paso de CÓMO llevar a cabo los controles de seguridad de la información, y no es obligatoria su elaboración por cada una de las políticas de gobierno o técnicas emitidas. En el caso de que para la aplicación de cada política se vea necesario recurrir necesariamente a la respectiva directriz, probablemente la política no fue definida de la manera más clara posible y genere confusión. Es una buena práctica revisar el entendimiento de las políticas antes de generar las directrices.

  Una ventaja considerable de la generación de directrices es que también sirven como respaldo de las actividades del personal operativo, permitiendo mantener una base de conocimiento a través del tiempo.

1.4.2.2. Capítulos a Desarrollar en las Políticas

Los temas o capítulos que deben ser abordados en las políticas se priorizan y son tomados en cuenta a través de algunos parámetros; uno de los más importantes es aquellos controles obligatorios por leyes locales, y en segundo lugar se debe observar la información que es crítica para la toma de las decisiones de la institución.

Luego de la priorización, se sugiere dividir los capítulos por subtemas, ya sea por sistema, aplicación o tecnología. De esa forma, es posible definir los capítulos de la política de gobierno y de las políticas técnicas. En la figura 1-6, se muestra un ejemplo de la jerarquía que ocupan estas categorías.

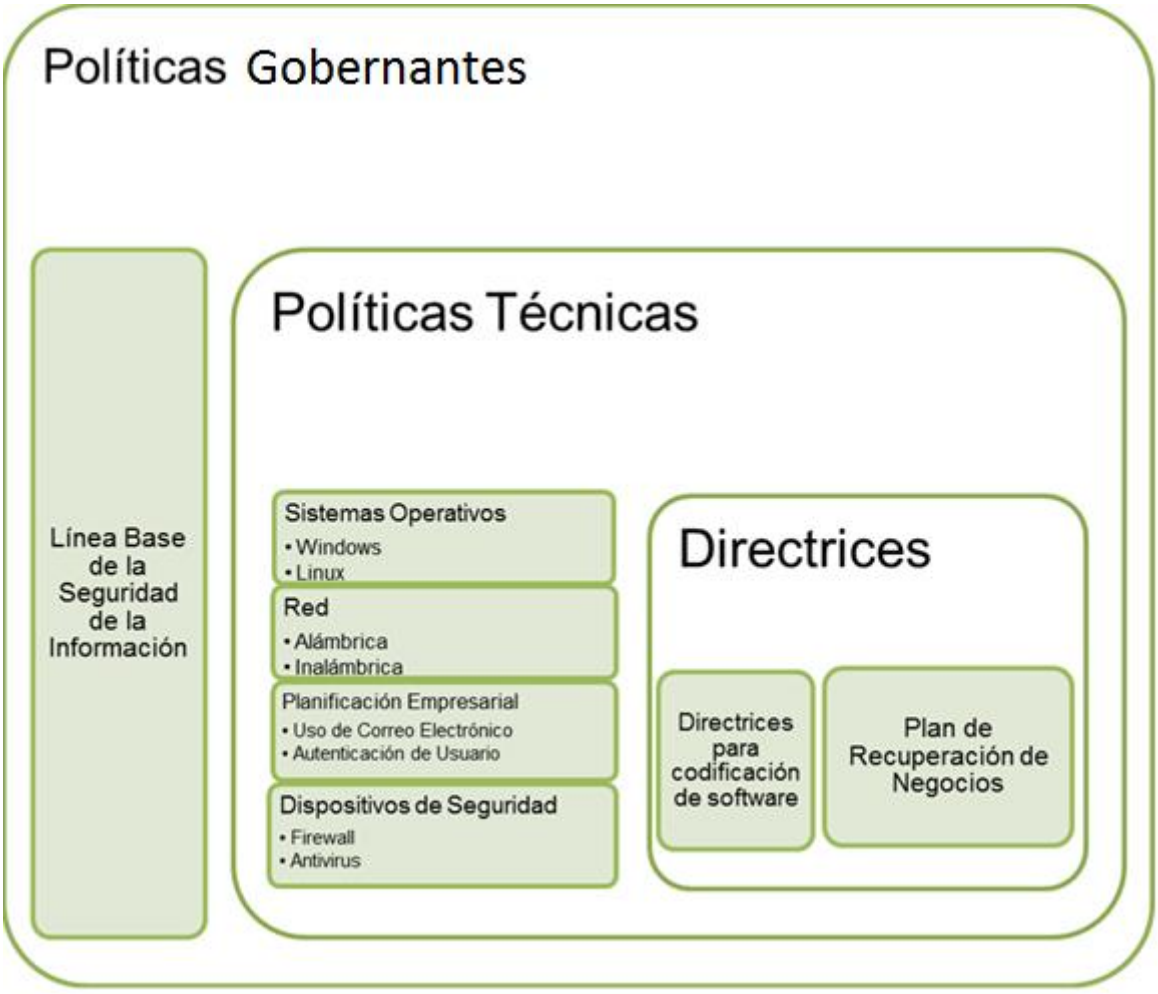


Figura 1-6: Ejemplo de agrupación de capítulos de los distintos tipos de políticas. (Elaborado por los autores)

1.4.2.3. Proceso de Desarrollo de las Políticas

El objetivo principal de la elaboración de las políticas de seguridad de la información es elevar el nivel de madurez de empresa, siendo recomendable que al iniciar la implementación de las mismas no se busque alcanzar un elevado nivel de madurez

sino más bien políticas generales que permitan al equipo adquirir experiencia sobre seguridad de la información. Los procesos iterativos son primordiales en este tipo de proyectos.

Incrementar el nivel de madurez incluye conducir procesos de capacitación y educación, sensibilización y comunicación, para finalmente modificar la cultura empresarial e impulsar los cambios en toda la empresa.

Los enfoques para desarrollar las políticas pueden ser “Top-Down” o “Bottom-Up”. A continuación, en las figuras se muestran los parámetros o entradas de información que se pueden utilizar en cada enfoque.

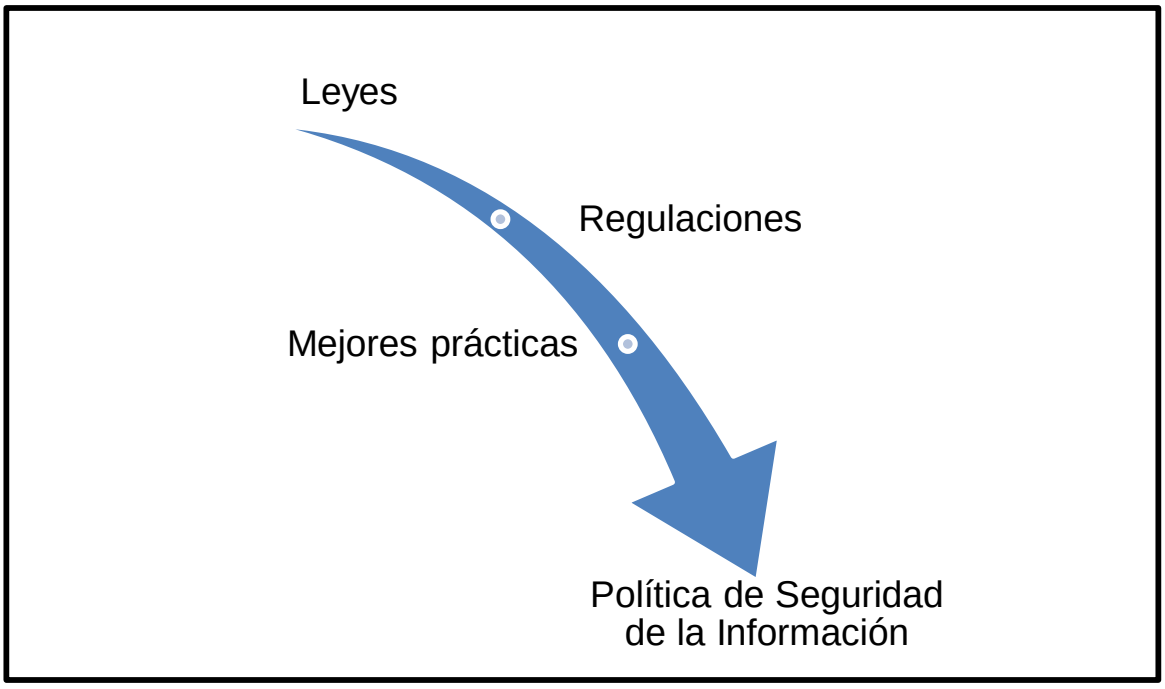


Figura 1-7: Enfoque Top-Down para la elaboración de políticas. (Elaborado por los autores)

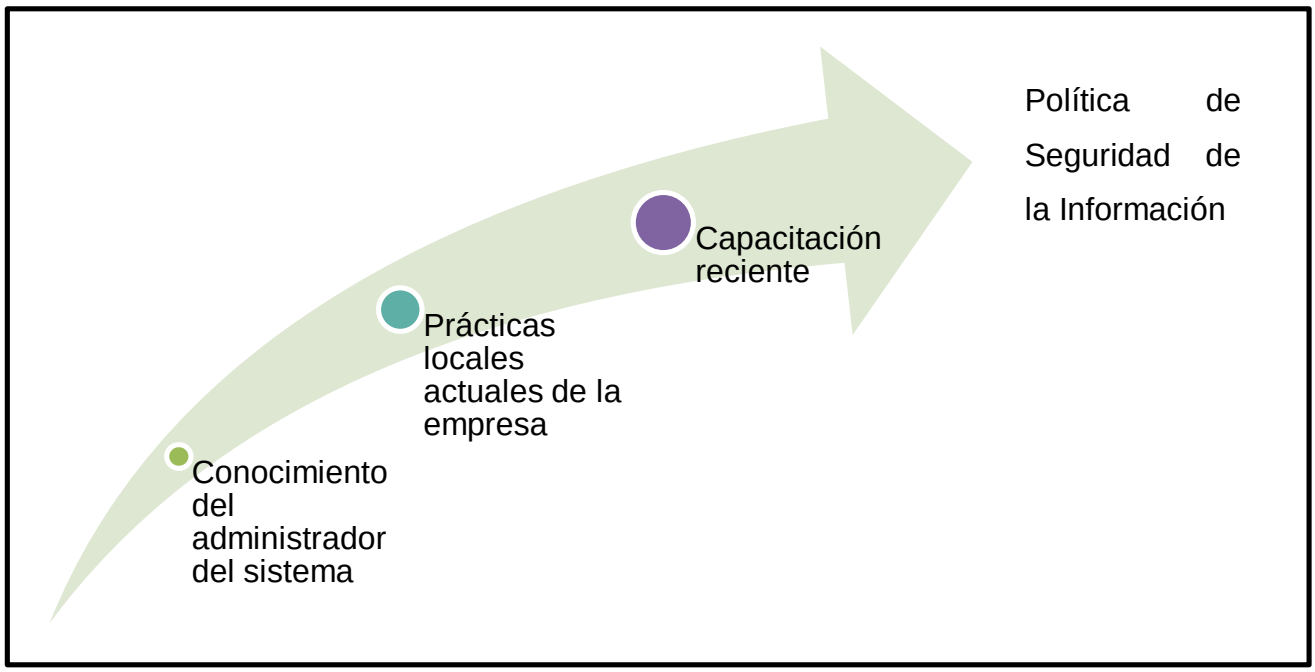


Figura 1-8: Enfoque Bottom-Up para la elaboración de políticas. (Elaborado por los autores)

Se deben analizar las desventajas de cada enfoque. En el enfoque "Top-Down", el resultado de las políticas podría ser poco realista y un tanto lejano a la realidad de la empresa. En cambio, en el enfoque "Bottom-Up" puede resultar una política demasiado específica a cierta área o entorno. Con estas consideraciones, se recomienda el empleo de un enfoque combinado de manera de obtener el mejor resultado posible.

Además de las entradas de información para la elaboración de políticas, se debe tomar en cuenta cuál es la práctica actual y compararla con el futuro que se desea alcanzar. Las políticas no solamente deben incluir prácticas actuales, sino buscar metas obtenibles dentro de la empresa.

1.4.2.4. Equipo de Desarrollo de las Políticas

En las etapas tempranas del desarrollo de las políticas, se debe involucrar un equipo de trabajo multidisciplinario que puede variar a lo largo de la elaboración de las políticas. En la siguiente figura, se describen los grupos primarios y secundarios del proyecto.

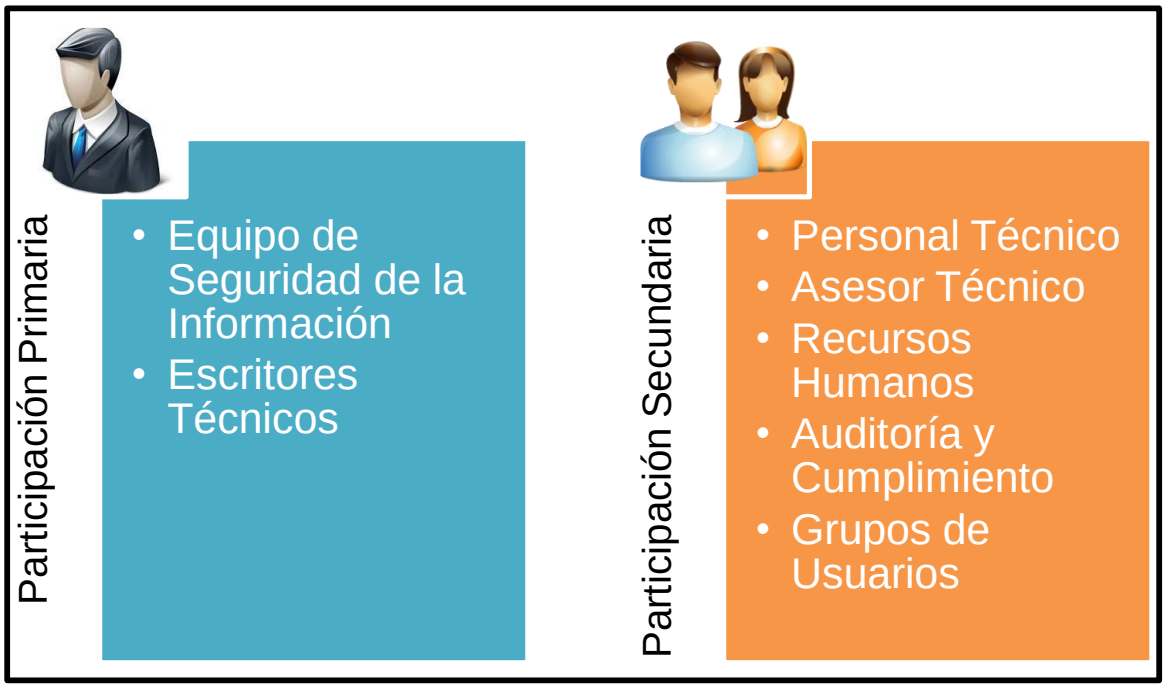


Figura 1-9: Grupos o individuos involucrados con la Política (Elaborado por los autores)

1.4.2.5. Ciclo de Vida del Desarrollo de las Políticas

Una vez definido el equipo que elaborará las políticas de seguridad de la información, se debe iniciar el proceso de desarrollo con el siguiente ciclo de vida que se ilustra en la figura 1-10:

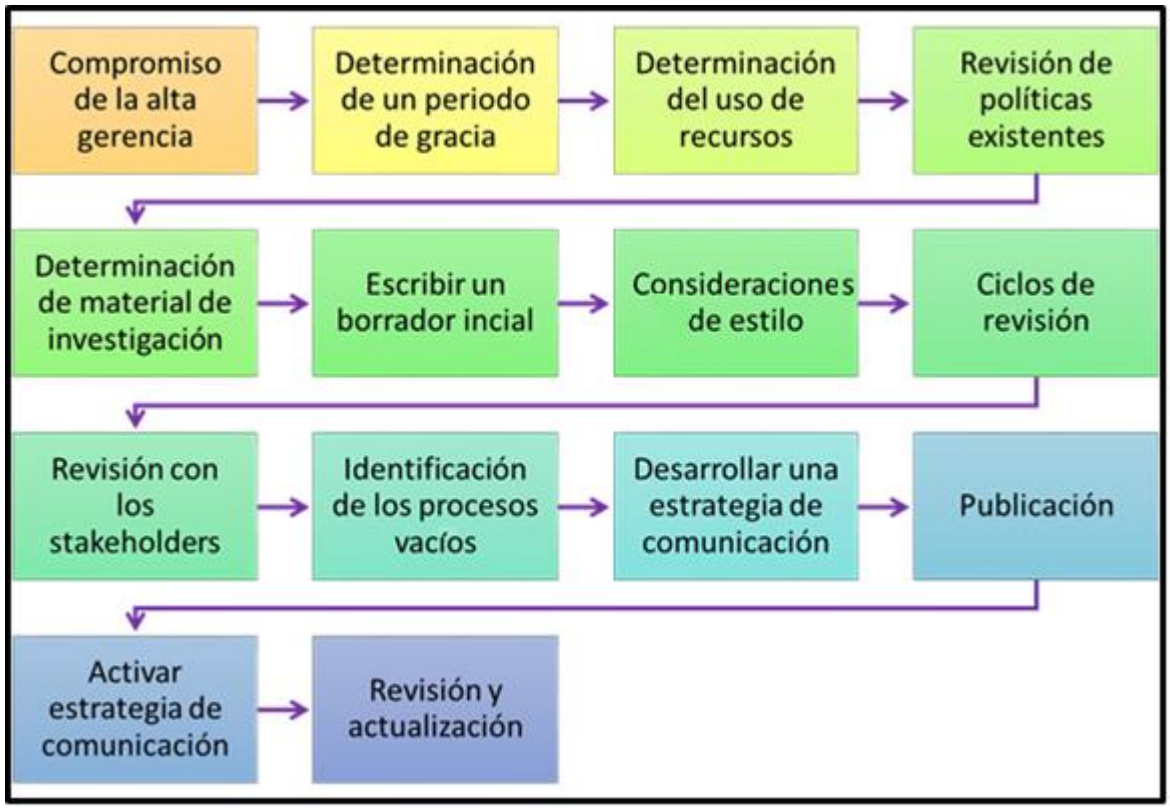


Figura 1-10: Fases del ciclo de vida para la elaboración de las políticas (Elaborado por los autores)

- Compromiso de la alta gerencia: Comprometer al personal directivo con la elaboración de las políticas.
- Determinar un período de gracia: Para la conformidad de los usuarios responsables del cumplimiento de los controles. Dependiendo de la entidad puede ser meses o hasta un año.
- Determinar el uso de recursos: Incluidos el personal así como el recurso físico.
- Revisión de políticas existentes: En los casos que existan políticas previas.
- Determinar material de investigación: Puede ser leyes, libros, internet, etc.
- Escribir un borrador inicial: Incluyendo la línea base de los controles requeridos en la empresa.
- Consideraciones de estilo: Tomando en cuenta la cultura organizacional y evitando frases negativas en el texto.

- Ciclos de revisión: Con el equipo del proyecto verificando que todos están conscientes de los controles y son factibles de aplicar.
- Revisión con los grupos de interés: De manera que se incluyan en el documento, todos los controles que requiere la empresa.
- Identificación de los procesos vacíos: Antes de la publicación, se debe validar que no existan procesos sin entradas o sin recursos, que no sean factibles de implementar.
- Desarrollar una estrategia de comunicación: Asegurando que todos los grupos serán debidamente informados de los motivos de la implementación de la política y sus beneficios.
- Publicación: Con la debida autorización, publicar y dar a conocer a toda la empresa la política.
- Activar una estrategia de comunicación: Mediante mecanismos efectivos que permitan a todo el personal conocer rápidamente cualquier modificación al respecto.
- Revisión y actualización: Durante periodos programados y frecuentes realizar retroalimentación sobre las políticas.

1.4.3. DETERMINACIÓN Y APLICACIÓN DE LA METODOLOGÍA ESCOGIDA

1.4.3.1. Determinación de la metodología

Luego del análisis de las metodologías planteadas para la elaboración de políticas de seguridad de la información, se utiliza en este proyecto la propuesta de la Universidad Nacional de Colombia, misma que contempla tanto definiciones claras acerca de términos que se utilizan en la implantación de seguridad de la información, como prácticas recomendadas para la definición de una política de seguridad de la información.

Para la selección de la metodología se analizan a continuación los siguientes parámetros de análisis, escogidos de acuerdo a las necesidades del proyecto:

- Diseño de la metodología: De acuerdo al Reglamento del Código Orgánico de Producción, Comercio e Inversiones, las empresas se pueden clasificar por el número de ingresos netos y el número de empleados que trabajan en ellas [14]. Ya que las entidades de la Administración Pública Central no se pueden clasificar por el número de ingresos netos, utilizando el parámetro de empleados se considera a éstas como medianas empresas con 200 funcionarios, esencialmente porque el personal que requieren para las actividades directamente relacionadas con su ámbito de negocio no supera esta cantidad de personal. El presente proyecto necesita una metodología que se aplique a medianas empresas.
- Enfocada en el proceso de elaboración de las Políticas: La metodología debe definir claramente el proceso que se deberá seguir para la elaboración de las Políticas.
- Base para los procedimientos: El alcance de este proyecto incluye la generación de los procedimientos generales para la aplicación de los controles por lo que se requiere que la metodología incluya la observancia de los procesos.
- Estructuración de la documentación: Para que se cumpla el objetivo de la generalidad del proyecto se requiere que la documentación propuesta en la metodología, así como su enfoque sea general y no conduzca a particularidades.

Parámetros de análisis	**Metodología de la UNC**	**Metodología de la SANS**
Diseño de la metodología	x	
Enfocada en el proceso de elaboración de políticas de seguridad de la información	x	x
Base para los procedimientos	x	
Estructura de los documentos	x	

Tabla 1-4: Resultados del análisis para la selección de la metodología

Como resultado de la tabla, se escoge la metodología de la UNC para el presente proyecto.

1.4.3.2. Aplicación de la metodología

El primer punto de la creación de una política es la identificación de la necesidad de su existencia. La Política de Seguridad de la Información en una entidad pública debe ser definida por la necesidad de la aplicación efectiva y segura de la LOTAIP, cumpliendo los tres dominios de la seguridad de la información. Además, debe definirse dando cumplimiento al Acuerdo Ministerial 166.

A continuación, se requiere definir el alcance de la política. En el hito No. 1, se establece que la máxima autoridad de la institución dispondrá la implementación del EGSI en la entidad. Esto da como resultado un alcance a todos los funcionarios y servidores de la entidad en la cual se implante el EGSI.

Como siguiente punto, la aplicabilidad se determina por la posibilidad de aplicar la política en la institución. A pesar de ser que la aplicación del EGSI es una disposición, en el Artículo 2 del Acuerdo Ministerial 166, la SNAP limita la aplicación del esquema de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información. Por tanto, el EGSI es aplicable en las instituciones, siempre y cuando exista un análisis de situación actual que permita determinar estrategias de implantación, así como hitos, que por su contenido o nivel de exigencia, no puedan ser implantados.

Los roles de la Política de Seguridad de la Información se definen en el capítulo 1 del EGSI. Entre los principales, encontramos el Comité de Gestión de la Seguridad de la Información (CGSI), el Oficial de Seguridad de la Información (OSI) y el Responsable de Seguridad de la Información de TI (RSITI).

Las responsabilidades de la Política también se encuentran descritas en el capítulo 1 de EGSI, siendo la de mayor relevancia la definición y mantenimiento de la política a cargo del CGSI.

La factibilidad se refiere a la disponibilidad de recursos necesarios para llevar a cabo la implementación de la política. Este punto debe ser considerado también en el análisis de la situación actual que se propone en este proyecto ya que se deberán diagnosticar las acciones a realizar dependiendo de la factibilidad técnica y de recursos.

Para concluir con los lineamientos de la etapa de la creación de la política, se resumen los puntos analizados en la Tabla 1-5.

Necesidad de la Política	Aplicación de la LOTAIP
Alcance	Todos los funcionarios de la institución pública
Aplicabilidad	En función de ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de seguridad de la información
Roles	Comité de Gestión de la Seguridad de la Información Oficial de Seguridad de la Información Responsable de Seguridad de la Información de TI
Responsabilidades	Definición y mantenimiento de la política a cargo del CGSI
Factibilidad	En función del análisis de situación actual

Tabla 1-5: Resultados del análisis para la creación de la Política de Seguridad de la Información.

Como resultado de este análisis, se precisa el Contenido de la política, el mismo que será utilizado en el capítulo 2 del presente proyecto:

1. OBJETO
2. ALCANCE
3. BASE LEGAL

4. DEFINICIONES

5. RESPONSABILIDAD Y AUTORIDAD

6. POLÍTICAS

7. ANEXOS

CAPÍTULO 2: FORMULACIÓN DE LA GUÍA

2.1. DETERMINACIÓN DEL ESTADO INICIAL DE LA SEGURIDAD DE LA INFORMACIÓN

Para la implantación de ésta Guía, se requiere una definición de la línea base de la Seguridad de la Información en la entidad, misma que se determina a través de un formato en que se fundamenta un cronograma de seguimiento de las actividades específicas del EGSI, tanto a corto como largo plazo. Esto se realiza con el objetivo de colaborar con el Oficial y el Responsable de TI, en la implantación y seguimiento de los ítems de control del EGSI.

Un factor determinante en la ejecución de esta Guía es el análisis de la documentación formal que las entidades requieren validar para el cumplimiento de obligaciones, de modo que las responsabilidades, los productos y las evidencias de cumplimiento sean definidas y clasificadas, y sirvan de sustento para futuras auditorías o similares procesos de control, generados por la SNAP u otros organismos.

Entonces, se considera obligatorio para el CSI, para el OSI y para el RSTI, definidos en la institución pública (designación obligatoria solicitada en los hitos 6, 7 y 8 de GPR) determinar la situación actual de la seguridad de la información en la entidad a la que se pertenecen.

Para el análisis de la situación actual, se proponen los siguientes criterios:

- Agrupar los hitos por cada uno de los once títulos del EGSI, de manera que sea entendible el alcance global del control que se pretender conseguir con su implantación (definidos en las matrices como Capítulos).
- Para cada título del EGSI, referir el respectivo objetivo de control que se define en la Norma INEN ISO/IEC 27002, consiguiendo así que se aclaren dudas que puedan surgir respecto al alcance de cada uno de los hitos que componen el título.
- Determinar aquellas actividades de corto plazo que permitan el cumplimiento de los ítems de control, tomando en cuenta la situación actual de la entidad.

Para todos los casos en los cuales los controles se encuentren aplicados en la institución con anterioridad por otros motivos diferentes al EGSI (como por ejemplo es uso de firewall o directorio activo, que son servicios comunes en las áreas de tecnologías de la información), se recomienda solicitar evidencia que corrobore lo indicado, con las firmas de responsabilidad necesarias de quienes lo han ejecutado, y de ser el caso, los informes técnicos de respaldo que deberían ser validados por el Responsable de TI.

Para todos los casos en los que no existan los controles requeridos por los hitos, es preciso definir claramente cada una de las actividades a ejecutarse para obtener la implantación de los mismos. No se recomienda definir actividades de corto plazo para los hitos que explícitamente requieren la generación de procedimientos formales, ya que con el plazo sugerido la obtención de procedimientos formales no se podría alcanzar. Pero siempre dependerá de la entidad, de la madurez y experticia de quién elabore los procedimientos:

- Determinar las actividades a mediano y largo plazo que permitan la continuidad en la ejecución de los ítems de control del EGSI. Se recomienda definir para todos los hitos actividades de mediano y largo plazo que aseguren a la entidad la continuidad de esta implantación, con revisiones periódicas de los controles implementados.

- Atendiendo a los plazos establecidos por la SNAP en el GPR, se sugiere para las actividades a corto plazo una planificación no mayor a seis meses en el cronograma a plantearse.
- Incluir en el detalle de actividades la firma de responsabilidad de al menos dos niveles jerárquicos responsables del área de TI en la institución, de modo que esté formalmente establecido el análisis de situación actual.

Con ésta descripción, se genera la Matriz de Definición de Situación Actual de la Implantación de EGSI; para ejemplificar la matriz se utiliza el Capítulo 6, Título 6.1, Hito 46 de EGSI en el formato de la Figura 2-1.

MATRIZ DE DEFINICIÓN DE SITUACIÓN ACTUAL PARA LA IMPLANTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.1 Documentación de los procedimientos de Operación

Objetivo de Control:
Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que necesitan

Hito:
49. Documentar los contactos de soporte, necesarios en caso de incidentes

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Corto Plazo																									
Acciones Largo Plazo																									

Elaborado por:	Revisado por:	Aprobado por:
Cargo:	Cargo:	Cargo:
Fecha:	Fecha:	Fecha:
Firma:	Firma:	Firma:

Figura 2-1: Matriz de definición de situación actual para la implantación de EGSI. (Elaborado por los autores)

En el Anexo A, se incluyen los formatos para el análisis de situación actual de todos los hitos prioritarios de EGSI de los capítulos 6 y 7.

2.2. DEFINICIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

2.2.1. OBJETO

Es el objeto de este documento definir la política institucional respecto a la Seguridad de la Información frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los dominios de confidencialidad, integridad, y disponibilidad de la información.

2.2.2. ALCANCE

Las políticas establecidas en este documento tendrán aplicación en todo el ámbito de la institución, sus recursos y la totalidad de los procesos internos o externos.

2.2.3. BASE LEGAL

La Ley Orgánica del Servicio Público, en el literal k) de su artículo 22, establece como uno de los deberes de los servidores públicos, “custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización.” [3]

La Ley Orgánica de Transparencia y Acceso a la Información Pública, en su artículo 6, considera como información confidencial, aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que

se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

El Acuerdo Ministerial Nro. 166 de la SNAP, en su anexo 1 determina que “las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.” [5]

La Norma de Control Interno (NCI) 401-10 -Seguridad de tecnología de la información, determina que: “la Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas de los medios físicos y la información que se procesa mediante sistemas informáticos.” [15]

2.2.4. DEFINICIONES [1] [12]

Activo: Cualquier cosa que tiene valor para la institución.

Activo de Información: Conocimiento o datos que tienen valor para la organización.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: Propiedad de que una entidad es lo que expresa ser.

Hardware: es la parte física de un computador y más ampliamente de cualquier dispositivo electrónico.

Internet: es una red de ordenadores a nivel mundial. Ofrece distintos servicios, como el envío y recepción de correo electrónico (e-mail), la posibilidad de ver información (científica, comercial, tecnológica, social, económica, etc.) en las páginas Web, de participar en foros de discusión, de enviar y recibir ficheros, de charlar en tiempo real, etc.

Redes: incluye cualquier sistema de cableado o equipo físico como enrutadores, switches, además de varios sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.

Seguridad de la información: se entiende como la preservación de sus siguientes características:

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Sistemas de información: incluyen cualquier sistema o aplicación de software que sea administrado por la Institución, y de los cuales es responsable, como aplicaciones de servidores y escritorio, sistemas operativos y aplicaciones de Internet.

Software: palabra proveniente del inglés, también denominado equipamiento o soporte lógico, es el conjunto de los componentes necesarios para hacer posible la realización de una tarea específica.

Usuario(s): incluye a todo personal, vinculado o no con la institución, a quien se le proporcione medios o niveles de autorización y accesos necesarios para hacer uso de sus servicios o sistemas de información.

2.2.5. RESPONSABILIDAD Y AUTORIDAD

La responsabilidad de elaborar este documento es del Oficial de Seguridad de la Información de la institución.

La responsabilidad de revisar éstas políticas y encargarle la aprobación de las políticas al CGSI es de la máxima autoridad de la institución.

El Comité de Gestión de la Seguridad de la Información de la institución, es responsable de la aprobación de estas políticas.

La responsabilidad de cumplir estas políticas es de todos los funcionarios de la institución que tienen la obligación de asegurar la integridad y exactitud de la información, protegiéndola contra la divulgación, manipulación, modificación o destrucción no autorizada o accidental.

La autoridad de hacer cumplir estas políticas es del Oficial de Seguridad de la Información.

2.2.6. POLÍTICAS

2.2.6.1. Políticas generales de la seguridad de la información

Se conformará oficialmente el Comité de Gestión de la Seguridad de la Información (CGSI) y se designará a sus participantes.

Se designará formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del CGSI. El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará a la máxima autoridad de la institución.

Se designará formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el Jefe de la Unidad de Tecnologías de la Información.

El Oficial de Seguridad de la Información analizará los activos de información institucional para proceder a su clasificación, basándose principalmente en los perjuicios que pudiera ocasionar su mal uso a la institución y/o a su personal.

Dichos perjuicios pueden ser de tipo:

a) Económico,
b) Financiero,
c) Político,
d) Sociales,
e) De imagen,
f) Legales, y/o
g) Gremiales.

El Oficial de Seguridad de la Información debe identificar los riesgos a los que está expuesta la información, teniendo en cuenta la posibilidad de que el personal interno y/o externo realice:

a) Divulgación no autorizada,
b) Modificación indebida, y
c) Destrucción de los soportes.

La clasificación de un activo de información se basará en los tres dominios de seguridad de la información: confidencialidad, integridad y disponibilidad.

a) Confidencialidad:

Nivel de Confidencialidad	Descripción
0	Activos de información que puede ser conocida o utilizada por todos los funcionarios de la institución y algunas entidades externas debidamente autorizadas.
1	Activos de información que puede ser conocida y utilizada por todos los funcionarios de la institución y algunas entidades

	externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas *leves* para la institución o terceros.
2	Activos de información que sólo puede ser conocida y utilizada por un grupo de funcionarios, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas *significativas* a la institución o terceros.
3	Activos de información que sólo puede ser conocida y utilizada por un grupo muy reducido de funcionarios, generalmente de la alta dirección de la institución, y cuya divulgación o uso no autorizados podría ocasionar pérdidas *graves* a la institución o terceros.

Tabla 2-1: Clasificación del dominio de confidencialidad [19]

b) Integridad:

Nivel de Integridad	Descripción
0	Activos de información cuya modificación no autorizada puede recuperarse fácilmente, o no afecta la operación de la institución.
1	Activos de información cuya modificación no autorizada puede recuperarse aunque podría ocasionar pérdidas leves para la Institución o terceros.
2	Activos de información cuya modificación no autorizada es difícil su recuperación y podría ocasionar pérdidas significativas para la Institución o terceros.
3	Activos de información cuya modificación no autorizada no podría recuperarse, ocasionando pérdidas graves a la Institución o terceros.

Tabla 2-2: Clasificación del dominio de Integridad [19]

c) Disponibilidad:

Nivel de Disponibilidad	Descripción
0	Activos de información cuya inaccesibilidad no afecta la operación de la institución.
1	Activos de información cuya inaccesibilidad permanente durante un plazo de tiempo establecido podría ocasionar pérdidas leves para la institución o terceros.
2	Activos de información cuya inaccesibilidad permanente en un plazo de tiempo determinado podría ocasionar pérdidas significativas a la institución o terceros.
3	Activos de información cuya inaccesibilidad permanente durante un plazo de tiempo indeterminado podría ocasionar pérdidas significativas a la institución o terceros.

Tabla 2-3: Clasificación del dominio de Disponibilidad [19]

La determinación del nivel de criticidad de los activos de información se definirá de acuerdo a los siguientes criterios:

- CRITICIDAD BAJA: ninguno de los niveles asignados a los tres dominios supera el 1.
- CRITICIDAD MEDIA: uno de los niveles asignados a los tres dominios es 2
- CRITICIDAD ALTA: uno de los niveles asignados a los tres dominios es 3

Todo activo de información cuya criticidad esté determinada como ALTA debe cumplir con las siguientes consideraciones para su uso y manipulación:

Autorización

a) El acceso a información deben estar expresamente autorizado por el correspondiente Director o Jefe de Área propietario de la información, en conjunto con el Oficial de Seguridad de la Información.

b) El acceso a los activos de información en los sistemas debe establecerse a través de un adecuado registro de auditorías.

c) El Director o Jefe de Área propietario de la información debe definir los tipos de permisos para que los funcionarios puedan acceder a la información, ya sean éstos permisos de lectura, modificación y/o eliminación.

d) El Director o Jefe de Área propietario de la información debe autorizar expresamente el uso de los activos de información para propósitos de prueba en el desarrollo y/o mantenimiento de los sistemas.

Conservación

a) La información confidencial no debe conservarse en los equipos informáticos del usuario, sino en los equipos de procesamiento centralizado (servidores de archivos o similares definidos para éste fin). Se deben incluir estos servidores en los procedimientos de respaldos.

Envíos

a) Acerca de la transmisión de datos mediante vías electrónicas, se deben definir controles sobre la integridad de los activos de información que aseguren la completa recepción de los mismos.

Divulgación a terceros

a) No se debe transmitir activos de información en forma verbal y/o escrita a personas externas a la institución sin la expresa autorización de la máxima autoridad.

2.2.6.2. Políticas de seguridad para las comunicaciones y operaciones

- Se debe utilizar de forma responsable y solamente para actividades laborales, las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, y el correo electrónico. Toda la información que se genera mediante los sistemas de comunicación institucionales; así como las copias de respaldo de los mismos, se consideran como propiedad de la institución.

- El uso personal de los sistemas de comunicación en forma ocasional es permisible, siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del funcionario ni con las actividades de la Institución.
- De existir personal temporal (por ejemplo, pasantes), no se les otorgará cuentas o perfiles donde se comprometa la seguridad de la información de la institución; como es el caso del correo electrónico.
- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento o diversión.
- Los funcionarios no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben colaborar con otros para que lo hagan.
- Queda prohibido el uso de software no autorizado por la institución. Para esto, se realizarán revisiones periódicas del contenido de software en los equipos informáticos (tabletas, computadores de escritorio y portátiles).
- Todo equipo informático que sea asignado a un usuario se lo debe entregar sin dejar información del anterior usuario de este equipo.
- Los respaldos de información se manejarán de la siguiente manera:

a) Personal que sale de la Institución: Se debe hacer un respaldo del equipo para proceder a formatearlo. La información se mantiene un número de días definido en el procedimiento para tal efecto.

b) Personal que se cambia de área: La información se mantiene un número de días definido en el procedimiento para tal efecto.

c) Personal que se cambia el computador: La información se mantiene se mantiene un número de días definido en el procedimiento para tal efecto.

d) La Unidad de Tecnologías de la Información respaldará todos los sistemas con sus respectivos archivos de configuración y base de datos, de manera que se asegure la continuidad del negocio.

2.2.6.3. Políticas de seguridad para el control de acceso

- Es responsabilidad del usuario, tanto interno como externo, el uso de las cuentas y contraseñas asignadas.
- Se dispone la utilización de una contraseña de complejidad media para los servicios de criticidad alta de la institución. La periodicidad de cambio será de hasta seis meses.
- Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, para lo cual deben cumplir con las siguientes directrices:

a) Mantener las contraseñas en secreto. Evitar escribirlas en papeles que se encuentran visibles en las estaciones de trabajo.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de error del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las siguientes recomendaciones:

   1. Sean fáciles de recordar.
   2. No estén basadas en algún dato que otra persona pueda adivinar fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
   3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Evitar almacenar contraseñas en los navegadores de manera que permitan accesos automáticos a los sistemas.

f) Notificar al Oficial de Seguridad de la Información cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o sospecha de pérdida de confidencialidad.

- La solicitud de una nueva cuenta o el cambio de privilegios debe ser formalmente realizado, y debidamente aprobado por el Director o Jefe de Área.

- Se prohíbe el uso de cuentas anónimas o de invitado y los usuarios deben ingresar a los sistemas mediante cuentas que indiquen claramente su identidad.
- Para proteger las estaciones de trabajo de los usuarios contra usos no autorizados, se debe habilitar el bloqueo automático del equipo luego de un periodo determinado que esté inactivo.
- Se debe mantener resguardada la información sensible o crítica de la institución, en especial cuando no esté siendo utilizada o no se encuentre personal en la oficina. No olvidar este tipo de información en las bandejas de impresión.
- Luego de utilizar cualquier tipo de dispositivos removibles, se debe retirarlos de los equipos informáticos.
- El acceso remoto para realizar actividades desde un lugar externo de las instalaciones de la institución sólo será autorizado por el Director o Jefe de Área a la cual pertenezca el usuario solicitante. El Responsable de Seguridad de la Información de TI verificará que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo que se cumpla con las políticas y procedimientos existentes.
- Para el uso de dispositivos informáticos móviles pertenecientes a la institución, se debe tener especial cuidado en garantizar que no se comprometa la información de la Institución, evitando su exposición en sitios inseguros, públicos y de alto riesgo. Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: computadores portátiles, PDA, teléfonos celulares, tarjetas de memoria, dispositivos de almacenamiento removibles, tales como CD, DVD, disquetes, cintas, y cualquier dispositivo de almacenamiento de conexión USB, tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.
- No se permite el uso de equipos de propiedad privada ajenos a la institución, que no estén bajo el control y monitoreo de la institución.

2.2.6.4. Políticas de seguridad para la adquisición, desarrollo y mantenimiento de sistemas de información

- Para toda adquisición o desarrollo de sistemas informáticos se definirán controles de seguridad, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger, y el daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.

2.2.6.5. Políticas de gestión de los incidentes de seguridad de la información

- El Oficial de Seguridad de la Información es el punto de contacto donde se deberán reportar todos los eventos relacionados con incidentes de seguridad de la información.
- La Unidad de Tecnologías de la Información se asegurará que todos los incidentes registrados en el área, relacionados con seguridad de la información, sean debidamente notificados al Oficial de Seguridad con al menos los siguientes datos: fecha, hora, nombres del responsable del incidente, departamento afectado y sistema involucrado.
- El cierre respectivo del incidente debe incluir la solución implementada, y en aquellos casos que se requiera las acciones para que el incidente no se repita.

2.2.6.6. Sanciones

La institución definirá, a través de la Unidad de Talento Humano, las sanciones a aplicarse por el incumplimiento u omisión de la aplicación de éstas políticas.

El Oficial de Seguridad de la Información debe evaluar periódicamente el cumplimiento de ésta política, tanto a nivel de usuarios como de los funcionarios de la Unidad de Tecnologías de la Información.

La política de seguridad de la información será revisada periódicamente. En caso de que surjan nuevos controles, únicos y particulares de la institución, éstos se deberán incorporar al presente documento. Formarán parte de esta política todos aquellos

documentos, memorandos, instrucciones, manuales, políticas o procedimientos que se notifiquen y que estén relacionados a la seguridad de la información en la institución.

2.2.7. ANEXOS

Se anexa a estas políticas el Acuerdo Ministerial Nro. 166 de la Secretaría Nacional de la Administración Pública.

2.3. DETERMINACIÓN DE LOS PROCEDIMIENTOS PARA LA IMPLANTACIÓN DEL EGSI.

Se han analizado las mejores prácticas de COBIT e ITIL de manera que las plantillas de procedimientos generados se encuentren estandarizadas y sean de fácil aplicación para cualquier entidad.

2.3.1. MEJORES PRÁCTICAS APLICADAS

De acuerdo al Instituto de Gobierno de TI, “COBIT es un marco de trabajo mundialmente aceptado para el Gobierno de TI basado en estándares de la industria y las mejores prácticas”. [8]

Se divide principalmente en 5 dominios que se presentan en la Figura 2-2.

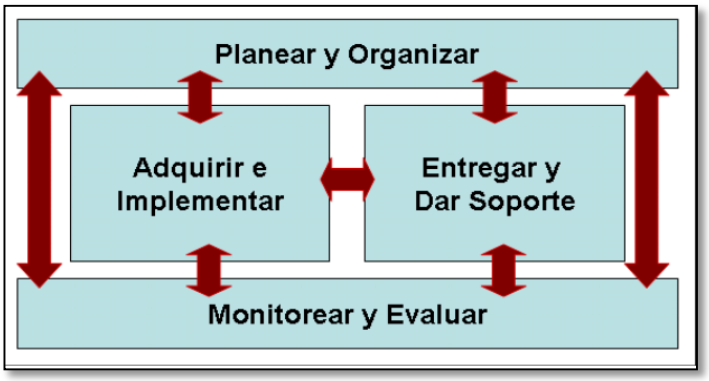


Figura 2-2: Dominios de COBIT y su interrelación (Tomado de COBIT 4)

De acuerdo al Instituto de Gobierno de TI, “ITIL proporciona un marco de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los

procesos conexos, la promoción de un enfoque de alta calidad para el logro de la eficacia empresarial y la eficiencia en la gestión de servicios de TI". [8]

Se divide principalmente en 5 publicaciones que se presentan en la Figura 2-3.

Figura 2-3: Publicaciones de ITIL y su interrelación (Tomado de ITIL v3)

2.3.2. DESARROLLO DE LOS PROCEDIMIENTOS

Debido a que EGSI se encuentra basado en la norma IEC/ISO 27002, se escogieron las versiones 4.2 y 3 de COBIT e ITIL respectivamente, para un mejor relacionamiento entre estos marcos de referencia. De igual manera, la SNAP determina a través del Acuerdo Ministerial Nro. 1580 directrices generales para el trabajo con procesos en las entidades del sector público que son tomadas en cuenta en la presente Guía.

En cuanto al contenido de los procedimientos, se utiliza la siguiente estructura: [11]

1. OBJETO: declaración del propósito de los requisitos de seguridad que se intentan satisfacer.

2. ALCANCE: aplicabilidad y límites de la institución donde este procedimiento es vinculante.
3. DEFINICIONES: definiciones de aquellos términos que aparezcan en el procedimiento y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar la ambigüedad en la interpretación al establecer el significado en el procedimiento de los términos utilizados.
4. DESARROLLO DEL PROCESO: determinación del conjunto de actividades y tareas a realizar en la ejecución del proceso.

Para cada procedimiento se incluye la alineación de EGSI con las mejores prácticas de TI, con la siguiente explicación: [10]

- Detalle de Hito EGSI en GPR: Descripción del o los hitos de EGSI relacionados con el subtítulo.
- Objetivo de control de COBIT: Se relacionan los hitos de EGSI con los objetivos de control de COBIT, asignando a cada uno de ellos las siglas del dominio al que corresponden, así:

    a) PO: Planear y Organizar

    b) AI: Adquirir e Implementar

    c) DS: Entregar y Dar Soporte

    d) ME: Monitorear y Evaluar

- Listas de control de ITIL v3: Se relacionan los hitos escogidos de EGSI con las listas de control de ITIL, asignando a cada uno de ellos las siglas de la publicación a la que corresponden, así:

    a) ES: Estrategia del Servicio

    b) DS: Diseño del Servicio

    c) OS: Operación del Servicio

d) TS: Transición del Servicio

e) MCS: Mejora Continua del Servicio

- Disparador: Actividad que inicia la ejecución del procedimiento.
- Insumos y Proveedores: Entradas del procedimiento y la entidad que lo genera.
- Productos y Clientes: Salidas del procedimiento y la entidad que lo recibe.
- Tipo de Proceso: De acuerdo al Acuerdo Ministerial Nro. 1580, pueden ser adjetivos, sustantivo o gobernantes.
- Responsable del Proceso: Persona o entidad que ejecuta el procedimiento.
- Métrica: Indicador que muestra el éxito de la aplicación del procedimiento.

5. ANEXOS: De requerirlo esencialmente en los documentos que se generan del procedimiento.

Para determinar los procedimientos para la Implantación del EGSI, se utiliza la Tabla 2-4 en la cual se detallan los aspectos fundamentales de cada procedimiento.

<table>
<tr><td>Nro. Hito</td><td colspan="3">Numero de Hito</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td colspan="3">Descripción del o los hitos de EGSI relacionados con el subtítulo. [5]</td></tr>
<tr><td>Objetivo de control de COBIT</td><td colspan="3">Se relacionan los hitos de EGSI con los objetivos de control de COBIT. [17]</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">Se relacionan los hitos escogidos de EGSI con las listas de control de ITIL [16]</td></tr>
<tr><td>Disparador:</td><td colspan="3">Actividad que inicia la ejecución del procedimiento</td></tr>
<tr><td>Insumos y Proveedores</td><td colspan="3"><table><tr><td>Entrada</td><td>Proveedor</td><td>Tipo de Proveedor</td></tr><tr><td>Entrada del procedimiento</td><td>Entidad que genera el procedimiento.</td><td>Interno o Externo</td></tr></table></td></tr>
<tr><td>Productos y Clientes</td><td colspan="3"><table><tr><td>Producto</td><td>Cliente</td><td>Tipo de Cliente</td></tr><tr><td>Salida del procedimiento</td><td>Entidad que recibe el procedimiento.</td><td>Interno o Externo</td></tr></table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Pueden ser adjetivos, sustantivo o gobernantes. [9]</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Persona o entidad que ejecuta el procedimiento.</td></tr>
<tr><td>Métrica</td><td colspan="3">Indicador que muestra el éxito de la aplicación del procedimiento. [17]</td></tr>
</table>

Tabla 2-4: Ejemplo de la Tabla a ser utilizada en el desarrollo de los procedimientos (Elaborada por los autores)

2.3.3. PROCEDIMIENTO DE SEGURIDAD PARA LAS COMUNICACIONES Y OPERACIONES

2.3.3.1. Objeto

Establecer una metodología para documentar, registrar, monitorear, elaborar, modificar y controlar las operaciones de los sistemas, todos los accesos a los mismos, y mantener dicha información respaldada bajo las normas requeridas por la institución.

2.3.3.2. Alcance

Mantener un control en la seguridad de la información de la institución que comprenda un registro, monitoreo y documentación de las comunicaciones operaciones de los sistemas que maneje la institución.

2.3.3.3. Definiciones

Disparador: Es una condición o evento que produce el inicio o activación del proceso.

Diagramas de Flujo: Es la representación gráfica de la secuencia de actividades que contiene el proceso.

Entradas: Se denomina “entradas” a los insumos que ingresan al proceso para ser transformados durante la ejecución del mismo, para producir salidas (productos) mediante las actividades que realizan un valor agregado.

Procedimiento: Se llama procedimiento a la forma específica de llevar a cabo las actividades de un proceso, las mismas que deben documentarse por parte del responsable del proceso, en especial cuando los procesos son críticos para la institución.

Proceso: Se define proceso a una serie de actividades definibles, predecibles y repetibles, que dan un resultado útil para un cliente interno o externo. Los procesos se interrelacionan en un sistema que agrega valor a sus clientes.

Proceso Adjetivo: Son los que proporcionan servicios o productos a los procesos gobernantes o sustantivos.

Responsable del Proceso: Es la persona que se encuentra obligado a responder por la ejecución de las actividades de un proceso organizacional.

2.3.3.4. Desarrollo del Proceso

2.3.3.4.1. Documentación de los Procedimientos de Operación

En la Tabla 2-5 se encuentra el detalle del procedimiento Documentación de los Procedimientos de Operación:

Nro. Hito	49			
Detalle Hito EGSI en GPR	Documentar los contactos de soporte, necesarios en caso de incidentes.			
Objetivo de control de COBIT	AI 4.4 Transferencia de conocimiento al personal de operaciones y soporte DS 13.1 Procedimientos e instrucciones de operación			
Listas de control de ITIL v3	ES - Portafolio de Servicios			
Disparador:	Necesidad de modificación o elaboración de un servicio			
Insumos y Proveedores	**Entrada**	**Proveedor**	**Tipo de Proveedor**	
	Información del servicio	Responsable del servicio	Interno	
Productos y Clientes	**Producto**	**Cliente**	**Tipo de Cliente**	

	Portafolio de Servicios Actualizado	Unidad de Tecnologías de la Información	Interno	
Tipo de Proceso:	Adjetivo			
Responsable del Proceso:	Área de Soporte			
Métrica	Número de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación			

Tabla 2-5: Documentación de los procedimientos de Operación

2.3.3.4.1.1 Diagrama de Flujo de la Documentación de los Procedimientos de Operación

En la Fig. 2-4 el diagrama de flujo de la Documentación de los Procedimientos de Operación

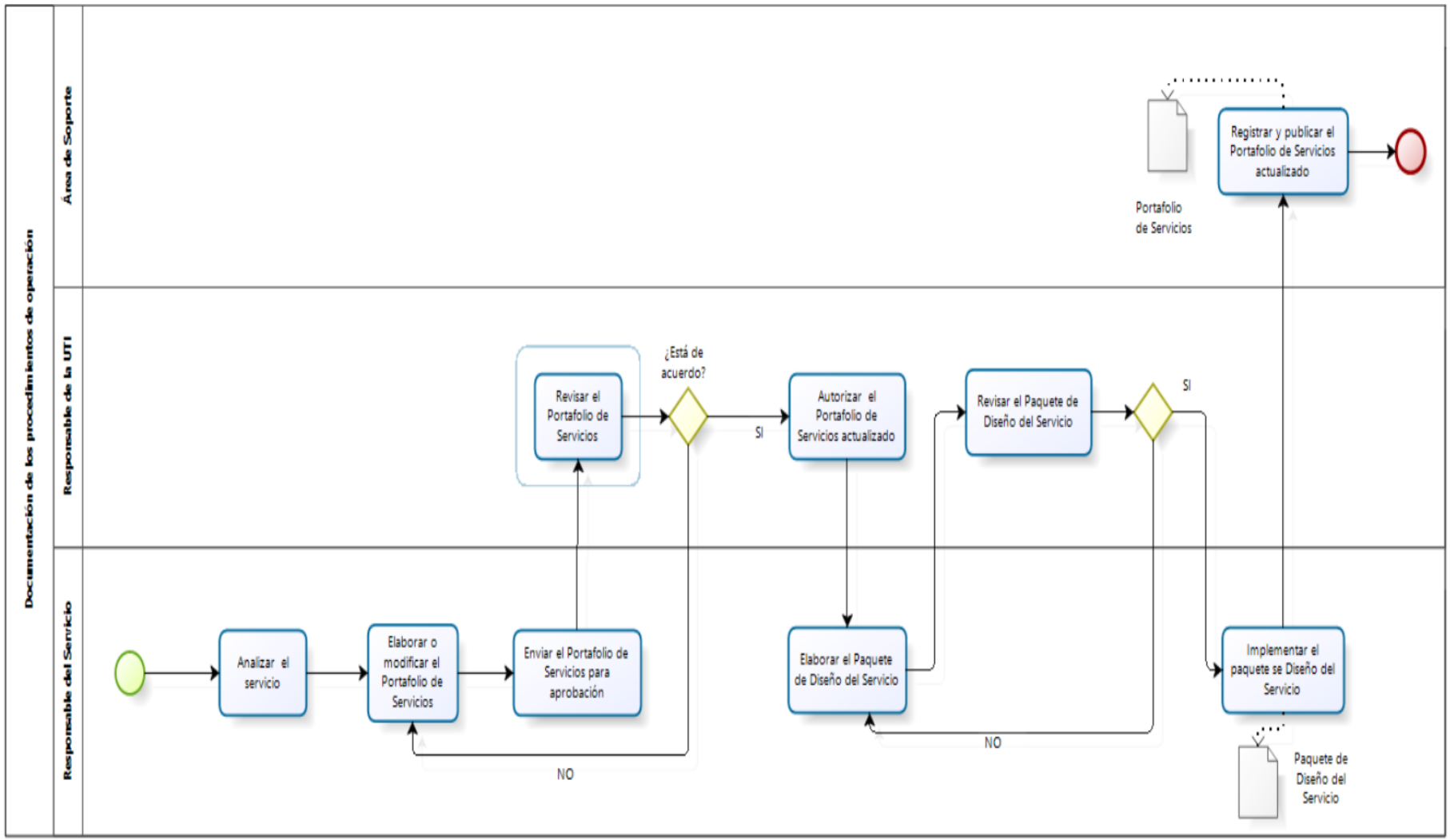


Figura 2-4: Diagrama de Flujo de Documentación de los procedimientos de Operación

2.3.3.4.2. Controles Contra Código Malicioso

En la Tabla 2-6 se encuentra el detalle del procedimiento Controles Contra Código Malicioso:

<table>
<tr><td>Nro. Hito</td><td colspan="3">50,51,52</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td colspan="3">• Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado.
• Instalar y actualizar periódicamente software de antivirus y contra código malicioso.
• Mantener los sistemas operativos y sistemas de procesamiento de información actualizados, con las últimas versiones de seguridad disponibles.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td colspan="3">DS 5.9 Prevención, detección y corrección de software malicioso.
DS 5.10 Seguridad en la red.</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">No aplica.</td></tr>
<tr><td>Disparador:</td><td colspan="3">Modificación del inventario de equipos informáticos de la institución.</td></tr>
<tr><td>Insumos y Proveedores</td><td colspan="3"><table><tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr><tr><td>Información del inventario</td><td>Área de Soporte</td><td>Interno</td></tr></table></td></tr>
<tr><td>Productos y Clientes</td><td colspan="3"><table><tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr><tr><td>Informe de control contra código malicioso.</td><td>Unidad de Tecnologías de la Información.</td><td>Interno</td></tr></table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
</table>

Responsable del Proceso:	Área de Soporte
Métrica	Número y tipo de código malicioso detectado vs. número y tipo de código malicioso eliminado

Tabla 2-6: Controles contra código malicioso

2.3.3.4.2.1 Diagrama de Flujo de Controles Contra Código Malicioso

En la Fig. 2-5 el diagrama de flujo de Controles Contra Código Malicioso.

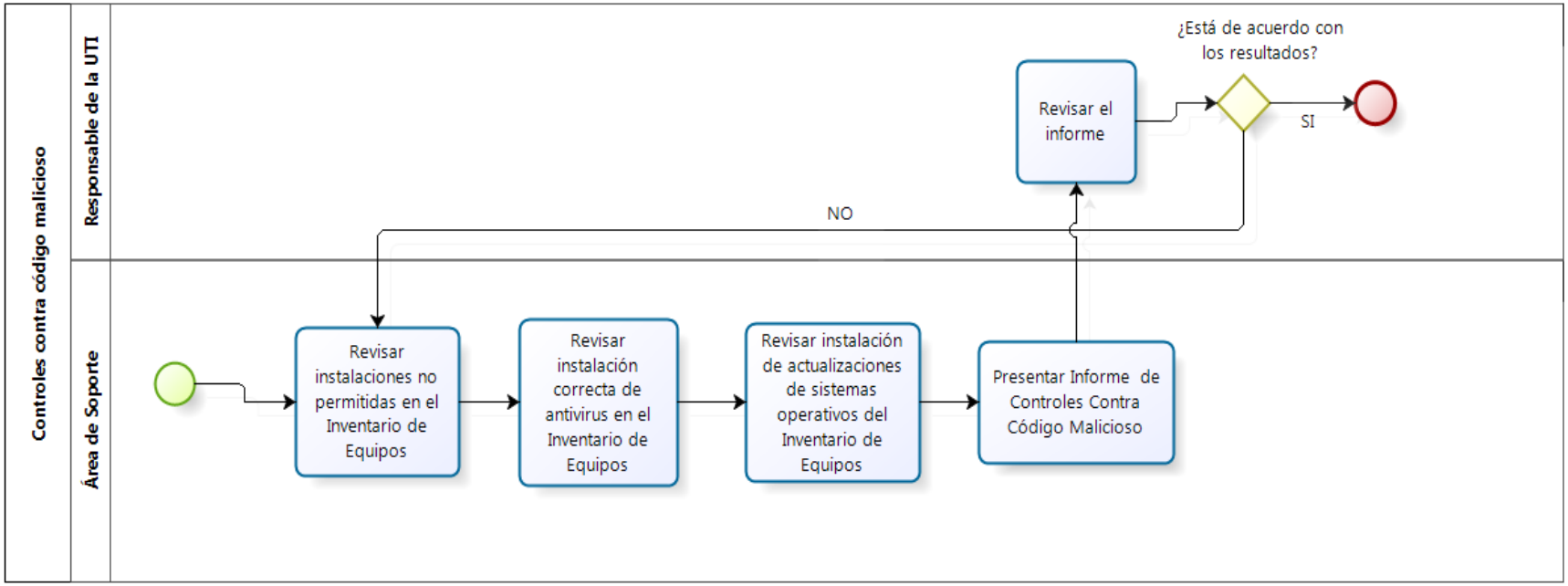


Figura 2-5: Diagrama de Flujo de Controles contra Código malicioso.

2.3.3.4.3. Respaldo de la Información

En la Tabla 2-7 se encuentra el detalle del procedimiento Respaldo de la Información:

<table>
<tr><td>Nro. Hito</td><td>53,54,55</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td>• Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.
• Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención.
• Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>DS 4.9 Almacenamiento de respaldos fuera de las instalaciones.
DS 11.2 Acuerdos de almacenamiento y conservación.
DS 11.5 Respaldo y restauración.
DS 11.6 Requerimientos de seguridad para la administración de datos.</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>DS - Paquete del diseño del servicio</td></tr>
<tr><td>Disparador:</td><td>Solicitud de servicio de respaldos</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del servicio de respaldos</td><td>Propietario de la Información</td><td>Interno</td></tr>
</table>
</td></tr>
</table>

Productos y Clientes:	**Producto**	**Cliente**	**Tipo de Cliente**
	Paquete del diseño del Servicio	Unidad de Tecnologías de la Información	Interno
Tipo de Proceso:	Adjetivo		
Responsable del Proceso:	Área de Infraestructura		
Métrica	Porcentaje de restauraciones de datos exitosas. Frecuencia de las prueba de los medios de respaldo.		

Tabla 2-7: Respaldo de la Información.

2.3.3.4.3.1 Diagrama de Flujo de Respaldo de la Información

En la Fig. 2-6 el diagrama de flujo de Flujo de Respaldo de la Información.

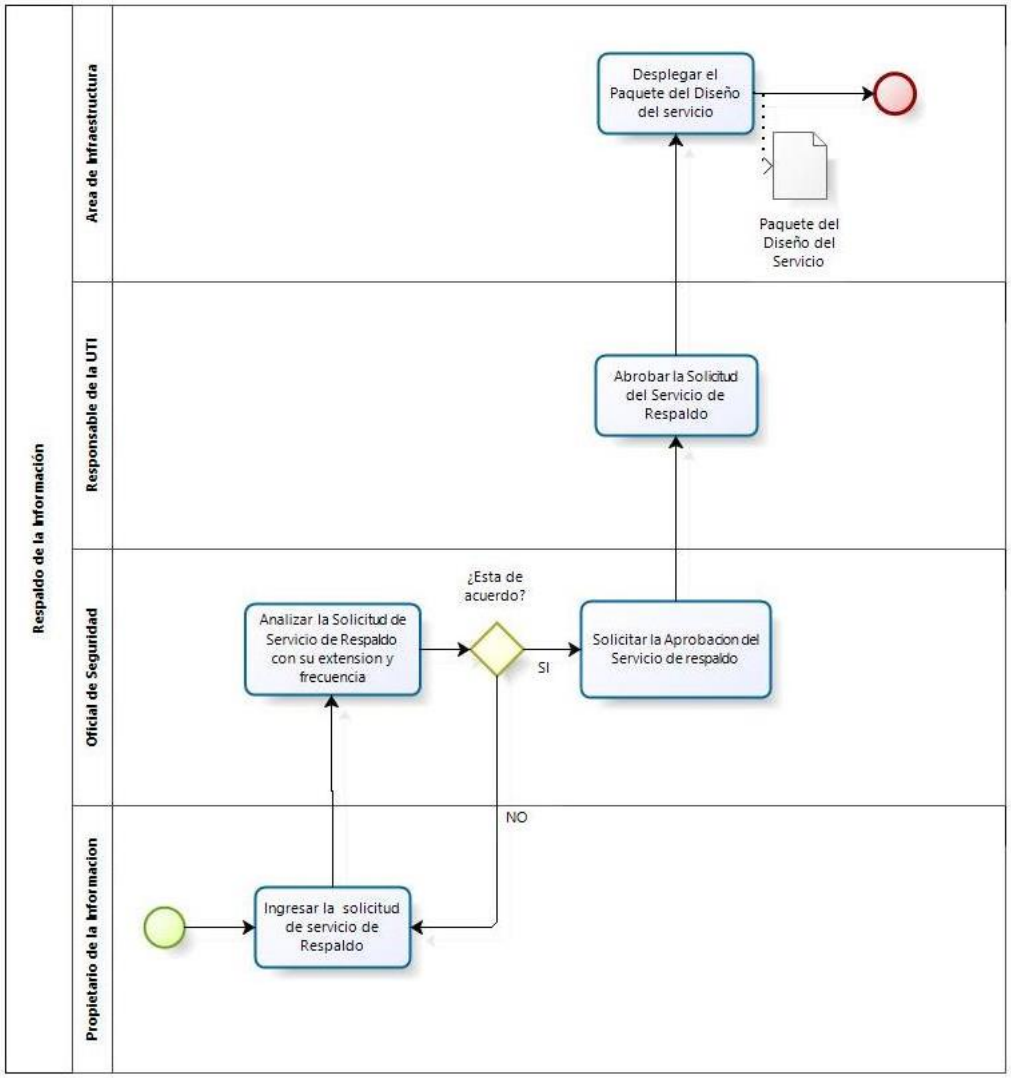


Figura 2-6: Diagrama de Flujo de Respaldo de la Información

2.3.3.4.4. Seguridad de los Servicios de la Red

En la Tabla 2-8 se encuentra el detalle del procedimiento Seguridad de los Servicios de la Red:

<table>
<tr><td>Nro. Hito</td><td colspan="4">56,57</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td colspan="4">• Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red.
• Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td colspan="4">DS 5.7 Protección de la tecnología de seguridad
DS 5.9 Prevención, detección y corrección de software malicioso
DS 5.11 Intercambio de datos sensitivos</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="4">DS - Paquete del diseño del servicio</td></tr>
<tr><td>Disparador:</td><td colspan="4">Necesidad de modificación o elaboración de un servicio</td></tr>
<tr><td rowspan="2">Insumos y Proveedores</td><td>Entrada</td><td>Proveedor</td><td>Tipo de Proveedor</td><td></td></tr>
<tr><td>Información del servicio</td><td>Responsable del servicio</td><td>Interno</td><td></td></tr>
<tr><td rowspan="2">Productos y Clientes</td><td>Producto</td><td>Cliente</td><td>Tipo de Cliente</td><td></td></tr>
<tr><td>Portafolio de Servicios Actualizado</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td><td></td></tr>
</table>

Tipo de Proceso:	Adjetivo
Responsable del Proceso:	Área de Soporte
Métrica	Número de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación

Tabla 2-8: Servicios de la Red.

2.3.3.4.4.1 Diagrama de Flujo de Seguridad de los Servicios de la Red

Remitirse al numeral 2.3.3.4.1.1

2.3.3.4.5. Registros de Auditorías

En la Tabla 2-9 se encuentra el detalle del procedimiento Registros de Auditorías:

Nro. Hito	58,59,60,61
Detalle Hito EGSI en GPR	• Registrar los accesos y tipos de acceso. • Registrar las direcciones y protocolos de red. • Definir alarmas originadas por el sistema de control de acceso. • Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS).

<table>
<tr><td>Objetivo de control de COBIT</td><td>AI 2.3 Control y posibilidad de auditar las aplicaciones
DS 5.7 Protección de la tecnología de seguridad</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>No Aplica</td></tr>
<tr><td>Disparador:</td><td>Registro de un problema</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Registro de incidentes</td><td>Área de soporte</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes:</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Registro de problema</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Infraestructura o Área de Software</td></tr>
<tr><td>Métrica</td><td>Número y tipo de violaciones de acceso reales y sospechadas
Número de logs activos vs logs deshabilitados.</td></tr>
</table>

Tabla 2-9: Registros de Auditorias

2.3.3.4.5.1 Diagrama de Flujo de los Registros de Auditorías

En la Fig. 2-7 el diagrama de flujo de los Registros de Auditorias.

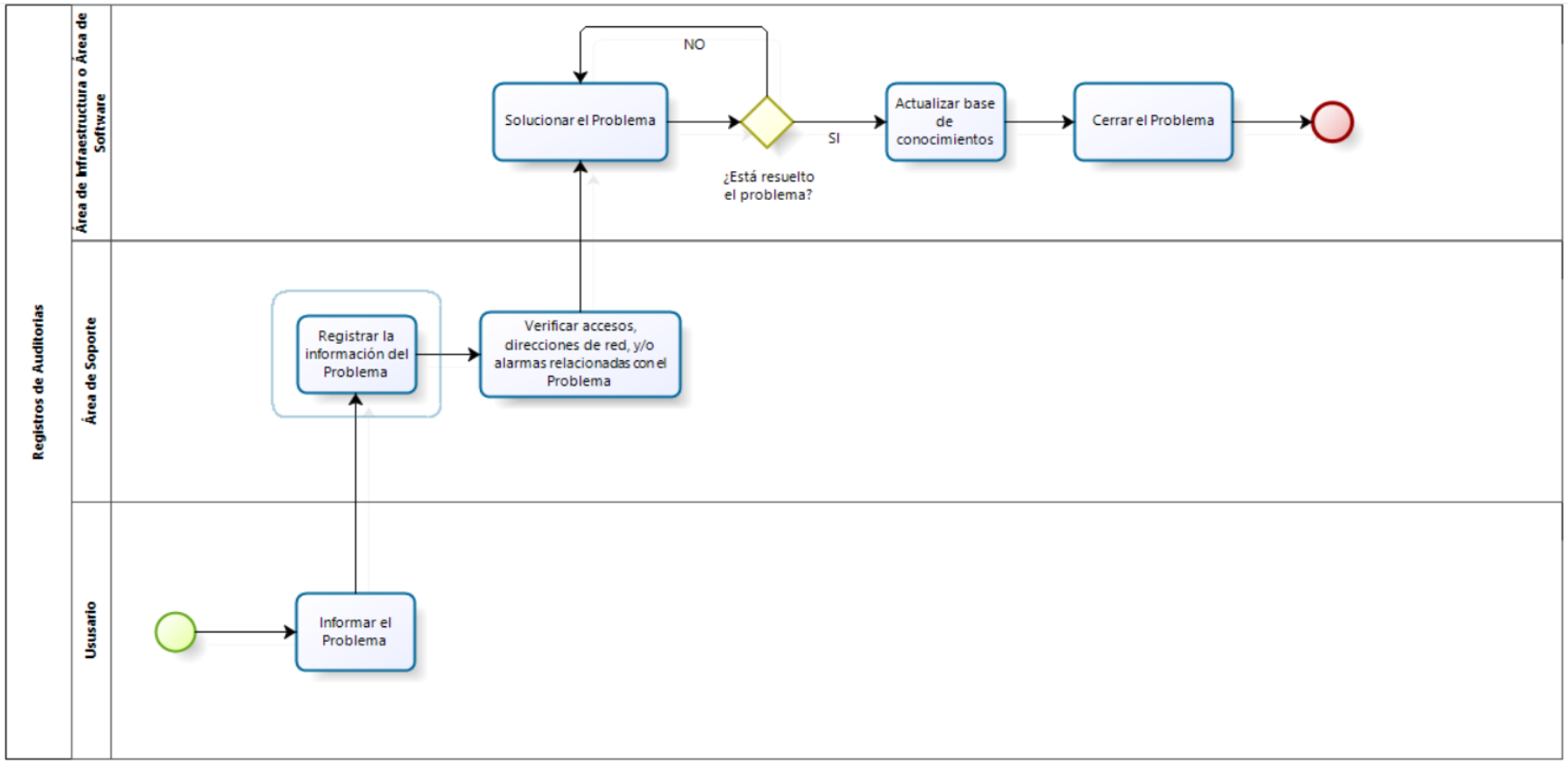


Figura 2-7: Diagrama de Registros de Auditorias.

2.3.3.4.6. Monitoreo del Uso del Sistema

En la Tabla 2-10 se encuentra el detalle del procedimiento Monitoreo del Uso del Sistema:

<table>
<tr><td>Nro. Hito</td><td>62,63,64,65</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td>• Registrar los accesos autorizados.
• Monitorear las operaciones privilegiadas.
• Monitorear intentos de acceso no autorizados.
• Revisar alertas o fallas del sistema.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>DS 5.5 Pruebas, vigilancia y monitoreo de la seguridad
ME 1.2 Definición y recolección de datos de monitoreo
ME 2.2 Revisiones de auditoría
ME 2.5 Aseguramiento de control interno
ME 4.7 Aseguramiento independiente</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Registro de incidente
OS - Registro de problema
PCS - Informe de evaluación de servicios</td></tr>
<tr><td>Disparador:</td><td>Requerimiento para monitorear operaciones e intentos de acceso a los sistemas</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información de los servidores</td><td>Área de Infraestructura</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes:</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
</table>
</td></tr>
</table>

	Informe de evaluación del sistema	Unidad de Tecnologías de la Información	Interno
Tipo de Proceso:	Adjetivo		
Responsable del Proceso:	Área de Infraestructura		
Métrica	Porcentaje de procesos críticos monitoreados		

Tabla 2-10: Monitoreo del uso del Sistema

2.3.3.4.6.1 Diagrama de Flujo del Monitoreo del Uso del Sistema

En la Fig. 2-8 el diagrama de flujo del Monitoreo del Uso del Sistema.

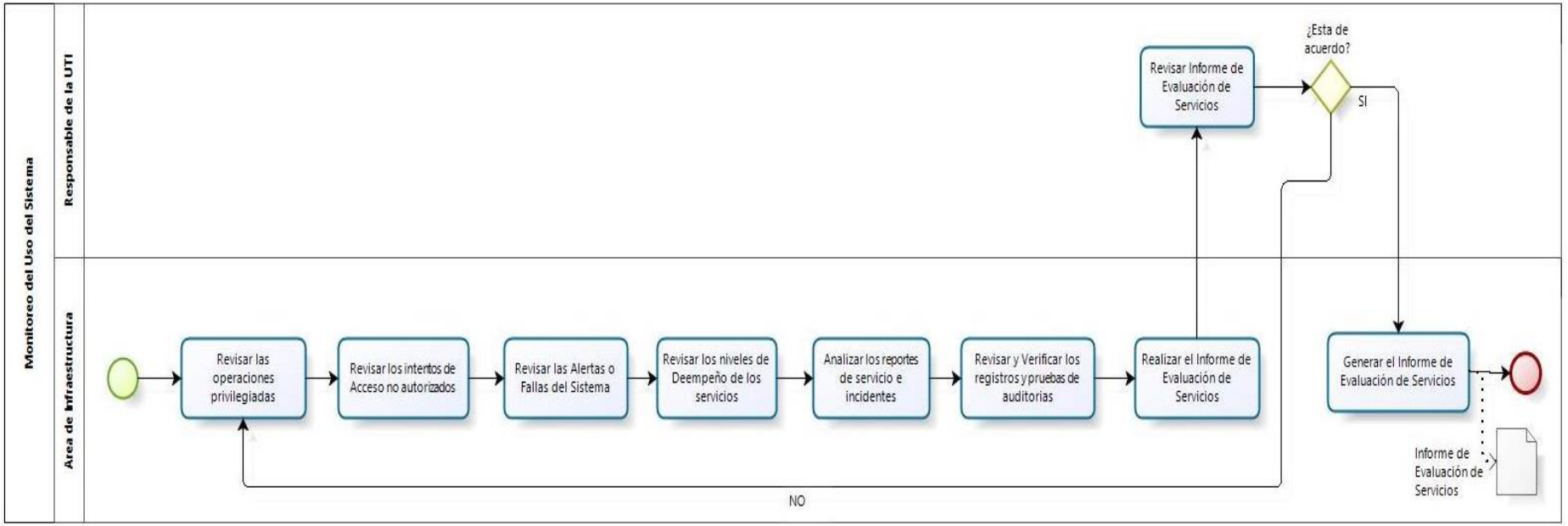


Figura 2-8: Diagrama del Monitoreo del Uso del Sistema

2.3.3.4.7. Registros del Administrador y el Operador

En la Tabla 2-11 se encuentra el detalle del procedimiento Registros del Administrador y el Operador:

Nro. Hito	66,67,68,69
	• Registrar la hora en la que ocurrió el evento. • Registrar información sobre el evento.

<table>
<tr><td>Detalle Hito EGSI en GPR</td><td>• Registrar la cuenta de administrador y operador que estuvo involucrado.
• Registrar los procesos que estuvieron implicados.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>DS 5.5 Pruebas, vigilancia y monitoreo de la seguridad
DS 5.7 Protección de la tecnología de seguridad
ME 2.2 Revisiones de auditoría
ME 2.5 Aseguramiento de control interno</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Registro de incidente
OS - Registro de problema</td></tr>
<tr><td>Disparador:</td><td>Registro de un incidentes</td></tr>
<tr><td>Insumos y Proveedores:</td><td><table><tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr><tr><td>Requerimiento de servicio</td><td>Área de soporte</td><td>Interno</td></tr></table></td></tr>
<tr><td>Productos y Clientes:</td><td><table><tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr><tr><td>Registro de incidente</td><td>Usuario</td><td>Interno</td></tr></table></td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica</td><td>Número de debilidades identificadas por reportes externos de calificación y certificación
Número de Incidentes Abiertos vs Incidentes Cerrados.</td></tr>
</table>

Tabla 2-11: Registros del Administrador y el Operador

2.3.3.4.7.1. Diagrama de Flujo de Registros del Administrador y el Operador

En la Fig. 2-9 el diagrama de flujo de Registros del Administrador y el Operador.

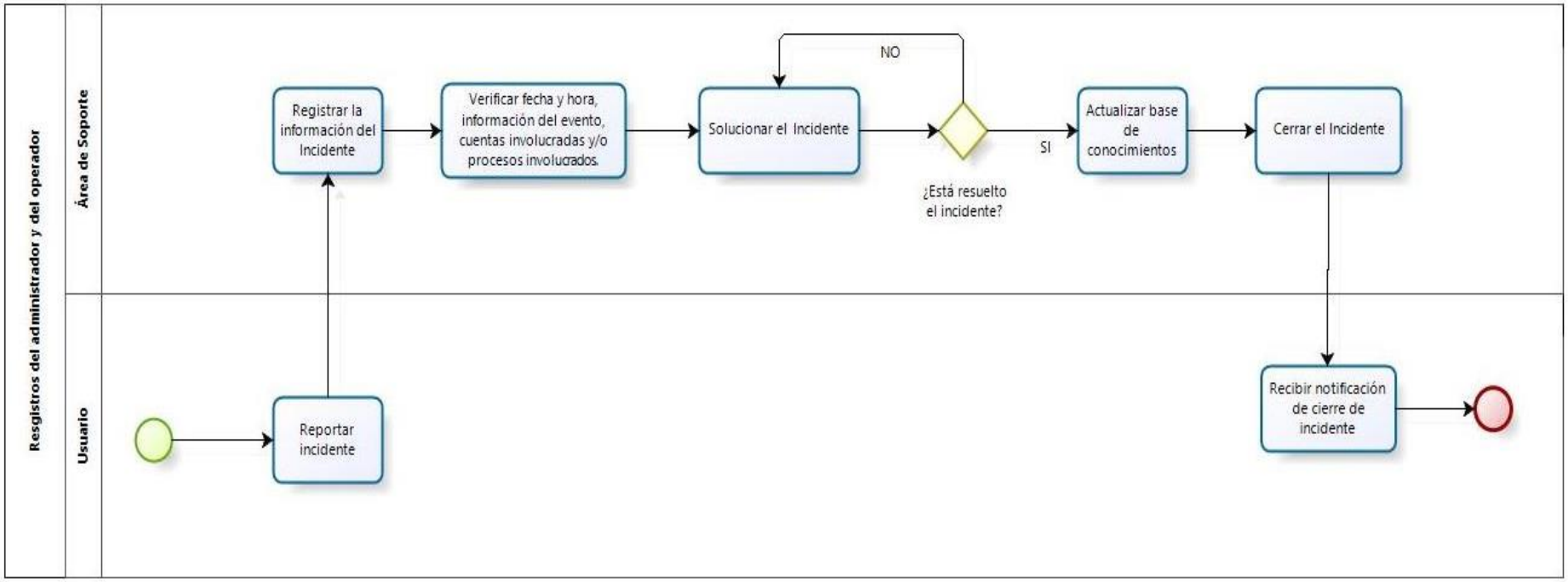


Figura 2-9: Diagrama de Registros del Administrador y del Operador.

2.3.3.4.8. Registros de Fallas

En la Tabla 2-12 se encuentra el detalle del procedimiento Registros de Fallas:

<table>
<tr><td>Nro. Hito</td><td>70,71,72</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td>• Revisar los registros de fallas o errores del sistema.
• Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles.
• Asegurar que el registro de fallas esté habilitado.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>AI 2.3 Control y posibilidad de auditar las aplicaciones
DS 5.7 Protección de la tecnología de seguridad</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Registro de problema</td></tr>
<tr><td>Disparador:</td><td>Registro de un incidentes</td></tr>
<tr><td>Insumos y Proveedores:</td><td><table><tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr><tr><td>Requerimiento de servicio</td><td>Área de soporte</td><td>Interno</td></tr></table></td></tr>
<tr><td>Productos y Clientes:</td><td><table><tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr><tr><td>Registro de incidente</td><td>Usuario</td><td>Interno</td></tr></table></td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica</td><td>Número de debilidades identificadas por reportes externos de calificación y certificación</td></tr>
</table>

	Numero de Errores Reportados vs Errores Corregidos.

Tabla 2-12: Registro de Fallas

2.3.3.4.8.1. Diagrama de Flujo de Registro de Fallas

Remitirse a los numerales 2.3.3.4.5.1 y 2.3.3.4.7.1

2.3.3.4.9. Monitoreo y Revisión de los Servicios, por Terceros

En la Tabla 2-13 se encuentra el detalle del procedimiento Monitoreo y Revisión de los Servicios, por Terceros:

Nro. Hito	73,74,75
Detalle Hito EGSI en GPR	• Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos. • Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos. • Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.
Objetivo de control de COBIT	DS 1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio DS2.4 Monitoreo del desempeño del proveedor ME 2.6 Control interno para terceros
	ES - Portafolio de servicios DS - Paquete del diseño del servicio

<table>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">PCS - Informe de evaluación de servicios</td></tr>
<tr><td>Disparador:</td><td colspan="3">Requerimiento para monitorear operaciones e intentos de acceso a los sistemas</td></tr>
<tr><td>Insumos y Proveedores:</td><td colspan="3"><table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información de los servidores</td><td>Área de Infraestructura</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Productos y Clientes:</td><td colspan="3"><table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Informe de evaluación del sistema</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Infraestructura</td></tr>
<tr><td>Métrica</td><td colspan="3">Porcentaje de procesos críticos monitoreados</td></tr>
</table>

Tabla 2-13: Monitoreo y Revisión de los Servicios, por Terceros

2.3.3.4.9.1. Diagrama de Flujo de Monitoreo y Revisión de los Servicios, por Terceros

Remitirse al numeral 2.3.3.4.6.1

2.3.3.4.10. Gestión de la Capacidad

En la Tabla 2-14 se encuentra el detalle del procedimiento Gestión de la Capacidad:

Nro. Hito	76		
Detalle Hito EGSI en GPR	Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.		
Objetivo de control de COBIT	DS 3.1 Planeación del desempeño y la capacidad DS 3.2 Capacidad y desempeño actual DS 3.3 Capacidad y desempeño futuros		
Listas de control de ITIL v3	DS- Informe de la capacidad		
Disparador:	Incremento en las necesidades de los usuarios respecto a los servicios de TI		
Insumos y Proveedores:	**Entrada**	**Proveedor**	**Tipo de Proveedor**
	Portafolio de Servicios	Área de soporte	Interno
	Paquete del Diseño del Servicio	Área de Infraestructura o Área de Software	Interno
	Registro de Incidentes	Área de Soporte	Interno
	Registro de Problemas	Área de Infraestructura o Área de Software	Interno
Productos y Clientes:	**Producto**	**Cliente**	**Tipo de Cliente**
	Informe de la Capacidad	Unidad de Tecnologías de la Información	Interno

Tipo de Proceso:	Adjetivo
Responsable del Proceso:	Área de Infraestructura
Métrica	Frecuencia de los pronósticos de desempeño y capacidad Diferencia entre los activos actuales y los activos requeridos

Tabla 2-14: Gestión de la Capacidad

2.3.3.4.10.1. Diagrama de Flujo de la Gestión de la Capacidad

En la Fig. 2-10 el diagrama de flujo de la Gestión de la Capacidad.

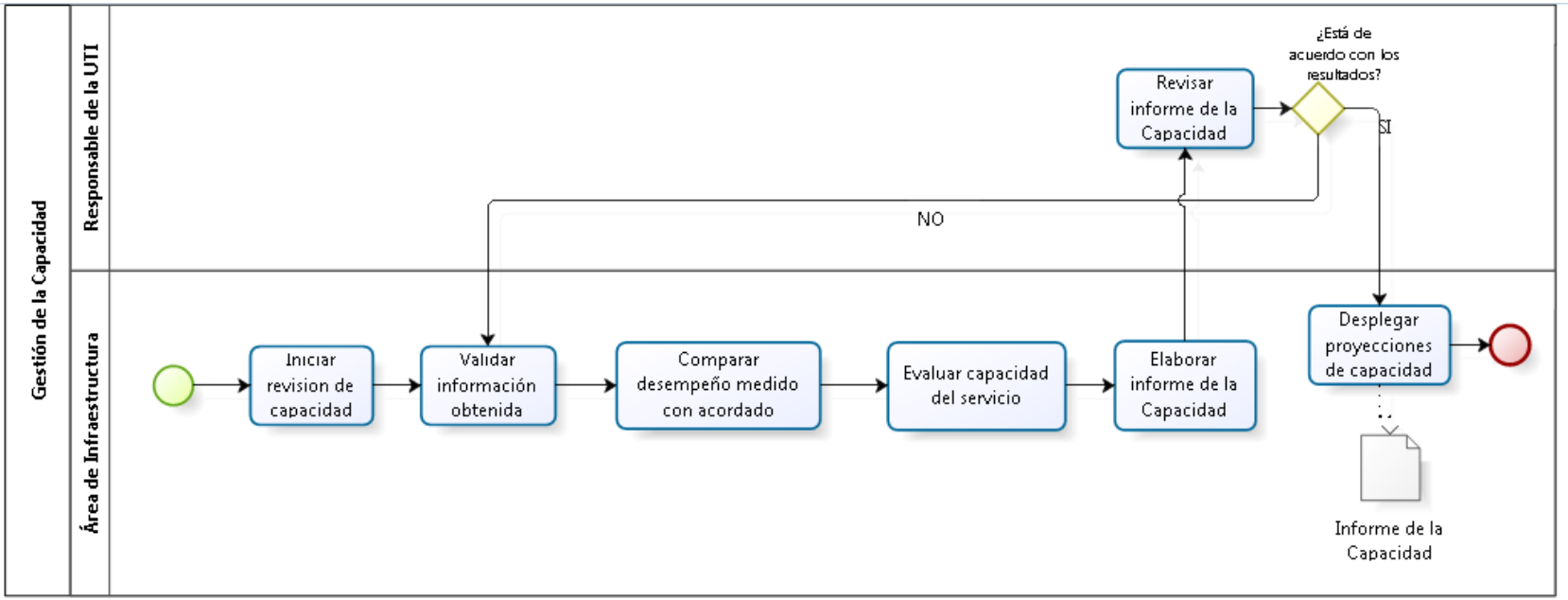


Figura 2-10: Diagrama de Gestión de Capacidad.

2.3.4. PROCEDIMIENTO DE SEGURIDAD PARA CONTROL DE ACCESO

2.3.4.1. Objeto

Establecer una metodología para documentar, registrar, monitorear y controlar las operaciones de los sistemas, todos los accesos a los mismos y mantener un monitoreo, registrando todas las eventualidades a nivel de la institución.

2.3.4.2. Alcance

Mantener un control y monitoreo del acceso a las aplicaciones e información de la institución.

2.3.4.3. Definiciones

Remitirse al numeral 2.3.3.3.

2.3.4.4. Desarrollo del Proceso

2.3.4.4.1. Autenticación de Usuarios para Conexiones Externas

En la Tabla 2-15 se encuentra el detalle del procedimiento Autenticación de Usuarios para Conexiones Externas:

Nro. Hito	77

<table>
<tr><td>Detalle Hito EGSI en GPR</td><td colspan="3">Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR)</td></tr>
<tr><td>Objetivo de control de COBIT</td><td colspan="3">DS 5.11 Intercambio de datos sensitivos</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">OS - Registro de Incidente
TS - Solicitud de cambio</td></tr>
<tr><td>Disparador:</td><td colspan="3">Necesidad de modificación o elaboración de un servicio</td></tr>
<tr><td>Insumos y Proveedores</td><td>Entrada</td><td>Proveedor</td><td>Tipo de Proveedor</td></tr>
<tr><td></td><td>Información del servicio</td><td>Responsable del servicio</td><td>Interno</td></tr>
<tr><td>Productos y Clientes</td><td>Producto</td><td>Cliente</td><td>Tipo de Cliente</td></tr>
<tr><td></td><td>Portafolio de Servicios Actualizado</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Soporte</td></tr>
<tr><td>Métrica</td><td colspan="3">Número de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación</td></tr>
</table>

Tabla 2-15: Autenticación de Usuarios para Conexión Externas

2.3.4.4.1.1. Diagrama de Flujo de Autenticación de Usuarios para Conexiones Externas

Remitirse al numeral 2.3.3.4.1.1

2.3.4.4.2. Identificación de Equipos en las Redes

En la Tabla 2-16 se encuentra el detalle del procedimiento Identificación de Equipos en la Redes:

<table>
<tr><td>Nro. Hito</td><td colspan="3">78</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td colspan="3">Identificar y documentar los equipos que se encuentran en las redes.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td colspan="3">DS 9.2 Identificación y mantenimiento de elementos de configuración</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">TS - Sistema de gestión de la configuración (CMS) / Base de datos de la configuración (CMDB)</td></tr>
<tr><td>Disparador:</td><td colspan="3">Modificación del inventario de equipos informáticos de la institución.</td></tr>
<tr><td>Insumos y Proveedores</td><td colspan="3"><table><tr><td>Entrada</td><td>Proveedor</td><td>Tipo de Proveedor</td></tr><tr><td>Información del inventario</td><td>Área de Soporte</td><td>Interno</td></tr></table></td></tr>
<tr><td>Productos y Clientes</td><td colspan="3"><table><tr><td>Producto</td><td>Cliente</td><td>Tipo de Cliente</td></tr><tr><td>Informe de control contra código malicioso.</td><td>Unidad de Tecnologías de la Información.</td><td>Interno</td></tr></table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Soporte</td></tr>
<tr><td>Métrica</td><td colspan="3">Número y tipo de código malicioso prevenido.</td></tr>
</table>

	Número de equipos Registrados vs Equipos dados de baja.

Tabla 2-16: Identificación de Equipos en las Redes

2.3.4.4.2.1. Diagrama de Flujo de Identificación de Equipos en las Redes

Remitirse al numeral 2.3.3.4.2.1

2.3.4.4.3. Protección de los Puertos de Configuración y Diagnóstico Remoto

En la Tabla 2-17 se encuentra el detalle del procedimiento Protección de los Puertos de Configuración y Diagnóstico Remoto:

Nro. Hito	79
Detalle Hito EGSI en GPR	Los puertos, servicios (p.ej. FTP) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.
Objetivo de control de COBIT	DS 5.7 Protección de la tecnología de seguridad DS 5.9 Prevención, detección y corrección de software malicioso DS 5.11 Intercambio de datos sensitivos
Listas de control de ITIL v3	TS - Solicitud de cambio
Disparador:	Descubrimiento de puertos habilitados y no usados del firewall

Insumos y Proveedores:	**Entrada**	**Proveedor**	**Tipo de Proveedor**
	Paquete del diseño del servicio	Área de Infraestructura o Área de Software	Interno
Productos y Clientes:	**Producto**	**Cliente**	**Tipo de Cliente**
	Solicitud de cambio	Unidad de Tecnologías de la Información	Interno
Tipo de Proceso:	Adjetivo		
Responsable del Proceso:	Área de Infraestructura		
Métrica:	Número y tipo de violaciones de acceso reales y sospechadas. Número de puertos inseguros encontrados vs puertos cerrados.		

Tabla 2-17: Protección de los puertos de configuración y diagnostico Remoto

2.3.4.4.3.1. Diagrama de Flujo de la Protección de los Puertos de Configuración y Diagnóstico Remoto

En la Fig. 2-11 el diagrama de flujo de la Protección de los Puertos de Configuración y Diagnóstico Remoto.

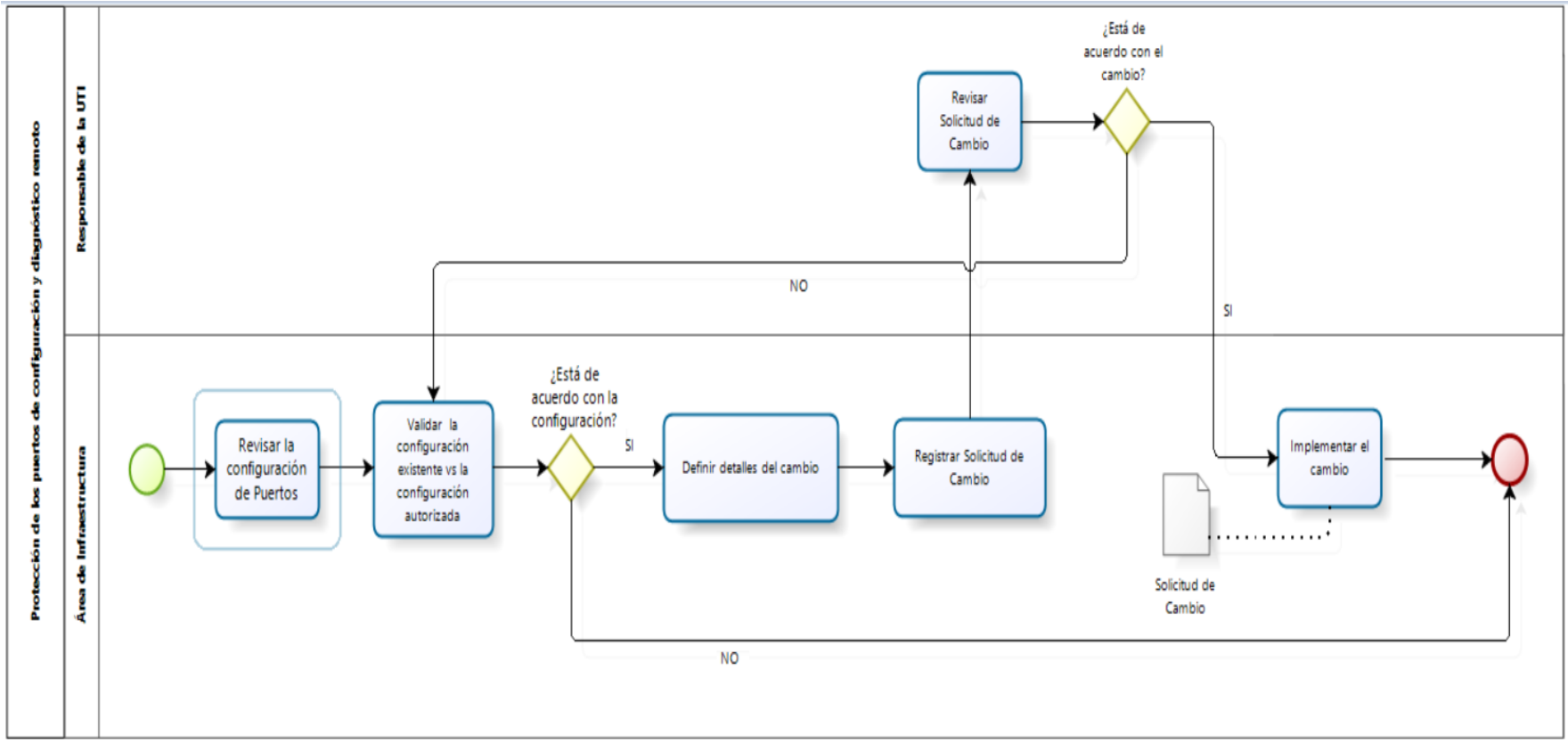


Figura 2-11: Diagrama de Protección de los Puertos de Configuración y Diagnostico Remoto

2.3.4.4.4. Separación en las Redes

En la Tabla 2-18 se encuentra el detalle del procedimiento Separación en las Redes:

<table>
<tr><td>Nro. Hito</td><td>80</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td>Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>DS 5.7 Protección de la tecnología de seguridad
DS 5.11 Intercambio de datos sensitivos</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>DS - Informe de la capacidad</td></tr>
<tr><td>Disparador:</td><td>Incremento en las necesidades de los usuarios respecto a los servicios de TI</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Portafolio de Servicios</td><td>Área de soporte</td><td>Interno</td></tr>
<tr><td>Paquete del Diseño del Servicio</td><td>Área de Infraestructura o Área de Software</td><td>Interno</td></tr>
<tr><td>Registro de Incidentes</td><td>Área de Soporte</td><td>Interno</td></tr>
<tr><td>Registro de Problemas</td><td>Área de Infraestructura o Área de Software</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes:</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Informe de la Capacidad</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Infraestructura</td></tr>
</table>

Métrica	Número de direcciones IP no autorizadas, puertos y tipos de tráfico no autorizados en activos críticos de la institución

Tabla 2-18: Separación en las Redes

2.3.4.4.4.1. Diagrama de Flujo de Separación en las Redes

Remitirse al numeral 2.3.3.4.10.1

2.3.4.4.5. Control del Enrutamiento de la Red

En la Tabla 2-19 se encuentra el detalle del procedimiento Control del Enrutamiento de la Red:

Nro. Hito	81		
Detalle Hito EGSI en GPR	Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.		
Objetivo de control de COBIT	DS 5.7 Protección de la tecnología de seguridad DS 5.11 Intercambio de datos sensitivos		
Listas de control de ITIL v3	DS - Paquete del diseño del servicio		
Disparador:	Necesidad de modificación o elaboración de un servicio		
Insumos y Proveedores	**Entrada**	**Proveedor**	**Tipo de Proveedor**

	Información del servicio	Responsable del servicio	Interno	
Productos y Clientes	**Producto**	**Cliente**	**Tipo de Cliente**	
	Portafolio de Servicios Actualizado	Unidad de Tecnologías de la Información	Interno	
Tipo de Proceso:	Adjetivo			
Responsable del Proceso:	Área de Soporte			
Métrica	Número de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación			

Tabla 2-19: Control de Enrutamiento de la Red.

2.3.4.4.5.1. Diagrama de Flujo de Control de Enrutamiento de la Red

Remitirse al numeral 2.3.3.4.1.1

2.3.4.4.6. Procedimiento de Registro de Inicio Seguro

En la Tabla 2-20 se encuentra el detalle del Procedimiento de Registro de Inicio Seguro:

Nro. Hito	82,83,84,85,86,87,88,89

Detalle Hito EGSI en GPR	• Autenticar usuarios autorizados, de acuerdo a la política de control de acceso a la institución, que deberá estar documentada, definida y socializada. • Llevar un registro de definición para el uso de privilegios especiales del sistema. • Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema. • Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios. • Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución. • Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente. • Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos. • Limitar el tiempo de dilación antes de permitir o rechazar más intentos al registro del inicio sin autorización específica.
Objetivo de control de COBIT	DS 5.4 Administración de cuentas del usuario DS 5.7 Protección de la tecnología de la seguridad
Listas de control de ITIL v3	OS - Requerimiento de servicio
Disparador:	Requerimiento de ingresar al sistema

<table>
<tr><td>Insumos y Proveedores:</td><td colspan="3"><table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del usuario</td><td>Jefe inmediato</td><td>Interno</td></tr>
<tr><td>Información del usuario</td><td>Unidad de Talento Humano</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Productos y Clientes:</td><td colspan="3"><table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Requerimiento de Servicio</td><td>Usuario</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Soporte</td></tr>
<tr><td>Métrica:</td><td colspan="3">Porcentaje de usuarios que no cumplen con los estándares de contraseñas.</td></tr>
</table>

Tabla 2-20: Procedimiento de Registro de Inicio Seguro

2.3.4.4.6.1. Diagrama de Flujo de Procedimiento de Registro de Inicio Seguro

En la Fig. 2-12 el diagrama de flujo de Procedimiento de Registro de Inicio Seguro.

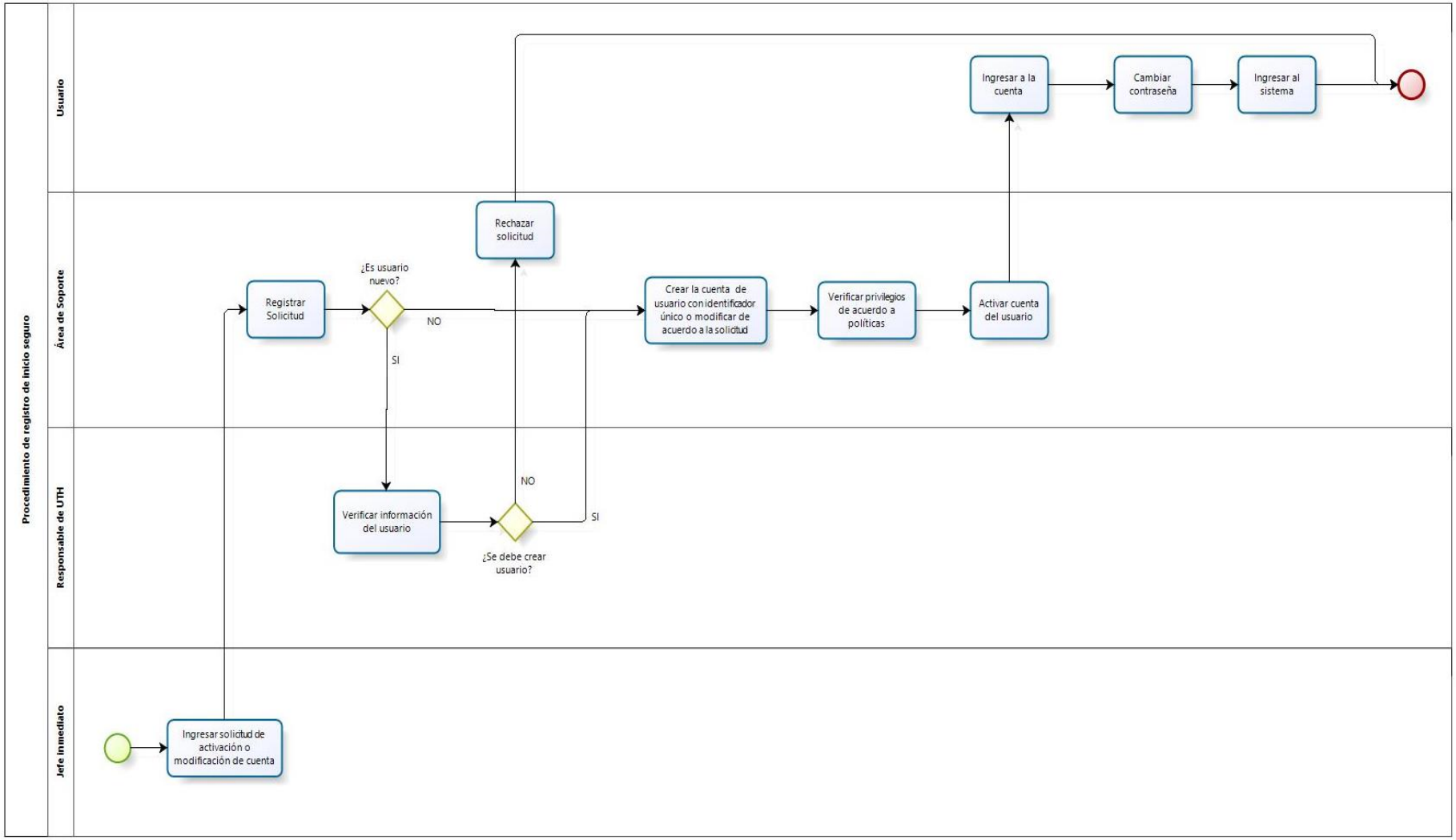


Figura 2-12: Diagrama de Procedimiento de Registro de Inicio Seguro

2.3.4.4.7. Identificación y Autenticación de Usuarios

En la Tabla 2-21 se encuentra el detalle del procedimiento Identificación y Autenticación de Usuarios:

<table>
<tr><td>Nro. Hito</td><td colspan="3">90,91,92,93</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td colspan="3">• Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución.
• Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado.
• Evitar el uso de usuarios genéricos.
• Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td colspan="3">DS 5.3 Administración de identidad</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">OS - Requerimiento de servicio</td></tr>
<tr><td>Disparador:</td><td colspan="3">Requerimiento de ingresar al sistema</td></tr>
<tr><td>Insumos y Proveedores:</td><td colspan="3"><table><tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr><tr><td>Información del usuario</td><td>Jefe inmediato</td><td>Interno</td></tr></table></td></tr>
</table>

	Información del usuario	Unidad de Talento Humano	Interno
Productos y Clientes:	**Producto**	**Cliente**	**Tipo de Cliente**
	Requerimiento de Servicio	Usuario	Interno
Tipo de Proceso:	Adjetivo		
Responsable del Proceso:	Área de Soporte		
Métrica:	Porcentaje de usuarios que no cumplen con los estándares de contraseñas.		

Tabla 2-21: Identificación y Autenticación de Usuarios

2.3.4.4.7.1. Diagrama de Flujo de Identificación y Autenticación de Usuarios.

Remitirse al numeral 2.3.3.4.6.1

2.3.4.4.8. Sistema de Gestión de Contraseñas

En la Tabla 2-22 se encuentra el detalle del procedimiento Sistema de Gestión de Contraseñas:

Nro. Hito	94,95,96
Detalle Hito EGSI en GPR	• Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible.

<table>
<tr><td></td><td>

Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad.
Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión.

</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>DS 5.4 Administración de cuentas del usuario</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Requerimiento de servicio</td></tr>
<tr><td>Disparador:</td><td>Requerimiento de ingresar al sistema</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del usuario</td><td>Jefe inmediato</td><td>Interno</td></tr>
<tr><td>Información del usuario</td><td>Unidad de Talento Humano</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes:</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Requerimiento de Servicio</td><td>Usuario</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica:</td><td>Porcentaje de usuarios que no cumplen con los estándares de contraseñas.</td></tr>
</table>

Tabla 2-22: Gestión de Contraseñas

2.3.4.4.8.1. Diagrama de Flujo de Gestión de Contraseñas.

Remitirse al numeral 2.3.3.4.6.1

2.3.4.4.9. Computación y Comunicaciones Móviles

En la Tabla 2-23 se encuentra el detalle del procedimiento Computación y Comunicaciones Móviles.

Nro. Hito	97		
Detalle Hito EGSI en GPR	Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo.		
Objetivo de control de COBIT	PO 6.2 Riesgo corporativo y marco de referencia de control interno de TI DS 5.2 Plan de seguridad de TI DS 5.7 Protección de la tecnología de seguridad		
Listas de control de ITIL v3	No aplica.		
Disparador:	Requerimiento de ingresar al sistema		
Insumos y Proveedores:	**Entrada**	**Proveedor**	**Tipo de Proveedor**
	Información del usuario	Jefe inmediato	Interno
	Información del usuario	Unidad de Talento Humano	Interno
Productos y Clientes:	**Producto**	**Cliente**	**Tipo de Cliente**
	Requerimiento de Servicio	Usuario	Interno

Tipo de Proceso:	Adjetivo
Responsable del Proceso:	Área de Soporte
Métrica:	Porcentaje de interesados que entienden las políticas de TI. Número de ocasiones en que se puso en riesgo la información confidencial

Tabla 2-23: Computación y Comunicaciones Móviles

2.3.4.4.9.1. Diagrama de Flujo de Computación y Comunicaciones Móviles

Remitirse al numeral 2.3.3.4.6.1

2.3.4.4.10. Trabajo Remoto

En la Tabla 2-24 se encuentra el detalle del procedimiento Trabajo Remoto.

Nro. Hito	98,99
Detalle Hito EGSI en GPR	• No se permite el uso de equipo de propiedad privada, que no esté bajo el control y monitoreo de la institución. • Deberá considerarse la protección de antivirus y reglas del Firewall.
Objetivo de control de COBIT	PO 3.4 Estándares tecnológicos PO 6.2 Riesgo corporativo y marco de referencia de control de TI DS 5.2 Plan de seguridad de TI DS 5.3 Administración de identidad

<table>
<tr><td></td><td colspan="3">DS 5.7 Protección de la tecnología de seguridad</td></tr>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">No aplica</td></tr>
<tr><td>Disparador:</td><td colspan="3">Necesidad de atención de requerimiento de servicio</td></tr>
<tr><td>Insumos y Proveedores:</td><td colspan="3"><table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del requerimiento</td><td>Usuario</td><td>Interno o Externo</td></tr>
</table></td></tr>
<tr><td>Productos y Clientes:</td><td colspan="3"><table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Requerimiento de Servicio</td><td>Usuario</td><td>Interno o Externo</td></tr>
</table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Soporte</td></tr>
<tr><td>Métrica:</td><td colspan="3">Número de direcciones IP no autorizadas, puertos y tipos de tráfico denegados.
Frecuencia y revisión del tipo de eventos de seguridad a ser monitoreados.</td></tr>
</table>

Tabla 2-24: Trabajo Remoto

2.3.4.4.10.1. Diagrama de Flujo del Trabajo Remoto

En la Fig. 2-13 el diagrama de flujo del Trabajo Remoto.

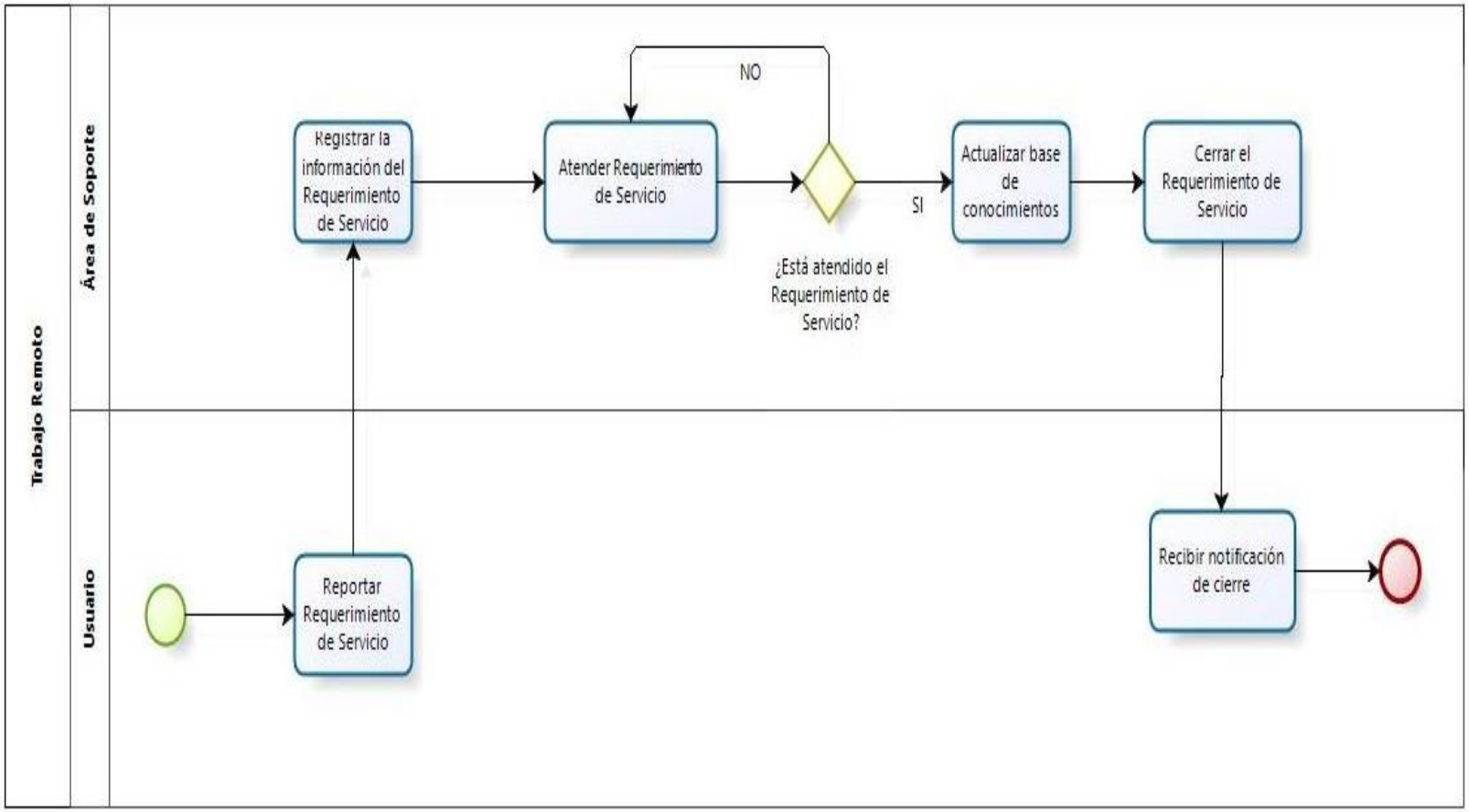


Figura 2-13: Diagrama de Trabajo Remoto

2.3.4.4.11. Gestión de Contraseñas para Usuarios

En la Tabla 2-25 se encuentra el detalle del procedimiento Gestión de Contraseñas para Usuarios.

<table>
<tr><td>Nro. Hito</td><td>100</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td>Establecer un proceso formal para la asignación y cambio de contraseñas.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>DS 5.3 Administración de identidad</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Requerimiento de servicio</td></tr>
<tr><td>Disparador:</td><td>Requerimiento de ingresar al sistema</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del usuario</td><td>Jefe inmediato</td><td>Interno</td></tr>
<tr><td>Información del usuario</td><td>Unidad de Talento Humano</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes:</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Requerimiento de Servicio</td><td>Usuario</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica:</td><td>Porcentaje de usuarios que no cumplen con los estándares de contraseñas.</td></tr>
</table>

Tabla 2-25: Gestión de Contraseñas para Usuarios

2.3.4.4.11.1. Diagrama de Gestión de Contraseñas para Usuarios

Remitirse al numeral 2.3.3.4.6.1

2.3.4.4.12. Uso de Contraseñas

En la Tabla 2-26 se encuentra el detalle del procedimiento Uso de Contraseñas.

Nro. Hito	101,102,103,104,105
Detalle Hito EGSI en GPR	• Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignadas. • Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta. • Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables. • Controlar el cambio periódico de contraseñas de los usuarios. • Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.
Objetivo de control de COBIT	PO 6.2 Riesgo corporativo y marco de referencia de control de TI DS 5.7 Protección de la tecnología de seguridad

<table>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">No aplica</td></tr>
<tr><td>Disparador:</td><td colspan="3">Requerimiento de ingresar al sistema</td></tr>
<tr><td>Insumos y Proveedores:</td><td colspan="3"><table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del usuario</td><td>Jefe inmediato</td><td>Interno</td></tr>
<tr><td>Información del usuario</td><td>Unidad de Talento Humano</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Productos y Clientes:</td><td colspan="3"><table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Requerimiento de Servicio</td><td>Usuario</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Soporte</td></tr>
<tr><td>Métrica:</td><td colspan="3">Porcentaje de usuarios que no cumplen con los estándares de contraseñas.</td></tr>
</table>

Tabla 2-26: Uso de Contraseñas.

2.3.4.4.12.1. Diagrama de Uso de Contraseñas

Remitirse al numeral 2.3.3.4.6.1

2.3.4.4.13. Equipos de Usuarios Desatendidos

En la Tabla 2-27 se encuentra el detalle del procedimiento Usuarios Desatendidos.

<table>
<tr><td>Nro. Hito</td><td>106</td></tr>
<tr><td>Detalle Hito EGSI en GPR</td><td>Implementar medidas para que, en un determinado tiempo (p. ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, éste se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>PO 6.2 Riesgo corporativo y marco de referencia de control de TI
DS 5.7 Protección de la tecnología de seguridad</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Registro de Incidente</td></tr>
<tr><td>Disparador:</td><td>Necesidad de modificación o elaboración de un servicio</td></tr>
<tr><td>Insumos y Proveedores</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del servicio</td><td>Responsable del servicio</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Portafolio de Servicios Actualizado</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica</td><td>Número de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación</td></tr>
</table>

Tabla 2-27: Usuarios Desatendidos.

2.3.4.4.13.1. Diagrama de Usuarios Desatendidos

Remitirse al numeral 2.3.3.4.1.1

2.3.4.4.14. Política de Puesto de Trabajo de Despejado y Pantalla Limpia

En la Tabla 2-28 se encuentra el detalle del procedimiento Política de Puesto de Trabajo de Despejado y Pantalla Limpia.

Nro. Hito	107,108,109,110,111,112
Detalle Hito EGSI en GPR	• Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina. • Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave. • Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas. • Retirar información sensible una vez que ha sido impresa. • Retirar información sensible, como las claves, de sus escritorios y pantallas. • Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.
Objetivo de control de COBIT	PO 6.2 Riesgo corporativo y marco de referencia de control de TI DS 5.7 Protección de la tecnología de seguridad

<table>
<tr><td>Listas de control de ITIL v3</td><td colspan="3">OS - Registro de Incidente</td></tr>
<tr><td>Disparador:</td><td colspan="3">Necesidad de modificación o elaboración de un servicio</td></tr>
<tr><td>Insumos y Proveedores</td><td colspan="3"><table>
<tr><td>Entrada</td><td>Proveedor</td><td>Tipo de Proveedor</td></tr>
<tr><td>Información del servicio</td><td>Responsable del servicio</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Productos y Clientes</td><td colspan="3"><table>
<tr><td>Producto</td><td>Cliente</td><td>Tipo de Cliente</td></tr>
<tr><td>Portafolio de Servicios Actualizado</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
</table></td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Área de Soporte</td></tr>
<tr><td>Métrica</td><td colspan="3">Número de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación</td></tr>
</table>

Tabla 2-28: Puesto de Trabajo de Despejado y Pantalla Limpia.

2.3.4.4.14.1. Diagrama de Puesto de Trabajo de Despejado y Pantalla Limpia

Remitirse al numeral 2.3.3.4.1.1

2.3.5. PROCEDIMIENTO DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

2.3.5.1. Objeto

Establecer una metodología para documentar, registrar y controlar todos los mantenimientos de los sistemas de información.

2.3.5.2. Alcance

Mantener un registro y control de todos los mantenimientos que sean realizados en los sistemas de la información.

2.3.5.3. Definiciones

Remitirse al numeral 2.3.3.3.

2.3.5.4. Desarrollo del Proceso

2.3.5.4.1. Análisis y Especificaciones de los Requerimientos de Seguridad

En la Tabla 2-29 se encuentra el detalle del procedimiento Análisis y Especificaciones de los Requerimientos de Seguridad.

Nro. Hito	113,114
Detalle Hito EGSI en GPR	• Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc. • Definir los controles apropiados, tanto automatizados como manuales.

<table>
<tr><td>Objetivo de control de COBIT</td><td>AI 1.2 Reporte de análisis de riesgos
AI 2.4 Seguridad y disponibilidad de las aplicaciones
AI 3.2 Protección y disponibilidad del recurso de infraestructura</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>DS - Paquete del diseño del servicio</td></tr>
<tr><td>Disparador:</td><td>Necesidad de modificación o elaboración de un servicio</td></tr>
<tr><td>Insumos y Proveedores</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Información del servicio</td><td>Responsable del servicio</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Portafolio de Servicios Actualizado</td><td>Unidad de Tecnologías de la Información</td><td>Interno</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica</td><td>Porcentaje de proyectos de software aplicativo con plan de aseguramiento de calidad del software desarrollado y ejecutado
Porcentaje de proyectos de software aplicativo con revisión y aprobación adecuadas de la conformidad con los estándares de desarrollo</td></tr>
</table>

Tabla 2-29: Análisis y Especificaciones de los Requerimientos de Seguridad

2.3.5.4.1.1. Diagrama de Análisis y Especificaciones de los Requerimientos de Seguridad.

Remitirse al numeral 2.3.3.4.1.1

2.3.5.5. ANEXOS

No aplica

2.3.6. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

2.3.6.1. Objeto

Establecer una metodología para documentar, registrar y controlar todos los incidentes de los sistemas de información.

2.3.6.2. Alcance

Mantener un registro y control de todos los incidentes que ocurran en los sistemas de la información.

2.3.6.3. Definiciones

Remitirse al numeral 2.3.3.3.

2.3.6.4. Desarrollo del Proceso

2.3.6.4.1. Reporte sobre los Eventos de Seguridad de la Información

En la Tabla 2-30 se encuentra el detalle del procedimiento Reporte sobre los Eventos de Seguridad de la Información.

Nro. Hito	115,116,117,118,119,120,121,122,123,124,125

Detalle Hito EGSI en GPR	• Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información, junto con un procedimiento de escalada y respuesta ante el incidente. • Identificar el incidente. • Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". • Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto. • Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente. • Notificar al Oficial de Seguridad de la Información de la Institución. • Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad. • Asignar una prioridad de atención al incidente, en el caso de que se produjeran varios en forma simultánea. • Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas, • Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. • Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.

<table>
<tr><td></td><td>

- Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.

</td></tr>
<tr><td>Objetivo de control de COBIT</td><td>PO 9.3 Identificación de eventos
DS 5.6 Definición de incidente de seguridad
DS 8.2 Registro de consultas de clientes</td></tr>
<tr><td>Listas de control de ITIL v3</td><td>OS - Registro de incidente</td></tr>
<tr><td>Disparador:</td><td>Registro de incidente relacionado con seguridad de la información</td></tr>
<tr><td>Insumos y Proveedores:</td><td>
<table>
<tr><th>Entrada</th><th>Proveedor</th><th>Tipo de Proveedor</th></tr>
<tr><td>Requerimiento de Servicio</td><td>Área de Soporte</td><td>Interno o Externo</td></tr>
</table>
</td></tr>
<tr><td>Productos y Clientes:</td><td>
<table>
<tr><th>Producto</th><th>Cliente</th><th>Tipo de Cliente</th></tr>
<tr><td>Registro de incidente de seguridad de la información</td><td>Usuario</td><td>Interno o Externo</td></tr>
</table>
</td></tr>
<tr><td>Tipo de Proceso:</td><td>Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td>Área de Soporte</td></tr>
<tr><td>Métrica</td><td>Porcentaje de incidentes relacionado con seguridad de la información de TI identificados que han sido evaluados</td></tr>
</table>

Tabla 2-30: Reporte sobre los eventos de seguridad de la información.

2.3.6.4.1.1. Diagrama de Flujo del Reporte sobre los Eventos de Seguridad de la Información

En la Fig. 2-14 el diagrama de flujo del Reporte sobre los Eventos de Seguridad de la Información.

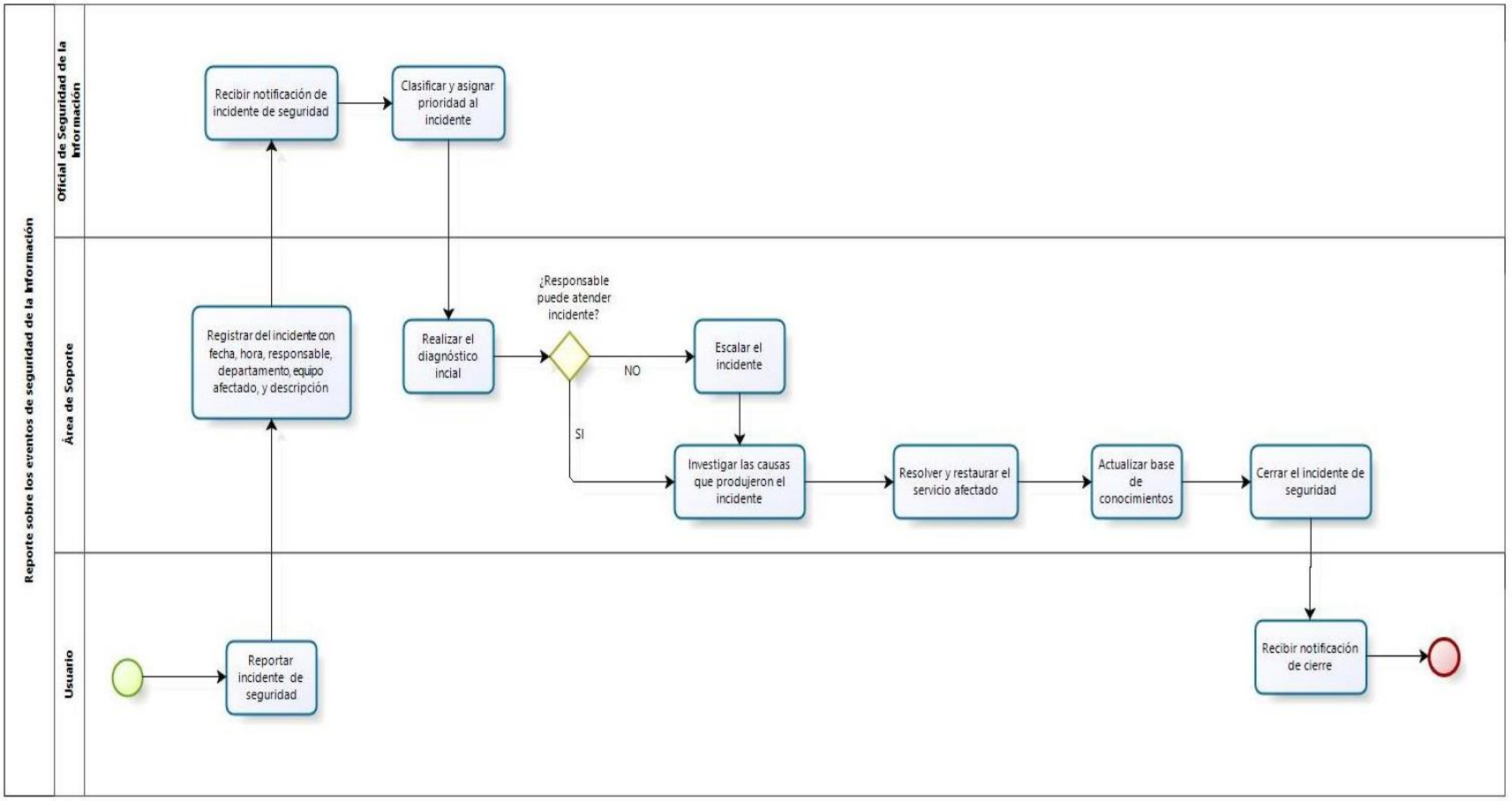


Figura 2-14: Diagrama de Reporte sobre los eventos de Seguridad de la Información

CAPÍTULO 3: VALIDACIÓN DE LA GUÍA

3.1. DESCRIPCIÓN DE LA ORGANIZACIÓN

De acuerdo al alcance del proyecto, la Guía se ha desarrollado para entidades del sector público de la Administración Pública Central, por lo que la validación se realiza con la Agencia de Regulación y Control de Electricidad (ARCONEL), dependiente del Ministerio de Electricidad y Energías Renovables (MEER).

Mediante la Ley Orgánica del Servicio Público de Energía Eléctrica expedida en el Tercer Suplemento, Registro Oficial No. 418 de 16 de enero de 2015, se prevé la creación de la Agencia de Regulación y Control de Electricidad (ARCONEL) como parte de la estructura institucional del Sector Eléctrico en reemplazo del actual CONELEC.

ARCONEL como ente regulador del sector eléctrico, administra información relacionada a toda la comercialización de energía eléctrica del país y siendo una entidad del sector público, también está obligada a precautelar la seguridad de la información. ARCONEL es una entidad que depende de la Función Ejecutiva y debe atender las directrices de la SNAP e implantar el EGSI. Por esta razón, se la utilizará para validar la guía propuesta en este proyecto.

La Unidad de Gestión de Tecnologías de la Información (UGTI) de ARCONEL se encuentra conformada por la Jefatura y siete funcionarios dedicados fundamentalmente a las áreas de Soporte, Infraestructura y Desarrollo; sin que ninguna de estas áreas se encuentre definida formalmente mediante procesos o procedimientos.

3.2. VALIDACIÓN

A continuación se realizará la aplicación de la Guía propuesta en este proyecto:

3.2.1. DETERMINACIÓN DEL ESTADO INICIAL DE LA SEGURIDAD DE LA INFORMACIÓN EN ARCONEL

A continuación se elaboran las matrices de definición de la situación actual de la implantación de EGSI en ARCONEL; la institución realizó modificaciones sobre el formato propuesto con las consideraciones que creyeron necesarias y para su llenado la matriz fue acompañada de un instructivo realizado por la Dirección de Planificación y el Oficial de Seguridad de la Información.

En la figura 3-1 se muestra la aplicación de la matriz del capítulo 6 Gestión de Comunicaciones y Operaciones, subtítulo 6.6 Monitoreo y revisión de los servicios por terceros del EGSI.

En la figura 3-2 se muestra la aplicación de la matriz del capítulo 7 Control de Acceso, subtítulo 7.6 Uso de contraseñas.

En la figura 3-3 se muestra la aplicación de la matriz del capítulo 8 Adquisición, desarrollo y mantenimiento de sistemas de información, subtítulo 8.1 Análisis y especificaciones de los requerimientos de seguridad.

En la figura 3-4 se muestra la aplicación de la matriz del capítulo 9 Gestión de los incidentes de la seguridad de la Información, subtítulo 9.1 Reporte sobre los eventos de seguridad de la Información.

Luego de realizar el llenado de la Matriz de Situación Inicial por cada subtitulo del EGSI en la UGTI de ARCONEL se pueden agrupar las actividades definidas de la siguiente manera:

a) Actividades a corto plazo

- Evidencia: Se refieren a aquellas actividades que involucran la presentación de informes técnicos con evidencia sobre la ejecución del control solicitado. Estas actividades pueden considerarse como la certificación de que el área ha implementado el control ya sea de una manera parcial o total, pero suficiente para la institución.

- Tarea: Se refieren a aquellas actividades que involucran la implantación del control solicitado. Estas actividades pueden considerarse cuando el área no ha implementado el control de ninguna manera

- Sustento: Se refieren a aquellas actividades que involucran la presentación de informes técnicos son un sustento suficiente de que el control solicitado no es posible aplicar en la institución. Estas actividades pueden considerarse cuando el control depende de medios externos a la institución o por limitantes tecnológicas no es posible su aplicación.

- Formalización: Se refieren a aquellas actividades que involucran la definición de documentos formales para respaldar con firmas de autorización de accesos o niveles de permisos. Estas actividades pueden considerarse como la base para los procedimientos que se requieren definir.

b) Actividades a largo plazo

- Éstas fueron descritas por la institución como una Solución Integral para todos los capítulos del EGSI se define como la implementación de los procedimientos. En todas las matrices se determina los plazos para la elaboración, validación, despliegue, aplicación y validación del procedimiento del respectivo Capitulo.

La aplicación de las Matrices de Definición de la Situación Actual de la Implantación del EGSI del Capítulo 6. Comunicaciones y Operaciones, contenidas en el Anexo B presentaron los siguientes resultados:

a) De un total de 19 actividades definidas en éste Capítulo, ocho fueron de tipo Evidencia, siete fueron de tipo Tarea, una de tipo Sustento y tres de tipo Formalización. Se puede entonces suponer que la gestión de la Comunicación y Operaciones de la UGTI posee un nivel de madurez aceptable en relación a la seguridad de la información, ya que casi la mitad de las actividades planteadas se refieren a evidencias de cumplimiento.

b) Dado que no existe ningún procedimiento formal referente a la gestión de la Comunicación y Operaciones, todas las matrices de éste capítulo en las actividades a largo plazo se refieren al proceso de implementación de dicho procedimiento.

c) Los plazos definidos dependieron de qué grupo de la UGTI debe realizar la ejecución de las actividades, siendo en este capítulo predominante el área de Infraestructura, y por la cantidad de personal de la mencionada área, los plazos de las actividades fueron definidas en secuencia.

La aplicación de las Matrices de Definición de la Situación Inicial del Capítulo 7. Control de Acceso, contenidas en el Anexo C presentaron los siguientes resultados:

a) De un total de 34 actividades definidas en éste Capítulo, diez fueron de tipo Evidencia, diecisiete fueron de tipo Tarea, tres de tipo Sustento y cuatro de tipo Formalización. Se puede entonces suponer que la gestión del Control de Acceso de la UGTI posee un nivel de madurez bajo en relación a la seguridad de la información, ya que casi la mitad de las actividades planteadas se refieren a tareas de implementación de los controles.

b) Dado que no existe ningún procedimiento formal referente a la gestión del Control de Acceso, todas las matrices de éste capítulo en las actividades a largo plazo se refieren al proceso de implementación de dicho procedimiento.

c) Los plazos definidos dependieron de qué grupo de la UGTI debe realizar la ejecución de las actividades, siendo en este capítulo predominante el área de Infraestructura, y por la cantidad de personal de la mencionada área, los plazos de las actividades fueron definidas en secuencia. Adicionalmente la implementación de estos controles afectaría directamente a los usuarios finales por lo que antes se recomendó incluir el proceso de socialización del EGSI antes de la ejecución del cronograma de éste Capítulo.

La aplicación de la Matriz de Definición de la Situación Inicial del Capítulo 8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información de la figura 3-3, presentó los siguientes resultados:

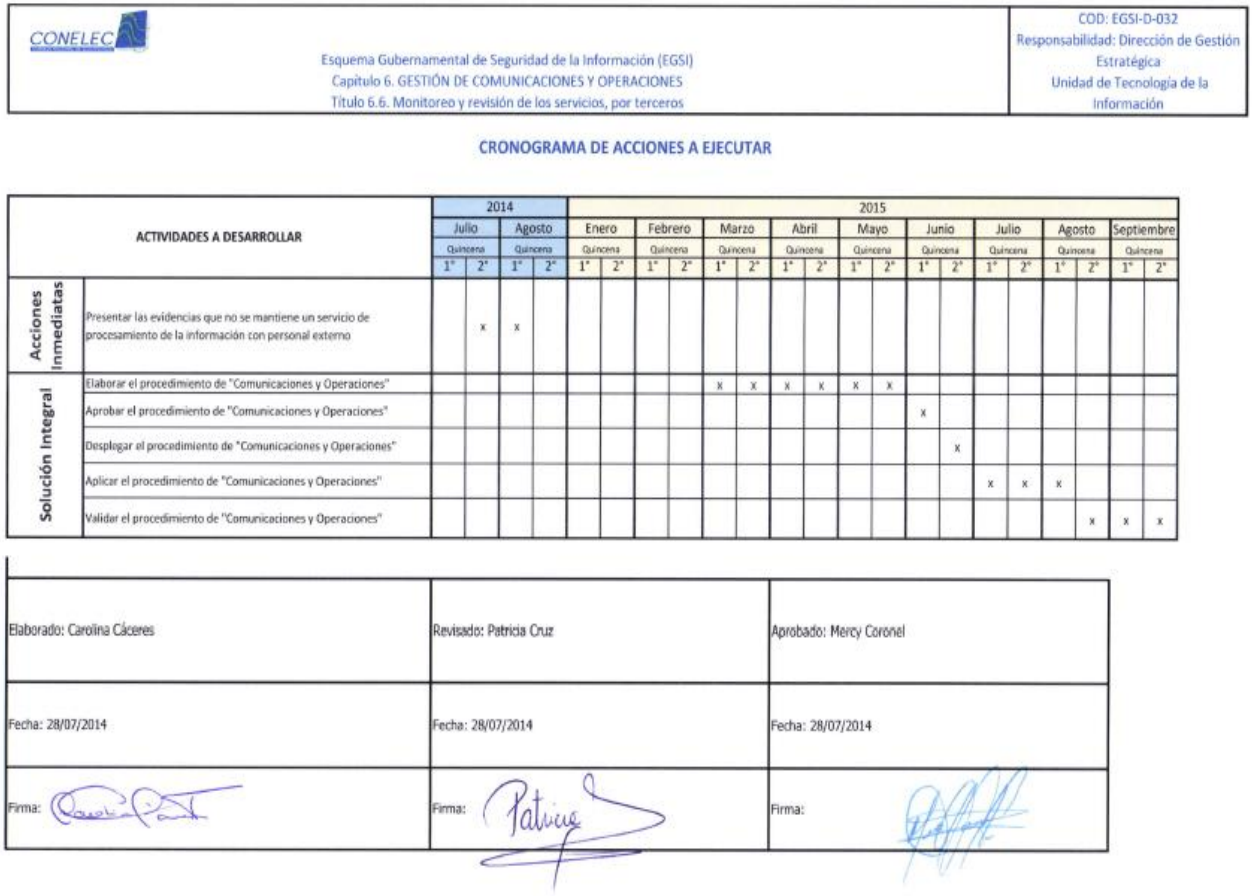
a) No se definieron actividades de corto plazo ya que los hitos prioritarios (siendo tres en este caso) de este capítulo no se refieren a implementación de controles efectivos sino más bien a una definición formal del procedimiento de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. Se incluyó entonces en las actividades a largo plazo la implementación del mencionado procedimiento.

b) Los plazos en este caso solamente dependieron del área de Desarrollo por lo tanto no presentaron restricciones.

La aplicación de la Matriz de Definición de la Situación Inicial del Capítulo 9. Gestión de los Incidentes de Seguridad de la Información de la figura 3-4 presentó los siguientes resultados:

a) De un total de 2 actividades definidas en éste Capítulo, una fue de tipo Tarea y una de tipo Formalización. La aplicación de los controles en este Capítulo se refiere al seguimiento exclusivo de los incidentes relacionados con seguridad de la información por tal motivo no se puede obtener una conclusión directa de la cantidad y tipo de las actividades definidas.

b) Los plazos en este caso solamente dependieron del área de Soporte por lo tanto no presentaron restricciones.



CONELEC

Esquema Gubernamental de Seguridad de la Información (EGSI)
Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES
Título 6.6. Monitoreo y revisión de los servicios, por terceros

COD: EGSI-D-032
Responsabilidad: Dirección de Gestión Estratégica
Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar las evidencias que no se mantiene un servicio de procesamiento de la información con personal externo		x	x																			
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"									x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"															x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																	x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																				x	x	x

Elaborado: Carolina Cáceres	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

Figura 3-1: Matriz de Situación Actual Subtítulo 6.6

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.6. Uso de contraseñas	COD: EGSI-D-016 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015													
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		na		na		na		na		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Verificar, en conjunto con el Oficial de Seguridad, que se incluya en la Política de Seguridad de la Información, los hitos 101, 102, 103,104 y 105.			x																									
	Implementar en el directorio activo una regla para la obligación de cambio de contraseñas de usuarios con perfil normal cada 6 meses y con uso de caracteres especiales (Item 7-18)							x	x																				
	Implementar en el directorio activo una regla para la obligación de cambio de contraseñas de los usuarios con perfil de administrador cada 3 meses y con uso de caracteres especiales y mayúsculas (Item 7-18)							x																					
	Implementar en el correo electrónico la obligación del cambio de contraseña cada 6 meses y con uso de caracteres especiales (Item 7-18)							x	x																				
Solución Integral	Elaborar el procedimiento de "Control de Acceso"															x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																					x							
	Desplegar el procedimiento de "Control de Acceso"																						x						
	Aplicar el procedimiento de "Control de Acceso"																							x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																											x	x

Elaborado: Carolina Cáceres Miguel Cevallos Patricio Coronel	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

Figura 3-2: Matriz de Situación Actual Subtítulo 7.6

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN Título 8.1. Análisis y especificaciones de los requerimientos de seguridad	COD: EGSI-D-029 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015											
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas																									
Solución Integral	Elaborar el procedimiento de "Adquisión, desarrollo y mantenimiento de sistemas de información"							x	x	x	x	x	x												
	Aprobar el procedimiento de "Adquisión, desarrollo y mantenimiento de sistemas de información"													x											
	Desplegar el procedimiento de "Adquisión, desarrollo y mantenimiento de sistemas de información"														x	x									
	Aplicar el procedimiento de "Adquisión, desarrollo y mantenimiento de sistemas de información"																x	x	x	x					
	Validar el procedimiento de "Adquisión, desarrollo y mantenimiento de sistemas de información"																				x	x	x	x	

Elaborado: Mauricio Oña	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

Figura 3-3: Matriz de Situación Actual Subtítulo 8.1

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN Título 9.1. Reporte sobre los eventos de seguridad de la información	COD: EGSI-D-030 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015											
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Implementar alertas de correo electrónico para el Oficial de Seguridad cuando se generen incidentes relacionados con seguridad de la información					x																			
	Elaborar un formato de informe de eventos de seguridad					x																			
Solución Integral	Elaborar el procedimiento de "Eventos de seguridad de la información"							x	x	x	x	x	x												
	Aprobar el procedimiento de "Eventos de seguridad de la información"													x	x										
	Desplegar el procedimiento de "Eventos de seguridad de la información"															x	x	x							
	Aplicar el procedimiento de "Eventos de seguridad de la información"																		x	x	x				
	Validar el procedimiento de "Eventos de seguridad de la información"																					x	x	x	x

Elaborado: Carolina Cáceres Patricio Coronel	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

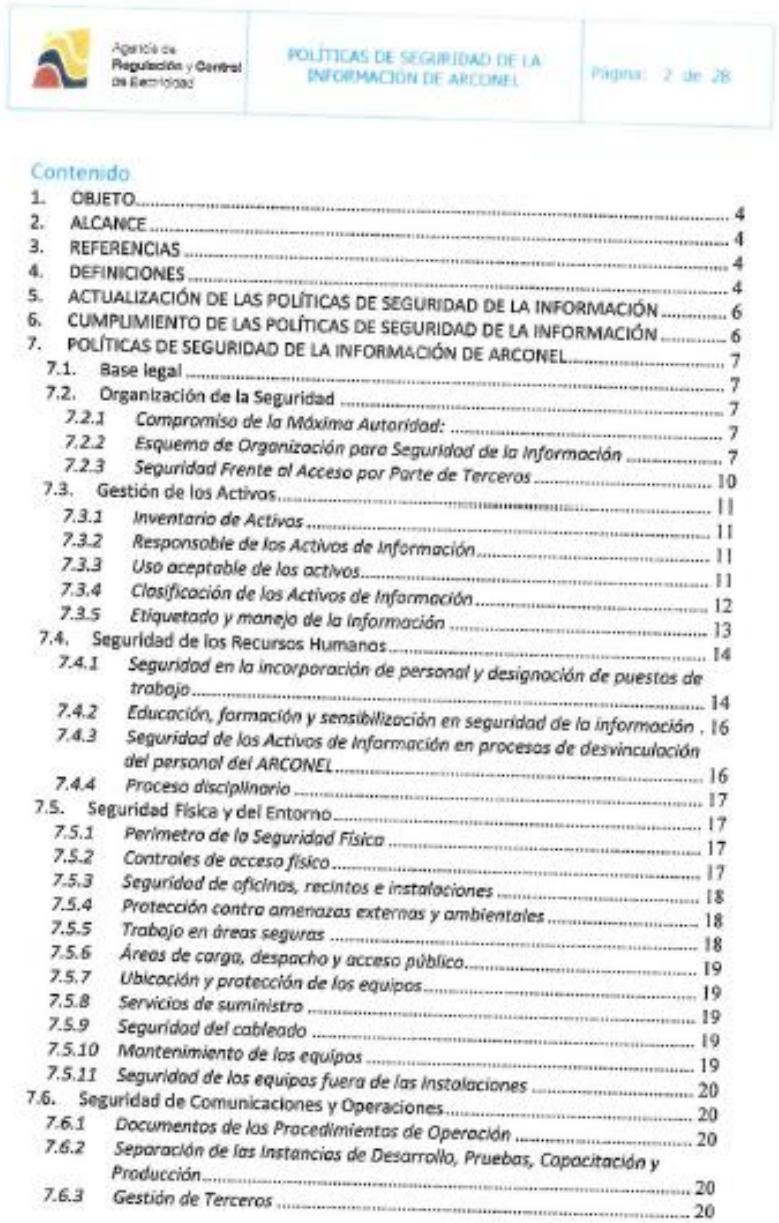
Figura 3-4: Matriz de Situación Actual Subtítulo 9.1

3.2.2. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

A continuación los capítulos de la Política de Seguridad de la Información del ARCONEL, aprobada en marzo del presente año y basada en la Guía del presente proyecto.

En la figura 3-5, la carátula con las respectivas firmas de aprobación. En la figura 3-6 el contenido de las políticas.

Figura 3-5: Carátula de la Política con las respectivas autorizaciones



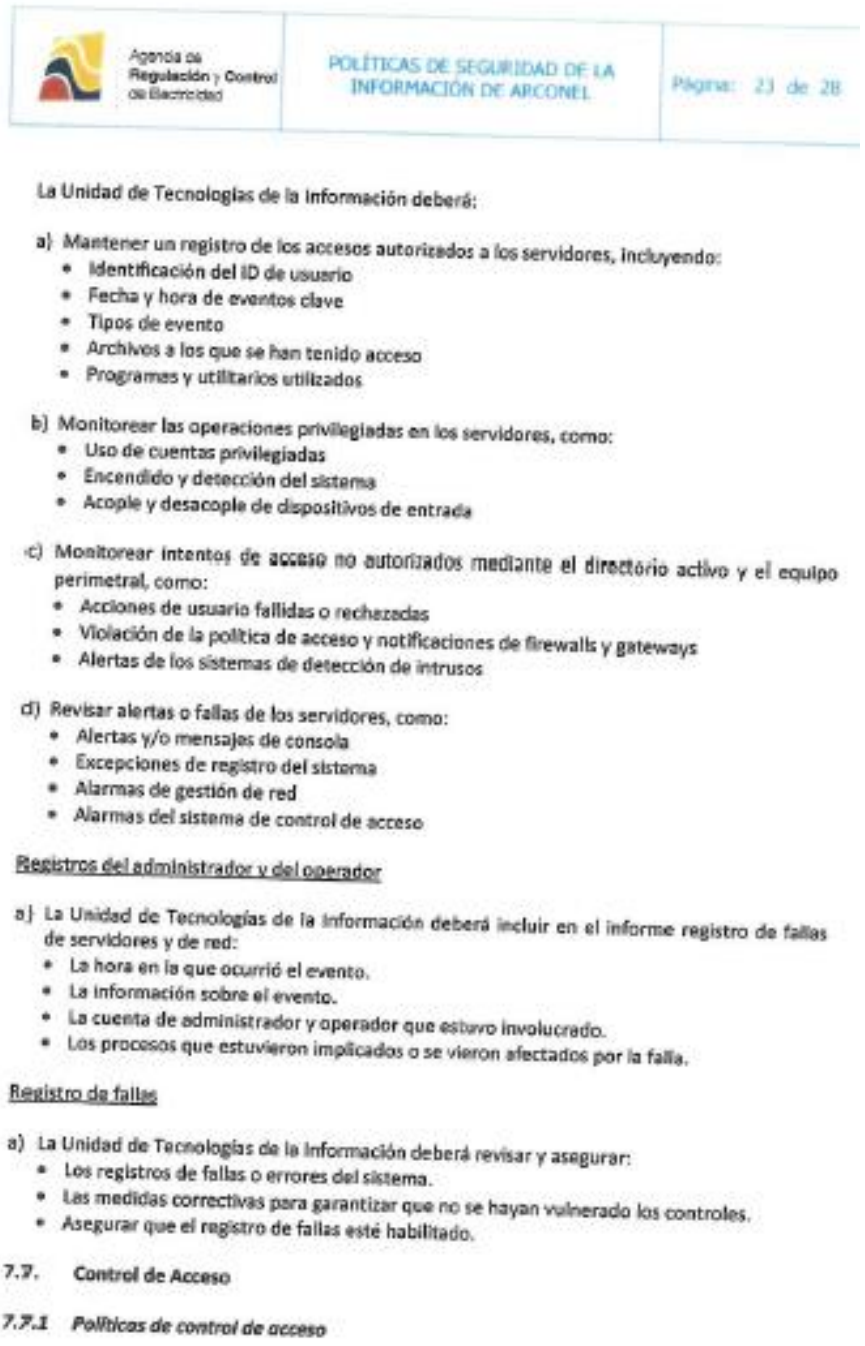
Agencia de Regulación y Control de Electricidad | POLÍTICAS DE SEGURIDAD DE LA INFORMACION DE ARCONEL | Página: 2 de 28

Contenido

Figura 3-6: Contenido de la Política

En las figuras 3-7, 3-8 y 3-9, se presentan las políticas de control de acceso basadas en el punto 2.2.6.3 Políticas de Control de Acceso de la Guía del presente proyecto. En las figuras se valida el uso de la Guía del presente proyecto en las Políticas de Seguridad de la Información de ARCONEL. Cabe indicar que la institución incluyó en

políticas, controles adicionales a los prioritarios por considerarlos necesarios para la correcta gestión de la seguridad de la información.



Agencia de Regulación y Control de Electricidad | POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE ARCONEL | Página: 23 de 28

La Unidad de Tecnologías de la Información deberá:

a) Mantener un registro de los accesos autorizados a los servidores, incluyendo:
- Identificación del ID de usuario
- Fecha y hora de eventos clave
- Tipos de evento
- Archivos a los que se han tenido acceso
- Programas y utilitarios utilizados

b) Monitorear las operaciones privilegiadas en los servidores, como:
- Uso de cuentas privilegiadas
- Encendido y detección del sistema
- Acople y desacople de dispositivos de entrada

c) Monitorear intentos de acceso no autorizados mediante el directorio activo y el equipo perimetral, como:
- Acciones de usuario fallidas o rechazadas
- Violación de la política de acceso y notificaciones de firewalls y gateways
- Alertas de los sistemas de detección de intrusos

d) Revisar alertas o fallas de los servidores, como:
- Alertas y/o mensajes de consola
- Excepciones de registro del sistema
- Alarmas de gestión de red
- Alarmas del sistema de control de acceso

Registros del administrador y del operador

a) La Unidad de Tecnologías de la Información deberá incluir en el informe registro de fallas de servidores y de red:
- La hora en la que ocurrió el evento.
- La información sobre el evento.
- La cuenta de administrador y operador que estuvo involucrado.
- Los procesos que estuvieron implicados o se vieron afectados por la falla.

Registro de fallas

a) La Unidad de Tecnologías de la Información deberá revisar y asegurar:
- Los registros de fallas o errores del sistema.
- Las medidas correctivas para garantizar que no se hayan vulnerado los controles.
- Asegurar que el registro de fallas esté habilitado.

7.7. Control de Acceso

7.7.1 Políticas de control de acceso

Figura 3-7: Capítulo referente al Control de Acceso (1)

a) Los usuarios podrán realizar solicitudes de acceso a los sistemas informáticos exclusivamente con el Formulario de Accesos y Servicios Informáticos, debidamente suscrito y con la autorización del Jefe o Director del área. El documento se entregará a la Unidad de Tecnologías de la Información para su respectiva ejecución.
b) La solicitud de una nueva cuenta o el cambio de privilegios deberá ser hecha por escrito, y deberá contar con la aprobación del Director de Área.
c) Se prohibe el uso de cuentas anónimas o de invitado, y los usuarios deben ingresar a los sistemas mediante cuentas que indiquen claramente su identidad.
d) Es responsabilidad del usuario de los sistemas informáticos el buen uso de la contraseña. En todos aquellos sistemas que sea posible se deberán implementar medios de autenticación únicos, de modo que los usuarios manejen el menor número de contraseñas posibles.

7.7.2 Registro de usuarios

a) La Unidad de Tecnologías de la Información deberá establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables para:
   - Gestionar el Formulario de Accesos y Servicios Informáticos tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);
   - Crear los accesos para los usuarios, para lo cual la Institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con la Unidad de Talento Humano en orden y completos.
   - Modificar y eliminar los accesos de los usuarios;
   - Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;
   - Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
   - Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

7.7.3 Gestión de usuarios y contraseñas de los sistemas informáticos

a) La Unidad de Tecnologías de la Información deberá:
   - Establecer un proceso formal para la asignación y cambio de contraseñas.
   - Controlar el cambio de contraseña del directorio activo de los usuarios cada 6 meses y del personal de tecnología y de los administradores de tecnología cada 4 meses manteniendo un nivel de complejidad alto.
   - Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un periodo máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio.
   - Evidenciar los cambios sobre los accesos en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.

Figura 3-8: Capítulo relativo al Control de Acceso (2)

b) Los usuarios tanto internos como externos serán responsables de:

- El uso de las cuentas y contraseñas asignadas.
- Establecer una contraseña de complejidad media y alta para los servicios de correo electrónico y de acceso a los equipos informáticos, considerando para el efecto el uso de: letras mayúsculas, minúsculas, caracteres especiales y numéricos; y proceder con su cambio con una periodicidad de máximo seis meses.
- No utilizar la identificación de usuario de otra persona, ya que toda actividad realizada con este identificador será atribuida al responsable al que la Unidad de Tecnologías de la Información entrega el identificador.
- Seguir buenas prácticas de seguridad en la selección y uso de contraseñas, para lo cual deben cumplir con las siguientes directrices:
  - ✓ Mantener las contraseñas en secreto. Evitar escribirlas en papeles que se encuentran visibles.
  - ✓ Pedir el cambio de la contraseña siempre que exista un posible indicio de error del sistema o de las contraseñas.
  - ✓ Seleccionar contraseñas de calidad, de acuerdo a las siguientes recomendaciones: Sean fáciles de recordar, no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabético, no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
  - ✓ Cambiar las contraseñas cada vez que el sistema se lo solicite, o con una periodicidad de máximo seis meses y, evitar reutilizar o reciclar viejas contraseñas.
  - ✓ Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
  - ✓ Notificar al Jefe de la Unidad de la Tecnologías de la Información cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

7.7.4 Gestión en el puesto de trabajo

a) La Unidad de Tecnologías de la Información deberá:

- Implementar medidas para que un tiempo no mayor a 10 minutos, si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.

b) Los usuarios internos deberán:

- Mantener bajo llave la información sensible, en especial cuando no estén en uso y no se encuentre personal en la oficina.
- Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas.
- Retirar información sensible una vez que ha sido impresa.
- Retirar información sensible, como las claves, de sus escritorios y pantallas.
- Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.

7.7.5 Gestión de las redes

c) La Unidad de Tecnología deberá:

Figura 3-9: Capítulo relativo al Control de Acceso (3)

3.2.3. DETERMINACIÓN DE LOS PROCEDIMIENTOS PARA LA IMPLANTACIÓN DEL EGSI.

Con el conocimiento de los procesos de la Unidad de Tecnologías de la Información de ARCONEL de una de las integrantes del presente proyecto que durante tres años realizó la gestión de la Mesa de Servicios del área, se desarrolla el procedimiento Gestión de los Incidentes de da Seguridad de da Información en base a la Guía del proyecto, que propone este procedimiento en el numeral 2.2.6.3.

3.2.3.1. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Objeto

Establecer una metodología para documentar, registrar y controlar todos los incidentes relacionados con los eventos se seguridad de la información.

Alcance

Mantener un registro y control de todos los incidentes referentes a seguridad de la información de la Unidad de Tecnologías de la Información de ARCONEL.

Definiciones

ARANDA Sistema de Mesa de Servicios de la UGTI.

Desarrollo del Proceso:

Reporte sobre los Eventos de Seguridad de la Información

Nro. Hito	115,116,117,118,119,120,121,122,123,124,125
Detalle Hito EGSI en GPR	• Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información, junto con un procedimiento de escalada y respuesta ante el incidente. • Identificar el incidente. • Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". • Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto. • Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente. • Notificar al Oficial de Seguridad de la Información de la Institución. • Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad. • Asignar una prioridad de atención al incidente, en el caso de que se produjeran varios en forma simultánea. • Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas,

	• Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. • Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente. • Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
Objetivo de control de COBIT	PO 9.3 Identificación de eventos DS 5.6 Definición de incidente de seguridad DS 8.2 Registro de consultas de clientes
Listas de control de ITIL v3	OS - Registro de incidente
Prerrequisitos	• El Oficial de Seguridad de la Información está registrado en el sistema ARANDA como especialista para la resolución de incidentes. • Se encuentra activa la regla Nro. 101 de la Mesa de Servicios y el correo registrado en la regla es del Oficial de Seguridad de la Información institucional. • El personal de la UGTI conoce que los incidentes relacionados a eventos de seguridad de la información deben ser clasificados como CRÍTICOS.
Disparador:	Registro de incidente relacionado con seguridad de la información a través de la Mesa de Servicios de la UGTI

<table>
<tr><td rowspan="2">Insumos y Proveedores:</td><td>Entrada</td><td>Proveedor</td><td>Tipo de Proveedor</td></tr>
<tr><td>Requerimiento de Servicio mediante correo electrónico a la dirección soporte@regulacionelectrica.gob.ec. El responsable de la mesa de servicios determina que el incidente tiene relación con seguridad de la información y lo clasifica como CRÍTICO.</td><td>Área de Soporte</td><td>Interno o Externo</td></tr>
<tr><td rowspan="2">Productos y Clientes:</td><td>Producto</td><td>Cliente</td><td>Tipo de Cliente</td></tr>
<tr><td>Notificación al Oficial de Seguridad de la Información</td><td>Usuario</td><td>Interno o Externo</td></tr>
<tr><td>Tipo de Proceso:</td><td colspan="3">Adjetivo</td></tr>
<tr><td>Responsable del Proceso:</td><td colspan="3">Responsable de la Mesa de Servicios de ARANDA</td></tr>
<tr><td>Métrica</td><td colspan="3">Porcentaje de eventos críticos de TI identificados que han sido evaluados</td></tr>
</table>

Tabla 3-1: Reporte sobre los eventos de seguridad de la información.

Diagrama de Flujo del Reporte sobre los Eventos de Seguridad de la Información

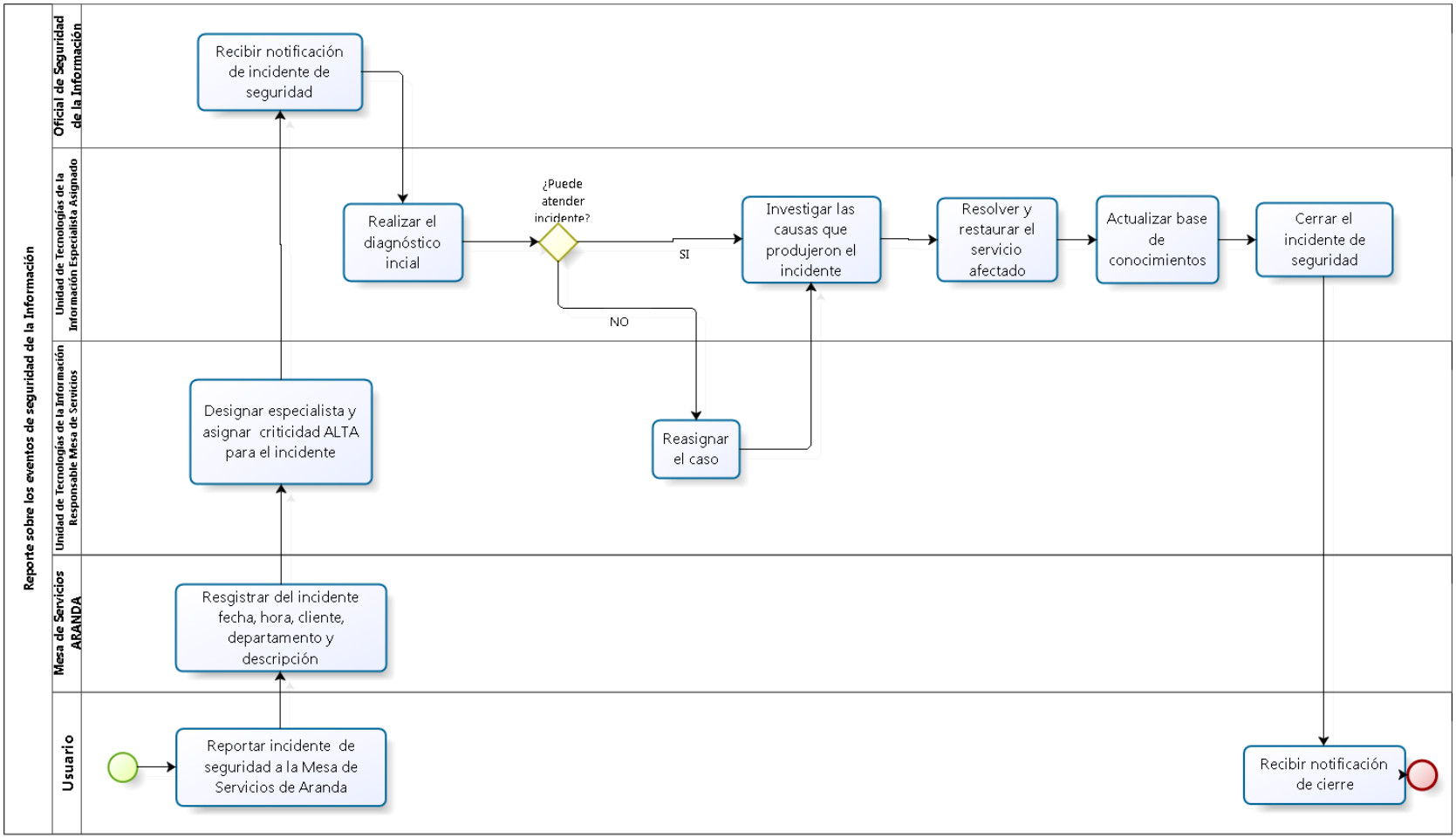


Figura 3-10: Diagrama de Reporte sobre los eventos de Seguridad de la Información

3.3. ANÁLISIS DE RESULTADOS

Luego de la utilización de la Guía para la determinación de la situación inicial, la elaboración de la Política General de Seguridad de la Información y la elaboración de los procedimientos se obtuvieron los siguientes resultados:

- La situación inicial respecto a seguridad de la información de la institución tenía un nivel de madurez de 0, lo que permitió a las áreas definir cronogramas con tareas específicas para el cumplimiento del EGSI. Los cronogramas fueron utilizados como medio de validación de los cumplimientos de cada área, logrando así emitir reportes verificables sobre los avances, tanto para la Dirección Ejecutiva como para la SNAP a través del GPR.
- La Política General de Seguridad de la Información incluyó además controles no prioritarios del EGSI que la institución consideró pertinentes incluir, uno de los aspectos más relevantes del uso de la presente Guía fue la definición de la criticidad de un activo de información, lo que permitió al equipo de seguridad de la información difundir al resto de la entidad la base para la obtención del inventario inicial de activos de la información y su respectiva clasificación.
- La definición de procedimientos requirió un conocimiento a detalle de las actividades y personal involucrado en el mismo, se invierte una gran cantidad de tiempo en la implantación de los procedimientos pero gracias a las plantillas se define claramente el objetivo que el EGSI busca en relación a la Seguridad de la Información.

El proyecto EGSI fase I de ARCONEL en el sistema GPR fue concluido gracias a la ejecución de éste proyecto, esto quiere decir que la contribución de la Guía permite alcanzar la implantación del Esquema de Gestión de Seguridad de la Información en la institución que se aplique.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- La Guía requirió que los involucrados conocieran sobre los estándares de TI relacionados con la seguridad de la información, lo que permitió un mejor entendimiento de la Guía y una más fácil aplicación.
- La normativa del SNAP limita el número de controles a alrededor de 100, pero en la realidad se comprobó que es necesario incrementar o seleccionar otros controles, para mejorar la seguridad de la información en las entidades de la Administración Pública Central.
- La ejecución de proyectos gubernamentales requiere un amplio conocimiento de leyes, normas y reglamentos, para estructurarlos de manera que cumplan con las definiciones existentes en el Estado. Es decir, los involucrados en el proyecto EGSI de las distintas entidades deben conocer no solamente información técnica sino fundamentar la base del proyecto en la legislación relacionada con seguridad de la información, como la LOTAIP.
- La metodología de la Universidad Nacional de Colombia utilizada en este proyecto permitió desarrollar las políticas de seguridad de la información de manera adecuada, por lo que cumplió con su propósito.
- La seguridad de la información en ARCONEL antes de la aplicación de la guía desarrollada estaba en un nivel de madurez muy bajo. Si esto es un ejemplo de lo que sucede, se puede concluir que la gran mayoría de Instituciones de la Administración Pública Central también se encuentran en este nivel preocupante de madurez. Lo que demuestra la urgencia de aplicar el EGSI acompañado de la guía desarrollada en este proyecto.
- Al validar la guía se comprobó su utilidad, por lo que se la recomienda para ser utilizada en cualquier entidad de la Administración Pública Central.
- La determinación de los procedimientos para la implementación del EGSI se facilitó con el uso de las buenas prácticas que proponen ITIL y COBIT.

4.2. RECOMENDACIONES

- Se recomienda que las disposiciones emitidas por organismos de control del sector público estén acompañadas de capacitación para el personal a cargo de su implantación, seguimiento y control de las actividades realizadas; se requiere que se elaboren formatos que claramente determinen los logros a obtenerse, de manera que se alcance el éxito en los proyectos de este tipo.
- Se recomienda que en los proyectos aplicados en entidades del Estado se incluya en el equipo de trabajo al menos una persona que conozca del sector público, de manera que se pueda utilizar ese conocimiento para una mejor ejecución del proyecto.
- Se recomienda utilizar en todo tipo de proyectos, prácticas generales y ampliamente aceptadas, como las relacionadas con el Gobierno de TI, ya que permiten el fácil traspaso de conocimientos entre quienes se encuentran laborando en las áreas de Tecnologías de la Información.
- Se recomienda a las entidades del sector público ampliar la aplicación de las políticas en el capítulo referente al desarrollo de software, ya que de no ser implementados controles efectivos en ésta área se puede encontrar amplias fallas de seguridad.

BIBLIOGRAFÍA

[1] <<Tecnología de la Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad de la Información – Descripción General y Vocabulario>> de Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000:2012, INEN, 2012

[2] J. Freire, <<La seguridad de la información es una prioridad para la industria financiera latinoamericana>> [En línea]. Available: http://www.doctortecno.com/noticia/seguridad-informacion-es-prioridad-para-industria-financiera-latinoamericana [Último acceso: 16 Noviembre 2014]

[3] <<Ley Orgánica de Transparencia y Acceso a la Información Pública LOTAIP>>, Registro Oficial Suplemento 337, 2004

[4] Secretaría Nacional de la Administración Pública, <<La Secretaría>> [En línea]. Available: http://www.administracionpublica.gob.ec/la-secretaria/ [Último acceso: 16 Noviembre 2014]

[5] Secretaría Nacional de la Administración Pública, <<Acuerdo Ministerial 166. Esquema Gubernamental de Seguridad de la Información>>, Registro Oficial Suplemento 88, 2013.

[6] Presidencia de la República del Ecuador, <<Estatuto Régimen Jurídico Administrativo Función Ejecutiva, ERJAFE>>, Registro Oficial Suplemento 536, 2002.

[7] Universidad Nacional de Colombia, <<Guía para elaboración de políticas de seguridad>> [En línea]. Available: Http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf [Último acceso: 16 Noviembre 2014]

[8] IT Governance Institute, <<COBIT Mapping: Mapping Of ITIL V3 with COBIT 4.1>>, EEUU, 2008

[9] Secretaría Nacional de la Administración Pública, <<Acuerdo Ministerial 1580. Norma Técnica de Administración por Procesos>>, Registro Oficial Suplemento 895, 2013.

[10] IT Governance Institute, <<Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit>>, EEUU, 2008

[11] J. Avellaneda, <<Guía para la elaboración del marco normativo de un sistema de gestión de la seguridad de la información (SGSI)>> [En línea]. Available: http://www.firma-e.com/documentos/Gu%EDa%20para%20la%20elaboraci%F3n%20del%20marco%20normativo-Creative%20common.pdf [Último acceso: 16 Noviembre 2014], 2007

[12] <<Tecnología de la Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad de la Información – Requisitos>> de Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2012, INEN, 2012

[13] SANS Institute, <<Information Security Policy – A Development Guide for Large and Small Companies>> [En línea]. Available: http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331 [Último acceso: 04 Mayo 2015], 2006

[14] Presidencia de la República del Ecuador, << REGLAMENTOS AL CÓDIGO ORGÁNICO DE LA PRODUCCIÓN, COMERCIO E INVERSIONES >> [En línea]. Available:http://www.produccion.gob.ec/wp-content/uploads/downloads/2013/01/ReglamentosCodigoProduccion.pdf [Último acceso: 14 Julio 2015], 2010

[15] Contraloría General del Estado, <<NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS>> [En línea]. Available:

http://www.utn.edu.ec/web/portal/images/doc-utn/normas-control-interno.pdf [Último acceso: 14 Mayo 2015], 2009

[16] S. Kempter, A. Kempter, <<WIKI de ITIL>> [En línea]. Available: http://wiki.es.it-processmaps.com/index.php/Portada [Último acceso: 14 Mayo 2015], 2015

[17] IT Governance Institute, << COBIT 4.1>>, EEUU, 2007

[18] Secretaría Nacional de la Administración Pública, <<MANUAL DE CREACIÓN DE LA COORDINACIÓN GENERAL DE GESTIÓN ESTRATÉGICA>> [En línea]. Available: http://www.ambiente.gob.ec/wp-content/uploads/downloads/2012/06/MANUAL_DE_CREACIO%C2%81N_DE_LA_COORDINACIO%C2%81N_GENERAL_DE_GESTIO%C2%81N_ESTRATE%C2%81GICA.pdf [Último acceso: 28 Junio 2015], 2012.

[19] Universidad Nacional de Luján, <<RIESGO VS. SEGURIDAD DE LA INFORMACIÓN>> [En línea]. Available: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf [Último acceso: 14 Julio 2015].

GLOSARIO

- **EGSI**

Esquema Gubernamental de Seguridad de la Información.

- **LOTAIP**

Ley Orgánica de Transparencia y Acceso a la Información Pública.

- **COBIT**

Control Objectives for Information and Related Technology.

- **ITIL**

Information Technology Infrastructure Library.

- **SNAP**

Secretaría Nacional de la Administración Pública.

- **ISO**

Organización Internacional de Estandarización.

- **ERJAFE**

Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

- **GPR**

Gobierno Por Resultados

- **CGSI**

Comité de Gestión de la Seguridad de la Información (CGSI),

- **OSI**

Oficial de Seguridad de la Información.

- **RSITI**

Responsable de Seguridad de la Información de TI.

- **ARCONEL**

Agencia de Regulación y Control de Electricidad.

- **UTI**

Unidad de Tecnologías de la Información

ANEXOS

ANEXO A – Plantillas de la Guía

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

		Año 1												Año 2											
Cronograma		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.6. Monitoreo y revisión de los servicios, por terceros

Objetivo de Control:

Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorias se deberían llevar a cabo a intervalos regulares

Hitos:

73. Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos
74. Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos
75. Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.8. Gestión de la capacidad

Objetivo de Control:

Se debería hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema

Hitos:

76. Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.10. Controles contra código malicioso

Objetivo de Control:

Se deberían implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concienciación de los usuarios

Hitos:

50. Prohibir el uso de software no autorizado por la institución. Elaborar un listado de software autorizado
51. Instalar y actualizar periodicamente software de antivirus contra código malicioso
52. Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles

Cronograma		2014												2015											
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.12. Respaldo de la Información

Objetivo de Control:

se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordado

Hitos:

53. Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información
54. Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención
55. Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.14. Seguridad de los servicios de la red

Objetivo de Control:

En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir las características de la seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios prestan en la organización o se contratan externamente

Hitos:

56. Incorporar tecnología para la seguridad de los servicios de red como autenticación, encriptación y controles de conexión de red
57. Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.26. Registro de auditorías

Objetivo de Control:

Se deberían elaborar y mantener durante un período acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso

Hitos:

58. Registrar los accesos y tipos de acceso
59. Registrar las direcciones y protocolos de red
60. Definir alarmas originadas por el sistema de control de acceso
61. Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS)

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.27. Monitoreo del uso del sistema

Objetivo de Control:

Se deberían establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deberían revisar con regularidad

Hitos:

62. Registrar los accesos autorizados incluyendo: identificacion del ID de usuario, fecha y hora de eventos clave, tipos de evento, archivos a los que se han tenido acceso, programas y utilizarios utilizados
63. Monitorear las operaciones privilegiadas como: uso de cuentas privilegiadas
64. Monitorear intentos de acceso no autorizados, como: acciones de usuario fallidos o rechazadas, violación de la política de acceso y notificaciones de firewalls y gateways, alertas de los sistemas de detección de intrusos
65. Revisar alertas o fallas del sistema, como: alertas y/o mensajes de consola, excepciones de registro del sistema, alarmas de gestión de red, alarmas del sistema de control de acceso

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.29. Registros del administrador y del operador

Objetivo de Control:

Se deberían registrar las actividades tanto del operador como del administrador del sistema

Hitos:

66. Incluir el registro, la hora en la que ocurrió el evento
67. Incluir al registro la información sobre el evento
68. Incluir al registro al cuenta de administrador y operador que estuvo involucrado
69. Añadir al registro los procesos que estuvieron implicados

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Título 6.30. Registro de fallas

Objetivo de Control:
Las fallas se deberían registrar y analizar, y se deberían tomar las acciones adecuadas

Hitos:
70. Revisar los registros de fallas o errores del sistemas
71. Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles
72. Asegurar que el registro de fallas esté hablitado

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.4. Gestión de contraseñas para usuarios

Objetivo de Control:
La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.

Hitos:
100. Establecer un proceso formal para la asignación y cambio de contraseñas

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.6. Uso de contraseñas

Objetivo de Control:
Se debería exigir a los usuarios el cumplimiento de buenas prácticas de la seguridad en la selección y el uso de contraseñas.

Hitos:
101. Documentar en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados.
102. Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir que cumplen una complejidad media y alta.
103. Evitar contraseñas en blanco o que vine por defecto según el sistema el fabricante del producto, puesto que son facilmente descifrables: por ejemplo, admin, administrador, user, usuario entre otros.
104. Controlar el cambio periódico de contraseñas de usuarios.
105. Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.7. Equipos de usuarios desatendido

Objetivo de Control:
Los usuarios deberían asegurarse que los equipos desatendidos tengan protección adecuada

Hitos:
106. Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, éste se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.8. Política de puesto de trabajo despejado y pantalla limpia

Objetivo de Control:
Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

Hitos:
107. Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.
108. Desconectar de la red, servicio o sistema, las computadores personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.
109. Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas.
110. Retirar información sensible una vez que ha sido impresa.
111. Retirar información sensible, como las claves, de sus escritorios y pantallas.
112. Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.10. Autenticación de usuarios para conexiones externas

Objetivo de Control:
Se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos

Hitos:
77. Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR)

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.11. Identificación de los equipos en las redes

Objetivo de Control:

La identificación automática de los equipos se debería considerar un medio para autenticar las conexiones de equipos y ubicaciones específicas

Hitos:

78. Identificar y documentar los equipos que se encuentran en las redes

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.12. Protección de los puertos de configuración y dianóstico remoto

Objetivo de Control:

El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estar controlado.

Hitos:

79. Los puertos, servicios (Ej.,ftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.13. Separación en las redes

Objetivo de Control:

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemas de información

Hitos:

80. Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.15. Control del enrutamiento en la red

Objetivo de Control:

Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio

Hitos:

81. Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.16. Procedimiento de registro de inicio seguro

Objetivo de Control:
El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro

Hitos:
82. Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución que deberá estar documentada , definida y socializada.
83. Llevar un registro de definición para el uso de privilegios especiales del sistema.
84. Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.
85. Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de accesos y directorios.
86. Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución.
87. Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente.
88. Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo , tres intentos.
89. Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICION DE CRITERIOS PARA LA IMPLEMENTACION DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.17. Identificación y autenticación de usuarios

Objetivo de Control:
Todos los usuarios deberían tener un identificador unico (ID de usuario) para su uso personal, y se debería elegir una técnica apropiada de autenticación para comprobar la identidad declara de un usuario.

Hitos:
90. Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución.
91. Usar como excepción y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo espécifico, el cual debe estar definido y documentado.
92. Evitar el uso de usuarios genéricos.
93. Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.18. Sistema de gestión de contraseñas

Objetivo de Control:

Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

Hitos:

94. Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible.
95. Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnologia en rangos de tiempo y complejidad.
96. Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.25. Computación y comunicaciones móviles

Objetivo de Control:
Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

Hitos:
97. Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 7. CONTROL DE ACCESO

Título 7.26. Trabajo remoto

Objetivo de Control:
Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Hitos:
98. No se permite el uso de equipo de propiedad privada que no esté bajo control y monitoreo de la institución.
99. Deberá considerarse la protección de antivirus y reglas del firewall.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Título 8.1. Análisis y especificaciones de los requerimientos de seguridad

Objetivo de Control:
Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de seguridad.

Hitos:
113. Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones.
114. Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal de requerimiento funcional y personal técnico que trabajarán en el sistema. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y el daño potencial que pudiera ocasionar a las actividades realizadas realizadas por falla o falta de seguridad.

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

MATRIZ DE DEFINICIÓN DE CRITERIOS PARA LA IMPLEMENTACIÓN DE EGSI

Capítulo 9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Título 9.1. Reporte sobre los eventos de seguridad de la información

Objetivo de Control:
Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

Hitos:
116. Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidentes, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.
117. -126. Cuando un incidente se produzca el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden:
- Identificar el incidente
- Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
- Notificar al Oficial de Seguridad de la Información de la institución
- Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad
- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios de forma simultánea
- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas
- Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberpa ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado
- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente
- Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes
- Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o sistema de que el incidente ha sido resuelto

Cronograma		Año 1												Año 2											
		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12		Mes 1		Mes 2		Mes 3		Mes 4		...		Mes 12	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'	1'	2'
		Fase 1						Fase 2						Fase 3						Fase 4					
Acciones Corto Plazo																									
Acciones Largo Plazo																									

ANEXO B– Aplicación de la Matriz de Definición de Situación Actual de la Implantación del EGSI. Capítulo 6. Gestión de Comunicación y Operaciones

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.1 Documentación de los procedimientos de Operación	COD: EGSI-D-031 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Generar una lista del personal técnico indicando números telefónicos, emails y una breve descripción del soporte a brindar		x																				
	Generar un listado de proveedores, indicando el servicio que brindan			x																			
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"									x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"															x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																	x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																				x	x	x

Elaborado: Patricia Cruz	Elaborado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar informe de la situación actual del espacio disponible en discos para sostener la operación		x	x																			
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"									x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"															x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																	x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																				x	x	x

Elaborado: Miguel Cevallos	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.10. Controles contra código malicioso	COD: EGSI-D-034 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014						2015															
		Julio		Agosto		Septiembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Elaborar el listado de software autorizado de la institución			x	x																				
	Presentar evidencias de que el antivirus se encuentre desplegado y actualizado en todos los computadores que se encuentren activos en el CONELEC					x																			
	Presentar evidencias de la actualización de los sistemas operativos de los equipos de los usuarios						x																		
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"											x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"																	x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																		x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																			x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																						x	x	x

Elaborado: Carolina Cáceres Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.12. Respaldo de la Información	COD: EGSI-D-035 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014						2015															
		Julio		Agosto		Septiembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar evidencias del etiquetado de respaldos y su almacenamiento fuera de las oficinas del CONELEC			x																					
	Elaborar un listado de los sistemas que se deben respaldar				x																				
	Elaborar un formato para el respaldo de información con firmas de responsabilidad del técnico que saca los respaldos y el técnico que entrega la información.				x	x																			
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"											x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"																	x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																		x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																			x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																						x	x	x

Elaborado: Patricio Coronel Mauricio Oña	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar evidencias del servicio de directorio activo para el uso de servicios en red			x																			
	Presentar evidencias del uso del antivirus				x																		
	Presentar evidencias del uso de firewall				x																		
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"									x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"															x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																	x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																				x	x	x

Elaborado: Miguel Cevallos Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.26. Registro de auditorías	COD: EGSI-D-037 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014										2015																	
		Julio		Agosto		Septiembre		Octubre		Noviembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Respaldar los log de acceso a los servidores (item 7-16)									x	x																		
	Presentar el inventario completo de equipos informáticos con su identificación de red (IP) (Item 7-11)							x	x																				
	Presentar evidencias de los registros de activación y desactivación del antivirus				x																								
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"															x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"																					x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																						x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																							x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																										x	x	x

Elaborado: Miguel Cevallos Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.27. Monitoreo del uso del sistema	COD: EGSI-D-038 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

ACTIVIDADES A DESARROLLAR		2014						2015															
		Julio		Agosto		Septiembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Identificar los riesgos en los servidores de base de datos y aplicaciones, determinar como debería ser realizada su implementación para mitigar los riesgos, al igual que su alcance				x	x	x																		
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"											x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"																	x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																		x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																			x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																						x	x	x

Elaborado: Miguel Cevallos	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.30. Registro de fallas	COD: EGSI-D-040 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

ACTIVIDADES A DESARROLLAR		2014				2015																	
		Julio		Agosto		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Realizar un formato en donde se lleve el registro de las fallas ocurridas en los sistemas de los servidores y acciones realizadas para solventar el inconveniente				x																		
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"									x	x	x	x	x	x								
	Aprobar procedimiento "Comunicaciones y Operaciones"															x							
	Desplegar procedimiento "Comunicaciones y Operaciones"																x						
	Aplicar procedimiento "Comunicaciones y Operaciones"																	x	x	x			
	Validar procedimiento "Comunicaciones y Operaciones"																				x	x	x

Elaborado: Miguel Cevallos	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES Título 6.29. Registros del administrador y del operador	COD: EGSI-D-039 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Realizar un formato en donde se lleve el registro de los eventos ocurridos en la red			x																			
Solución Integral	Elaborar el procedimiento de "Comunicaciones y Operaciones"									x	x	x	x	x	x								
	Aprobar el procedimiento de "Comunicaciones y Operaciones"															x							
	Desplegar el procedimiento de "Comunicaciones y Operaciones"																x						
	Aplicar el procedimiento de "Comunicaciones y Operaciones"																	x	x	x			
	Validar el procedimiento de "Comunicaciones y Operaciones"																				x	x	x

Elaborado: Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma: Daniela Gutiérrez	Firma: Patricia	Firma:

ANEXO C– Aplicación de la Matriz de Definición de Situación Actual de la Implantación del EGSI. Capítulo 7. Control de Acceso

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.7. Equipos de usuarios desatendido	COD: EGSI-D-017 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014								2015																	
		Julio		Agosto		Septiembre		Octubre		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Implementar el bloqueo de sesion de los equipos desatendidos luego de 20 minutos. (Item 7-8)							x	x																				
Solución Integral	Elaborar el procedimiento de "Control de Acceso"															x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																					x							
	Desplegar el procedimiento de "Control de Acceso"																						x						
	Aplicar el procedimiento de "Control de Acceso"																							x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																											x	x

Elaborado: Miguel Cevallos	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.8. Política de puesto de trabajo despejado y pantalla limpia	COD: EGSI-D-018 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014								2015																	
		Julio		Agosto		Septiembre		Octubre		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Verificar en conjunto con el Oficial de Seguridad que en la Política de Seguridad consten los hitos 107, 110, 111, 112			x																									
	Implementar el bloqueo de sesion de los equipos desatendidos luego de 20 minutos. (item 7 - 7)							x	x																				
	Presentar las evidencias técnicas de la imposibilidad de bloquear las copiadoras				x																								
Solución Integral	Elaborar el procedimiento de "Control de Acceso"															x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																					x							
	Desplegar el procedimiento de "Control de Acceso"																						x						
	Aplicar el procedimiento de "Control de Acceso"																							x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																											x	x

Elaborado: Carolina Cáceres Patricio Coronel Miguel Cevallos	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.10. Autenticación de usuarios para conexiones externas	COD: EGSI-D-019 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014								2015																	
		Julio		Agosto		Septiembre		Octubre		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Verificar permisos de acceso de todos los usuarios en del directorio activo		x	x	x	x	x																						
	Depurar el listado de personal que tiene acceso a la VPN del CONELEC					x	x																						
	Incrementar el nivel de complejidad de las contraseñas de proxy para los funcionarios con acceso a la VPN							x	x																				
Solución Integral	Elaborar el procedimiento de "Control de Acceso"															x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																					x							
	Desplegar el procedimiento de "Control de Acceso"																						x						
	Aplicar el procedimiento de "Control de Acceso"																							x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																											x	x

Elaborado: Miguel Cevallos Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma: Daniela Gutiérrez	Firma: Patricia	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.11. Identificación de los equipos en las redes	COD: EGSI-D-020 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014								2015																	
		Julio		Agosto		Septiembre		Octubre		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar el inventario completo de equipos informáticos con su identificación de red (IP)					x	x	x	x																				
Solución Integral	Elaborar el procedimiento de "Control de Acceso"															x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																					x							
	Desplegar el procedimiento de "Control de Acceso"																						x						
	Aplicar el procedimiento de "Control de Acceso"																							x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																											x	x

Elaborado: Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma: Daniela Gutiérrez	Firma: Patricia	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.12. Protección de los puertos de configuración y dianóstico remoto	COD: EGSI-D-021 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

ACTIVIDADES A DESARROLLAR		2014												2015																	
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Elaborar y aprobar el Formulario de Habilitación de Puertos que incluya como mínimo la descripción del servicio y usuario requirente con firma de responsabilidad .			x	x																										
	Verificar todos los puertos habilitados en el Firewall y deshabilitar aquellos que no sean necesarios					x	x	x																							
	Presentar el Formulario de Habilitación de Puertos por cada servicio que se mantenga habilitado en el Firewall								x	x	x	x																			
Solución Integral	Elaborar el procedimiento de "Control de Acceso"																			x	x	x	x	x	x						
	Aprobar el procedimiento de "Control de Acceso"																									x					
	Desplegar el procedimiento de "Control de Acceso"																										x				
	Aplicar el procedimiento de "Control de Acceso"																											x	x	x	x
	Validar el procedimiento de "Control de Acceso"																													x	x

Elaborado: Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.13. Separación en las redes	COD: EGSI-D-022 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015																	
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Gestionar todos los servidores mediante un único segmento de red, en este segmento no se deben incluir equipos de usuario.							x	x	x	x	x	x																						
	Presentar evidencias de los segmentos de red de la institución			x																															
Solución Integral	Elaborar el procedimiento de "Control de Acceso"																					x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																											x							
	Desplegar el procedimiento de "Control de Acceso"																												x						
	Aplicar el procedimiento de "Control de Acceso"																													x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																																	x	x

Elaborado: Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.15. Control del enrutamiento en la red	COD: EGSI-D-023 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																			
		Julio		Agosto		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar evidencias del enrutamiento en la red actual y las seguridades que brinda				x																				
Solución Integral	Elaborar el procedimiento de "Control de Acceso"											x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																	x							
	Desplegar el procedimiento de "Control de Acceso"																		x						
	Aplicar el procedimiento de "Control de Acceso"																			x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																							x	x

Elaborado: Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.16. Procedimiento de registro de inicio seguro	COD: EGSI-D-024 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015																							
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar evidencias del servicio de directorio activo de la institución. (Item 7-17)				x																																
	Elaborar y aprobar el formato de Autorización del Privilegios Especiales para directorio activo de la institución		x	x																																	
	Respaldar los log de acceso a los servidores									x	x																											
	Limitar la cantidad de intentos de autenticación en los equipos a máximo 5 intentos							x																													
	Presentar evidencias de la imposibilidad de limitar el tiempo de dilación para permitir o rechazar intentos adicionales de ingreso al directorio activo				x																																
	Verificar en conjunto con el Oficial de Seguridad que en la Política de Seguridad de la Información se incluya el modelo de la autenticación de usuarios			x																																	
Solución Integral	Elaborar el procedimiento de "Control de Acceso"																							x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																													x							
	Desplegar el procedimiento de "Control de Acceso"																														x						
	Aplicar el procedimiento de "Control de Acceso"																															x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																																			x	x

Elaborado: Miguel Cevallos Carolina Cáceres	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.17. Identificación y autenticación de usuarios	COD: EGSI-D-025 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015																					
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar evidencias del servicio de directorio activo de la institución. (item 7- 16)				x																														
	Elaborar y aprobar el formato de Autorización de Grupos de Usuarios en el directorio activo que incluya como mínimo el nombre del grupo y el nombre del funcionario responsable del grupo.					x																													
	Aplicar el formato de Autorización de Grupos de en el directorio activo para todos los grupos existentes.							x	x																										
	Presentar evidencias de la imposibilidad tecnológica de utilizar medios criptográficos o tarjetas inteligentes, tokens o medios biométricos de autenticación.						x																												
Solución Integral	Elaborar el procedimiento de "Control de Acceso"																							x	x	x	x	x	x						
	Aprobar el procedimiento de "Control de Acceso"																											x							
	Desplegar el procedimiento de "Control de Acceso"																												x						
	Aplicar el procedimiento de "Control de Acceso"																															x	x	x	x
	Validar el procedimiento de "Control de Acceso"																																	x	x

Elaborado: Miguel Cevallos Mauricio Oña	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.18. Sistema de gestión de contraseñas	COD: EGSI-D-026 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014												2015																							
		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre		Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Verificar en conjunto con el Oficial de Seguridad que en la Política de Seguridad de la Información se incluya la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible		x																																
	Implementar en el directorio activo una regla para la obligación de cambio de contraseñas de usuarios con perfil normal cada 6 meses y con uso de caracteres especiales (Item 7-6)							x	x																										
	Implementar en el directorio activo una regla para la obligación de cambio de contraseñas de los usuarios con perfil de administrador cada 3 meses y con uso de caracteres especiales y mayúsculas (Item 7-6)							x																												
	Presentar evidencias de la obligatoriedad de cambio de contraseña en el primer inicio de sesión del equipo				x																														
	Implementar en el correo electrónico la obligación del cambio de contraseña cada 6 meses y con uso de caracteres especiales (Item 7-6)							x	x																										
Solución Integral	Elaborar el procedimiento de "Control de Acceso"																							x	x	x	x	x	x						
	Aprobar el procedimiento de "Control de Acceso"																													x					
	Desplegar el procedimiento de "Control de Acceso"																														x				
	Aplicar el procedimiento de "Control de Acceso"																															x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																																			x	x

Elaborado: Carolina Cáceres Miguel Cevallos Patricio Coronel	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.25. Computación y comunicaciones móviles	COD: EGSI-D-027 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Verificar en conjunto con el Oficial de Seguridad que en la Política de Seguridad de la Información se incluya la responsabilidad de la exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo.			x																					
Solución Integral	Elaborar el procedimiento de "Control de Acceso"											x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																	x							
	Desplegar el procedimiento de "Control de Acceso"																		x						
	Aplicar el procedimiento de "Control de Acceso"																			x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																							x	x

Elaborado: Carolina Cáceres	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma:

CONELEC	Esquema Gubernamental de Seguridad de la Información (EGSI) Capítulo 7. CONTROL DE ACCESO Título 7.26. Trabajo remoto	COD: EGSI-D-028 Responsabilidad: Dirección de Gestión Estratégica Unidad de Tecnología de la Información

CRONOGRAMA DE ACCIONES A EJECUTAR

	ACTIVIDADES A DESARROLLAR	2014				2015																	
		Julio		Agosto		Marzo		Abril		Mayo		Junio		Julio		Agosto		Septiembre		Octubre		Noviembre		Diciembre	
		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena		Quincena	
		1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
Acciones Inmediatas	Presentar las evidencias necesarias de que en el CONELEC no se brinda este servicio			x																					
Solución Integral	Elaborar el procedimiento de "Control de Acceso"											x	x	x	x	x	x								
	Aprobar el procedimiento de "Control de Acceso"																	x							
	Desplegar el procedimiento de "Control de Acceso"																		x						
	Aplicar el procedimiento de "Control de Acceso"																			x	x	x	x		
	Validar el procedimiento de "Control de Acceso"																							x	x

Elaborado: Daniela Gutiérrez	Revisado: Patricia Cruz	Aprobado: Mercy Coronel
Fecha: 28/07/2014	Fecha: 28/07/2014	Fecha: 28/07/2014
Firma:	Firma:	Firma: