ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"APLICACIÓN DE LA METODOLOGÍA SCRUM PARA IMPLEMENTAR EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN ORIENTADO A SERVICIOS TECNOLÓGICOS"

INFORME DE PROYECTO DE GRADUACIÓN

Previo a la obtención del Título de:
INGENIERO EN TELEMÁTICA

Presentado por:
Adib Abrain Manssur Nicola

Guayaquil – Ecuador

2015

AGRADECIMIENTO

A mi equipo de trabajo en la implementación del EGSI.

A mis compañeros politécnicos por su ayuda.

A los directivos de la FIEC, que siempre dieron una solución a mis problemas.

DEDICATORIA

Dedicada a Dios, por la fuerza y perseverancia que me ha dado.

A mis padres Adib y Taili, a mis hermanas Mercedes y Rannia y a mi sobrina Sadya, a mis familiares, a mis profesores y a mis amigos.

A Ashley y a CEPIFAN.

TRIBUNAL DE SUSTENTACIÓN

MSc. Sara Rios Orellana
SUBDECANA DE LA FIEC

MSc. Patricia Chávez Burbano
DIRECTOR DEL PROYECTO DE GRADUACIÓN

MET. Miguel Molina Villacis
MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Informe me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral."

(Reglamento de Graduación de la ESPOL)

_____

Adib Abrain Manssur Nicola

RESUMEN

La metodología SCRUM aplicado al EGSI es sin duda uno de los proyectos que podrá hacer dar el siguiente paso a la Seguridad de la Información en el Ecuador. El desarrollo de esta nueva forma de implementar la normativa, a la cual llamamos EGSI-SCRUM, es una forma ágil, colaborativa y eficaz de realizar la implementación de lo que nos dicta el Acuerdo 166 dada por SNAP.

Es una manera de saber qué hacer en el día a día, de saber cuánto porcentaje de cierta tarea se deberá cumplir en un momento específico, de reevaluar esfuerzos, de solicitar apoyo directamente a quien se debe, de reunirse a diario con el equipo de trabajo para percibir si las cosas marchan bien o si hay que hacer un cambio. Todo esto bajo el marco SCRUM.

El EGSI-SCRUM nos detalla además quienes serán los responsables de realizar las tareas o hitos específicos, esto con el afán de proponer un orden en la implementación, sin embargo no quiere decir que otros miembros del equipo puedan colaborar. El modelo se podrá visualizar en un GANTT, de tal manera que podremos ver fechas, conocer responsables, modificar variables, y lo más importantes consultar los Sprints y todos sus campos.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CSI	Comité de Gestión de Seguridad de la Información
DTIC	Dirección de Tecnologías de la Información y Comunicaciones
EGSI	Esquema Gubernamental de Seguridad de la Información
GPR	Gobierno Por Resultados
MREMH:	Ministerio de Relaciones Exteriores y Movilidad Humana
MTOP	Ministerio de Transporte y Obras Públicas
SENAGUA	Secretaría del Agua
SGSI	Sistema de Gestión de Seguridad de la Información
SNAP	Secretaría Nacional de Administración Pública

GLOSARIO DE TÉRMINOS

Activo: Todo bien que tiene valor para la Institución.

Amenaza: Escenario o posible acontecimiento que puede causar daño.

Cloud: Término también conocido como “la nube”. Se lo emplea como lugar en donde se va a almacenar información.

Comité de Gestión de Seguridad de la Información: Estará integrado al menos por: el Director Administrativo, el Responsable del área de Recursos Humanos, el Responsable del área de Tecnologías de la Información, el Responsable de Auditoría Interna y el Oficial de Seguridad de la Información. Este ente contará con un Coordinador (Oficial de Seguridad de la Información), quien cumplirá la función de impulsar la implementación del EGSI. [1]

Confidencialidad: Deberán tener acceso a la Información solo las personas autorizadas.

Disponibilidad: Se deberá garantizar el tener acceso a la Información en el momento en que la necesiten.

Impacto: La valoración de cuánto afecta la intrusión en algún activo, en función de los pilares de la Información.

Integridad: Se deberá garantizar que la Información sea exacta y no modificada.

Oficial de Seguridad de la Información: Será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información. El oficial de Seguridad de la Información deberá ser un miembro independiente de las áreas de tecnología o sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la institución y tecnología. [1]

Probabilidad de Riesgo: En el presente documento no está asociado a un número del 0 al 1, sino a una escala descrita en el documento, que valora la posibilidad de que una amenaza se materialice producto de la vulnerabilidad.

Riesgo: El riesgo es una variable que considera que tan sensible es un activo de información y que tan posible es que este sea afectado.

Riesgo Residual: Riesgo que queda luego de su tratamiento.

SCRUM: Es una metodología utilizada para agilizar el desarrollo de proyectos, mediante el trabajo regular e incremental, y el trabajo colaborativo.

SCRUM Master: Es el líder que está al servicio del equipo SCRUM, es el responsable de hacer entender y de que sea aplicada la metodología.

Sprint: Es el núcleo de SCRUM, el cual dura un mes o menos, en este se elabora un incremento del producto terminado.

SQLi: Del término “SQL Injection”, es una técnica de inyección SQL que consiste en hacer consultas a través de los datos de entrada en una aplicación web del cliente. Estas consultas no solo permitirán ver información confidencial, sino modificar y borrar información. [2]

Vulnerabilidad: Algún tipo de desacierto en la seguridad de la Institución con respecto a la Información.

XSS: Del término en inglés “Cross-site scripting”, es un tipo de agujero de seguridad o de inseguridad informático que es típico de las aplicaciones web, son un tipo de inyección, en el que las secuencias de comandos malintencionadas se inyectan en los sitios web. [2]

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La Seguridad de la Información es sin duda una preocupación del siglo XXI, las grandes empresas en la actualidad tienen mayores activos basados en su información que en toda su infraestructura, es esta la razón principal para que este sea un tema que en la actualidad sea muy discutido. Esta preocupación también la tienen las grandes instituciones públicas, aquellas que no solamente contienen información que podrían afectar al ejecutivo en el ámbito político-social, sino que existe información que podría afectar directamente a los ciudadanos, datos como la dirección domiciliaria, como números de teléfono, lugar de trabajo, número de cédula, imágenes de la firma, cuentas bancarias y otras igual de importantes.

El presente documento se enfoca en garantizar una forma ágil de implementar el Esquema de la Seguridad de la Información en las Instituciones Públicas, esquema que está basado en la Norma Internacional ISO 27001. De la misma manera se proponen técnicas para lograr aquello, basándose en una metodología ágil de implementación de proyectos de alto nivel, esta metodología es la SCRUM. Podemos referirnos entonces que es aquí donde la Seguridad de la Información va a concebirse, no solamente en la realización técnica de la misma, sino también en su gestión de desarrollo, planteando tiempos con límite, personas claves en su desarrollo, técnicas

para la mejora continua y muchas otras las cuales funcionan para el EGSI en el contexto del SCRUM.

Se cree que el EGSI-SCRUM deberá irse desarrollando más a fondo a medida de que sea implementado en varias situaciones específicas, para denotar su efectividad y su amplitud, por supuesto que la metodología utilizada no es específica, sin embargo las situaciones podrían ser muy variables, y para ser acordes con lo que se desarrollará, la mejora continua es uno de los puntos claves.

CAPÍTULO 1

1. ANTECEDENTES Y OBJETIVOS

La seguridad de la información cada vez tiene más razones para potencializarse, hace algunas décadas era proteger información gubernamental, de instituciones públicas altamente reconocidas y con información extremadamente confidencial, e incluso se utilizaba solamente en países como Estados Unidos y de la Unión Europea. Más adelante se empezó a utilizar para proteger sitios web, los cuales no eran tan numerosos, y la idea principal de los atacantes o hackers era de hacerse conocer y de que sepan que han sido vulnerados, era una especie de honor hacerlo. Actualmente, todo ha ido creciendo en la digitalización, y lo que antes solo era para instituciones gubernamentales y para ciertos sitios web, ahora es hasta para nuestros hogares y para cualquier sitio web (que son millones) o para algún blog que tenga la víctima, y no solo eso, sino

que los atacantes también han ido mejorando sus técnicas, a tal punto que podríamos estar siendo atacados en este momento sin siquiera saberlo.

1.1. Descripción del problema

La información hoy en día representa uno de los mayores poderes que se puede poseer, sin duda alguna conocemos casos como el de Edward Snowden o el de Julian Assange, los cuales con la información que difundieron provocaron desestabilizar relaciones entre países hermanos. Como estos casos hay muchos, pero lo importante aquí es que los gobiernos que antes no consideraban importante o no lo priorizaban, hoy en día lo hacen, y uno de los gobiernos que lo hace es el ecuatoriano.

Mediante el Acuerdo 166 de la SNAP, el 19 de septiembre del 2013, se estableció que las entidades de la Administración Pública Central, Institucional y que dependen de la función ejecutiva, deberán implementar el EGSI dentro de los próximos 18 meses a la fecha antes mencionada, esto quiere decir que lo deberían tener implementado hasta el 19 de marzo del 2015. Además se menciona también que es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para

mantener la seguridad de la información que se genera y se custodia en diferentes medios y formatos de dichas entidades. [1]

La mayoría de estas entidades gubernamentales ha reportado un cumplimiento menor al 50% del EGSI. Esto se debe a que no hay una forma estandarizada de implementarlo, y más aún, no hay una forma ágil de hacerlo. Sin duda alguna el EGSI nos da directrices de qué hacer para implementarlo, sin embargo no nos dice el cómo.

1.2. Justificación

A pesar de que el objetivo del Acuerdo 166 es asegurar la información de las entidades públicas, podría ser contraproducente, ya que por cumplir la normativa, puede que no se lo haga con el fin que este debería tener, crear un sistema de gestión de seguridad de la información. Por supuesto que las entidades buscan cumplir la normativa, no todas conscientes de lo que significa asegurar la información que manejan, o no todas conscientes del riesgo que podría provocar que su información sea filtrada a un ente externo.

La razón de este documento es crear una manera escalable y ágil de implementar el EGSI, en este caso lo hemos orientado a servicios

tecnológicos para fines prácticos, sin embargo se deberá poder replicar a otro tipo de servicios, como comercial, financiero, entre otros.

Además usaremos la metodología SCRUM, una metodología de trabajo actualmente usada por muchas empresas dedicadas a realizar proyectos, la aplicaremos en el EGSI para así lograr un estándar metodológico, y poder replicarla en las entidades gubernamentales que lo requieran.

1.3. Solución Propuesta

Al pensar en la implementación de una normativa en una Institución del Estado se nos vienen a la cabeza un montón de variables a considerar, como el número de funcionarios, los tipos de servicios que tienen, cuantos servicios tienen, que tanto afecta políticamente los cambios en esta institución a las otras, o al ejecutivo. Por lo tanto la solución conveniente será analizar todos estos puntos en un principio y de una manera estandarizada, y definiremos parámetros o alcances según los valores de las variables antes mencionadas. De esta manera podremos implementar dicha normativa de una manera correcta y ordenada.

Dentro de las metodologías que existen para implementación de proyectos, elegiremos a SCRUM, ya que esta implementación deberá hacerse en un tiempo adecuado, no tan largo, ya que la rotación en las Instituciones Públicas es bastante frecuente, y además dicha metodología es bastante flexible, por lo tanto podremos realizar cambios en el momento adecuado.

1.4. Objetivos

Se detalla a continuación los objetivos necesarios para el estudio y la aplicación de la metodología SCRUM para implementar el EGSI.

1.4.1. Objetivo general

Contribuir a la Confidencialidad, Integridad y Disponibilidad de la Información de los Procesos de apoyo tecnológico, Personas y Recursos Tecnológicos de la entidad gubernamental.

1.4.2. Objetivos específicos

- Incrementar el cumplimiento del EGSI en las entidades gubernamentales, de tal manera que se alcancen niveles aceptables de cumplimiento en los controles que se exigen.
- Establecer procedimientos que nos permitan implementar el EGSI de forma eficaz, óptima y adecuada.
- Alcanzar el cumplimiento gradual y sostenido de lo establecido por el EGSI.
- Reducir progresivamente los riesgos a los niveles aceptables.

1.5. Metodología

En la realización de este proyecto se planificará la implementación gradual del EGSI, de tal forma que se seguirán las directrices que nos brinda el esquema.

- Política 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.

Cada punto tiene concordancia con la garantía de la Seguridad de la Información, y es por eso que nos sirve como metodología. Cabe recalcar que para realizar esta metodología, usaremos otra, la metodología SCRUM, que nos brindará varios lineamientos y alternativas para alcanzar los objetivos planificados.

1.6. Resultados esperados

Con la realización de este proyecto se espera que las entidades gubernamentales puedan gozar de esta contribución para asegurar la Confidencialidad, Integridad y Disponibilidad de la Información que manejan y procesan. Así mismo se espera que el EGSI, más allá de que sea una normativa impuesta por el ejecutivo, pueda concientizar a la mayoría de servidores públicos y que conozcan los riesgos que pueden recaer en ellos al manejar de manera incorrecta un activo de información.

Por último esperaría, que no solo las entidades gubernamentales (instituciones públicas) tengan que implementar un EGSI, sino que la concientización llegue más allá, y que todas las empresas empiecen a asegurar su información, y que luego de esto, quizás, en nuestros hogares, escuelas, dispositivos personales, información personal esté asegurada mediante mecanismos seguros y prácticos.

CAPÍTULO 2

2. MARCO TEÓRICO

Sin lugar a duda la implementación de una Normativa a nivel nacional es importante, y más aún cuando lo que está en juego es la información de millones de ecuatorianos, las negociaciones que se tienen, las agendas del ejecutivo y muchas otras razones por las cuales se debe proteger información de las Instituciones Públicas, sin embargo la pregunta es ¿se lo está haciendo de la forma correcta? Y para respondernos aquello, es necesario conocer a fondo la norma a aplicar, las metodologías, el estado actual del país referente a la Seguridad de la Información y, cuál será la contraparte y de qué forma lo hará en este proceso de implementación.

2.1. EGSI, Esquema Gubernamental de Seguridad de la Información

El EGSI definido por la SNAP como Esquema Gubernamental de Seguridad de la Información es la norma ecuatoriana que deberán

implementar las entidades de Administración Pública Central, Institucional y que dependen de la Función Ejecutiva para tener Gestión en la Seguridad de la Información, el EGSI se basa en las normas técnicas ecuatorianas NTE INEN-ISO/IEC 27000.

Todas las entidades mencionadas en el párrafo anterior deberán implementar el EGSI obligatoriamente, el plazo es de 18 meses y empezó el miércoles 25 de septiembre del 2013, con excepción de ciertos controles prioritarios los cuales debieron implementarse en un plazo de 6 meses después de la fecha mencionada.

Dentro del EGSI, al igual que la normativa internacional ISO 27001:2013, existen dominios que dividen a la norma, estas son: Política 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 y Cumplimiento. [1]

2.2. Metodología SCRUM

SCRUM está basada en la teoría de control de procesos empírica. Y tal y como se define a la palabra empírica, que es un resultado basado en la experiencia, que solo se funda en la observación de los hechos, SCRUM es iterativo e incremental, para que de esta manera la predictibilidad sea óptimo y haya un mayor control de riesgo.

Las metodologías ágiles, de la cual SCRUM forma parte, han alcanzado mejores rendimientos en la elaboración de proyectos, en la comparación en el CHAOS MANIFESTO del 2012 se hizo la comparación entre este tipo de metodologías versus la metodología tipo cascada, en la cual uno de los puntos que sobresale es que la efectividad de las metodologías ágiles supera en gran proporción a las de tipo cascada. [3]

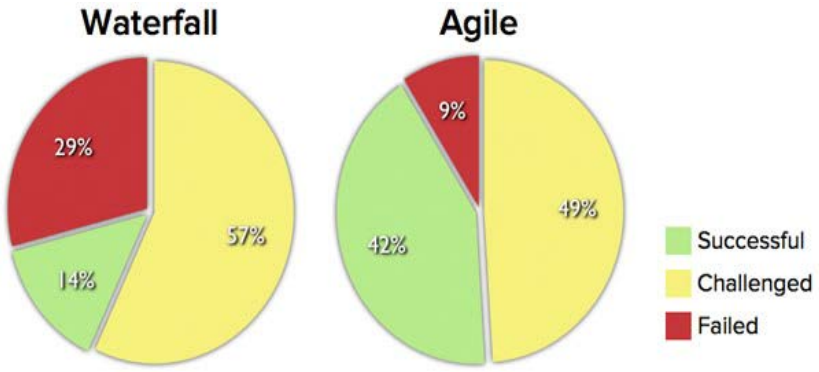


Figura 2.1 Comparación entre metodologías, ágil versus cascada. [3]

La teoría de control de procesos empíricos está basados en tres pilares fundamentales, que son: transparencia, inspección y adaptación. Transparencia: Todos los resultados de los procesos deberán ser visibles para los responsables de dichos resultados, de esta manera podrán observar si son válidos los procesos o si hay que modificarlos para optimizar. Además se deberá tener un estándar en los procesos para que así todos los involucrados puedan entender los resultados y no basarse en interpretaciones, y así eliminar la subjetividad. Por ejemplo: se deberán tener formatos específicos para la entrega de trabajos y resultados finales. Inspección: Por motivos de mejoramiento en los procesos, se deberán inspeccionar los procesos de manera regular, no tan frecuente para no afectar a las operaciones, pero sí en tiempos específicos y adecuados, por ejemplo: realizar una inspección a la tercera semana de trabajo. Además lo recomendable es que la inspección la haga una entidad externa para evitar conflicto de intereses. Adaptación: Una vez que la transparencia esté efectuada y que la inspección se haya realizado, se deberán adaptar los procesos para que no se desvíen de límites aceptables y así obtener resultados aceptables, por lo tanto se deberán realizar ajustes a los procedimientos, de ser necesario, y deberán hacerse cuanto antes para disminuir la posibilidad de error en el resultado final. [3]

2.2.1. Equipo SCRUM

El Equipo SCRUM estará conformado por un dueño del producto, el Equipo de Desarrollo y un SCRUM Master, que es el “líder” del equipo, o la persona que tiene más experiencia para resolver problemas que el resto del equipo no podrá. La principal característica del Equipo SCRUM es de ser auto-organizados y multifuncionales. Sin duda alguna que estas dos características hacen que este equipo no dependa de ningún ente externo, el ser auto-organizado garantiza que los trabajos se realicen sin depender de alguien, y el ser multifuncional hace que este equipo pueda realizar varios trabajos a la vez sin depender de alguien. El objetivo de este equipo de optimizar la flexibilidad, la creatividad y la productividad. El Equipo SCRUM deberá alinear su trabajo con los pilares fundamentales de SCRUM, para que de esta manera al presentar sus trabajos de manera iterativa se pueda lograr una adecuada retroalimentación. En la figura 2.1 se ilustra a los componentes del Equipo SCRUM. [3]

Figura 2.2 Equipo SCRUM [4]

El Dueño del Producto es el encargado de velar por el resultado, por la calidad del producto y por el trabajo del Equipo de Desarrollo. Éste es un aspecto de SCRUM el cual lo hace muy variable entre las organizaciones que apliquen esta metodología. Para garantizar el trabajo, el Dueño del Producto deberá gestionar una Lista de Producto, y será el Dueño del Producto el responsable de que esta lista exprese claramente los elementos de la Lista de Productos, de ordenar los elementos de la lista para garantizar el cumplimiento de los objetivos y misiones óptimamente, de optimizar el valor del trabajo realizado por el Equipo de Desarrollo, de asegurar que la Lista de Producto es visible y transparente para todos, y que

muestra aquello en lo que el equipo trabajará a continuación; y, de asegurar de que el Equipo de Desarrollo entiende los elementos de la Lista de Producto, de tal manera que puedan realizarlo. [3]

El Dueño del Producto podría realizar este trabajo como responsable, o delegarlo al Equipo de Desarrollo. Sin embargo, el único responsable por esta Lista es el Dueño del Producto. El Dueño del Producto deberá ser una persona, no un comité. Si bien la Lista de Producto podría incluir los deseos de algún comité, será el Dueño del Producto el encargado de realizar esta Lista. Además, para modificar esta lista deberá pasar por la aprobación del Dueño del Producto. [3]

De parte de la institución donde se esté trabajando, se deberá brindar todo el apoyo y la autoridad necesaria para que el Dueño del Producto pueda hacer gestión sin ningún problema. Además se deberá garantizar que el liderazgo no se salga del Equipo de Trabajo, y que el Equipo de Desarrollo no trabaje en base a requerimientos externos y que no actúe en base a lo que diga cualquier persona.

El Equipo de Desarrollo está conformado por profesionales en el campo, y son los que van a implementar los controles y a desarrollar las tareas mediante los Sprints, y entregarán las tareas con una etiqueta de “Terminado”, y estas tareas estarán listas para ponerlas en producción. El incremento de algún producto estarán dadas por los “Terminado” en cada Sprint sin embargo la implementación es incremental, tal y como lo define SCRUM. Además estos incrementos solo deberán ser realizados por el Equipo de Desarrollo. Los Equipos de Desarrollo deberán tener el suficiente empoderamiento y deberán tener la estructura adecuada para organizar y gestionar su propio trabajo. Además deberán ser auto-organizados, nadie deberá indicarles cómo convertir elementos de la Lista de Productos en elementos de funcionalidad potencialmente desplegables, deberán ser multifuncionales, deberán estar capacitados para desarrollar tareas que incluyen diferentes tipos de habilidades, no existirán títulos individuales en el equipo, a pesar de las diferentes actividades que realicen y de las aptitudes que tengan, todos serán considerados como desarrolladores, no se reconocerá sub-equipos al Equipo de Desarrollo, no importan los dominios o tareas particulares que

tengan que ser tomadas en cuenta y además cada miembro de este equipo podrá tener habilidades especiales, como ser programador, otro ser experto en Hacking Ético, entre otras. Sin embargo la responsabilidad deberá recaer sobre el Equipo de Desarrollo. [3]

El Equipo de Desarrollo deberá ser lo suficientemente pequeño como para ser ágil y flexible, y deberá ser lo suficientemente grande para garantizar que los trabajos potencialmente grandes y complicados se realicen. La Guía define que este equipo no deberá ser integrado por menos de tres personas, ya que esto podría afectar a la hora de entregar trabajos, y no deberá tener más de nueve personas, ya que esto podría afectar el correcto desenvolvimiento de la metodología, por ejemplo a la hora de realizar un Sprint se deberá garantizar que se sigan cumpliendo los pilares de SCRUM, el que tenga muchos integrantes hará que cada miembro del equipo deban evaluar esto, lo cual complica la gestión. Quienes deberán definir este tamaño deberán ser quienes estén trabajando en la Lista de Pendientes de Sprint, los cuales no incluyen al Master SCRUM ni al Dueño del Producto, a menos que decidan trabajar también en esta Lista de Pendientes.

El servicio del SCRUM Master al Dueño del Producto; el SCRUM Master brinda apoyo y servicios al Dueño del Producto, como encontrar técnicas para gestionar la Lista de Producto de manera efectiva, ayudar al Equipo SCRUM a entender la necesidad de contar con una Lista de Producto claros y concisos, entender la planificación del producto en un entorno empírico, asegurar que el Dueño del Producto sepa cómo priorizar y ordenar la Lista de Producto para maximizar el valor, entender y practicar la agilidad y facilitar los eventos de SCRUM según se requiere o se necesite. [3]

El servicio del SCRUM Master al Equipo de Desarrollo; el SCRUM Master brinda apoyo y servicios al Equipo de Desarrollo, como guiar al Equipo de Desarrollo en ser auto-organizado y multifuncional, ayudar al Equipo de Desarrollo a crear productos de alto valor, eliminar impedimentos para el progreso del Equipo de Desarrollo, facilitar los eventos de SCRUM según se requiera o necesite y guiar al Equipo de Desarrollo en el entorno de organizaciones en las que SCRUM aún no ha sido adoptado y entendido por completo. [3]

El servicio del SCRUM Master a la Organización; el SCRUM Master brinda apoyo y servicios a la Organización, como liderar y guiar a la organización en la adopción de SCRUM, planificar las implementaciones de SCRUM en la organización, ayudar a los empleados e interesados a entender y llevar a cabo SCRUM y el desarrollo empírico de producto, motivar cambios que incrementen la productividad del Equipo SCRUM y trabajar con otros SCRUM Masters para incrementar la efectividad de la aplicación de SCRUM en la organización. [3]

2.2.2. Eventos SCRUM

La idea de definir eventos en la metodología es predefinir reuniones para analizar la regularidad que se va teniendo, y evitar cualquier reunión no planificada inicialmente. Todo evento deberá tener definido un tiempo específico, el cual no deberá ser alargado ni cortado, claro que el tiempo deberá ser el adecuado. Los tiempos en los Sprints deberán ser adecuados, y podrán ser cerrados los eventos siempre que los objetivos sean alcanzados. Siendo fieles a los pilares de SCRUM, los eventos dan la oportunidad para inspeccionar y lograr la adaptación

según convenga. Por lo tanto, los eventos deberán estar diseñados para lograr la transparencia e inspección, de tal manera que si no se realizan, se estarán perdiendo insumos que podrán poner en riesgo la transparencia y con ello toda la metodología.

Se podrá cancelar un Sprint antes de que el bloque de tiempo llegue a su fin. El único autorizado para cancelar un Sprint es el Dueño del Producto, el cual puede hacerlo recibiendo insumos de los interesados, como el SCRUM Master o el Equipo de Desarrollo.

La razón principal de cancelar un Sprint es que el Objetivo del Sprint haya quedado obsoleto. Esto podría darse por diferentes razones, una de ellas es que la Institución cambie la dirección, o si las condiciones externas cambian también. En general un Sprint deberá cancelarse si es que no tuviese sentido seguir con éste dado el entorno. Sin embargo, por la duración que tienen los Sprints, que es muy corto, rara vez se tiene que cancelar uno.

Cuando se cancela un Sprint, se revisan todos los Elementos de la Lista de Producto que se hayan completado y “Terminado”. Si una parte del trabajo es potencialmente entregable, el Dueño de Producto normalmente lo acepta. Todos los Elementos de la Lista de Producto no completados se vuelven a estimar y se vuelven a introducir en la Lista de Producto. El trabajo finalizado en ellos pierde valor con rapidez y frecuentemente debe volverse a estimar.

Las cancelaciones de Sprint consumen recursos, ya que todos deben reagruparse en otra Reunión de Planificación de Sprint para empezar otro Sprint. Las cancelaciones de Sprint son a menudo traumáticas para el Equipo SCRUM y son muy poco comunes.

El Objetivo del Sprint es una meta establecida para el Sprint que puede ser alcanzada mediante la implementación de la Lista de Producto. Proporciona una guía al Equipo de Desarrollo acerca de por qué está construyendo el incremento. Es creado durante la reunión de Planificación del Sprint. El objetivo del Sprint ofrece al equipo de desarrollo cierta flexibilidad con

respecto a la funcionalidad implementada en el Sprint. Los elementos de la Lista del Producto seleccionados ofrecen una función coherente, que puede ser el objetivo del Sprint. El objetivo del Sprint puede representar otro nexo de unión que haga que el Equipo de Desarrollo trabaje en conjunto y no en iniciativas separadas.

A medida que el equipo de desarrollo trabaja, se mantiene el objetivo del Sprint en mente. Con el fin de satisfacer el objetivo del Sprint se implementa la funcionalidad y la tecnología. Si el trabajo resulta ser diferente de lo que el Equipo de Desarrollo espera, ellos colaboran con el Dueño del Producto para negociar el alcance de la Lista de pendientes del Sprint.

SCRUM describe 4 procesos formales dentro de un Sprint que son: Reunión de Planificación de un Sprint, SCRUM diario, Revisión del Sprint y Retrospectiva del Sprint, estos deberán hacerse de forma secuencial e iterativa. En la figura 2.3 se ilustra el proceso formal de SCRUM.

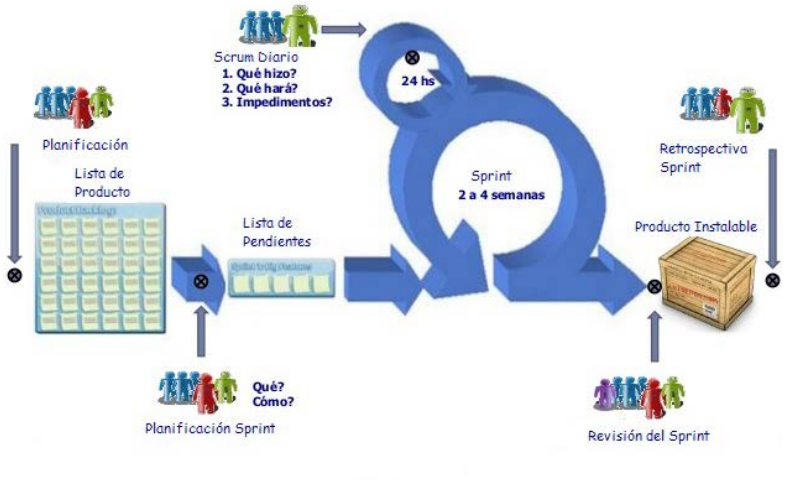


Figura 2.3 Proceso de SCRUM [5]

Reunión de Planificación de Sprint.- El trabajo a realizar durante el Sprint se planifica en la Reunión de Planificación de Sprint. Este plan se crea mediante el trabajo colaborativo del Equipo SCRUM completo. La Reunión de Planificación de Sprint tiene un máximo de duración de ocho horas para un Sprint de un mes. Para Sprints más cortos, el evento es usualmente más corto. El SCRUM Master se asegura de que el evento se lleve a cabo y que los asistentes entiendan su propósito. El SCRUM Master enseña al Equipo SCRUM a mantenerse dentro del bloque de tiempo. La Reunión de Planificación de Sprint deberá ser capaz de entregar el incremento resultante del Sprint que comienza, y de saber cómo

se conseguirá hacer el trabajo necesario para entregar dicho incremento. [3]

El primer tema que deberá desarrollarse es que el Equipo de Desarrollo trabaja para proyectar la funcionalidad que se desarrollará durante el Sprint. El Dueño de Producto discute el objetivo que el Sprint debería lograr y los Elementos de la Lista de Producto que, si se completan en el Sprint, lograrían el Objetivo del Sprint. El Equipo SCRUM completo colabora en el entendimiento del trabajo del Sprint. La entrada a esta reunión está constituida por la Lista de Producto, el último Incremento de producto, la capacidad proyectada del Equipo de Desarrollo para el Sprint, y el rendimiento pasado del Equipo de Desarrollo. El número de elementos de la Lista de Producto seleccionados para el Sprint depende únicamente del Equipo de Desarrollo. Solo el Equipo de Desarrollo puede evaluar qué es capaz de lograr durante el Sprint que comienza. Después de que el Equipo de Desarrollo proyecta qué elementos de la Lista de Producto entregará en el Sprint, el Equipo SCRUM elabora un Objetivo del Sprint. El Objetivo del Sprint debería lograrse durante el Sprint a través de la implementación de la Lista de

Producto, y provee una guía al equipo de desarrollo de por qué se está construyendo el incremento.

El segundo tema que deberá establecerse son los elementos de la Lista de Producto para el Sprint, el Equipo de Desarrollo decide cómo construirá esta funcionalidad para formar un Incremento de producto “Terminado”. Los elementos de la Lista de Producto seleccionados para este Sprint, más el plan para terminarlos, recibe el nombre de Lista de Pendientes del Sprint. El Equipo de Desarrollo por lo general comienza diseñando el sistema y el trabajo necesario para convertir la Lista de Producto en un Incremento de producto funcional. El trabajo podría ser de tamaño o esfuerzo estimado variables. Sin embargo, durante la Reunión de Planificación del Sprint, se planifica suficiente trabajo como para que el Equipo de Desarrollo pueda hacer una proyección de lo que cree que puede completar en el Sprint que comienza. Para el final de esta reunión, el trabajo planificado por el Equipo de Desarrollo para los primeros días del Sprint es descompuesto en unidades de un día o menos. El Equipo de desarrollo se auto-organiza para asumir el trabajo de la Lista de Pendientes de Sprint, tanto

durante la reunión de Planificación de Sprint como a lo largo del Sprint. [3]

El Dueño de Producto puede ayudar a clarificar los elementos de la Lista de Producto seleccionados y hacer concesiones. Si el Equipo de Desarrollo determina que tiene demasiado trabajo o que no tiene suficiente trabajo, podría renegociar los elementos de la Lista de Producto seleccionados con el Dueño de Producto. El Equipo de Desarrollo podría también invitar a otras personas a que asistan con el fin de que proporcionen asesoría técnica o relacionada con el dominio. Al finalizar la Reunión de Planificación de Sprint, el Equipo de Desarrollo debería ser capaz de explicar al Dueño de Producto y al SCRUM Master cómo pretende trabajar como un equipo auto-organizado para lograr el Objetivo del Sprint y crear el Incremento esperado.

SCRUM diario.- El SCRUM Diario es una reunión con un bloque de tiempo de 15 minutos para que el Equipo de Desarrollo sincronice sus actividades y cree un plan para las siguientes 24 horas. Esto se lleva a cabo inspeccionando el

trabajo avanzado desde el último SCRUM Diario y haciendo una proyección acerca del trabajo que podría completarse antes del siguiente. El SCRUM Diario se realiza a la misma hora y en el mismo lugar todos los días para reducir la complejidad. Durante la reunión, cada miembro del Equipo de Desarrollo explica sus actividades del día anterior para lograr objetivos del Sprint, las actividades del presente día para ayudar a lograr el objetivo y da a conocer razones por las cuales cree que no se podrán cumplir los objetivos planteados.

El Equipo de Desarrollo usa el SCRUM Diario para evaluar el progreso hacia el Objetivo del Sprint y para evaluar qué tendencia sigue este progreso hacia la finalización del trabajo contenido en la Lista del Sprint. El SCRUM Diario optimiza las posibilidades de que el Equipo de Desarrollo cumpla el Objetivo del Sprint. Cada día, el Equipo de Desarrollo debería entender cómo intenta trabajar en conjunto como un equipo auto-organizado para lograr el Objetivo del Sprint y crear el Incremento esperado hacia el final del Sprint. El Equipo de Desarrollo o los miembros del equipo a menudo se vuelven a reunir inmediatamente después del SCRUM Diario, para tener

discusiones detalladas, o para adaptar, o re-planificar el resto del trabajo del Sprint.

El SCRUM Master se asegura de que el Equipo de Desarrollo tenga la reunión, pero el Equipo de Desarrollo es el responsable de dirigir el SCRUM Diario. El SCRUM Master enseña al Equipo de Desarrollo para que mantenga el SCRUM Diario en los límites del bloque de tiempo de 15 minutos. El SCRUM Master se asegura de que se cumpla la regla de que solo los miembros del Equipo de Desarrollo participan en el SCRUM Diario. [3]

Los SCRUM Diarios mejoran la comunicación, eliminan la necesidad de mantener otras reuniones, identifican y eliminan impedimentos relativos al desarrollo, resaltan y promueven la toma de decisiones rápida, y mejoran el nivel de conocimiento del Equipo de Desarrollo. El SCRUM Diario constituye una reunión clave de inspección y adaptación.

Revisión del Sprint.- Al final del Sprint se lleva a cabo una Revisión de Sprint para inspeccionar el Incremento y adaptar la Lista de Producto si fuese necesario. Durante la Revisión de

Sprint, el Equipo SCRUM y los interesados colaboran acerca de lo que se hizo durante el Sprint. Basándose en esto, y en cualquier cambio a la Lista de Producto durante el Sprint, los asistentes colaboran para determinar las siguientes cosas que podrían hacerse para optimizar el valor. Se trata de una reunión informal, no una reunión de seguimiento, y la presentación del Incremento tiene como objetivo facilitar la retroalimentación de información y fomentar la colaboración. [3]

Se trata de una reunión restringida a un bloque de tiempo de cuatro horas para Sprints de un mes. Para Sprints más cortos, se reserva un tiempo proporcionalmente menor. El SCRUM Master se asegura de que el evento se lleve a cabo y que los asistentes entiendan su propósito. El SCRUM Master enseña a todos a mantener el evento dentro del bloque de tiempo fijado. En la Revisión de Sprint deberá asistir obligatoriamente el Equipo SCRUM y los interesados clave deberán ser invitados por el Dueño de Producto, según crea conveniente. En la revisión se deberá explicar qué elementos de la Lista de Producto se han “Terminado” y cuales no se han “Terminado” y lo deberá hacer el Dueño del Producto; el Equipo de Desarrollo deberá comunicar acerca de qué fue bien durante el Sprint, qué

problemas aparecieron y cómo fueron resueltos esos problemas, también deberán demostrar el trabajo que se ha “Terminado” y responder preguntas acerca del Incremento; además se deberá comunicar acerca de la Lista de Producto en el estado actual. Proyecta fechas de finalización probables en el tiempo basándose en el progreso obtenido hasta la fecha (si es necesario) lo cual deberá hacer el Dueño del Producto; y todos deberán colaborar acerca de qué hacer a continuación, de modo que la Revisión del Sprint proporcione información de entrada valiosa para Reuniones de Planificación de Sprints subsiguientes. Se deberá revisar de cómo el mercado o el uso potencial del producto podría haber cambiado y afectar las próximas operaciones, y revisar la línea de tiempo, presupuesto, capacidades potenciales y mercado para la próxima entrega prevista del producto. [3]

El resultado de la Revisión de Sprint es una Lista de Producto revisada, que define los elementos de la Lista de Producto posibles para el siguiente Sprint. Es posible además que la Lista de Producto reciba un ajuste general para enfocarse en nuevas oportunidades.

Retrospectiva del Sprint.- La Retrospectiva de Sprint es una oportunidad para el Equipo SCRUM de inspeccionarse a sí mismo y crear un plan de mejoras que sean abordadas durante el siguiente Sprint.

La Retrospectiva de Sprint tiene lugar después de la Revisión de Sprint y antes de la siguiente Reunión de Planificación de Sprint. Se trata de una reunión restringida a un bloque de tiempo de tres horas para Sprints de un mes. Para Sprints más cortos se reserva un tiempo proporcionalmente menor. El SCRUM Master se asegura de que el evento se lleve a cabo y que los asistentes entiendan su propósito. El SCRUM Master enseña a todos a mantener el evento dentro del bloque de tiempo fijado. El SCRUM Master participa en la reunión como un miembro del equipo ya que la responsabilidad del proceso SCRUM recae sobre él. [3]

El propósito de la Retrospectiva de Sprint es inspeccionar cómo fue el último Sprint en cuanto a personas, relaciones, procesos y herramientas; identificar y ordenar los elementos más

importantes que salieron bien y las posibles mejoras; y, crear un plan para implementar las mejoras a la forma en la que el Equipo SCRUM desempeña su trabajo. [3]

El SCRUM Master alienta al equipo para que mejore, dentro del marco de proceso SCRUM, su proceso de desarrollo y sus prácticas para hacerlos más efectivos y amenos para el siguiente Sprint. Durante cada Retrospectiva de Sprint, el Equipo SCRUM planifica formas de aumentar la calidad del producto mediante la adaptación de la Definición de "Terminado" según sea conveniente. [3]

Para el final de la Retrospectiva de Sprint, el Equipo SCRUM debería haber identificado mejoras que implementará en el próximo Sprint. El hecho de implementar estas mejoras en el siguiente Sprint, constituye la adaptación subsecuente a la inspección del Equipo de Desarrollo a sí mismo. Aunque las mejoras pueden implementarse en cualquier momento, la Retrospectiva de Sprint ofrece un evento dedicado para este fin, enfocado en la inspección y la adaptación.

2.2.3. Artefactos SCRUM

Los artefactos de SCRUM representan trabajo o valor en diversas formas que son útiles para proporcionar transparencia y oportunidades para la inspección y adaptación. Los artefactos definidos por SCRUM están diseñados específicamente para maximizar la transparencia de la información clave, que es necesaria para asegurar que todos tengan el mismo entendimiento del artefacto.

La Lista de Producto es una lista ordenada de todo lo que podría ser necesario en el producto, y es la única fuente de requisitos para cualquier cambio a realizarse en el producto. El Dueño de Producto es el responsable de la Lista de Producto, incluyendo su contenido, disponibilidad y ordenación.

Una Lista de Producto nunca está completa. El desarrollo más temprano de la misma solo refleja los requisitos conocidos y mejor entendidos al principio. La Lista de Producto evoluciona a medida de que el producto y el entorno en el que se usará también lo hacen. La Lista de Producto es dinámica; cambia constantemente para identificar lo que el producto necesita para

ser adecuado, competitivo y útil. Mientras el producto exista, su Lista de Producto también existe.

La Lista de Producto enumera todas las características, funcionalidades, requisitos, mejoras y correcciones que constituyen cambios a ser hechos sobre el producto para entregas futuras. Los elementos de la Lista de Producto tienen como atributos la descripción, la ordenación, la estimación y el valor.

A medida que un producto es utilizado y se incrementa su valor, y el mercado proporciona retroalimentación, la Lista de Producto se convierte en una lista más larga y exhaustiva. Los requisitos nunca dejan de cambiar, así que la Lista de Producto es un artefacto vivo. Los cambios en los requisitos de negocio, las condiciones del mercado o la tecnología podrían causar cambios en la Lista de Producto.

A menudo, varios Equipos SCRUM trabajan juntos en el mismo producto. Para describir el trabajo a realizar sobre el producto, se utiliza una única Lista de Producto. En ese caso podría

emplearse un atributo de la Lista de Producto para agrupar los elementos. El refinamiento de la Lista de Producto es el acto de añadir detalle, estimaciones y orden a los elementos de la Lista de Producto. Se trata de un proceso continuo, en el cual el Dueño de Producto y el Equipo de Desarrollo colaboran acerca de los detalles de los elementos de la Lista de Producto. Durante el refinamiento de la Lista de Producto, se examinan y revisan sus elementos. El Equipo SCRUM decide cómo y cuándo se hace el refinamiento. Este usualmente consume no más del 10% de la capacidad del Equipo de Desarrollo. Sin embargo, los elementos de la Lista de Producto pueden actualizarse en cualquier momento por el Dueño de Producto o a criterio suyo. [3]

Los elementos de la Lista de Producto de orden más alto son generalmente más claros y detallados que los de menor orden. Los elementos de la Lista de Producto de los que se ocupará el Equipo de Desarrollo en el siguiente Sprint tienen una granularidad mayor, habiendo sido descompuestos de forma que cualquier elemento puede ser “Terminado” dentro de los límites del bloque de tiempo del Sprint. Los elementos de la Lista de Producto que pueden ser “Terminados” por el Equipo

de Desarrollo en un Sprint son considerados “preparados” o “accionables” para ser seleccionados en una reunión de Planificación de Sprint. Los elementos de la Lista de Producto normalmente adquieren este grado de transparencia mediante las actividades de refinamiento descritas anteriormente. [3]

El Equipo de Desarrollo es el responsable de proporcionar todas las estimaciones. El Dueño de Producto podría influenciar al Equipo ayudándoles a entender y seleccionar soluciones de compromiso, pero las personas que harán el trabajo son las que hacen la estimación final.

La Lista de Pendientes del Sprint es el conjunto de elementos de la Lista de Producto seleccionados para el Sprint, más un plan para entregar el Incremento de producto y conseguir el Objetivo del Sprint. La Lista de Pendientes del Sprint es una predicción hecha por el Equipo de Desarrollo acerca de qué funcionalidad formará parte del próximo Incremento y del trabajo necesario para entregar esa funcionalidad en un Incremento “Terminado”. [3]

La Lista de Pendientes del Sprint hace visible todo el trabajo que el Equipo de Desarrollo identifica como necesario para alcanzar el Objetivo del Sprint. La Lista de Pendientes del Sprint es un plan con un nivel de detalle suficiente como para que los cambios en el progreso se puedan entender en el SCRUM Diario. El Equipo de Desarrollo modifica la Lista de Pendientes del Sprint durante el Sprint y esta Lista de Pendientes del Sprint emerge a lo largo del Sprint. Esto ocurre a medida que el Equipo de Desarrollo trabaja sobre el plan y aprende más acerca del trabajo necesario para conseguir el Objetivo del Sprint. [3]

Según se requiere nuevo trabajo, el Equipo de Desarrollo lo añade a la Lista de Pendientes del Sprint. A medida que el trabajo se ejecuta o se completa, se va actualizando la estimación de trabajo restante. Cuando algún elemento del plan pasa a ser considerado innecesario, es eliminado. Solo el Equipo de Desarrollo puede cambiar su Lista de Pendientes del Sprint durante un Sprint. La Lista de Pendientes del Sprint es una imagen visible en tiempo real del trabajo que el Equipo de

Desarrollo planea llevar a cabo durante el Sprint, y pertenece únicamente al Equipo de Desarrollo. [3]

SCRUM se basa en la transparencia. Las decisiones para optimizar el valor y controlar el riesgo se toman basadas en el estado percibido de los artefactos. En la medida en que la transparencia sea completa, estas decisiones tienen unas bases sólidas. En la medida en que los artefactos no son completamente transparentes, estas decisiones pueden ser erróneas, el valor puede disminuir y el riesgo puede aumentar.

El SCRUM Master debe trabajar con el Dueño de Producto, el Equipo de Desarrollo y otras partes involucradas para entender si los artefactos son completamente transparentes. Hay prácticas para hacer frente a la falta de transparencia; el SCRUM Master debe ayudar a todos a aplicar las prácticas más apropiadas si no hay una transparencia completa. Un SCRUM Master puede detectar la falta de transparencia inspeccionando artefactos, reconociendo patrones, escuchando atentamente lo que se dice y detectando diferencias entre los resultados esperados y los reales. [3] La labor del SCRUM Master es

trabajar con el Equipo SCRUM y la organización para mejorar la transparencia de los artefactos. Este trabajo usualmente incluye aprendizaje, convicción y cambio. La transparencia no ocurre de la noche a la mañana, sino que es un camino.

2.3. Seguridad de Información en el Ecuador

Los profesionales de la Seguridad de la Información tienen la obligación profesional de educar y enseñar técnicas para lograr que nuestra información esté segura. Antes, cuando nuestros documentos estaban en papel, de manera física en algún repositorio, era fácil saber cuándo hacía falta o no, sin embargo buscarlo y encontrarlo en el mismo repositorio era un trabajo en el cual una persona podría tardarse dependiendo del orden y tamaño del mismo desde 5 minutos hasta varios días. Esto sin duda alguna se resolvió con la digitalización de la información, para encontrar documentos digitales, en un repositorio digital, basta con llenar uno o varios campos y hacer un clic. Cada vez más nuestra información es digital, cada vez más usamos servicios para evitar trabajo que podemos hacerlo tan solo con un clic. Para realizar transferencias bancarias, para registrarnos en materias de nuestra Universidad, para pagar las cuentas de los servicios básicos, entre otras. Esta es una realidad que la vivimos en el Ecuador, y sin duda alguna deberíamos hacer conciencia sobre

aquello, deberíamos empezar a identificar si nuestras contraseñas son lo suficientemente robustas y qué significa que sean robustas, si existe información delicada en nuestro buzón de correo, el tener planes de contingencia por si nos roban el teléfono celular, deberíamos poder proteger nuestra información. Y así podríamos señalar muchas otras situaciones sobre la Seguridad de la Información en el Ecuador, y sin duda alguna, deberíamos empezar a hacer conciencia desde ya. A este paso, con la rapidez que se desarrolla y que se implementa nueva tecnología en nuestro país, tendremos casas inteligentes muy pronto (ya existen unas cuantas) y si no protegemos nuestra información en la actualidad, podríamos imaginar qué pasaría con casas inteligentes.

Sin duda alguna, la Seguridad de la Información va de la mano con la confianza, esta nos ayuda a crear una cadena de confianza mediante la cual la mayoría de personas nos sentimos seguros de lo que tenemos.

En el Ecuador, al igual que en el mundo entero se tiene que empezar a concientizar sobre la Seguridad de la Información. Actualmente la disposición presidencial de implementar el EGSI nos dice que estamos

pasando esa barrera, sin duda alguna que no será fácil, no solo la implementación sino mantener el sistema, ya que si las personas no están totalmente involucradas con proteger la información, puede no funcionar.

2.4. La SNAP y su contribución a la Seguridad de la Información

La Secretaría Nacional de Administración Pública mediante el Acuerdo Ministerial 166 ha avanzado en lo que respecta a la Seguridad de la Información en el Ecuador. Si bien este acuerdo es obligatorio para las Instituciones Públicas, y el cumplimiento que se ha dado hasta ahora es eso, simple cumplimiento, se está empezando por algo, creo que la Seguridad de la Información debería ir de menos a más, empezando en la escuela con los niños, luego los niños lo llevarán a las familias, las personas lo llevarán al trabajo y finalmente se tendrá una armonía de lo que se necesita, pero si es que funciona de esta manera, bienvenido sea, y más aún cuando son los funcionarios públicos en las Instituciones Públicas los que están dando o darán el ejemplo de cómo asegurar nuestra información, nuestra porque es de todos los ecuatorianos.

Sin duda alguna el trabajo que ha venido realizando la SNAP ha sido exhaustivo, sin embargo hay muchas observaciones que realizar a los procesos se deben implementar, los Sistemas de Seguridad de la Información se basan en eso, en una mejora continua con revisiones frecuentes, por lo tanto el EGSI está dentro del marco que debería estar.

Cabe recalcar que la mayoría de Instituciones Públicas no han dado cumplimiento total con el EGSI, en primera instancia con los 126 hitos o controles que establece la SNAP, y mucho menos con el resto. Y las que sí han dado cumplimiento, lo han venido realizando sin un enfoque preciso, por ejemplo: en un control se menciona el etiquetado de CDs, si bien es cierto es un control tácito y que hay que cumplir, pero deberíamos saber si la información dentro de estos es importante, y si no lo es poder obviar este control, o previo al etiquetado de CDs, definir un alcance del Sistema, ya que no es posible implementar de golpe un Sistema riguroso en toda una Institución, que en este caso es pública, y esto en promedio de servidores podría estar entre 300 y 600 funcionarios. Por lo tanto, nuevamente es responsabilidad de los profesionales de la Seguridad de la Información en brindar observaciones relevantes, para que la

contribución que hace el SNAP, la cual es positiva y muy buena, sea más efectiva.

CAPÍTULO 3

3. CONCEPTOS DEL EGSI

El EGSI ha sido el primer gran paso para evolucionar a las Instituciones Públicas en lo que concierne a la Seguridad de la Información, sin embargo es nuestro deber preguntarnos si el paso fue el correcto, si hay observaciones al respecto, qué podemos mejorar. Y para dar insumos interesantes al respecto debemos dar un recorrido por esta normativa, debemos pensar en su ciclo de implementación y saber qué es lo estrictamente necesario y que no lo es. Cabe recalcar que el EGSI está basado en la mayoría de su contenido a la norma internacional de Seguridad de la Información, la ISO 27001:2005, y actualmente ya existe una nueva versión de la norma la ISO 27001:2013, la cual sí tiene cambios significativos con respecto a su anterior versión. Este capítulo nos hará entender en su totalidad la normativa impuesta por el SNAP, el EGSI.

3.1. Recorrido por las cláusulas

Existen 11 dominios que deberán ser analizadas, para conocer qué controles son los que se deberán implementar sin desconocer el enfoque que se le da en la normativa.

Tal y como en la normativa internacional ISO 27001, el EGSI tiene cláusulas de cumplimiento mandatorio y otras de cumplimiento recomendado, las cuales deberán ser clasificadas para saber cuál es el esfuerzo que se utilizará.

3.1.1. Política de Seguridad de la Información

Se deberá disponer de parte de la máxima autoridad la implementación del EGSI en toda la institución, esta máxima autoridad deberá garantizar que los controles se implementen para así dar cumplimiento.

Además se deberá difundir la política de la Seguridad de la Información en la Institución, la cual el EGSI ya cita: “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" [1]. Cabe recalcar que esta política no es tácitamente obligatoria y la entidad pública podrá ampliarla como desee, sin embargo no deberá irse en contra de las leyes que rigen a esta institución ni del EGSI.

3.1.2. Organización de Seguridad de la Información

La máxima autoridad de la institución deberá estar comprometida con el Sistema de Gestión de la Seguridad de la Información (SGSI), dos de los controles más importante es la creación del Comité de Gestión de la Seguridad de la Información (CSI) y la designación del Oficial de Seguridad de la Información, asignando al CSI y al Oficial sus respectivos roles y responsabilidades.

Con respecto a los servicios tecnológicos, el EGSI dispone a un Responsable del Área de Tecnologías de la Información, el cual tiene como tarea controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones o sistemas, evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos, administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento, monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, controlar la obtención de copias de resguardo de información, asegurar el registro de las actividades realizadas por el personal operativo, desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas, implementar controles de seguridad definidos como evitar software malicioso o accesos no autorizados, definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, gestionar los incidentes de seguridad y otras que por naturaleza de la seguridad de la información deban ser atendidas.

3.1.3. Gestión de los Activos

Dentro de los controles de la gestión de activos, se encuentra el inventariar los mismos, dentro de los activos que son prioritarios para el EGSI se encuentran los procesos estratégicos, normas y reglamentos, planes estratégicos y operativos, archivos generados por los servidores públicos, manuales e instructivos de sistemas informáticos, de la operación de los aplicativos informáticos, del desarrollo de los aplicativos, del soporte de los aplicativos, de la imagen corporativa de la institución, además de todo esto el inventario del software y hardware de la Institución. Dentro de la Gestión de Activos también se asignarán responsables de los activos y se indicarán procedimientos para el uso aceptable de los mismos. Además se exigen lineamientos para la clasificación de la información, y el etiquetado y manejo de la información.

3.1.4. Seguridad de los Recursos Humanos

Dentro de las cláusulas ubicadas en este dominio se establecerán controles de seguridad en el aspecto laboral de los funcionarios, como la revisión de sus antecedentes previo a su contratación, el cerciorarse de sus competencias previo a su contratación y a los que ya son funcionarios, la adquisición de competencias cuando ya se labora, los roles y

responsabilidades asignadas, la entrega de activos, y en el momento de despedir a algún funcionario, se deberán adquirir controles como la devolución de activos, eliminar los accesos a los sistemas de la Institución, eliminar sus cuentas Institucionales, adquirir un respaldo de su información.

3.1.5. Seguridad Física y del Entorno

En esta sección el EGSI plantea mecanismos para evitar intrusión a la Institución, tanto para personas que no son funcionarios como para funcionarios sin autorización de acceso, además se dispondrán controles de seguridad de oficinas, recintos e instalaciones. Se deberán disponer de medidas de contingencia contra amenazas o catástrofes naturales, así como la creación de áreas seguras, de carga, de despacho y de acceso público. En este dominio también se menciona la correcta ubicación de los equipos informáticos, para que de esta manera el personal no autorizado no necesite entrar a lugares con acceso restringido.

3.1.6. Gestión de Comunicaciones y Operaciones

Para asegurar las operaciones en las Instituciones Públicas, el EGSI nos pide documentar todos los procedimientos operativos, distribuir las funciones correctamente, gestionar cambios en las operaciones que se realicen sin importar lo pequeño que sea este cambio, separar ambientes de desarrollo, producción, pruebas y capacitación. Los cambios en los servicios ofrecidos por terceros a la Institución también deberán gestionarse, la capacidad de los sistemas deberán ser suficientes para que las operaciones no se caigan, con respecto al código de los sistemas que manejen los programadores, se deberán disponer controles contra código malicioso, el aislamiento de dispositivos móviles debe ser un control necesario en la Institución, se deberá respaldar la información, se deberá incorporar sistemas de seguridad para los servicios ofrecidos en la red, se deberá crear procedimientos seguros para la disposición de medios, tanto de la información que contiene como para el dispositivo en sí, se deberán establecer lineamientos para el control de la mensajería instantánea, se deberán tener toda clase de registros de auditorías que se hayan realizado en la Institución, se deberán también los accesos autorizados y los accesos privilegiados, para el correcto desempeño de los sistemas de procesamiento de

información se deberán sincronizar los relojes de estos sistemas.

3.1.7. Control de Acceso

El EGSI nos habla sobre una política de control de acceso, la cual debe de indicar que se registren a los funcionarios que accedan a los sistemas de información que la organización considere como información importante, además deberá definir los permisos que tengan los funcionarios y deberá definir quien otorga estos permisos. Dentro del acceso al usuario se deberán tener acciones muy fijas para cierta información que los funcionarios manejen, por ejemplo la gestión de contraseñas para usuarios, la revisión de derechos de acceso al usuario, la política del puesto de trabajo, la política de uso de servicios de red y otras que se consideren importantes en el acceso a los sistemas de información de los usuarios, cabe recalcar que al mencionar accesos a sistemas de información no solo estamos hablando de sistemas informáticos, sino de un puesto de trabajo, un manual de funcionario o algo relacionado con información relevante para la institución.

3.1.8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Se deberán definir los requerimientos de seguridad de la información para los Sistemas de Información, el fin de esto será adquirir tecnología para proteger información acorde con las necesidades. Los controles que se implementen podrán ser automatizados o manuales, se deberán validar datos de entrada y de salida de los sistemas, se deberán usar controles criptográficos, controlar el acceso al código fuente del programa, el cual podría ser vulnerado por SQLi, XSS o alguna otra técnica de intrusión que algún Hacker conozca y esté interesado en nuestra organización.

3.1.9. Gestión de los Incidentes de la Seguridad de la Información

El EGSI en esta sección define que se deben crear políticas y procedimientos sobre toda la gestión de eventos de seguridad de la información, así como reportes, correcciones, acciones correctivas, acciones preventivas, análisis y evaluación de riesgos, tratamiento de los riesgos y así cualquier tipo de evento que relacione a la seguridad de la información. Luego del debido tratamiento de los riesgos, se deberán realizar informes para tomar estos riesgos como aprendizaje para el SGSI de la

organización, además se deberán crear métricas para ir evaluando el cumplimiento del EGSI e ir abarcando más incidentes que puedan materializarse. Es importante también definir que no todos los incidentes podrán ser tratados, y si la organización está consciente de aquello, a estos se los tratarán como riesgos residuales.

3.1.10. Gestión de la Continuidad del Negocio

La continuidad del negocio es algo de lo que las empresas hoy en día se están preocupando en su totalidad, y esto empieza por un plan de contingencia para su personal, luego para sus bienes, podría seguir sus equipos en los cuales estén ya incluidos sus equipos informáticos y por último sus servicios informáticos, que finalmente son los que los clientes usan, por ejemplo imaginemos una catástrofe natural en los Estados Unidos, la cual no es muy alejada de la realidad, que pasaría si esto afectara a los servidores donde están alojados las plataformas informáticas de Facebook, o donde están los datos de usuarios, todo el servicio se caería sin remediación alguna, es por eso que la continuidad del negocio es un tema importante y es justo aquí donde se definen políticas en la empresa, roles y responsabilidades, estructura para la

planificación, pruebas, mantenimiento y revisión de los planes de continuidad. De esta manera, al evitar que los servicios pierdan su continuidad, estamos logrando que el ser de la Institución no deje de estar, lo cual si pasara en una Institución pública, podría representar consecuencias a nivel económico, social y político en todo un estado.

3.1.11. Cumplimiento

Además de cumplir con la normativa del EGSI se deben cumplir las leyes que están por encima de esta norma, como son la Constitución del Ecuador, la LOTAIP, el Código Civil, el estatuto de la Institución y cualquier otra. Es importante saber esto, porque a la hora de dar cumplimiento con el EGSI podemos afectar a normativas mucho más importantes. También se debe tener en cuenta a los derechos de propiedad intelectual, se deberán proteger los registros de cada entidad, de deberán adquirir controles criptográficos.

3.2. Ciclo de implementación del EGSI

El ciclo de implementación del EGSI se divide en controles prioritarios y controles no prioritarios, a los cuales llamaremos mandatorios y

recomendados. Sabiendo que desde el 25 de septiembre del 2013 el EGSI fue expedido por la SNAP y debió ser implementado a partir de esa fecha, los controles mandatorios en 6 meses y los recomendados en 18 meses, esto significa que el 25 de marzo del 2014 debieron estar implementados los mandatorios y que el 25 de marzo del 2015 se debió completar toda la implementación del EGSI en las entidades públicas. Sin duda alguna el tiempo que debemos preparar para la implementación del EGSI deberá ser menor, esa es la razón de este documento, pero por motivos de tiempos exigidos por la norma no podremos cumplir en su totalidad, sin embargo esperaremos reducir los tiempos exigidos y aun así alcanzar el cumplimiento en su totalidad. Los controles mandatorios y recomendados deberemos separarlos y clasificarlos para su futuro uso, sin embargo lo lógico será implementar los mandatorios antes que los recomendados.

Otro aspecto clave en la implementación de todos estos controles es saber en qué ámbito lo haremos y para qué herramientas, a eso lo conoceremos como alcance de la implementación.

3.3. Información y procedimientos mandatorios

Existen 126 hitos mandatorios que deberán ser implementados, según el EGSI, en 6 meses. Los 126 hitos se los adjuntará como anexo en el presente documento. Sin embargo es importante para entender cómo será la elaboración de estos indicando cuantos hitos deberán cumplirse por cada dominio del EGSI, lo cual se referencia mediante la Tabla 3.1.

Tabla 1 Hitos del EGSI por dominio

Dominio	**Cantidad de Hitos**
Política de Seguridad de la Información	2
Organización de Seguridad de la Información	10
Gestión de los Activos	20
Seguridad de los Recursos Humanos	3
Seguridad Física y del Entorno	12
Gestión de Comunicaciones y Operaciones	28
Control de Acceso	36
Adquisición, Desarrollo y Mantenimiento de SI	2
Gestión de los Incidentes de la Seguridad de la Información	13
Gestión de la Continuidad del Negocio	0
Cumplimiento	0
Total	**126**

Donde podemos notar que los dominios de Control de Acceso, Gestión de Comunicaciones y Operaciones, y de Gestión de Activos exigen 84 hitos, lo que representa más del 65% de la totalidad de los mandatorios. Justamente en estas se concentra la implementación tecnológica, configuraciones de red, el aseguramiento del código

fuente, las buenas prácticas y controles en donde se pueda evidenciar que la Institución no solo ha hecho inversión en equipos, sino en personal especializado en seguridad de la información, en este caso más específico, en seguridad informática.

A estos dominios podríamos sumarle incluso la de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, sin embargo bastó con esas tres para demostrar que el proyecto, sea la Institución que sea, es totalmente tecnológico, y además de Gestión.

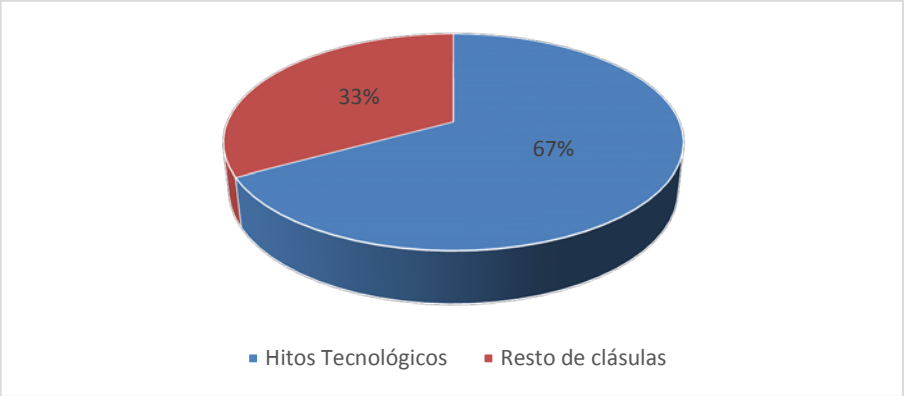


Figura 3.1 Porcentaje de dominios con aplicación tecnológica

3.4. Información y procedimientos recomendados

Al igual que en los controles mandatorios, el resto de controles o los no mandatorios también tienen una fecha para dar cumplimiento en los mismos. Los controles en específico se encontrarán como anexo en el presente documento, sin embargo debemos tener información

específica sobre esta parte del EGSI. En el Anexo A se encuentran las cláusulas que deberán cumplirse para dar cumplimiento a los controles recomendados, o también conocidos como hitos del EGSI Fase 2.

Podemos darnos cuenta de que las cláusulas son muchas, y que para cada cláusula hay varios controles que exige el EGSI, sin embargo es prudente mencionar que si existen controles definidos, implementados y aplicados para las cláusulas la SNAP da cumplimiento, lo cual hace sentido con el ser de la Seguridad de la Información.

Estos controles debieron estar implementados el 25 de marzo del 2015, sin embargo las Instituciones Públicas han demorado en la implementación del EGSI, y eso es algo que nos conviene, de no ser así, este documento no tendría sentido. Resulta que recién el 15 de enero del 2015 la SNAP da un ranking de las Instituciones Públicas que han cumplido el mandato y las que no, lo hacen mediante porcentajes de cumplimiento por cada hito, pero lo hacen sobre los 126 hitos, esto quiere decir que apenas este 10 de enero la SNAP ha auditado la primera fase, y aun así existe un incumplimiento de las Instituciones Públicas de casi el 70%.

La siguiente tabla nos mostrará detalladamente como ha ido evolucionando la implementación del EGSI en su fase inicial, indicando que se han dado 4 cortes, el primero fue el 25 de marzo del 2014, el segundo el 1 de julio del 2014, el tercero el 10 de octubre y el último el 15 de enero del presente año.

LEYENDA										
% DE HITOS CUMPLIDOS EGSI	SEMÁFORO	NIVEL DE CUMPLIMIENTO EGSI	AL 25 DE MARZO DE 2014		AL 1 DE JULIO DE 2014		AL 10 DE OCTUBRE DE 2014		AL 15 DE ENERO DE 2014	
			CANTIDAD DE ENTIDADES	% DE ENTIDADES DENTRO DEL NIVEL DE CUMPLIMIENTO DEL EGSI	CANTIDAD DE ENTIDADES	% DE ENTIDADES DENTRO DEL NIVEL DE CUMPLIMIENTO DEL EGSI	CANTIDAD DE ENTIDADES	% DE ENTIDADES DENTRO DEL NIVEL DE CUMPLIMIENTO DEL EGSI	CANTIDAD DE ENTIDADES	% DE ENTIDADES DENTRO DEL NIVEL DE CUMPLIMIENTO DEL EGSI
90% a 100%	Verde	Alto	1	0,78%	12	9,30%	21	16,28%	39	30,23%
75% a 89 %	Amarillo	Medio	7	5,43%	12	9,30%	16	12,40%	18	13,95%
50% a 74 %	Naranja	Regular	7	5,43%	10	7,75%	12	9,30%	20	15,50%
Menor a 50%	Rojo	Bajo	114	88,37%	95	73,64%	80	62,02%	53	40,32%
TOTAL			129	100,00%	129	100,00%	129	100,00%	129	100,00%

Figura 3.2 Porcentaje del cumplimiento del EGSI [4]

Y aun así entre el amarillo, naranja y rojo hacen un total del 69,77% lo cual nos demuestra que aún hay mucho trabajo por hacer, y más aún en la forma de implementar el EGSI.

El tiempo para alcanzar estos niveles ha sido de 18 meses, para lo cual estaba presupuestado hacerlo en 6 meses. La fase dos o la implementación total del EGSI se debió alcanzar en 18 meses, sin embargo aún es incierto el tiempo que va a demorar esta fase, y esto es algo que deberemos definirlo en algún momento.

CAPÍTULO 4

4. CONFIGURACIÓN DEL SCRUM PARA APLICABILIDAD EN EL EGSI

Una vez estudiado el EGSI y sus componentes, y conociendo en teoría todo sobre SCRUM, podemos usar estas herramientas que hemos adquirido para configurar el SCRUM de tal manera que podamos aplicarlo en el EGSI en su totalidad, recordando que hay entes que el EGSI pide de forma obligatoria, y conociendo también que SCRUM pide que en su aplicación se conforme su estructura de cierta manera, por lo tanto, la idea de este capítulo es asociar lo obligatorio tanto por la metodología como por la norma y hacerlo una sola, y luego asociar lo recomendado por ambas y hacerlo una sola. Finalmente lo que deberíamos obtener es, las mismas tareas del EGSI de forma ordenada, de una manera lista para implementar, con sus respectivos responsables, con sus tiempos de implementación y por supuesto con sus respectivos entregables.

Es aquí donde la aplicación de la metodología empieza a tomar forma, y una vez que obtengamos los insumos suficientes para poder implementar, procederemos a realizarlo en forma de prueba en una entidad gubernamental.

4.1. Parametrización de la metodología

Analizando detenidamente la metodología SCRUM y el EGSI nos damos cuenta de que tienen bastante en común, y al menos lo suficiente para parametrizar la metodología y hacerlo lo necesariamente aplicable a la normativa. En el caso de SCRUM podemos notar gracias a la Figura 2.1 al Equipo SCRUM, que es lo necesario para comenzar con esta metodología, en el caso del EGSI podemos recordar que es necesario conformar el CSI para proceder con la mayor parte de la implementación, la cual es dirigida por el Oficial de Seguridad de la Información, al igual que el Dueño del Producto con el Equipo de Desarrollo en SCRUM.

En la Tabla 4.1 se puede apreciar cuales son las funciones asociadas a los entes principales. Si bien es cierto la comparación de los roles del personal en la metodología y en la normativa no fue complicada,

no solo es eso lo que hay que comparar, todo lo contrario, la implementación de los controles que nos da el EGSI es lo más importante y así mismo el SCRUM se preocupa por cosas más importantes, y recordemos que el Sprint es conocido como el núcleo en esta metodología.

Tabla 2 Equipo SCRUM – EGSI

SCRUM	EGSI	Función
Dueño del Producto	Oficial de Seguridad	Será el encargado de velar por el cumplimiento de los productos terminados. Será quien convoque a las reuniones con el equipo de trabajo (CSI). Será el que presida las reuniones con el equipo de trabajo (CSI). Otras tareas de alto nivel que estarán bajo su responsabilidad.
Equipo de Desarrollo	CSI	Este comité o equipo estará conformado por varios miembros, los cuales deberán tener diferentes tipos de aptitudes para así poder dominar diferentes aspectos a la hora de la implementación de un control. Este comité o equipo será el encargado de realizar las tareas que deban ejecutarse para el cumplimiento del EGSI, y si bien pueden delegar tareas, no se reconocerán a un sub-equipo a este, por lo tanto quienes tendrán la responsabilidad de cumplimiento será este comité.

SCRUM	EGSI	Función
SCRUM Master	Consultor de Seguridad (experto)	Como bien se lo menciona en la definición, el SCRUM Master es un miembro de apoyo del equipo, para las instituciones públicas podría funcionar como un asesor, que tenga que ser un experto en la seguridad de la información, con conocimientos técnicos y de gestión, capaz de resolver problemas que el CSI no pueda resolver. Por lo tanto lo recomendable es que la entidad contrate con consultor de seguridad, que deberá ser quien asesore en la implementación del EGSI.

Recordando un poco la función del Sprint, es para elaborar incrementos del producto en cuestión, en este caso será para elaborar incrementos en los controles, varios controles van a ejecutarse en paralelo y es por eso que debemos clasificarlos de la forma correcta. Además cada iteración deberá dar paso a un incremento o a un producto terminado de la Lista de Producto, la cual estará basada en un Project realizado por el Oficial de Seguridad, sin embargo para efectos demostrativos deberemos generar ese documento. Los SCRUM diarios deberán realizarse con normalidad, el horario y el lugar se lo deberá definir una vez se tenga identificado el caso. La cancelación de un Sprint solo podrá ser realizada por el Oficial de Seguridad con la debida justificación, la cual deberá ser presentada ante el CSI. Además recordando la Figura 2.2 que se refiere al proceso SCRUM, deberemos planificar inicialmente la Lista de

Producto que podrá ser modificada por el Oficial de Seguridad, como cada Sprint se deberá hacer de manera frecuente, se deberá planificar cada Sprint con la misma frecuencia y en nuestro caso lo haremos seguido de las revisiones del Sprint, la metodología menciona que para Sprints de un mes es necesaria una reunión de aproximadamente 4 horas, sin embargo esta revisión será tanto para presentar adelantos o productos terminados, seguido de dar observaciones y finalmente plantear el siguiente Sprint, recordando que a diario se realizarán reuniones es bastante certero de que esta reunión sea solo para presentar productos, y para eso necesitaremos realizar los SCRUM diarios como ya lo mencionamos antes, se deberá revisar objetivos del día como qué se logrará o cuánto se avanzará, se deberá tener al tanto los avances del día anterior, de tal manera que se pueda cambiar el rumbo del Sprint si es que este no satisface como se requiere a los adelantos del producto terminado, a esto lo conoceremos como retrospectiva del Sprint, y en las revisiones del Sprint se podrá modificar la Lista de Producto si las directrices de la Institución cambia, lo cual es muy probable en las Instituciones Públicas debido a la rotación tan alta de personal, esto solamente podrá hacerlo el Oficial de Seguridad, siempre y cuando haya la debida justificación y esta sea presentada ante el CSI. Otro de los artefactos SCRUM importante es la Lista de Pendientes, recordemos

que la metodología define a esta lista como aquella que el Equipo de Desarrollo va elaborando en beneficio de qué podrá faltar en el presente Sprint o de qué va a ser útil en un Sprint futuro, es una lista que nos ayudará y nos proporcionará información necesaria para elaborar correctamente el siguiente Sprint, es por eso que se pedirá al Equipo de Desarrollo o al CSI que en cada SCRUM diario presente insumos para la Lista de Pendientes. Por lo tanto, la parametrización de SCRUM a EGSI se ha realizado en su totalidad, con el fin de lograr una implementación más ágil, más rápida y más eficaz.

4.2. Estimación del tamaño del EGSI en la entidad gubernamental

Sin lugar a dudas que al obtener la parametrización nos damos cuenta de que SCRUM es aplicable a proyectos de cualquier tipo, en nuestro caso un proyecto mayoritariamente tecnológico, sin embargo es importante denotar eso a la hora de la implementación del EGSI, que el alcance sea tecnológico. Para esto haremos referencia a ciertos hitos específicos que nos da la normativa. En la Gestión de Activos es necesario inventariar a los mismos, tanto al software como al hardware, pero el EGSI nos exige inventariar activos como teclados, ratones, micrófonos, cámaras y otros parecidos, y es correcto hacerlo, hasta para que no haya perjuicio para la Institución a la hora de manejar estos objetos, sin embargo, imaginemos que no tenemos

ningún inventario y que no se ha hecho nunca, algo que es raro y más aún si es una Institución Pública, pero imaginemos que no se ha hecho nunca, donde deberíamos enfocarnos para dar cumplimiento de la norma, pues si bien lo que queremos es proteger la información sensible de la Institución, deberíamos empezar por las Áreas donde más se maneje información de este tipo. La propuesta entonces será la siguiente, analizar la Institución, analizar los servicios que son más utilizados por los ciudadanos o por sus clientes, analizar la información que se maneja en estos servicios y de ahí dar un alcance, e implementar los controles más amplios del EGSI en esas áreas, sin duda alguna que el SGSI deberá ser continuo y acaparar más áreas, pero si la idea es ser eficaz y ágil debemos priorizar.

Con todo lo mencionado es necesario enfocar en donde obligatoriamente debemos interceder con la normativa, sin olvidarnos del análisis previo. Para esto nos basaremos en lo que dice la norma dentro sus controles. Mediante la siguiente tabla explicaremos a todas las áreas que van a estar involucradas, y para esto nos bastaremos con los 126 hitos, que son los que deberán implementarse en menor tiempo que los restantes.

Como observamos en el Anexo B la máxima autoridad juega un rol importante en el EGSI y es justamente la de crear el equipo de trabajo y dar un seguimiento adecuado, si bien es cierto un Ministro o un Secretario de Gobierno tiene otras ocupaciones igual de importantes, pero alguien debe de hacerlas, entonces la responsabilidad de la implementación del EGSI recaerían en el CSI y el Oficial de Seguridad, dos entes ya parametrizados en SCRUM.

En el caso del Oficial de Seguridad o Dueño del Producto es impetuosamente necesario que esté involucrado en todas las tareas, sin embargo hay tareas específicas que él debe cumplir, las cuales están señaladas en el Anexo C.

Si bien es cierto el caso debe ser generalizado y no específico para alguna estructura organizacional de alguna Institución Pública, podemos elegir los factores comunes que estas tienen e ir planteando ciertos argumentos, para esto hemos elegido al azar tres Instituciones del Estado que se encuentran en el listado de las 129 del ranking por cumplimiento del EGSI. Las cuales son: MREMH, MTOP y SENAGUA. Por lo tanto filtraremos las áreas que nos puedan ayudar en la implementación de controles del EGSI y filtraremos por las que tengan

en común. Para esto hemos escogido las tres estructuras orgánicas de estas Instituciones [5] [6] [7] y hemos procedido a hacer el análisis previsto.

Las áreas comunes y de interés son: Dirección de Administración de Recursos Humanos, Dirección Administrativa, Dirección de Auditoría Interna, Dirección de Comunicación Social, Dirección de Tecnologías de la Información y Comunicación, y dentro de las Coordinaciones tenemos: Coordinación General Jurídica, Coordinación General de Planificación. La Secretaría General es el ente que está encargada de administrar toda la parte documental, y finalmente un Área de Procesos, que puede estar con diferentes nombres sin embargo es el área dedicada a estructurar debidamente todos los procesos que ocurren en la Institución. Por lo tanto podremos encaminar ciertos hitos o controles a estas direcciones.

La Dirección Administrativa estará encargada de velar por los procesos de inventarios, de control de acceso de personal o de dispositivos electrónicos, por los mantenimientos, por la seguridad física de la Institución y actividades similares tal y como nos muestra la en Anexo D.

Un área imprescindible para cualquier norma de la Seguridad de la Información es la de Talento Humano, o en el caso de las Instituciones Públicas de nuestro país la Administración de Recursos Humanos, esta es la que vela justamente por el personal, por la revisión de antecedentes, por saber si tienen las competencias necesarias para adquirir un puesto en la Institución, por clarificar los roles dentro de un puesto de trabajo, por capacitar al personal para que adquieran nuevas competencias y actividades similares tal y como nos muestra el Anexo E, recordando que este departamento o área no vela por ningún concepto tecnológico, sin embargo se suele decir que el eslabón más débil en una cadena de confianza es el Talento Humano.

Si bien es cierto toda las Áreas anteriormente clasificadas como importantes y como comunes entre las Instituciones Públicas las utilizaremos, sin embargo para ser coherentes con los objetivos nos centraremos en esta última sección, en el núcleo de la Información, la DTIC. La DTIC es en donde se concentra toda la información, desde el almacenamiento, el procesamiento, hasta la entrega de productos terminados a los clientes, sin duda alguna que si este departamento tiene huecos en su seguridad, toda la información que maneje la

Institución quedará expuesta, es por eso que es aquí en donde se concentra la mayor parte de la implementación, ver Anexo F.

Por lo tanto es claro que el EGSI será primero aplicado en aquellas áreas que son sustanciales en la implementación, y para aquellos controles que sean muy generales, lo recomendable será enfocarlos en un servicio que sea muy demandado y que la Institución lo considere dentro de los servicios con los cuales se identifiquen, esto lo podemos denotar con los objetivos institucionales.

4.3. Estimación del esfuerzo necesario para implementación del EGSI

Una de las partes más importantes de esta implementación es el estimar el esfuerzo necesario para implementar el EGSI, ya es la principal razón por la cual decidiríamos implementar o no esta norma, en caso de que fuere opcional, el esfuerzo que realiza la Institución implica horas de trabajo para sus funcionarios, contratar más personal o quizás contratar personal externo como consultores y esto conlleva inversión económica, la cual la mayoría de los funcionarios públicos cuidan y prefieren invertirla en nuevas herramientas o servicios que consideren más relevantes para elevar a la Institución la cual presiden, sin embargo cuando se conoce el fondo de la Seguridad de la

Información y de lo que podría pasar si existe alguna falla de seguridad que podríamos haber evitado, es justo ahí cuando tomamos conciencia y daríamos el esfuerzo necesario para implementar esta normativa de seguridad. Recordemos un poco a las áreas que estarán involucradas en dicha implementación, la Dirección Administrativa, la Dirección de Administración de Recursos Humanos, la DTIC, la máxima autoridad y el Oficial de Seguridad, hasta ahí ellos deberán conformar el CSI necesariamente, y con esto tenemos 4 funcionarios sin contar la máxima autoridad que por razones de tiempo no estará y que las Direcciones mencionadas solo tengan un funcionario.

Recordando que hay 126 hitos necesitaremos más personal en el Equipo de Desarrollo, y a pesar de que los representantes de las Direcciones vayan a delegar trabajo a sus subalternos, deberemos tener personas oficialmente encargadas, ya que la metodología SCRUM no reconoce sub-equipos al Equipo de Desarrollo. Imaginemos que tenemos 10 personas en este equipo, y que para cumplir un hito, el promedio de tiempo sean 15 horas por, quiere decir que un funcionario cumple un adelanto del producto en 5 días laborables trabajando 3 horas a la semana en el EGSI, o sea que en una semana podría cumplir 10 hitos, los cuales en 3 meses ya estarían cubiertos. Y el resto podría estar en otros 9 meses,

asumiendo que el cálculo es lineal. Sin embargo esto es algo que lo calcularemos efectuando un levantamiento inicial del estado de la Institución, estimando por control cuanto demoraría en implementarse una solución, conociendo con cuanto personal trabajaríamos y en qué áreas están especializados, para que de esta manera podamos enfocarlos en lo que mejor hacen y poder optimizar el trabajo del Equipo de Desarrollo, y desarrollando la implementación en el día a día con errores que podrían ocurrir pero que podríamos corregir, estimar el esfuerzo necesario para lograr la implementación del EGSI.

Además de todo lo mencionado, debemos ser enfáticos en que a la hora de implementar el EGSI, todo podrá cambiar, empezando por el personal, es por eso que el primer paso será lo más importante, el primer paso deberá definir el compromiso entre la Institución y el Equipo de Trabajo, y no entre una persona, que representa a una Institución, y un grupo de trabajo que está elaborando un proyecto. Es justamente aquí donde el esfuerzo empieza, y si hay un completo compromiso de la alta dirección, el trabajo se terminará.

Por lo tanto, las estimaciones han sido realizadas con su respectivo margen de error, sin embargo se considera que lo que se ha realizado

previamente es una línea base del trabajo que se deberá realizar, sin duda alguna será más amplio, pero es algo que necesariamente deberá ir en cualquier trabajo futuro.

4.4. Análisis de tiempo necesario de implementación

El EGSI define claramente que para implementar la fase inicial se debió hacerlo desde el 25 de septiembre del 2013 al 25 de marzo del 2014, y que la fase final se debió hacer desde el 25 de septiembre del 2013 al 25 de marzo del 2015, sin embargo en la mayoría de Instituciones Públicas aún no se da cumplimiento de la fase inicial hasta el 15 de Enero del 2015, en otras palabras, la mayoría de Instituciones se han demorado casi dieciséis (16) meses en lugar de los seis (6) meses estipulados, mientras que la fase final con un plazo de dieciocho (18) meses tampoco fue cumplida.

El tiempo es uno de los aspectos más importantes en la aplicación del EGSI, por lo cual hemos elegido una metodología ágil, que nos ayude con la implementación del EGSI de una manera más rápida y eficaz. Para organizar de mejor manera la implementación lo adecuado será dividirla en dos fases: Fase 1 y Fase 2, tal y como lo recomienda la

norma. En la Fase 1 se implementarán los 126 hitos base y en la Fase 2 los restantes.

Fase 1: Conociendo esta es la fase más crítica del proyecto, es aquí donde debemos enfocar todo el esfuerzo necesario para llevar el sistema a algo cotidiano y normal dentro de la Institución. Desde que se empiece la implementación, no solo se tratará de cumplir la normativa al pie de la letra, sino de buscar que la normativa signifique algo para la Institución, que signifique una forma de trabajo, que se vea reflejado por sus buenas prácticas y que quizás en algún momento se transforme en una forma de vida. Sin embargo, retomando la Fase 1 nos damos cuenta de que son 126 hitos que deberemos cumplir en un tiempo menor a 6 meses, aproximando horas de trabajo para un individuo en seis (6) meses, serían 960 horas, asumiendo que trabaja 20 días en un mes y ocho (8) horas diarias, esto nos da como resultado que por hito un elemento debería demorar 7,6 horas, lo cual es un poco complicado debido a que esto significaría que por cada día debería cumplir un nuevo control, dedicando todo su esfuerzo a esta implementación, por lo tanto la propuesta es formar un equipo de trabajo, el cual sea avalado por la dirección, no dedicar todo el esfuerzo de trabajo al proyecto, sino tres (3) o cuatro (4) horas diarias por persona en el equipo, e

incrementaremos la hora por hito cumplido, que deberá rondar entre diez (10) y veinte (20) horas. En un equipo de trabajo de entre diez y quince personas, tenemos los siguientes escenarios:

El peor escenario será contar con 10 personas en el equipo y con que los 126 hitos sean de 20 horas, esto supondría que para completar los 126 hitos deberíamos ocupar 2520 horas en total. Sin embargo, en el caso de que tengamos a 10 integrantes en el equipo, y que cada uno dedique solamente 3 horas diarias al proyecto, tendríamos 30 horas diarias disponibles (150 horas por semana), lo cual resulta en 17 semanas de trabajo (poco más de 4 meses). Dado que tan solo el 30% de las Instituciones Públicas han cumplido con la implementación de la Fase inicial del EGSI en 16 meses, este tiempo es conveniente y alentador.

El mejor escenario es contar con 15 personas y que los 126 hitos sean de 10 horas, lo cual debería ocuparnos un total de 1260 horas. Y al contar con 15 individuos en el equipo y que cada uno de ellos dedicará 3 horas diarias al proyecto, tenemos 45 horas diarias (225 horas semanales), lo cual representa seis (6) semanas aproximadamente para implementación. Esto sería una gestión

envidiable, puesto que esta fase fue programada para 6 meses, y lamentablemente ha tomado más de 16 meses en la mayoría de los casos, se podría completar en un mes y medio.

Porcentualmente hemos descendido en el peor escenario un 34% en el tiempo de implementación, y en el mejor escenario hemos reducido un 75% en el tiempo de implementación.

Fase 2: Una vez hayamos superado la Fase 1, la Fase 2 deberá realizada de la misma manera con la que realizó la Fase 2. En esta fase no nos concentraremos en el número de hitos, sino en el número de cláusulas y porcentualmente lo que estas significan.

Tabla 3 Número de Cláusulas por Dominio de la Fase 2

Dominio	**Cláusulas Fase 2**
Política de Seguridad de la Información	1
Organización de Seguridad de la Información	9
Gestión de los Activos	5
Seguridad de los Recursos Humanos	9
Seguridad Física y del Entorno	13
Gestión de Comunicaciones y Operaciones	29
Control de Acceso	23
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	16
Gestión de los Incidentes de la Seguridad de la Información	5

Dominio	Cláusulas Fase 2
Gestión de la Continuidad del Negocio	5
Cumplimiento	10
Total	**125**

Como podemos observar, nuevamente la implementación se concentra mayoritariamente en el aspecto tecnológico, en los 4 dominios donde más se debe intervenir es prioritaria la implementación de equipos tecnológicos, de configuraciones, de mejoramientos de procesos en los cuales puedan incluirse controles automatizados. Sin embargo, en esta ocasión el dominio de Cumplimiento es uno de los que más tiene cláusulas, que además de tener implementación tecnológica al igual que los otros, también se concentra en la gestión.

Para hacer un análisis del tiempo que será necesario en la Fase 2, retomamos las recomendaciones del EGSI con respecto al tiempo para implementar esta fase, la cual fue de dieciocho (18) meses. Aplicando linealidad nos podemos dar cuenta de que si estas 125 cláusulas necesitan 18 meses (2880 horas), entonces se debería invertir tres días de trabajo (23 horas). La propuesta será parecida a la de la Fase 1, y es por eso que la reducción porcentual deberá ser similar. Para el mejor de los casos deberemos descender 34% del

tiempo necesario y en el mejor de los casos 75% del mismo. Por lo tanto, la implementación de la Fase 2 deberá durar entre 720 horas y 1900 horas, lo cual significa de cuatro (4) meses y medio hasta casi un (1) año. Finalmente, se reparten las horas para cada dominio según las cláusulas que estos tengan.

Tabla 4 Horas por dominio Fase 2

Dominio	**# de horas mejor caso**	**# de horas peor caso**
Política de Seguridad de la Información	5,76	15,2
Organización de Seguridad de la Información	51,84	136,8
Gestión de los Activos	28,8	76
Seguridad de los Recursos Humanos	51,84	136,8
Seguridad Física y del Entorno	74,88	197,6
Gestión de Comunicaciones y Operaciones	167,04	440,8
Control de Acceso	132,48	349,6
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	92,16	243,2
Gestión de los Incidentes de la Seguridad de la Información	28,8	76
Gestión de la Continuidad del Negocio	28,8	76
Cumplimiento	57,6	152
Total de horas	**720**	**1900**

CAPÍTULO 5

5. APLICACIÓN DE LA METODOLOGÍA SCRUM EN LA IMPLEMENTACIÓN DEL EGSI

Las condiciones en las que se realice la aplicación de la metodología son cruciales para determinar el tamaño del EGSI, el esfuerzo necesario y el tiempo de implementación que tendrá nuestra metodología. Es aquí donde se reconocerán los parámetros que tenderemos y desde ahí aplicar nuestra metodología para una correcta implementación desde el punto de vista de SCRUM. A pesar de esto, se debe entender que así como funcionarán para estos parámetros, deberán funcionar para otros, o iguales pero con diferentes valores, eso es transparente para nuestra metodología. Deberemos ser específicos a la hora de describir el caso, de tal manera que podamos identificar rápidamente y sin tanto esfuerzo ciertas cosas que nos ayuden a plantear de manera óptima la implementación

Así mismo deberemos plantear aplicaciones de esta metodología a toda la normativa en general, así como a las dos fases que hemos identificado, la primera basada en controles prioritarios y la segunda de toda la norma. Y al final deberemos plantear adecuadamente cual es el EGSI-SCRUM tan buscado.

5.1. Descripción del caso

La Institución a la que haremos referencia existe, sin embargo por motivos de proteger su Información y todo lo que con esta viene, no revelaremos el nombre de la Institución. Además de esto los datos que se mostrarán serán válidos pero no reales, esto lo haremos multiplicando cada valor utilizado en esta entidad por una constante.

Deben de haber ciertos parámetros que ya los describimos con anterioridad que deberán ser transparentes, entre ellos la estructura orgánica de la Institución, los Objetivos Institucionales, los servicios que se ofrecen, los activos que hagan funcionar a estos servicios, las personas a cargo de los activos y lo que la norma considere como necesario.

Como ya lo mencionamos hay estructuras orgánicas muy parecidas entres las Instituciones Públicas, lo cual hace que pueda replicarse una implementación en otra. En este el Anexo G nos muestra la estructura orgánica en la cual simularemos la implementación.

Se han omitido ciertos nombres y ciertos departamentos para mantener confidencial a la Institución. Como podemos observar se encuentran las áreas que considerábamos que estaban en la mayoría de Instituciones Públicas, y en función de eso pudimos saber a priori quien podría estar en el Equipo de Desarrollo o también llamado CSI utilizando la norma. Pero no es suficiente, en el caso de que los servicios de agregación de valor, sean justamente los que hagan que nuestros objetivos institucionales se cumplan, entonces algo primordial será que el encargado de estas direcciones se incluya también.

De igual manera los objetivos estarán simplificados, dado que si se los redacta de igual manera que en el Estatuto Orgánico podría repercutir a la Institución. Los objetivos se centran en: Incrementar la inserción estratégica del Ecuador en la comunidad internacional, en mantener la soberanía del país entre la comunidad internacional, que los intereses regionales correspondan a los intereses nacionales, incrementar la

cobertura de los servicios ofrecidos a nivel internacional, garantizar calidad de los servicios ofrecidos, incrementar la difusión y promoción de los derechos de las personas a través de los servicios.

De la misma manera no se especificarán detalles de los servicios ofrecidos por las mismas razones por las cuales no revelamos el nombre de la Institución, sin embargo no podremos omitir que activos de información usan estos servicios de forma general. Los servicios que hacen que los objetivos institucionales se cumplan son: e-SIGEX, sistema informático utilizado por la Institución para verificar datos de ciudadanos, para realizar pagos a la Institución y que sirve conjuntamente a otras herramientas como base de datos. PS, herramienta utilizada por los ciudadanos para adquirir documentos de forma rápida y sencilla. Y CV, herramienta que engloba a todos los servicios de manera que los ciudadanos se enteren de todo lo que ofrece esta Institución a través de ella. Estas tres herramientas generan servicios que van acorde con los objetivos institucionales, obviamente no todos, pero si los que se le ofrece algo a la ciudadanía.

5.2. Aplicación general

En función de lo que tenemos, deberemos conformar lo que SCRUM nos pide en función del EGSI. Mediante la tabla 5.1 expondremos al equipo de trabajo, junto con su rol en SCRUM y en el EGSI.

Tabla 5 Equipo EGSI – SCRUM

SCRUM	**EGSI**	**Integrantes**
Dueño del Producto	Oficial de Seguridad	Oficial de Seguridad
Equipo de Desarrollo	CSI	Viceministro de Gestión Interna
		Director de Administración de Talento Humano
		Director Administrativo
		Director de Asuntos Legales de Gestión Interna
		Director de Servicios, Procesos y Calidad
		Director de la Gestión Documental y Archivo
		Coordinador General de TIC'S
		Director de Desarrollo TI
		Director de Infraestructura y Operaciones TI
		Director de Seguridad Informática TI
		Director de Servicio y Soporte al Usuario
		Coordinador General de Auditoría Interna
		Director de Comunicación Social
		Director de Documentos y Servicios
		Director de Gestión y Servicios
SCRUM Master	Especialista en Seguridad de la Información	Consultor de empresa externa

Como podemos observar hemos obtenido una de las variables más importantes en nuestra metodología, el número de personas en el

equipo, y particularmente en el Equipo de Desarrollo, las cuales son 15 personas.

Para desarrollar de mejor manera las tareas, deberemos asignar lo que deberá corresponderles según sus competencias. Separaremos a nuestro equipo en las siguientes áreas: Área de Servicios Generales, Área de Recursos Humanos y Área Tecnológica. De tal manera que las áreas de trabajo quedarán conformadas según la Tabla 5.2.

En este caso al viceministro se le asignarán tareas de alto nivel, como son el aprobar documentos o convertirlos en materia institucional, esto quedará implícito en tareas en las cuales se deba tener aprobación del señor Ministro. Como podemos observar en la Tabla 5.2 la mayor cantidad de integrantes la tiene el Área Tecnológica, y esto por la cantidad de tareas tecnológicas que se deberán implementar. Además cada grupo de trabajo tendrá a su disposición al SRUM-Master, al Oficial de Seguridad y a miembros de otras áreas en caso de ser necesario.

Tabla 6 Áreas de trabajo

Área	**Personal**
Servicios Generales	Director Administrativo
	Director de Asuntos Legales de Gestión Interna
	Director de Servicios, Procesos y Calidad

Área	Personal
	Director de la Gestión Documental y Archivo
	Coordinador General de Auditoría Interna
	Director de Comunicación Social
Recursos Humanos	Director de Administración de Talento Humano
	Director Administrativo
	Director de Asuntos Legales de Gestión Interna
	Director de Servicios, Procesos y Calidad
	Director de la Gestión Documental y Archivo
Tecnológica	Coordinador General de TIC'S
	Director de Desarrollo TI
	Director de Infraestructura y Operaciones TI
	Director de Seguridad Informática TI
	Director de Servicio y Soporte al Usuario
	Coordinador General de Auditoría Interna
	Director de Documentos y Servicios
	Director de Gestión y Servicios

5.3. Aplicación por dominio del EGSI

Para tener concordancia con lo analizado por áreas, las tareas también serán clasificadas por áreas, y en este caso ya se les asignarán horas de trabajo, además de qué producto será el necesario para tener conformidad. El Anexo H nos detalla la información mencionada.

Cabe recalcar que hay tareas que no pertenecen a ningún área como tal, es el caso de Viceministro o de Oficial de Seguridad, justamente son tareas de alto nivel que deberán ser realizadas en el tiempo que se considere adecuado, en nuestro caso hemos previsto el más alto

número de horas, además que existe concordancia con que el Viceministro no pertenezca a ningún área en específico.

Gracias al Anexo H podremos asignar tareas directamente a sus responsables, y así determinar las tareas que cada uno de los integrantes del CSI deberá realizar, o al menos será el responsable por que se cumpla.

Como ya lo hemos mencionado la Fase 2 no la consideraremos con tareas tan específicas, ya que el GPR, herramienta que planifica la gestión en las Instituciones Públicas, permite a dichas instituciones considerar que hitos se cumplirán por control, y eso basándose en función del alcance del SGSI, y también de los objetivos Institucionales que además deberán estar implícitos en el SGSI, en nuestro caso particular, la herramienta CV. Ver Anexo I.

De esta manera conocemos que tareas puntuales se deberán realizar, y por la variedad de los hitos por dominio, no se les asignará un área en específico, ya que esta se la debe asignar por hito, y por la cantidad de hitos de la segunda fase no es lo recomendable. Recordemos que los hitos asignados en la tabla son aquellos que

hacen sentido con el SGSI, el cual hace sentido con los objetivos Institucionales y además que son valorados por la herramienta CV.

Por lo tanto los dominios del EGSI han sido llevados a la planificación según SCRUM, la cual no está completa sin un mapa de actividades, y además un cronograma de actividades detallado.

Para ciertas tareas deberemos plantear mecanismos para reducir riesgos hasta alcanzar niveles aceptables, para esto se deberá inicialmente reconocer a los Activos de Información y clasificarlos según su Confidencialidad (C), Disponibilidad (D) e Integridad (I), tal y como nos muestra la Tabla 5.3.

Tabla 7 Clasificación de Activos de Información

Activos de Información (SGSI)	**Dueño de Activo**	**C**	**I**	**D**	**Impacto**
Servidor de Correos	TI	3	3	2	8
Servidor de Chat	TI	3	3	1	7
Servidor de Telefonía	TI	3	3	1	7
Infraestructura de Virtualización Local	TI	3	3	1	7
PCs de Operadores	TI	3	3	2	8
Servidores Físicos	TI	3	3	2	8
Servidores Virtuales	TI	3	3	3	9
Operador	TI	3	3	2	8
Sistema e-SIGEX	TI	2	2	3	7
Web (Liferay)	TI	3	3	3	9
BDN(Postgres)	TI	2	2	3	7
BDP(Mysql)	TI	1	1	3	5

Usuarios (Ldap)	TI	3	3	3	9
BPM (Intalio)	TI	1	1	3	5
Docs (Alfresco)	TI	3	3	2	8

Se debe mencionar que estos activos son los directa o indirectamente involucrados con las herramientas con las que trabajaremos. La manera de calcular la Disponibilidad, Integridad y Confidencialidad están basados en las tablas 5.4, 5.5 y 5.6

El impacto del riesgo se lo determinará en función de los activos de información que participan dentro de cada proceso o sub proceso en evaluación. El impacto se valorará de acuerdo a la pérdida de: Disponibilidad, Integridad y Confidencialidad. El valor será la suma de estas tres variables.

Tabla 8 Criterio de valoración del Impacto según la Disponibilidad

IMPACTO – DISPONIBILIDAD		**VALOR**
Alto (A)	Paraliza completamente el proceso o subproceso.	3
Medio (M)	Paraliza parcialmente el proceso o subproceso.	2
Bajo (B)	No paraliza el proceso o subproceso.	1

Tabla 9 Criterio de valoración del Impacto según la Confidencialidad

IMPACTO – CONFIDENCIALIDAD		**VALOR**
Alto (A)	La información procesada por el activo, es información de usuario final.	3
Medio (M)	La información procesada por el activo, es	2

	información de uso interno de la Institución.	
Bajo (B)	La información procesada por el activo, es información transaccional o de registro de actividades.	1

Tabla 10 Criterio de valoración del Impacto según la Integridad

IMPACTO – INTEGRIDAD		**VALOR**
Alto (A)	La información procesada por el activo, es información de usuario final.	3
Medio (M)	La información procesada por el activo, es información de uso interno de la Institución.	2
Bajo (B)	La información procesada por el activo, es información transaccional o de registro de actividades.	1

Luego de reconocer y calcular el Impacto de cada activo, se deberá reconocer el nivel de madurez de cada Activo de Información. Para esto se elaboró la Tabla 5.7, la cual nos ayuda a clasificar lo mencionado.

Tabla 11 Nivel de madurez de Controles

Nivel de Madurez de Controles		
Nombre	**Nivel**	**Descripción**
Reconocido	1	Se reconoce la necesidad del control. Pero no se lo ha puesto en marcha o se planea hacerlo en el futuro.
Repetible	2	Se ejecuta el control como parte de las operaciones, es evidenciable su repetitividad.
Documentado	3	Se encuentra tipificado en un documento controlado su operación. Establecimiento formal según las condiciones de la Institución.

Auditado	4	Ha pasado por un proceso de auditoría o es auditable.
Optimizado	5	Ha sido revisado y acciones correctivas o de mejora documentadas que se han puesto en marcha.

Lo siguiente será realizar un Análisis y Evaluación de Riesgos, con el cual se podrá disminuir los niveles de riesgo hasta alcanzar niveles aceptables. Para hacer esto deberemos analizar las Amenazas, Vulnerabilidades y Probabilidad del Riesgo, una vez que obtenemos este valor podremos obtener el valor del Riesgo por cada Amenaza y Vulnerabilidad, el cual será la multiplicación de la Probabilidad de Riesgo y el Impacto del Activo.

Dentro del análisis del activo R.1, se encontraron dos riesgos, los cuales tienen el ID de R.1.1 y R.1.2 con una valoración de Riesgo de 48 y 64 respectivamente. Las amenazas y las vulnerabilidades están especificadas en el Anexo J. Luego realizamos el plan de tratamiento de riesgos, el cual podrá tener más de una tarea a realizar por riesgo, en el caso de R.1, tenemos A.1, A.2 y A.3 para R.1.1 y a B.1 para R.1.2, mediante las cuales se obtuvo un riesgo residual de 24. Ver Anexo K.

Para el activo R.2, se encontró una amenaza asociada a una vulnerabilidad, dando como resultado un Riesgo de 56. De tal manera que se plantearon dos tareas a realizar para así obtener un Riesgo Residual de 21. Ver Anexo L y M.

El activo R.3 tiene una amenaza asociada a una vulnerabilidad, obteniendo un Riesgo en este activo de 35, para lo cual se plantearon dos tareas, dando como resultado un Riesgo Residual de 21. Ver Anexo N y O.

El activo R4 tiene dos amenazas, A y B, asociadas a dos vulnerabilidades, A.1 y B.1, las cuales nos dieron valores de 42 y 28 respectivamente como Riesgo asociado a Activos de Información. El plan de tratamiento de Riesgos plantea una tarea a realizar por cada amenaza/vulnerabilidad, y así obtener un riesgo residual de 21. Ver Anexo P y Q.

Para el activo R.5 pasa algo en particular, una amenaza tiene asociada tres vulnerabilidades, en estos casos se considera la que tenga mayor Probabilidad de Riesgo, en este caso el Riesgo es de 56.

Al plantear la tarea del plan de tratamiento de Riesgo, el riesgo residual es de 24. Ver Anexo R y S.

El activo R.6 tiene seis (6) amenazas/vulnerabilidades asociadas, con esto los valores del Riesgo son de: 56, 56, 48, 48, 56 y 48 para R.6.1, R.6.2, R.6.3, R.6.4, R.6.5 y R.6.6, respectivamente. El tratamiento de estos riesgos está involucrado con siete (7) tareas, de las cuales dos (2) son para el riesgo R.6.4, con esto obtenemos un Riesgo Residual de 21. Ver Anexo T y U.

El activo R.7 tiene dos (2) amenazas/vulnerabilidades, y cada una de ellas con riesgo de 54. Existen dos tareas en el plan de tratamiento de riesgo por lo que el Riesgo Residual es de 27. Ver Anexo V y W.

En el activo R.8 también tenemos dos (2) amenazas/vulnerabilidades asociadas, cada una de ellas con 48 y 56 como valor del Riesgo. El plan de tratamiento de Riesgo plantea dos (2) tareas para reducir a 24 el Riesgo Residual. Ver Anexo X y Y.

El activo R.9 tiene cuatro (4) amenazas/vulnerabilidades, todas asociadas a un valor de 42 como Riesgo. El plan de tratamiento de Riesgo consiste en cuatro (4) tareas para alcanzar el valor de 21 como Riesgo Residual. Ver Anexo Z y AA.

El activo R.10 contiene nueve (9) amenazas/vulnerabilidades, A.1, B.1, C.1, D.1, E.1, F.1, G.1, H.1, I.1, con los valores de 54, 54, 54, 45, 63, 54, 54, 54 y 36 respectivamente. El plan de tratamiento de riesgos tiene nueve (9) tareas asignadas, de esta manera conseguiremos que el Riesgo Residual sea de 27. Ver Anexo AB y AC.

El activo R.11 contiene seis (6) amenazas/vulnerabilidades, cada una con los siguientes valores de Riesgo: 42, 28, 42, 42, 42 y 28. Para tratar estos riesgos se plantearon seis (6) tareas, de esta manera el Riesgo Residual será de 21. Ver Anexo AD y AE.

Las amenazas/vulnerabilidades del activo R.12 son seis (6), los valores del Riesgo de cada una son: 30, 20, 30, 30, 30 y 20. Para las cuales existirán seis (6) tareas en el plan de tratamiento de riesgos. Con esto el Riesgo Residual será de 15. Ver Anexo AF y AG.

El activo R.13 que asocia seis (6) amenazas con vulnerabilidades tiene valoraciones de riesgo para cada una de 63, 54, 63, 36, 54 y 54. Las seis (6) tareas del plan de tratamiento de riesgo harán que el Riesgo Residual sea de 27. Ver Anexo AH y AI.

El activo R.14 tiene la misma cantidad de amenazas/vulnerabilidades que el R.13, y sus valores son: 35, 20, 30, 30, 30 y 20. El número de tareas a realizar según el Plan de tratamiento de Riesgo es el mismo que el de R.13, y esto nos ayuda a obtener un Riesgo Residual de 15. Ver Anexo AJ y AK.

Por último el activo R.15 que tiene tres (3) amenazas/vulnerabilidades asociadas, con los valores de Riesgo de 40, 32 y 48. Para que el plan de tratamiento de riesgo, con el mismo número de tareas que de amenazas/vulnerabilidades, nos da una valor de 24 como Riesgo Residual. Ver Anexo AL y AM.

Una vez analizados todos los activos con sus campos: Amenazas, Vulnerabilidades, Probabilidad de Riesgo, Impacto, Riesgo, Tratamiento, Control, Tarea a Realizar y Riesgo Residual. De lo cual

nos enfocaremos en obtener el valor de Probabilidad de Riesgo, ya que es la variable cuantitativa que hasta ahora no hemos indicado como calcularla. La probabilidad de riesgo de cada Amenaza/Vulnerabilidad está calculada según la Tabla 5.38.

Tabla 12 Criterios de valoración de probabilidad del incidente

PROBABILIDAD DEL INCIDENTE (ACTIVO-AMENAZA-VULNERABILIDAD)		**P Parcial**	**Nivel de P Total**
Alto (A)	1.- No existen controles para atender este incidente. 2.- Incidente con elevada recurrencia (semanal). 3.- Existen varias vulnerabilidades presentes.	3 3 3	(7 - 9]
Medio (M)	1.- Existe al menos un control para atender este incidente. 2.- Incidente con mediana recurrencia (mensual). 3.- Existe a lo sumo una vulnerabilidad presente.	2 2 2	[5 - 7]
Bajo (B)	1.- Existen varios controles para atender este incidente. 2.- Nula o casi nula ocurrencia (anual). 3.- No existen vulnerabilidades presentes.	1 1 1	[3 –5)

De esta manera podemos considerar que los riesgos han sido disminuidos hasta alcanzar los niveles aceptables, que son aquellos que la Institución puede aceptar.

Tabla 13 Clasificación de los riesgos

Tipo de Riesgo	Escala
Riesgo alto	50 – 81
Riesgo medio	26 – 49
Riesgo bajo	09 – 25

Según la Tabla 5.39 podrán existir tres (3) tipos de riesgos, los cuales deberán ser aceptados o no por la Alta Dirección. Esto en función de la valoración a los activos. Sin embargo, se deberán denotar los posibles tratamientos que se les debe dar a los riesgos, estos son: Aceptar, Se decide operar el SGSI con los riesgos identificados y no se dispone la implementación de controles para su mitigación. Evitar: Se decide no operar el SGSI con los riesgos identificados y se dispone dejar de usar los activos que generan estos riesgos. Transferir: Se decide no operar el SGSI con los riesgos identificados y se dispone dejar de usar los activos que generan estos riesgos. Mitigar: Se decide no operar el SGSI con los riesgos identificados y se propone atenuar los riesgos mediante la aplicación de controles.

La forma objetiva de saber qué tratamiento darle a un riesgo en particular se realizará según las variables para calcular el Riesgo, las cuales son Impacto y Probabilidad de Riesgo.

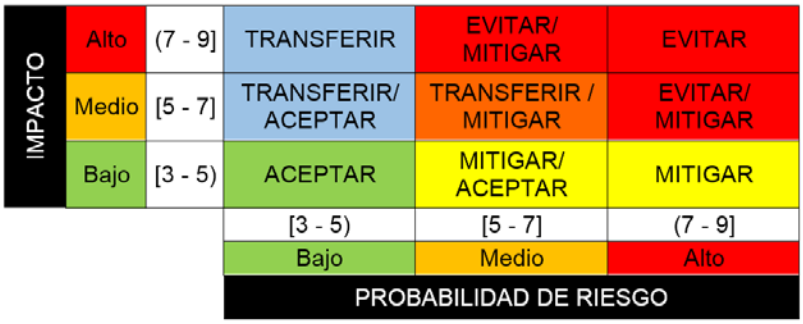


Figura 5.1 Tratamiento de riesgos según su impacto y probabilidad

5.4. Presentación del EGSI – SCRUM

Finalmente la presentación de la metodología SCRUM aplicada en el EGSI, bajo un caso en específico que debería servirnos como guía para cualquier otra implementación. De esta manera podemos realizar las tareas e hitos que nos exige el EGSI con horas límite para la realización de la respectiva tarea, esto es muy importante, ya que si no se exigen resultados en un tiempo determinado, el sistema simplemente no despega, obviamente lo más importante no es que despegue sino que sea estable, y para eso hay tareas que si se las realiza correctamente estarán en sintonía con este objetivo.

El cronograma que se presentará no será obligatorio cumplirlo al pie de la letra, pero es necesario que cuando una tarea se pase del tiempo propuesto, haya una leve modificación del cronograma, de esta manera se estaría reevaluando incluso el EGSI-SCRUM. Las

reuniones exigidas por SCRUM son obligatorias cumplirlas, para estas no deberían haber prórrogas, por el contrario, si algún miembro del equipo faltase, se deberá reportar esto a la Alta Dirección, por medio del CSI o del Oficial de Seguridad.

La Fase 1, la cual en el EGSI está planteada para realizarla en 6 meses, según la planificación, la podremos realizar en 71 días que resulta aproximadamente en tres meses y seis días, según nuestro planteamiento. Esto lo realizaremos ejecutando siete (7) Sprints, cada uno de dos (2) semanas, y en los Sprints encontraremos las tareas a realizar, que serían la Lista de Producto, lo restante, que sería la Lista de Pendientes, la Revisión del Sprint y la Retrospectiva del mismo, los responsables de los hitos a realizar también se encuentran, estos no tienen asignadas tareas en mismo rango de fecha, salvo excepciones. Quiere decir que hemos logrado reducir el tiempo de implementación en un 50%. Cabe recalcar que se han sobredimensionado ciertos hitos, que resultan un tanto más burocráticos, y esto ha hecho que aumente el número de horas en la Fase 1, además que hay miembros en el Equipo de Desarrollo que han dado cumplimiento de sus hitos antes que otros miembros logren los suyos, esto se da particularmente por la implementación tecnológica, los miembros del Área Tecnológica

tienen más tareas asignadas, lo cual era de esperarse por el sentido del EGSI.

La Fase 2, fue planificada para realizarla en 18 meses, pero con nuestra solución podría ser realizada en 191 días, que aproximadamente nos da nueve (9) meses de implementación, otro ahorro del 50% del tiempo. Además, por la gran cantidad de tareas a realizar, también aumentaron los Sprints, de tal manera que se plantearon 19 Sprints, cada uno de dos semanas de duración. Los campos del Sprint son los mismos que en la Fase 1, sin embargo las responsabilidades recaerán en los grupos de trabajo identificados por Área, de tal manera que a la hora de estar en una cláusula que pertenece a un dominio específico, y que esta tenga varias tareas asignadas, se asignen automáticamente según las competencias demostradas.

En el Anexo AN podemos observar la metodología aterrizada a un GANTT, el cual describe todo lo mencionado anteriormente.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Dado que cada institución debe aceptar o rechazar los riesgos residuales, basándose en sus objetivos institucionales y su nivel de madurez en el SGSI; los riesgos residuales que hemos obtenido en el presente trabajo podrían ser rechazados en algún otro marco.

2. El tiempo de implementación de la “Fase 1” en la institución piloto del EGSI-SCRUM propuesto en el presente trabajo fue de aproximadamente el 50% (tres meses y seis días) de lo que plantea la SNAP. Por lo tanto, nuestro esquema tendrá un tiempo de implementación de entre noventa y ciento treinta cinco días (entre el 50% y 75%) como planteamiento inicial para así hacer más flexible la aplicación del EGSI-SCRUM.

Recomendaciones:

1. Debido a que la Fase 2 tiene mayor cantidad de hitos que la Fase 1, la cantidad de Sprints pudo ser mayor a dos (2) semanas. Sin embargo, lo recomendable es no cambiar el sistema.

2. El EGSI incluye la mejora continua como uno de sus puntos de gestión clave, es por eso que mediante se vayan realizando implementaciones del EGSI-SCRUM en diferentes instituciones, este documento se deberá ir actualizando en función de las sugerencias obtenidas.

3. Algunas tareas necesarias del EGSI tomaron más del tiempo planificado, debido a que la Institución piloto requería de ciertos trámites específicos cuyo seguimiento en algunos casos era complejo. Debido a esto es necesario será tener un plan de contingencia, como poner aquellas tareas al principio del proyecto de manera que no afecten de manera significativa la implementación del mismo.

ANEXOS

Anexo A: Cláusulas de la fase II del EGSI

Dominio		Control
1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		1.2 Revisión de la Política
2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		2.2 Coordinación de la Gestión de la Seguridad de la Información
		2.3 Asignación de responsabilidades para la seguridad de la información
		2.4 Proceso de autorización para nuevos servicios de procesamiento de la información
		2.6 Contacto con las autoridades
		2.7 Contactos con grupos de interés especiales
		2.8 Revisión independiente de la seguridad de la información
		2.9 Identificación de los riegos relacionados con las partes externas
		2.10 Consideraciones de la seguridad cuando se trata de ciudadanos o clientes
		2.11 Consideraciones de la seguridad de los acuerdos con terceras partes
3 GESTIÓN DE LOS ACTIVOS		3.1 Inventario de activos
		3.2 Responsable de los activos
		3.3 Uso aceptable de los activos
		3.4 Directrices de clasificación de la

		información
		3.5 Etiquetado y manejo de la información
4 SEGURIDAD DE LOS RECURSOS HUMANOS		4.1 Funciones y responsabilidades
		4.2 Selección
		4.3 Términos y condiciones laborales
		4.4 Responsabilidades de la dirección a cargo del funcionario
		4.5 Educación formación y sensibilización en seguridad de la información
		4.6 Proceso disciplinario
		4.7 Responsabilidades de la terminación de contrato
		4.8 Devolución de activos
		4.9 Retiro de los privilegios de acceso
5 SEGURIDAD FÍSICA Y DEL ENTORNO		5.1 Perímetro de la seguridad física
		5.2 Controles de acceso físico
		5.3 Seguridad de oficinas, recintos e instalaciones
		5.4 Protección contra amenazas externas y ambientales
		5.5 Trabajo en áreas seguras
		5.6 Áreas de carga, despacho y acceso público
		5.7 Ubicación y protección de los equipos
		5.8 Servicios de suministro
		5.9 Seguridad del cableado
		5.10 Mantenimiento de los equipos
		5.11 Seguridad de los

		equipos fuera de las instalaciones
		5.12 Seguridad de la reutilización o eliminación de los equipos
		5.13 Retiro de activos de la propiedad
6 GESTIÓN DE COMUNICACIONES Y OPERACIONES		6.1 Documentación de los procedimientos de Operación
		6.2 Gestión del cambio
		6.3 Distribución de funciones
		6.4 Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción
		6.5 Presentación del servicio
		6.6 Monitoreo y revisión de los servicios, por terceros.
		6.7 Gestión de los cambios en los servicios ofrecidos por terceros
		6.8 Gestión de la capacidad
		6.9 Aceptación del Sistema
		6.10 Controles contra código malicioso
		6.11 Controles contra códigos móviles
		6.12 Establecer controles criptográficos para autenticar de forma única el código móvil.
		6.13 Controles de la redes
		6.14 Seguridad de los servicios de la red
		6.15 Gestión de los medios removibles
		6.16 Eliminación de los medios
		6.17 Procedimiento para

		el manejo de la información
		6.18 Seguridad de la documentación del sistema
		6.19 Políticas y procedimientos para el intercambio de información
		6.20 Acuerdos para el intercambio
		6.21 Medios físicos en tránsito
		6.22 Mensajería electrónica
		6.23 Sistemas de información del negocio
		6.24 Transacciones en línea
		6.25 Información disponible al público
		6.26 Registros de auditorías
		6.27 Monitoreo del uso del sistema
		6.28 Protección del registro de la información
		6.31 Sincronización de relojes
7 CONTROL DE ACCESO		7.1 Política de control de acceso
		7.2 Registro de usuarios
		7.3 Gestión de privilegios
		7.5 Revisión de los derechos de accesos de los usuarios
		7.8 Política de puesto de trabajo despejado y pantalla limpia
		7.9 Política de uso de los servicios de red
		7.10 Autenticación de usuarios para conexiones externas
		7.11 Identificación de los equipos en las redes

		7.12 Protección de los puertos de configuración y diagnóstico remoto
		7.13 Separación en las redes
		7.14 Control de conexión a las redes
		7.15 Control del enrutamiento en la red
		7.16 Procedimiento de registro de inicio seguro
		7.17 Identificación y autenticación de usuarios
		7.18 Sistema de gestión de contraseñas
		7.19 Uso de las utilidades del sistema
		7.20 Tiempo de inactividad de la sesión
		7.21 Limitación del tiempo de conexión
		7.22 Control de accesos a las aplicaciones y a la información
		7.23 Restricciones de acceso a la información
		7.24 Aislamiento de sistemas sensibles
		7.25 Computación y comunicaciones móviles
		7.26 Trabajo remoto
8 ADQUISICIÓN, DESARROLLO, Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		8.1 Análisis y especificaciones de los requerimientos de seguridad
		8.2 Validación de datos de entrada
		8.3 Control de procesamiento interno
		8.4 Integridad del mensaje
		8.5 Validación de datos de salidas
		8.6 Política sobre el uso de controles criptográficos
		8.7 Gestión de claves

		8.8 Control de software operativo
		8.9 Protección de los datos de prueba del sistema
		8.10 Control de acceso al código fuente de los programas
		8.11 Procedimiento de control de cambios
		8.12 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo
		8.13 Restricción del cambio de paquetes de software
		8.14 Fuga de información
		8.15 Desarrollo de software contratado externamente
		8.16 Control de las vulnerabilidades técnicas
9 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		9.1 Reporte sobre los eventos de seguridad de la información
		9.2 Reporte sobre las debilidades en la seguridad
		9.3 Responsabilidades y procedimientos
		9.4 Aprendizaje debido a los incidentes de seguridad de la información
		9.5 Recolección de evidencias
10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		10.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
		10.2 Continuidad del negocio y evaluación de riesgos
		10.3 Desarrollo e

		implementación de planes de continuidad que incluyan la seguridad de la información
		10.4 Estructura para la planificación de la continuidad del negocio
		10.5 Pruebas, mantenimiento y revisión de los planes de continuidad del negocio.
11 CUMPLIMIENTO		11.1 Identificación de la legislación aplicable
		11.2 Derechos de propiedad intelectual
		11.3 Protección de registros en cada entidad
		11.4 Protección de los datos y privacidad de la información personal
		11.5 Prevención del uso inadecuado de servicios de procesamiento de información
		11.6 Reglamentación de controles criptográficos
		11.7 Cumplimiento con las políticas y normas de la seguridad
		11.8 Verificación del cumplimento técnico
		11.9 Control de auditoría de los sistemas de Información
		11.10 Protección de las herramientas de auditoría de los sistemas de Información

Anexo B: Hitos por Áreas – Máxima Autoridad

HITO	ÁREA RESPONSABLE
1.1.1.- (*) EJECUCIÓN: Implementación del EGSI en la institución dispuesta por la máxima autoridad.	Máxima Autoridad
2.1.3.- (*) EJECUCIÓN: Comité de Gestión de la Seguridad de la Información oficialmente Conformado	Máxima Autoridad
2.2.1.1.- (*) EJECUCIÓN: Oficial de Seguridad de la Información quien actuará como coordinador del CSI oficialmente designado.	Máxima Autoridad
DEFINICIÓN: Acuerdo de implementación del Esquema Gubernamental de Seguridad de la Información emitido	Máxima Autoridad

Anexo C: Hitos por Áreas – Oficial de Seguridad

HITO	ÁREA RESPONSABLE
2.1.1.- (*) EJECUCIÓN: Seguimiento de la puesta en marcha de las normas EGSI realizado	Oficial de Seguridad Delegado por el CSI
3.4.1.- (*) EJECUCIÓN: Información clasificada como pública o confidencial	Oficial de Seguridad Delegado por el CSI
4.4.1.- (*)EJECUCIÓN: Funciones y las responsabilidades respecto a la seguridad de la información explicadas y definidas, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles	Oficial de Seguridad, Delegado por el CSI

HITO	ÁREA RESPONSABLE
6.6.1.- (*) EJECUCIÓN: Niveles de desempeño de los servicios monitoreados para verificar el cumplimiento de los acuerdos	Oficial de Seguridad Delegado por el CSI
6.6.2.- (*) EJECUCIÓN: Reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos analizados	Oficial de Seguridad Delegado por el CSI
6.6.3.- (*) EJECUCIÓN: 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	Oficial de Seguridad Delegado por el CSI
7.16.5.- (*) EJECUCIÓN: Tiempo definido de conexión de los usuarios, considerando las necesidades de la institución	Oficial de Seguridad Delegado por el CSI
7.18.1.- (*) EJECUCIÓN: Política de accesos implementada donde se indica la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible	Oficial de Seguridad Delegado por el CSI
7.18.3.- (*) EJECUCIÓN: Lineamientos de cambio de contraseña obligatorio en el primer registro de acceso o inicio de sesión implementado	Oficial de Seguridad Delegado por el CSI
7.6.1.- (*) EJECUCIÓN: Procedimiento de accesos documentado donde se indique las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados	Oficial de Seguridad Delegado por el CSI
7.6.2.- (*) EJECUCIÓN: Lineamientos de generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta implementados	Oficial de Seguridad Delegado por el CSI
7.6.3.- (*) EJECUCIÓN: Lineamientos para contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables implementadas	Oficial de Seguridad Delegado por el CSI

HITO	ÁREA RESPONSABLE
7.6.5.- (*)EJECUCIÓN: Revisiones periódicas de la gestión de usuarios generadas y documentadas incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información	Oficial de Seguridad Delegado por el CSI
8.1.1.- (*) EJECUCIÓN: Requerimientos de seguridad definidos. Por ejemplo: criptografía, control de sesiones, etc.	Oficial de Seguridad Delegado por el CSI
8.1.2.- (*) EJECUCIÓN: Controles apropiados definidos, tanto automatizados como manuales	Oficial de Seguridad Delegado por el CSI
9.1.1.- (*) EJECUCIÓN: Procedimiento formal instaurado/implementado para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente	Oficial de Seguridad Delegado por el CSI
9.1.2.- (*) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden	Oficial de Seguridad Delegado por el CSI

Anexo D: Hitos por Áreas – Dirección Administrativa

HITO	ÁREA RESPONSABLE
3.1.2.1.- (*) EJECUCIÓN: inventario de Equipos móviles: teléfono inteligente (Smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc. Realizado	Dirección Administrativa
5.1.1.- (*) EJECUCIÓN: Área definida de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio	Dirección Administrativa
5.2.1.- (*) EJECUCIÓN: Hora y fecha de ingreso y salida de permanencia de visitantes en las áreas restringidas registradas y supervisadas.	Dirección Administrativa

HITO	ÁREA RESPONSABLE
5.2.2.- (*) EJECUCIÓN: Código de uso de una identificación visible para todo el personal y visitantes y de acompañamiento de visitas a áreas restringidas implementado.	Dirección Administrativa
5.3.1.- (*) EJECUCIÓN: Instalaciones claves protegidas de acceso a personal no autorizado	Dirección Administrativa
5.4.1.- (*) EJECUCIÓN: Mantenimientos de las instalaciones eléctricas y UPS realizados	Dirección Administrativa
5.4.2.- (*) EJECUCIÓN: Mantenimientos en los sistemas de climatización y ductos de ventilación realizados / ejecutados	Dirección Administrativa
5.6.1.- (*) EJECUCIÓN: Código de acceso al área de despacho y carga, únicamente a personal identificado y autorizado implementado	Dirección Administrativa
5.9.1.- (*) EJECUCIÓN: Diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc. identificados/documentados	Dirección Administrativa
7.8.1.- (*) EJECUCIÓN: Lineamientos de resguardo de Información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina implementado/ejecutado	Dirección de Administrativa

Anexo E: Hitos por Áreas – Dirección de Administración de Recursos Humanos

HITO	ÁREA RESPONSABLE
2.5.2.- (*) EJECUCIÓN: Acuerdos de confidencialidad de la información, documento físico o electrónico firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción	Dirección de Administración de Recursos Humanos

2.5.3.- (*) EJECUCIÓN: Acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos custodiados/archivados	Dirección de Administración de Recursos Humanos
2.5.4.- (*) EJECUCIÓN: Firma de los acuerdos de confidencialidad vinculados/anexados a los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción	Dirección de Administración de Recursos Humanos
2.5.5.- (*) EJECUCIÓN: Aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros realizados/ejecutados	Dirección de Administración de Recursos Humanos
4.1.1.- (*) EJECUCIÓN: Candidatos verificados, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida.	Dirección de Administración de Recursos Humanos
4.1.2.- (*) EJECUCIÓN: Funciones y responsabilidades entregadas formalmente a los funcionarios.	Dirección de Administración de Recursos Humanos
4.4.1.- (*)EJECUCIÓN: Funciones y las responsabilidades respecto a la seguridad de la información explicadas y definidas, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles	Dirección de Administración de Recursos Humanos

Anexo F: Hitos por Áreas – DTICS

HITO	ÁREA RESPONSABLE
1.1.2.- (*) EJECUCIÓN: Política de seguridad de la información de referencia o propia de la institución difundida	DTICS
2.5.1.- (*) EJECUCIÓN: Acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI elaborados y aprobados	DTICS
3.1.2.1.- (*) EJECUCIÓN: inventario de Equipos móviles: teléfono inteligente (Smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc. Realizado	DTICS

HITO	ÁREA RESPONSABLE
3.1.2.2.- (*) EJECUCIÓN: Inventario de Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc. Realizado	DTICS
3.1.2.3.- (*) EJECUCIÓN: Inventario de Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc. Realizado	DTICS
3.1.2.4.- (*) EJECUCIÓN: Inventario de Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc. Realizado	DTICS
3.1.2.5.- (*) EJECUCIÓN: Inventario de Periféricos y dispositivos de almacenamiento realizado	DTICS
3.1.2.6.- (*) EJECUCIÓN: Inventario de Periféricos de comunicaciones realizado	DTICS
3.1.2.7.- (*) EJECUCIÓN: Inventario de Tableros: de transferencia (bypass) de la unidad permanente de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc. Realizado	DTICS
3.1.2.8.- (*)EJECUCIÓN: Inventario de Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc. Realizado	DTICS
3.1.3.1.- (*) EJECUCIÓN: Inventario de Sistemas operativos realizado	DTICS
3.1.3.2.- (*) EJECUCIÓN: Inventario de Software de servicio, mantenimiento o administración realizado	DTICS
3.1.3.3.- (*)EJECUCIÓN: Inventario de Paquetes de software o software base realizado	DTICS
3.1.3.4.- (*) EJECUCIÓN: Inventario de Aplicativos informáticos del negocio realizado	DTICS
3.1.4.1.- (*) EJECUCIÓN: Inventario de Cables de comunicaciones realizado	DTICS

HITO	ÁREA RESPONSABLE
3.1.4.2.- (*) EJECUCIÓN: Inventario de Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.) realizado	DTICS
3.1.4.3.- (*) EJECUCIÓN: Inventario de Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc. Realizado	DTICS
3.1.4.4.- (*) EJECUCIÓN: Inventario de Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc. Realizado	DTICS
3.3.1.- (*) EJECUCIÓN: Uso de correo electrónico institucional reglamentado	DTICS
3.3.2.- (*) EJECUCIÓN: Acceso y uso de la Internet y sus aplicaciones/servicios reglamentado	DTICS
3.3.3.- (*) EJECUCIÓN: Uso de los sistemas de video-conferencia reglamentado	DTICS
5.3.2.- (*)EJECUCIÓN: Impresoras, copiadoras, etc. ubicadas en un área protegida	DTICS
5.4.1.- (*) EJECUCIÓN: Mantenimientos de las instalaciones eléctricas y UPS realizados	DTICS
5.5.1.- (*) EJECUCIÓN: Código de uso equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc., implementado	DTICS
5.7.1.- (*) EJECUCIÓN: Directrices establecidas para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información	DTICS
5.8.1.- (*) EJECUCIÓN: 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 identificados	DTICS

HITO	ÁREA RESPONSABLE
5.9.1.- (*) EJECUCIÓN: Diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc. identificados/documentados	DTICS
6.10.1.- (*) EJECUCIÓN: Prohibir el uso de software no autorizado por la institución. Listado del software autorizado elaborado.	DTICS
6.10.2.- (*) EJECUCIÓN: Software de antivirus y contra código malicioso instalado y actualizado periódicamente	DTICS
6.10.3.- (*) EJECUCIÓN: Los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles	DTICS
6.12.1.- (*) EJECUCIÓN: Procedimientos determinado para el resguardo y contención de la información por parte de los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información.	DTICS
6.12.2.- (*) EJECUCIÓN: Procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención definido	DTICS
6.12.3.- (*) EJECUCIÓN: Extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución definida	DTICS
6.14.1.- (*) EJECUCIÓN: Tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red incorporada/implementada	DTICS
6.14.2.- (*)EJECUCIÓN: Soluciones implementadas que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.	DTICS
6.26.1.- (*) EJECUCIÓN: Accesos y tipos de acceso registrados	DTICS

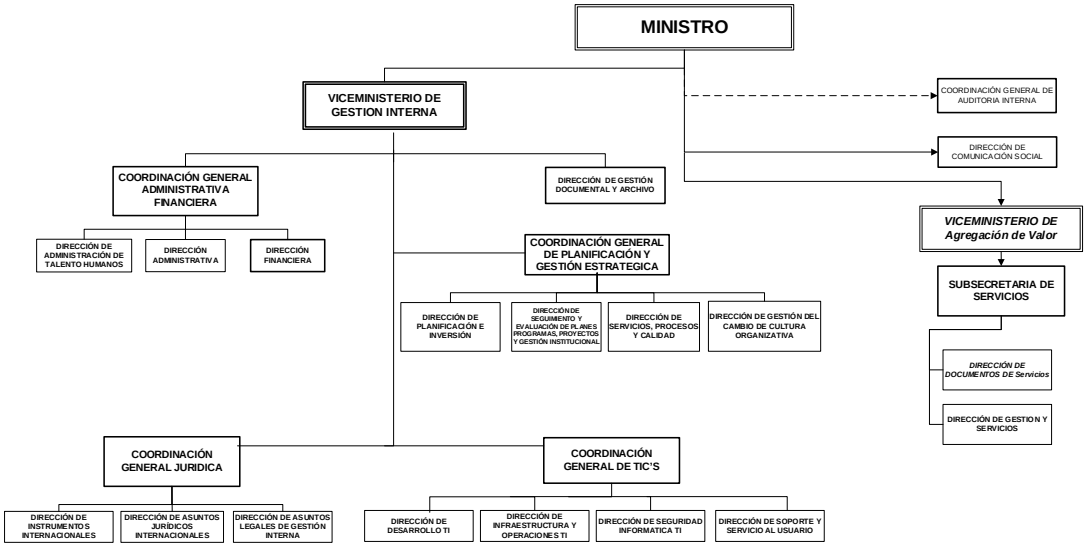
HITO	ÁREA RESPONSABLE
6.26.2.- (*) EJECUCIÓN: Direcciones y protocolos de red registrados	DTICS
6.26.3.- (*) EJECUCIÓN: Alarmas originadas por el sistema de control de acceso definidas	DTICS
6.26.4.- (*) EJECUCIÓN: Sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS) activados y desactivados	DTICS
6.27.1.- (*) EJECUCIÓN: Accesos autorizados, incluyendo registrados	DTICS
6.27.2.- (*) EJECUCIÓN: Operaciones privilegiadas monitoreadas	DTICS
6.27.3.- (*) EJECUCIÓN: Intentos de acceso no autorizados monitoreados	DTICS
6.27.4.- (*) EJECUCIÓN: Alertas o fallas del sistema revisados	DTICS
6.29.1.- (*) EJECUCIÓN: Hora en la que ocurrió el evento registrados	DTICS
6.29.2.- (*) EJECUCIÓN: Información sobre el evento registrados	DTICS
6.29.3.- (*) EJECUCIÓN: Cuenta de administrador y operador que estuvo involucrado registrados	DTICS
6.29.4.- (*) EJECUCIÓN: Procesos que estuvieron implicados registrados	DTICS
6.30.1.- (*) EJECUCIÓN: Registros realizados de fallas o errores del sistema revisados	DTICS
6.30.2.- (*)EJECUCIÓN: Medidas correctivas realizadas para garantizar que no se hayan vulnerado los controles revisados	DTICS
6.30.3.- (*) EJECUCIÓN: Registro de fallas esté habilitado	DTICS
6.8.1.- (*) EJECUCIÓN: Proyecciones realizadas de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos	DTICS

HITO	ÁREA RESPONSABLE
7.10.1.- (*) EJECUCIÓN: Mecanismos generados/implementados para asegurar la información transmitida por los canales de conexión remota	DTICS
7.11.1.- (*) EJECUCIÓN: Equipos que se encuentran en las redes documentados e identificados	DTICS
7.12.1.- (*) EJECUCIÓN: Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, eliminados o deshabilitados	DTICS
7.13.1.- (*) EJECUCIÓN: Evaluación de riesgos realizada para identificar los segmentos de red donde se encuentren los activos críticos para la institución	DTICS
7.15.1.- (*) EJECUCIÓN: Políticas de control de acceso configuradas para el enrutamiento en la red, basándose en los requerimientos de la institución	DTICS
7.16.1.- (*) EJECUCIÓN: Usuarios autorizados autenticados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada	DTICS
7.16.2.- (*) EJECUCIÓN: Registro de definición documentado para el uso de privilegios especiales del sistema	DTICS
7.16.3.- (*) EJECUCIÓN: 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 documentados	DTICS
7.16.4.- (*) EJECUCIÓN: Mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios utilizados/ejecutados	DTICS
7.16.6.- (*) EJECUCIÓN: Identificadores de aplicación controlados para que no muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro se haya completado exitosamente.	DTICS

HITO	ÁREA RESPONSABLE
7.16.7.- (*) EJECUCIÓN: Cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos	DTICS
7.16.8.- (*) EJECUCIÓN: Tiempo de dilación limitado antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica	DTICS
7.17.1.- (*) EJECUCIÓN: Actividades evidenciadas de las personas responsables de administraciones críticas de la institución, rastreados utilizando los identificadores de usuario	DTICS
7.17.2.- (*) EJECUCIÓN: Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, definido y documentado	DTICS
7.17.3.- (*) EJECUCIÓN: Uso de usuarios genéricos restringido	DTICS
7.17.4.- (*) EJECUCIÓN: Métodos alternos utilizados a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación	DTICS
7.18.2.- (*) EJECUCIÓN: Contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad cambiados	DTICS
7.25.1.- (*) EJECUCIÓN: Exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo registrados/controlados	DTICS
7.26.1.- (*) EJECUCIÓN: Uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución reportado/registrado.	DTICS
7.26.2.- (*) EJECUCIÓN: Protección de antivirus y reglas del Firewall definidas/ reguladas	DTICS
7.4.1.- (*)EJECUCIÓN: Proceso formal para la asignación y cambio de contraseñas establecido	DTICS

HITO	ÁREA RESPONSABLE
7.6.4.- (*) EJECUCIÓN: Cambio periódico de contraseñas de los usuarios controlados	DTICS
7.7.1.- (*) EJECUCIÓN: Medidas implementadas para que, en un determinado tiempo, 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	DTICS
7.8.2.- (*) EJECUCIÓN: Desconectar de la red, servicio o sistema, cuando se encuentren desatendidas	DTICS
7.8.3.- (*) EJECUCIÓN: Copiadoras bloqueadas y control de acceso especial dispuesto para horario fuera de oficinas	DTICS
7.8.4.- (*) EJECUCIÓN: Información sensible retirada una vez que ha sido impresa	DTICS
7.8.5.- (*) EJECUCIÓN: Información sensible retirada, como las claves, de sus escritorios y pantallas	DTICS
7.8.6.- (*) EJECUCIÓN: Dispositivos removibles retirados una vez que se hayan dejado de utilizar	DTICS
9.1.2.8.- (*) EJECUCIÓN: Causas Investigadas y diagnosticadas en forma definitiva las por las cuales se produjo el incidente	DTICS
9.1.2.9.- (*) EJECUCIÓN: 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 resueltos y restaurados	DTICS

Anexo G: Estructura Orgánica de la Institución objetivo



Anexo H: Número de horas programadas por tareas

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
1.1.1.- (*) EJECUCIÓN: Implementación del EGSI en la institución dispuesta por la máxima autoridad.	Viceministro Oficial de Seguridad	Documentación de la Implementación del EGSI	20
1.1.2.- (*) EJECUCIÓN: Política de seguridad de la información de referencia o propia de la institución difundida	Área Tecnológica	Políticas Establecidas y Difundidas.	15
2.1.1.- (*) EJECUCIÓN: Seguimiento de la puesta en marcha de las normas EGSI realizado	Oficial de Seguridad Área Tecnológica	Informes de seguimiento de todas las unidades	10
2.1.2.- (*) EJECUCIÓN: La difusión, capacitación y sensibilización del contenido del EGSI dispuesta	Área Tecnológica	Área Tecnológica	12
2.1.3.- (*) EJECUCIÓN: Comité de Gestión de la Seguridad de la Información oficialmente Conformado	Viceministro	Comité conformado	20
2.2.1.1.- (*) EJECUCIÓN: Oficial de Seguridad de la Información quien actuará como coordinador del CSI oficialmente designado.	Viceministro	Oficial designado	20
2.2.1.2.- (*) EJECUCIÓN: Responsable de seguridad del área de Tecnologías de la Información oficialmente designado.	Área Tecnológica	Director Designado	10

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
2.5.1.- (*) EJECUCIÓN: Acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI elaborados y aprobados	Área Tecnológica Área de Servicios Generales	Acuerdos elaborados	12
2.5.2.- (*) EJECUCIÓN: Acuerdos de confidencialidad de la información, documento físico o electrónico firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción	Área de Recursos Humanos Oficial de Seguridad	Acuerdos firmados	10
2.5.3.- (*) EJECUCIÓN: Acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos custodiados/archivados	Área de Recursos Humanos Oficial de Seguridad	Acuerdos firmados/archivados	10
2.5.4.- (*) EJECUCIÓN: Firma de los acuerdos de confidencialidad vinculados/anexados a los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción	Área de Recursos Humanos Oficial de Seguridad	Generación de Acuerdos/Firma de Acuerdos	5
2.5.5.- (*) EJECUCIÓN: Aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros realizados/ejecutados	Área de Recursos Humanos Oficial de Seguridad	Generación de Acuerdos/Firma de Acuerdos	15
3.1.2.1.- (*) EJECUCIÓN: inventario de Equipos móviles: teléfono inteligente (Smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc. Realizado	Área Tecnológica Área de Servicios Generales	Inventarios	10
3.1.2.2.- (*) EJECUCIÓN: Inventario de Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc. Realizado	Área Tecnológica	Inventarios	10
3.1.2.3.- (*) EJECUCIÓN: Inventario de Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc. realizado	Área Tecnológica	Inventarios	10

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
3.1.2.4.- (*) EJECUCIÓN: Inventario de Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc. realizado	Área Tecnológica	Inventarios	10
3.1.2.5.- (*) EJECUCIÓN: Inventario de Periféricos y dispositivos de almacenamiento realizado	Área Tecnológica	Inventarios	10
3.1.2.6.- (*) EJECUCIÓN: Inventario de Periféricos de comunicaciones realizado	Área Tecnológica	Inventarios	10
3.1.2.7.- (*) EJECUCIÓN: Inventario de Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc. Realizado	Área Tecnológica	Inventarios	10
3.1.2.8.- (*)EJECUCIÓN: Inventario de Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc. Realizado	Área Tecnológica	Inventarios	10
3.1.3.1.- (*) EJECUCIÓN: Inventario de Sistemas operativos realizado	Área Tecnológica	Inventarios	10
3.1.3.2.- (*) EJECUCIÓN: Inventario de Software de servicio, mantenimiento o administración realizado	Área Tecnológica	Inventarios	10
3.1.3.3.- (*)EJECUCIÓN: Inventario de Paquetes de software o software base realizado	Área Tecnológica	Inventarios	10
3.1.3.4.- (*) EJECUCIÓN: Inventario de Aplicativos informáticos del negocio realizado	Área Tecnológica	Inventarios	10
3.1.4.1.- (*) EJECUCIÓN: Inventario de Cables de comunicaciones realizado	Área Tecnológica	Inventarios	10
3.1.4.2.- (*) EJECUCIÓN: Inventario de Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.) realizado	Área Tecnológica	Inventarios	10

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
3.1.4.3.- (*) EJECUCIÓN: Inventario de Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc. Realizado	Área Tecnológica	Inventarios	10
3.1.4.4.- (*) EJECUCIÓN: Inventario de Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc. Realizado	Área Tecnológica	Inventarios	10
3.3.1.- (*) EJECUCIÓN: Uso de correo electrónico institucional reglamentado	Área Tecnológica Oficial de Seguridad	Reglamento de uso de correo electrónico institucional	12
3.3.2.- (*) EJECUCIÓN: Acceso y uso de la Internet y sus aplicaciones/servicios reglamentado	Área Tecnológica Oficial de Seguridad	Reglamento de acceso y uso de internet, aplicaciones y servicios	12
3.3.3.- (*) EJECUCIÓN: Uso de los sistemas de video-conferencia reglamentado	Área Tecnológica	Reglamento de uso de los sistemas de video-conferencia	12
3.4.1.- (*) EJECUCIÓN: Información clasificada como pública o confidencial	Oficial de Seguridad Área de Servicios Generales	Informes de Cumplimiento del Hito	20
4.1.1.- (*) EJECUCIÓN: Candidatos verificados, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida.	Área de Recursos Humanos Oficial de Seguridad	Proceso de Verificación Implementado	10
4.1.2.- (*) EJECUCIÓN: Funciones y responsabilidades entregadas formalmente a los funcionarios.	Área de Recursos Humanos	Funciones entregadas a la firma del contrato	12
4.4.1.- (*)EJECUCIÓN: Funciones y las responsabilidades respecto a la seguridad de la información explicadas y definidas, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles	Oficial de Seguridad Área de Recursos Humanos Área Tecnológica	Acta de funciones entregadas y firmadas a la firma del contrato	12
5.1.1.- (*) EJECUCIÓN: Área definida de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio	Área de Servicios Generales	Áreas Establecidas	15

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
5.2.1.- (*) EJECUCIÓN: Hora y fecha de ingreso y salida de permanencia de visitantes en las áreas restringidas registradas y supervisadas.	Área de Servicios Generales Oficial de Seguridad	Proceso de Registro	5
5.2.2.- (*) EJECUCIÓN: Código de uso de una identificación visible para todo el personal y visitantes y de acompañamiento de visitas a áreas restringidas implementado.	Área de Servicios Generales	Proceso de Uso de Identificación	5
5.3.1.- (*) EJECUCIÓN: Instalaciones claves protegidas de acceso a personal no autorizado	Área de Servicios Generales Oficial de Seguridad	Implementación de Control de Acceso	20
5.3.2.- (*)EJECUCIÓN: Impresoras, copiadoras, etc. ubicadas en un área protegida	Área Tecnológica	Informes de Ubicación de las Impresoras	10
5.4.1.- (*) EJECUCIÓN: Mantenimientos de las instalaciones eléctricas y UPS realizados	Área Tecnológica Área de Servicios Generales	Cronogramas e Informes de mantenimiento	15
5.4.2.- (*) EJECUCIÓN: Mantenimientos en los sistemas de climatización y ductos de ventilación realizados / ejecutados	Área de Servicios Generales	Cronogramas e Informes de mantenimiento	15
5.5.1.- (*) EJECUCIÓN: Código de uso equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc., implementado	Área Tecnológica Oficial de Seguridad	Elaboración, entrega e implementación del procedimiento de uso	10
5.6.1.- (*) EJECUCIÓN: Código de acceso al área de despacho y carga, únicamente a personal identificado y autorizado implementado	Área de Servicios Generales Oficial de Seguridad	Implementación de Sistema de Acceso	15
5.7.1.- (*) EJECUCIÓN: Directrices establecidas para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información	Área Tecnológica	Elaboración y Formalización de la Directriz	12
5.8.1.- (*) EJECUCIÓN: 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 identificados	Área Tecnológica	Informe de Funcionamiento de UPS	20

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
5.9.1.- (*) EJECUCIÓN: Diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc. identificados/documentados	Área Tecnológicas Área de Servicios Generales	Entrega de Diagramas de Conexión	20
6.1.1.- (*) EJECUCIÓN: Contactos de soporte, necesarios en caso de incidentes documentados	Área Tecnológica	Elaboración de listado de Contactos	10
6.10.1.- (*) EJECUCIÓN: Prohibir el uso de software no autorizado por la institución. Listado del software autorizado elaborado.	Área Tecnológica	Elaboración de listado de SOFTWARE no permitido e Informes de monitoreo	10
6.10.2.- (*) EJECUCIÓN: Software de antivirus y contra código malicioso instalado y actualizado periódicamente	Área Tecnológica	Informes de monitoreo	15
6.10.3.- (*) EJECUCIÓN: Los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles	Área Tecnológica	Informes de monitoreo	15
6.12.1.- (*) EJECUCIÓN: Procedimientos determinado para el resguardo y contención de la información por parte de los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información.	Área Tecnológica Oficial de Seguridad	Procedimientos establecidos y aplicados	20
6.12.2.- (*) EJECUCIÓN: Procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención definido	Área Tecnológica Oficial de Seguridad	Respaldos realizados, etiquetados y almacenados	12
6.12.3.- (*) EJECUCIÓN: Extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución definida	Área Tecnológica Oficial de Seguridad	Esquemas definidos y aplicados	15
6.14.1.- (*) EJECUCIÓN: Tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red incorporada/implementada	Área Tecnológica	Informes de implementación y monitoreo	20

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
6.14.2.- (*)EJECUCIÓN: Soluciones implementadas que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.	Área Tecnológica	Informes de implementación y monitoreo	20
6.26.1.- (*) EJECUCIÓN: Accesos y tipos de acceso registrados	Área Tecnológica	Esquemas definidos y aplicados	18
6.26.2.- (*) EJECUCIÓN: Direcciones y protocolos de red registrados	Área Tecnológica	Registro de direcciones y protocolos de red	18
6.26.3.- (*) EJECUCIÓN: Alarmas originadas por el sistema de control de acceso definidas	Área Tecnológica	Informes de implementación y monitoreo	20
6.26.4.- (*) EJECUCIÓN: Sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS) activados y desactivados	Área Tecnológica	Registro de Configuración	15
6.27.1.- (*) EJECUCIÓN: Accesos autorizados, incluyendo registrados	Área Tecnológica	Registros de perfiles de acceso	12
6.27.2.- (*) EJECUCIÓN: Operaciones privilegiadas monitoreadas	Área Tecnológica	Reportes de monitoreo	12
6.27.3.- (*) EJECUCIÓN: Intentos de acceso no autorizados monitoreados	Área Tecnológica	Reportes de monitoreo	8
6.27.4.- (*) EJECUCIÓN: Alertas o fallas del sistema revisados	Área Tecnológica	Análisis de alertas o fallas	8
6.29.1.- (*) EJECUCIÓN: Hora en la que ocurrió el evento registrados	Área Tecnológica	Reportes de monitoreo	8
6.29.2.- (*) EJECUCIÓN: Información sobre el evento registrados	Área Tecnológica	Reportes de monitoreo	8
6.29.3.- (*) EJECUCIÓN: Cuenta de administrador y operador que estuvo involucrado registrados	Área Tecnológica	Reportes de monitoreo	8
6.29.4.- (*) EJECUCIÓN: Procesos que estuvieron implicados registrados	Área Tecnológica	Reportes de monitoreo	8
6.30.1.- (*) EJECUCIÓN: Registros realizados de fallas o errores del sistema revisados	Área Tecnológica	Reportes de monitoreo	8

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
6.30.2.- (*)EJECUCIÓN: Medidas correctivas realizadas para garantizar que no se hayan vulnerado los controles revisados	Área Tecnológica	Informes de implementación de recomendaciones y observaciones	15
6.30.3.- (*) EJECUCIÓN: Registro de fallas esté habilitado	Área Tecnológica	Registro de Configuración	15
6.6.1.- (*) EJECUCIÓN: Niveles de desempeño de los servicios monitoreados para verificar el cumplimiento de los acuerdos	Oficial de Seguridad Área Tecnológica	Evaluación de informes y reportes de implementación y monitoreo	18
6.6.2.- (*) EJECUCIÓN: Reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos analizados	Oficial de Seguridad Área Tecnológica	Resultados de evaluaciones y análisis de reportes	20
6.6.3.- (*) EJECUCIÓN: 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	Oficial de Seguridad Área Tecnológica	Resultados de evaluaciones y auditorias contratadas	18
6.8.1.- (*) EJECUCIÓN: Proyecciones realizadas de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos	Área Tecnológica	Planificación de compras o contrataciones relacionadas	20
7.10.1.- (*) EJECUCIÓN: Mecanismos generados/implementados para asegurar la información transmitida por los canales de conexión remota	Área Tecnológica	Estrategias o protocolos definidos	15
7.11.1.- (*) EJECUCIÓN: Equipos que se encuentran en las redes documentados e identificados	Área Tecnológica	Reportes periódicos	8
7.12.1.- (*) EJECUCIÓN: Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, eliminados o deshabilitados	Área Tecnológica	Informes de implementación	20
7.13.1.- (*) EJECUCIÓN: Evaluación de riesgos realizada para identificar los segmentos de red donde se encuentren los activos críticos para la institución	Área Tecnológica Oficial de Seguridad	Informes de evaluación de riesgos relacionados	20

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
7.15.1.- (*) EJECUCIÓN: Políticas de control de acceso configuradas para el enrutamiento en la red, basándose en los requerimientos de la institución	Área Tecnológica	Registro de Configuración	20
7.16.1.- (*) EJECUCIÓN: Usuarios autorizados autenticados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada	Área Tecnológica	Registro de Configuración e informes periódicos de usuarios autenticados	20
7.16.2.- (*) EJECUCIÓN: Registro de definición documentado para el uso de privilegios especiales del sistema	Área Tecnológica	Protocolo definido	10
7.16.3.- (*) EJECUCIÓN: 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 documentados	Área Tecnológica	Reporte de monitoreo	15
7.16.4.- (*) EJECUCIÓN: Mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios utilizados/ejecutados	Área Tecnológica	Reportes periódicos	15
7.16.5.- (*) EJECUCIÓN: Tiempo definido de conexión de los usuarios, considerando las necesidades de la institución	Oficial de Seguridad Área Tecnológica	Esquema de tiempos de conexión por usuarios	18
7.16.6.- (*) EJECUCIÓN: Identificadores de aplicación controlados para que no muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro se haya completado exitosamente.	Área Tecnológica Oficial de Seguridad	Registro de Configuración	20
7.16.7.- (*) EJECUCIÓN: Cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos	Área Tecnológica	Registro de Configuración	15
7.16.8.- (*) EJECUCIÓN: Tiempo de dilación limitado antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica	Área Tecnológica	Registro de Configuración	15

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
7.17.1.- (*) EJECUCIÓN: Actividades evidenciadas de las personas responsables de administraciones críticas de la institución, rastreados utilizando los identificadores de usuario	Área Tecnológica Oficial de Seguridad	Reportes de actividades de personas responsables de administraciones criticas	15
7.17.2.- (*) EJECUCIÓN: Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, definido y documentado	Área Tecnológica Oficial de Seguridad	Registro de Configuración	20
7.17.3.- (*) EJECUCIÓN: Uso de usuarios genéricos restringido	Área Tecnológica Oficial de Seguridad	Registro de Configuración	18
7.17.4.- (*) EJECUCIÓN: Métodos alternos utilizados a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación	Área Tecnológica Oficial de Seguridad	Inventario de medios alternativos de autenticación y políticas de uso	20
7.18.1.- (*) EJECUCIÓN: Política de accesos implementada donde se indica la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible	Oficial de Seguridad Área Tecnológica	Política de accesos definida e implementada	12
7.18.2.- (*) EJECUCIÓN: Contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad cambiados	Área Tecnológica Oficial de Seguridad	Esquemas de definición y uso de claves para personal de TICS	15
7.18.3.- (*) EJECUCIÓN: Lineamientos de cambio de contraseña obligatorio en el primer registro de acceso o inicio de sesión implementado	Oficial de Seguridad Área Tecnológica	Lineamientos establecidos	15
7.25.1.- (*) EJECUCIÓN: Exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo registrados/controlados	Área Tecnológica	Control de ubicación de los equipos portátiles/informe	15
7.26.1.- (*) EJECUCIÓN: Uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución reportado/registrado.	Área Tecnológica	Control de ubicación de los equipos portátiles/informe	15
7.26.2.- (*) EJECUCIÓN: Protección de antivirus y reglas del Firewall definidas/ reguladas	Área Tecnológica Oficial de Seguridad	Registro de Configuración	20

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
7.4.1.- (*)EJECUCIÓN: Proceso formal para la asignación y cambio de contraseñas establecido	Área Tecnológica Oficial de Seguridad	Registro de Configuración	20
7.6.1.- (*) EJECUCIÓN: Procedimiento de accesos documentado donde se indique las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados	Oficial de Seguridad Área Tecnológica	Registro de claves por usuarios	20
7.6.2.- (*) EJECUCIÓN: Lineamientos de generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta implementados	Oficial de Seguridad Área Tecnológica	Lineamientos establecidos	20
7.6.3.- (*) EJECUCIÓN: Lineamientos para contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables implementadas	Oficial de Seguridad Área Tecnológica	Lineamientos establecidos	15
7.6.4.- (*) EJECUCIÓN: Cambio periódico de contraseñas de los usuarios controlados	Área Tecnológica Oficial de Seguridad	Registro de Configuración	12
7.6.5.- (*)EJECUCIÓN: Revisiones periódicas de la gestión de usuarios generadas y documentadas incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información	Oficial de Seguridad Área Tecnológica	Informe de revisión periódica	12
7.7.1.- (*) EJECUCIÓN: Medidas implementadas para que, en un determinado tiempo, 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	Área Tecnológica	Informes de implementación	12
7.8.1.- (*) EJECUCIÓN: Lineamientos de resguardo de Información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina implementado/ejecutado	Área de Servicios Generales	Lineamientos establecidos	15
7.8.2.- (*) EJECUCIÓN: Desconectar de la red, servicio o sistema, cuando se encuentren desatendidas	Área Tecnológica	Registro de Configuración	15

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
7.8.3.- (*) EJECUCIÓN: Copiadoras bloqueadas y control de acceso especial dispuesto para horario fuera de oficinas	Área Tecnológica	Informes de implementación	15
7.8.4.- (*) EJECUCIÓN: Información sensible retirada una vez que ha sido impresa	Área Tecnológica	Informes de implementación o informes de incidentes	10
7.8.5.- (*) EJECUCIÓN: Información sensible retirada, como las claves, de sus escritorios y pantallas	Área Tecnológica	Informes de implementación o informes de incidentes	10
7.8.6.- (*) EJECUCIÓN: Dispositivos removibles retirados una vez que se hayan dejado de utilizar	Área Tecnológica	Informes de implementación o informes de incidentes	20
8.1.1.- (*) EJECUCIÓN: Requerimientos de seguridad definidos. Por ejemplo: criptografía, control de sesiones, etc.	Oficial de Seguridad Área Tecnológica	Procesos de seguridad definidos	15
8.1.2.- (*) EJECUCIÓN: Controles apropiados definidos, tanto automatizados como manuales	Oficial de Seguridad Área Tecnológica	Procesos de seguridad definidos	15
9.1.1.- (*) EJECUCIÓN: Procedimiento formal instaurado/implementado para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente	Oficial de Seguridad Área Tecnológica	Procedimiento Implementado	15
9.1.2.- (*) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden	Oficial de Seguridad Área Tecnológica	Procedimiento Implementado	18
9.1.2.1.- (*) EJECUCIÓN: Incidentes Identificados	Área Tecnológica	Informe de Identificación del incidente	20
9.1.2.2.- (*) EJECUCIÓN: 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 registrado.	Área Tecnológica	Registro de los Incidentes	10
9.1.2.3.- (*) EJECUCIÓN: Incidentes de Seguridad de la Información de la institución notificados al Oficial de Seguridad	Área Tecnológica Oficial de Seguridad	Notificación de los Incidentes	12

HITO	ÁREA RESPONSABLE	PRODUCTO	HORAS DE TRABAJO
9.1.2.4.- (*) EJECUCIÓN: Incidentes clasificados de acuerdo al tipo de servicio afectado y al nivel de severidad	Área Tecnológica	Clasificación de los Incidentes	12
9.1.2.5.- (*) EJECUCIÓN: Incidentes priorizados en el caso de que se produjeran varios en forma simultanea	Área Tecnológica	Priorización del Incidente	12
9.1.2.6.- (*) EJECUCIÓN: Diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causa, realizado	Área Tecnológica	Diagnóstico del Incidente	12
9.1.2.7.- (*) EJECUCIÓN: Incidentes escalados, en el caso que el funcionario en turno no pueda solucionarlo	Área Tecnológica	Escalamiento del incidente	12
9.1.2.8.- (*) EJECUCIÓN: Causas Investigadas y diagnosticadas en forma definitiva las por las cuales se produjo el incidente	Área Tecnológica Oficial de Seguridad	Informe de causas de incidentes	12
9.1.2.9.- (*) EJECUCIÓN: 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 resueltos y restaurados	Área Tecnológica	Registro de la Solución	15
CIERRE: Reporte de ejecución de primera fase finalizada.	Área Tecnológica	Reporte de primera fase	12
DEFINICIÓN: Acuerdo de implementación del Esquema Gubernamental de Seguridad de la Información emitido	Viceministro	Generación de Acuerdo Ministerial	20

Anexo I: Tareas para cumplimiento Fase 2

SISTEMA DE GOBIERNO POR RESULTADOS (GPR)

PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN"

INFORME DE CUMPLIMIENTO DE HITOS FASE II

ENTIDAD / (SIGLAS):	*CONFIDENCIAL*

Dominio	Control	Hitos a cumplir
1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	1.2 Revisión de la Política	1.2.1
2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.2 Coordinación de la Gestión de la Seguridad de la Información	2.2.1.1 2.2.1.2 2.2.1.4 2.2.1.9
	2.3 Asignación de responsabilidades para la seguridad de la información	2.3.1.1 2.3.1.5 2.3.1.6 2.3.2.1 2.3.2.4 2.3.2.5 2.3.2.7
	2.4 Proceso de autorización para nuevos servicios de procesamiento de la información	2.4.4 2.4.5
	2.6 Contacto con las autoridades	2.6.1 2.6.2 2.6.3
	2.7 Contactos con grupos de interés especiales	2.7.2 2.7.3
	2.8 Revisión independiente de la seguridad de la información	2.8.1 2.8.3
	2.9 Identificación de los riegos relacionados con las partes externas	2.9.1 2.9.3 2.9.4
	2.10 Consideraciones de la seguridad cuando se trata de ciudadanos o clientes	2.10.1
	2.11 Consideraciones de la seguridad de los acuerdos con terceras partes	2.11.1

3 GESTIÓN DE LOS ACTIVOS	3.1 Inventario de activos	3.1.1 3.1.5 3.1.7 3.1.10 3.1.11 3.1.13 3.1.15 3.1.17 3.1.18 3.1.19 3.1.20 3.1.21 3.1.22 3.1.23 3.1.24 3.1.25 3.1.26 3.1.27 3.1.29
	3.2 Responsable de los activos	3.2.1
	3.3 Uso aceptable de los activos	3.3.1 3.3.2
	3.4 Directrices de clasificación de la información	3.4.2
	3.5 Etiquetado y manejo de la información	3.5.1 3.5.2 3.5.4 3.5.7
	4.1 Funciones y responsabilidades	4.1.4
	4.2 Selección	4.2.1
	4.3 Términos y condiciones laborales	4.3.1 4.3.2 4.3.3
	4.4 Responsabilidades de la dirección a cargo del funcionario	4.4.2 4.4.3
	4.5 Educación formación y sensibilización en seguridad de la información	4.5.1
	4.6 Proceso disciplinario	4.6.1 4.6.2
	4.7 Responsabilidades de la terminación de contrato	4.7.1 4.7.2 4.7.3 4.7.4
	4.8 Devolución de activos	4.8.1 4.8.2

4 SEGURIDAD DE LOS RECURSOS HUMANOS	4.9 Retiro de los privilegios de acceso	4.9.1
5 SEGURIDAD FÍSICA Y DEL ENTORNO	5.1 Perímetro de la seguridad física	5.1.1 5.1.4 5.1.5 5.1.6
	5.2 Controles de acceso físico	5.2.2
	5.3 Seguridad de oficinas, recintos e instalaciones	5.3.3 5.3.5
	5.4 Protección contra amenazas externas y ambientales	5.4.1 5.4.2 5.4.6
	5.5 Trabajo en áreas seguras	5.5.1
	5.6 Áreas de carga, despacho y acceso público	5.6.3 5.6.4 5.6.5
	5.7 Ubicación y protección de los equipos	5.7.1 5.7.2 5.7.5
	5.8 Servicios de suministro	5.8.1 5.8.2 5.8.5
	5.9 Seguridad del cableado	5.9.1 5.9.2 5.9.3 5.9.6
	5.10 Mantenimiento de los equipos	5.10.1 5.10.2 5.10.3
	5.11 Seguridad de los equipos fuera de las instalaciones	5.11.1
	5.12 Seguridad de la reutilización o eliminación de los equipos	5.12.1 5.12.2
	5.13 Retiro de activos de la propiedad	5.13.1 5.13.2 5.13.3 5.13.4

6.1 Documentación de los procedimientos de Operación	6.1.1 6.1.2 6.1.3 6.1.4 6.1.6 6.1.7 6.1.8
6.2 Gestión del cambio	6.2.1 6.2.2 6.2.3 6.2.6 6.2.7
6.3 Distribución de funciones	6.3.1 6.3.2
6.4 Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción	6.4.1 6.4.2 6.4.3 6.4.5 6.4.6 6.4.7 6.4.8
6.5 Presentación del servicio	6.5.1 6.5.2
6.6 Monitoreo y revisión de los servicios, por terceros.	6.6.1
6.7 Gestión de los cambios en los servicios ofrecidos por terceros	6.7.1 6.7.2 6.7.3
6.8 Gestión de la capacidad	6.8.2
6.9 Aceptación del Sistema	6.9.1 6.9.2 6.9.5 6.9.6 6.9.7
6.10 Controles contra código malicioso	6.10.2 6.10.5 6.10.6 6.10.7 6.10.9 6.10.10
6.11 Controles contra códigos móviles	6.11.1 6.11.2 6.11.4

6 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6.12 Establecer controles criptográficos para autenticar de forma única el código móvil.	6.12.5 6.12.6 6.12.8 6.12.9
	6.13 Controles de la redes	6.13.1 6.13.2 6.13.3
	6.14 Seguridad de los servicios de la red	6.14.3
	6.15 Gestión de los medios removibles	6.15.1 6.15.2 6.15.3
	6.16 Eliminación de los medios	6.16.1 6.16.2 6.16.3 6.16.4
	6.17 Procedimiento para el manejo de la información	6.17.1 6.17.2
	6.18 Seguridad de la documentación del sistema	6.18.1 6.18.2
	6.19 Políticas y procedimientos para el intercambio de información	6.19.2 6.19.4 6.19.5 6.19.6 6.19.7 6.19.9 6.19.10
	6.20 Acuerdos para el intercambio	6.20.2 6.20.3 6.20.5 6.20.7 6.20.8
	6.21 Medios físicos en tránsito	6.21.1 6.21.3 6.21.4 6.21.5
	6.22 Mensajería electrónica	6.22.1 6.22.2 6.22.3 6.22.4

	6.23 Sistemas de información del negocio	6.23.1 6.23.2 6.23.3 6.23.4 6.23.6 6.23.7
	6.24 Transacciones en línea	6.24.1 6.24.2 6.24.3 6.24.4 6.24.5 6.24.6
	6.25 Información disponible al público	6.25.1 6.25.2 6.25.3
	6.26 Registros de auditorías	6.26.1 6.26.2 6.26.5
	6.27 Monitoreo del uso del sistema	6.27.2 6.27.5
	6.28 Protección del registro de la información	6.28.1 6.28.2 6.28.4
	6.31 Sincronización de relojes	6.31.1 6.31.2 6.31.3
	7.1 Política de control de acceso	7.1.1 7.1.2
	7.2 Registro de usuarios	7.2.1
	7.3 Gestión de privilegios	7.3.1 7.3.3
	7.5 Revisión de los derechos de accesos de los usuarios	7.5.1 7.5.2
	7.8 Política de puesto de trabajo despejado y pantalla limpia	7.8.1 7.8.9
	7.9 Política de uso de los servicios de red	7.9.1 7.9.2 7.9.4
	7.10 Autenticación de usuarios para conexiones externas	7.10.2
	7.11 Identificación de los equipos en las redes	7.11.2 7.11.3
	7.12 Protección de los puertos de configuración y diagnóstico remoto	7.12.1

7 CONTROL DE ACCESO	7.13 Separación en las redes	7.13.2 7.13.3 7.13.4 7.13.6
	7.14 Control de conexión a las redes	7.14.1 7.14.2
	7.15 Control del enrutamiento en la red	7.15.3
	7.16 Procedimiento de registro de inicio seguro	7.16.8
	7.17 Identificación y autenticación de usuarios	7.17.6
	7.18 Sistema de gestión de contraseñas	7.18.4 7.18.5 7.18.6
	7.19 Uso de las utilidades del sistema	7.19.1
	7.20 Tiempo de inactividad de la sesión	7.20.1 7.20.2
	7.21 Limitación del tiempo de conexión	7.21.1 7.21.2 7.21.3
	7.22 Control de accesos a las aplicaciones y a la información	7.22.1 7.22.3
	7.23 Restricciones de acceso a la información	7.23.1 7.23.2 7.23.3
	7.24 Aislamiento de sistemas sensibles	7.24.1 7.24.2 7.24.3
	7.25 Computación y comunicaciones móviles	7.25.4 7.25.5
	7.26 Trabajo remoto	7.26.1 7.26.8 7.26.10
	8.1 Análisis y especificaciones de los requerimientos de seguridad	8.1.3
	8.2 Validación de datos de entrada	8.2.1 8.2.2
	8.3 Control de procesamiento interno	8.3.1 8.3.2 8.3.7 8.3.8 8.3.9
	8.4 Integridad del mensaje	8.4.1

8.5 Validación de datos de salidas	8.5.3 8.5.4
8.6 Política sobre el uso de controles criptográficos	8.6.2 8.6.4 8.6.6 8.6.7 8.6.8 8.6.9 8.6.10
8.7 Gestión de claves	8.7.1.1 8.7.1.2 8.7.1.5 8.7.1.6 8.7.1.7 8.7.1.9 8.7.1.12 8.7.1.15 8.7.2.1 8.7.2.2 8.7.2.3 8.7.2.5 8.7.2.9
8.8 Control de software operativo	8.8.1 8.8.2 8.8.3 8.8.4 8.8.5 8.8.8 8.8.8 8.8.10
8.9 Protección de los datos de prueba del sistema	8.9.1 8.9.2 8.9.3 8.9.5 8.9.6
8.10 Control de acceso al código fuente de los programas	8.10.1.1 8.10.1.2 8.10.1.3 8.10.1.5 8.10.1.7 8.10.2 8.10.5 8.10.7 8.10.8 8.10.10

8 ADQUISICIÓN, DESARROLLO, Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	8.11 Procedimiento de control de cambios	8.11.1 8.11.2 8.11.3 8.11.4 8.11.8 8.11.9
	8.12 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	8.12.1 8.12.2 8.12.3 8.12.5
	8.13 Restricción del cambio de paquetes de software	8.13.1 8.13.2 8.13.4 8.13.5 8.13.7
	8.14 Fuga de información	8.14.1 8.14.2 8.14.3 8.14.4 8.14.5 8.14.6 8.14.7 8.14.8
	8.15 Desarrollo de software contratado externamente	8.15.1 8.15.2 8.15.3 8.15.5
	8.16 Control de las vulnerabilidades técnicas	8.16.1 8.16.2 8.16.4 8.16.5 8.16.7 8.16.8 8.16.12 8.16.13 8.16.14 8.16.16
	9.1 Reporte sobre los eventos de seguridad de la información	9.1.2
	9.2 Reporte sobre las debilidades en la seguridad	9.2.1 9.2.2

9 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	9.3 Responsabilidades y procedimientos	9.3.2 9.3.3 9.3.4 9.3.5 9.3.6
	9.4 Aprendizaje debido a los incidentes de seguridad de la información	9.4.1 9.4.2 9.4.3 9.4.4 9.4.5
	9.5 Recolección de evidencias	9.5.1 9.5.2 9.5.3
10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	10.1.1 10.1.2 10.1.3 10.1.4
	10.2 Continuidad del negocio y evaluación de riesgos	10.2.1 10.2.2 10.2.4 10.2.5 10.2.6
	10.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	10.3.1 10.3.2 10.3.3 10.3.4
	10.4 Estructura para la planificación de la continuidad del negocio	10.4.1 10.4.2 10.4.3 10.4.4 10.4.5 10.4.6
	10.5 Pruebas, mantenimiento y revisión de los planes de continuidad del negocio.	10.5.1 10.5.2 10.5.3
	11.1 Identificación de la legislación aplicable	11.1.1 11.1.2 11.1.3

	11.2 Derechos de propiedad intelectual	11.2.1 11.2.2 11.2.3 11.2.5 11.2.9 11.2.11
	11.3 Protección de registros en cada entidad	11.3.1 11.3.2 11.3.3 11.3.4 11.3.5 11.3.9
	11.4 Protección de los datos y privacidad de la información personal	11.4.1 11.4.2 11.4.3
	11.5 Prevención del uso inadecuado de servicios de procesamiento de información	11.5.1 11.5.2 11.5.4 11.5.5 11.5.6 11.5.7
	11.6 Reglamentación de controles criptográficos	11.6.1 11.6.2 11.6.3 11.6.4
	11.7 Cumplimiento con las políticas y normas de la seguridad	11.7.1 11.7.2 11.7.3 11.7.4
	11.8 Verificación del cumplimento técnico	11.8.1 11.8.2 11.8.3 11.8.4
	11.9 Control de auditoría de los sistemas de Información	11.10.1 11.10.2 11.10.3 11.10.5 11.10.6 11.10.7 11.10.8
11 CUMPLIMIENTO	11.10 Protección de las herramientas de auditoría de los sistemas de Información	11.10.2 11.10.3 11.10.4 11.10.5

PIE DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*CONFIDENCIAL*
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD:	**FIRMA: CONFIDENCIAL**
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI:	**FIRMA: CONFIDENCIAL**

Anexo J: Valoración de Riesgos por A/V del Activo R1

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.1	**Servidor de Correos**	A. Fallo de sistema por falta de capacidad	A.1 No se dispone de capacidad de crecimiento y bajo la demanda actual del sistema.	2+2+2	8	**R.1.1**	**48**

		B. Errores en administración y uso de la plataforma.	B.1 Falta de procedimientos e instructivos de operación y mantenimiento.	3+3+2		**R.1.2**	**64**

Anexo K: Tareas a realizar en Activo R1 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Mitigar/ Evitar	A.1 Establecimiento de políticas de aceptación de uso del activo de información. Donde se especifique la capacidad y tiempo de retención a ser asignado por rol.	R1.1	A.1 Realizar las políticas de aceptación de uso del activo de información.	**24**

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
	A.2 Planificación de capacidad y adquisición de capacidad necesaria.	R.1.1	A.2 Identificación de necesidades del sistema.	
	A.3 Establecimiento de un sistema de monitoreo de capacidad de los sistemas de información. Memoria, CPU, Disco y respuesta ICMP	R.1.1	A.3 Verificar que todos los activos dentro del alcance se encuentren en el sistema NAGIOS.	
	B.1 Establecimiento de los procedimientos e instructivos de operación y mantenimiento.	R.1.2	B.1 Realizar procedimientos e instructivos de operación y mantenimiento. La parte lógica de lo que está en el CLOUD. Evaluación de los recursos. A nivel de DATA CENTER deberá hacerse acerca de la parte lógica y física.	

Anexo L: Valoración de Riesgos por A/V del Activo R2

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.2	**Servidor de Chat**	A. Perdida de información ante la caída de servidor de virtualización.	A.1 No se dispone de respaldo de la información depositada en el sistema	3+3+2	7	**R.2.1**	**56**

Anexo M: Tareas a realizar en Activo R2 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Mitigar/ Evitar	A.1 Establecimiento de mecanismos de respaldo de información.	R.2.1	A.1 Obtener respaldos de información del sistema de CHAT en el servidor de respaldos.	**21**
			A.2 Implementar un procedimiento de respaldo de información.	

Anexo N: Valoración de Riesgos por A/V del Activo R3

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo

R.3	**Servidor de Telefonía**	A. Errores en administración y uso.	A.1 Desconocimiento de procedimientos e instructivos de operación y mantenimiento.	1+2+2	7	**R.3.1**	**35**

Anexo O: Tareas a realizar en Activo R3 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual

Transferir/ Mitigar	A.1 Establecer procedimientos de administración y uso del sistema de telefonía.	R.3.1	A.1 Solicitar al proveedor los manuales del sistema, de usuario y mantenimiento del servidor de telefonía. A.2 Instruir o capacitar a los funcionarios de la Dirección de Soporte TI y Servicio al Usuario y Dirección de Infraestructura y Operaciones TI en el manejo del servidor de telefonía.	**21**

Anexo P: Valoración de Riesgos por A/V del Activo R4

ID	Activos de	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo

	información			de Riesgo			
R.4	**Infraestructura de Virtualización Local**	A. Pérdida de información ante fallo de sistemas y respaldo en la nube.	A.1 Incapacidad de restaurar la información del consulado virtual en la nube.	3+1+2	7	**R.4.1**	**42**
		B. Fallo en configuración por cambios en los sistemas de información.	B.1 Falta de capacitación de personal en tecnologías que se mantiene.	1+1+2		**R.4.2**	**28**

Anexo Q: Tareas a realizar en Activo R4 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Transferir/ Mitigar	A.1 Implementar un sistema de respaldo de información mediante un servidor físico dispuesto en la infraestructura de Telconet.	R.4.1	A.1 Realizar el estudio de factibilidad y de capacidad para conocer sobre las propiedades del sistema de respaldo. Implementar dicho estudio.	**21**
	B.1 Implementar un plan de formación a personal para cubrir tecnologías usadas.	R.4.2	B.1 Realizar capacitaciones para la adopción tecnológica de las herramientas en todas las direcciones.	

Anexo R: Valoración de Riesgos por A/V del Activo R5

ID	Activos de	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo

	información			de Riesgo			
R.5	**PCs de Operadores**	A. Equipo hackeado, exponiendo la información y accesos.	A.1 No están legalizadas las licencias.	2+2+3	8	**R.5.1**	**56**
			A.1. ESIGEX solo usa Windows.				
			A.1. Pasaportes solo funciona en Windows, está configurado en una red distinta al ESIGEX.				

Anexo S: Tareas a realizar en Activo R5 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Evitar/ Mitigar	A.1 Se deberá implementar licencias originales de los S.O. a las PCs de los operadores.	R.5.1	A.1 La Dirección de Soporte y Servicio al Usuario deberá encargarse de licenciar a las máquinas. Deberá de dar un reporte sobre el estado de las máquinas.	**24**

Anexo T: Valoración de Riesgos por A/V del Activo R6

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.6	**Servidores Físicos**	A. Daño del equipamiento del DataCenter y Servidores.	A.1 Falta de continuidad en los contratos de soporte con proveedores, de DataCenter y Servidores.	2+3+2	8	**R.6.1**	**56**
		B. Fallo de servidores por uso de equipamiento fuera de su ciclo de vida.	B.1 Retrasos en el proceso de adquisición de equipamiento nuevo.	3+2+2		**R.6.2**	**56**
		C. Daños del equipamiento ante catástrofes naturales, terremoto.	C.1 Falta de un respaldo de datos de los servidores críticos en un centro de datos alterno, Esigex.	3+1+2		**R.6.3**	**48**
		D. Daño o Robo de cintas de respaldo de información.	D.1 Falta de condiciones apropiadas.	3+1+2		**R.6.4**	**48**
		E. Incendio de instalaciones cercanas al cuarto de equipos.	E.1 Centro de Datos expuesto a posibles riesgos de inseguridad industrial.	3+2+2		**R.6.5**	**56**
		F. Fallo en configuración.	F.1 Falta de capacitación de personal en tecnologías que se mantiene.	2+2+2		**R.6.6**	**48**

Anexo U: Tareas a realizar en Activo R6 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Evitar/ Mitigar	A.1 Se deberá implementar procedimientos de continuidad en los contratos para garantizar el correcto funcionamiento de los servicios del CV.	R.6.1	A.1 Renovar los contratos de soporte para DataCenter y Servidores	**24**
	B.1 Se deberán establecer revisiones periódicas de los equipamientos que son utilizados por el sistema CV.	R.6.2	B.1 Renovación de equipamiento	
	C.1 Se deberá realizar de manera periódica copias de respaldos de los Servidores físicos.	R.6.3	C.1 Establecer copia de respaldo de información fuera del centro de datos principal.	
	D.1 Establecimiento de protocolo de respaldo y mantenimiento de respaldo en cintas.	R.6.4	D.1 Contratación o implementación de centro de almacenamiento de cinta de respaldo.	
			D.1 Establecimiento de un sistema de respaldo digital para mantenimiento de respaldo frecuente (incremental) y cinta para respaldo acumulado (totales).	
	E.1 Implementar condiciones adecuadas de seguridad industrial en alrededores del cuarto de equipamiento eléctrico.	R.6.5	E.1 De parte de la Dirección Administrativa realizar la gestión correspondiente para asegurar las condiciones de los servidores físicos.	

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
	F.1 Implementar un plan de formación de personal para cubrir tecnologías usadas.	R.6.6	F.1 Realizar capacitaciones en la cual se incluya transferencia tecnológica entre todas las direcciones.	

Anexo V: Valoración de Riesgos por A/V del Activo R7

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo

R.7	**Servidores Virtuales**	A. Perdida de información ante fallo de sistemas y respaldo en la nube.	A.1 Falta de un respaldo de información fuera de la infraestructura en la nube.	3+1+2	9	**R.7.1**	**54**
		B. Fallo en configuración por cambios en los sistemas de información	B.1 Falta de capacitación de personal en tecnologías que se mantiene.	2+2+2		**R.7.2**	**54**

Anexo W: Tareas a realizar en Activo R7 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual

Evitar/ Mitigar	A.1 Implementar un sistema de respaldo de información mediante un servidor físico dispuesto en la infraestructura de la empresa externa	R.7.1	A.1 Implementar un sistema de respaldo de información mediante un servidor físico dispuesto en la infraestructura de empresa externa.	**27**
	B.1 Implementar un plan de formación a personal para cubrir tecnologías usadas.	R.7.2	B.1 Implementar un plan de formación a personal para cubrir tecnologías usadas.	

Anexo X: Valoración de Riesgos por A/V del Activo R8

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo

ID	Activos de	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo	
R.8	**Operador**	A. Desatención de los procesos establecidos.	A.1. Gran parte de los operadores no tienen conocimiento informático.	2+2+2	8	**R.8.1**	**48**
		B. Ausencia de soporte a los operadores.	B.1 Solo existe una persona para dar soporte limitado.	3+2+2		**R.8.2**	**56**

Anexo Y: Tareas a realizar en Activo R8 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Evitar/ Mitigar	A.1. Realizar capacitaciones a los operadores.	R.8.1	A.1. Las capacitaciones antes, durante y después de que se salga de misión.	**24**
	B.1. Capacitar más personal para dar soporte a los operadores en el sistema de CV.	R.8.2	B.1 Transferir conocimiento en el soporte de uso de la herramienta del CV.	

Anexo Z: Valoración de Riesgos por A/V del Activo R9

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.9	**Sistema e-SIGEX**	A. Congestión del trámite.	A.1. El sistema permite el inicio de trámites de extranjeros con información no válida.	2+3+1	7	**R.9.1**	**42**
		B. Registro de información errónea.	B.1. El sistema permite el registro una misma persona extranjera con varios ID (cuentas de correo) y número de pasaporte ficticio.	2+3+1		**R.9.2**	**42**
		C. Ataque de denegación de servicios (DoS).	C.1. En los registros no se comprueba la validez del ID.	1+3+2		**R.9.3**	**42**
		D. Usurpación de credenciales de ingreso.	D.1 Para un tipo de usuarios no se valida la información.	2+3+1		**R.9.4**	**42**

Anexo AA: Tareas a realizar en Activo R9 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Transferir/ Mitigar	A.1 Se deberán cambiar la función de búsqueda para uso del operador que incluya por ID, nombres completos, nacionalidad y fecha de nacimiento.	R.9.1	A.1 Depurar los registros duplicados para que de esta manera se optimicen memoria, procesos, registros e informes.	**21**
	C.1 Gestionar la implementación del CAPTCHA para mitigar el ingreso de información basura.	R.9.3	C.1 Modificar el portal de ingreso y registro de usuario y añadir CAPTCHA.	
	D.1 Se debe validar la documentación declarada de forma presencial.	R.9.4	D.1 Se deberá establecer procedimientos de verificación de la documentación digital y física entregada.	

Anexo AB: Valoración de Riesgos por A/V del Activo R10

ID	Activos de	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo

	información			de Riesgo			
R.10	**Web (Liferay)**	A. Edición ilegal del portal, defacement.	A.1 CMS (sistema de gestión de contenidos) es susceptible a ataques, chequear actualizaciones.	3+1+2	9	**R.10.1**	**54**
		B. Fallo del software.	B.1 Software desactualizado. El cliente tendrá que hacerse cargo de la revisión y monitoreo de este sistema.	3+1+2		**R.10.2**	**54**
		C. Hackeo al sitio.	C.1 Errores de código. Falta de buenas prácticas, parametrización. C.2 Consideración de requisitos de seguridad.	1+2+3		**R.10.3**	**54**
		D. Fuga de información - Configuraciones e información depositada en el Liferay.	D.1 Que no se firmen acuerdos de confidencialidad con los proveedores del servicio.	2+1+2		**R.10.4**	**45**
		E. Indisponibilidad del servicio (3 veces al año)	E.1 No hay alta disponibilidad. No tienen alta disponibilidad: Liferay, Intalio.	3+2+2		**R.10.5**	**63**
		F. Materialización de incidentes.	F. Falta de procedimientos, instructivos, capacitación.	2+2+2		**R.10.6**	**54**
		G. Errores al ejecutar cambios.	G.1 Inexistencia o control de cambios defectuoso.	2+2+2		**R.10.7**	**54**

ID	Activos de	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo	
		H. Fallo a la hora de realizar los cambios.	H.1 Ausencia de versionamiento de software.	2+2+2		**R.10.8**	**54**
		I. Fallos en los procedimientos normales.	I.1 Ausencia de verificación del código del proveedor.	1+1+2		**R.10.9**	**36**

Anexo AC: Tareas a realizar en Activo R10 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Evitar/ Mitigar	A.1 Revisión permanente de las aplicaciones.	R.10.1	A.1 Realizar un Ethical Hacking al CV.	**27**
	B.1 Un operador de la Institución deberá estar pendiente de las actualizaciones y deberá verificar antes de actualizar.	R.10.2	B.1 Designar personal de la Dirección de Desarrollo TI para que sea el responsable de las actualizaciones de los sistemas de CV, recordar que no todos los parches son adecuados, podrían involucrar daños severos al servicio.	
	C.1 Se utilizan metodologías, se deberá hacer revisión exhaustiva del código.	R.10.3	C.1 Política general utiliza en JAVA. Metodología JAVA Code Convention.	
	D.1 Firma de acuerdos de confidencialidad del proveedor.	R.10.4	D.1 Acuerdo de confidencialidad entre empresas.	
	E.1 Implementación de alta disponibilidad.	R.10.5	E.1 Establecimiento de la arquitectura (la recomendada) para lograr alta disponibilidad, buenas prácticas.	
	F.1 Se deberá reportar sobre las debilidades del sistema.	R.10.6	F.1 Solicitar informes de los incidentes presentados.	
	G.1 Establecer procedimiento y política formales de control de cambios.	R.10.7	G.1 Tratar con la institución. Primer nivel: Política. Segundo nivel: Procedimiento. Tercer nivel: Formato de control de cambios.	
	H.1 Establecer un procedimiento de control de versionamiento de los sistemas en CV.	R.10.8	H.1 Verificar el control de versionamiento y disponer sobre aquello del ya realizado. Si no realizar un procedimiento interno.	
	I.1 Revisión de código fuente exhaustivo.	R.10.9	I.1 Designar personal de la Dirección de Desarrollo TI para que sea el responsable de recibir el código fuente.	

Anexo AD: Valoración de Riesgos por A/V del Activo R11

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo

R.11	**BDN(Postgres)**	A. Pérdida o daño de información.	A.1 No haya respaldo, se puede corromper la data.	2+2+2	7	**R.11.1**	**42**
		B. Fuga de información.	B.1 Que no se firmen acuerdos de confidencialidad con los proveedores del servicio.	2+1+1		**R.11.2**	**28**
		C. Materialización de incidentes.	C. Falta de procedimientos, instructivos, capacitación.	2+2+2		**R.11.3**	**42**
		D. Errores al ejecutar cambios.	D.1 Inexistencia o control de cambios defectuoso.	2+2+2		**R.11.4**	**42**
		E. Fallo a la hora de realizar los cambios.	E.1 Ausencia de versionamiento de software.	2+2+2		**R.11.5**	**42**
		F. Fallos en los procedimientos normales.	F.1 Ausencia de verificación del código del proveedor.	1+1+2		**R.11.6**	**28**

Anexo AE: Tareas a realizar en Activo R11 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Transferir/ Mitigar	A.1 Respaldo programado y respaldo antes de un evento importante sobre cambios en el sistema.	R.11.1	A.1 Realizar procedimientos de la institución para Backup.	**21**
	B.1 Firma de acuerdos de confidencialidad del proveedor.	R.11.2	B.1 Acuerdo de confidencialidad entre empresas.	
	C.1 Se deberá reportar sobre las debilidades del sistema y recolectar información sobre los incidentes para próximos eventos.	R.11.3	C.1 Solicitar informes de los incidentes presentados.	
	D.1 Establecer procedimiento y política formales de control de cambios.	R.11.4	D.1 Tratar con la institución. Primer nivel: Política. Segundo nivel: Procedimiento. Tercer nivel: Formato de control de cambios.	
	E.1 Establecer un procedimiento de control de versionamiento de los sistemas en CV.	R.11.5	E.1 Verificar el control de versionamiento y disponer sobre aquello del ya realizado. Si no realizar un procedimiento interno.	
	F.1 Revisión de código fuente exhaustivo.	R.11.6	F.1 Designar personal de la Dirección de Desarrollo TI para que sea el responsable de recibir el código fuente y realizar una revisión exhaustiva del mismo.	

Anexo AF: Valoración de Riesgos por A/V del Activo R12

ID	Activos de	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo

	información			de Riesgo			
R.12	**BDP(Mysql)**	A. Pérdida o daño de información.	A.1 No haya respaldo, se puede corromper la data.	2+2+2	5	**R.12.1**	**30**
		B. Fuga de información.	B.1 Que no se firmen acuerdos de confidencialidad con los proveedores del servicio.	2+1+1		**R.12.2**	**20**
		C. Materialización de incidentes.	C. Falta de procedimientos, instructivos, capacitación.	2+2+2		**R.12.3**	**30**
		D. Errores al ejecutar cambios.	D.1 Inexistencia o control de cambios defectuoso.	2+2+2		**R.12.4**	**30**
		E. Fallo a la hora de realizar los cambios.	E.1 Ausencia de versionamiento de software.	2+2+2		**R.12.5**	**30**
		F. Fallos en los procedimientos normales.	F.1 Ausencia de verificación del código del proveedor.	1+1+2		**R.12.6**	**20**

Anexo AG: Tareas a realizar en Activo R12 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Transferir/Mitigar	A.1 Respaldo programado y respaldo antes de un evento importante sobre cambios en el sistema y alta disponibilidad, activo-pasivo.	R.12.1	A.1 Implementar alta disponibilidad en MySQL.	**15**
	B.1 Firma de acuerdos de confidencialidad del proveedor.	R.12.2	B.1 Acuerdo de confidencialidad entre empresas.	
	C.1 Se deberá reportar sobre las debilidades del sistema y recolectar información sobre los incidentes para próximos eventos.	R.12.3	C.1 Solicitar informes de los incidentes presentados.	
	D.1 Establecer procedimiento y política formales de control de cambios.	R.12.4	D.1 Tratar con la institución. Primer nivel: Política. Segundo nivel: Procedimiento. Tercer nivel: Formato de control de cambios.	
	E.1 Establecer un procedimiento de control de versionamiento de los sistemas en CV.	R.12.5	E.1 Verificar el control de versionamiento y disponer sobre aquello del ya realizado. Si no realizar un procedimiento interno.	
	F.1 Revisión de código fuente exhaustivo.	R.12.6	F.1 Designar personal de la Dirección de Desarrollo TI para que sea el responsable de recibir el código fuente y realizar una revisión exhaustiva del mismo.	

Anexo AH: Valoración de Riesgos por A/V del Activo R13

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.13	**Usuarios (Ldap)**	A. Usuario malicioso obtenga cuentas de personas para que ellos no accedan al CV.	A.1 Creación de usuarios con datos públicos.	2+3+2	9	**R.13.1**	**63**
		B. Pérdida o daño de información.	B.1 No hay respaldo del Ldap.	2+2+2		**R.13.2**	**54**
		C. Creación de cuentas falsas.	C.1 No existe validación de datos para los usuarios extranjeros en el registro.	2+3+2		**R.13.3**	**63**
		D. Fuga de información - Configuraciones e información depositada en el Ldap.	D.1 Que no se firmen acuerdos de confidencialidad con los proveedores del servicio.	2+1+1		**R.13.4**	**36**
		E. Incidentes a la hora de ejecutar cambios.	E.1 Inexistencia de control de cambios en el Ldap, error al ejecutar este proceso.	2+2+2		**R.13.5**	**54**
		F. Fallo a la hora de realizar los cambios en el LDAP (aplicación).	F.1 Ausencia de versionamiento de software.	2+2+2		**R.13.6**	**54**

Anexo AI: Tareas a realizar en Activo R13 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Evitar/Mitigar	A.1. Incluir la validación de los datos ingresados con otra fuente, ej.: el registro civil.	R.13.1	A.1 Implementar la validación de datos personales de ecuatorianos.	**27**
	B.1 Respaldo programado y respaldo antes de un evento importante sobre cambios en el sistema y alta disponibilidad, activo-pasivo.	R.13.2	B.1 Implementar alta disponibilidad en el activo Ldap.	
	C.1 Validación de Datos y la implementación del CAPTCHA para la contención de bots.	R.13.3	C.1 Investigar la opción de validación de datos con fuentes externas e implementar el CAPTCHA.	
	D.1 Firma de acuerdos de confidencialidad del proveedor.	R.13.4	D.1 Acuerdo de confidencialidad entre empresas.	
	E.1 Establecer procedimiento y política formales de control de cambios.	R.13.5	E.1 Tratar con la institución. Primer nivel: Política. Segundo nivel: Procedimiento. Tercer nivel: Formato de control de cambios.	
	F.1 Establecer un procedimiento de control de versionamiento del LDAP.	R.13.6	F.1 Verificar el control de versionamiento del LDAP.	

Anexo AJ: Valoración de Riesgos por A/V del Activo R4

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.14	**BPM (Intalio)**	A. Fallo del servidor/servicio.	A.1 No hay alta disponibilidad.	3+2+2	5	**R.14.1**	**35**
		B. Fuga de información (BPM Código Fuente).	B.1 Que no se firmen acuerdos de confidencialidad con los proveedores del servicio.	2+1+1		**R.14.2**	**20**
		C. Materialización de Incidentes.	C.1 Falta de procedimientos, instructivos, capacitación.	2+2+2		**R.14.3**	**30**
		D. Errores al ejecutar cambios.	D.1 Inexistencia o control de cambios defectuoso.	2+2+2		**R.14.4**	**30**
		E. Uso de versión de código no validado.	E.1 Ausencia de versionamiento de software.	2+2+2		**R.14.5**	**30**
		F. Comportamiento inesperado o no deseado en la aplicación Consulado Virtual.	F.1 Ausencia de verificación del código del proveedor.	1+1+2		**R.14.6**	**20**

Anexo AK: Tareas a realizar en Activo R14 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Transferir/Mitigar	A.1 Realizar el estudio de alta disponibilidad para implementarlo.	R.14.1	A.1 Realizar el estudio de factibilidad de crear alta disponibilidad en un CLOUD externo al ya utilizado.	**15**
	B.1 Firma de acuerdos de confidencialidad del proveedor.	R.14.2	B.1 Acuerdo de confidencialidad entre empresas.	
	C.1 Se deberá reportar sobre las debilidades del sistema y recolectar información sobre los incidentes para próximos eventos.	R.14.3	C.1 Solicitar informes de los incidentes presentados.	
	D.1 Establecer procedimiento y política formales de control de cambios.	R.14.4	D.1 Tratar con la institución. Primer nivel: Política. Segundo nivel: Procedimiento. Tercer nivel: Formato de control de cambios.	
	E.1 Establecer un procedimiento de control de versionamiento de los sistemas en CV.	R.14.5	E.1 Verificar el control de versionamiento y disponer sobre aquello del ya realizado. Si no realizar un procedimiento interno.	
	F.1 Revisión de código fuente exhaustivo.	R.14.6	F.1 Designar personal de la Dirección de Desarrollo TI para que sea el responsable de recibir el código fuente y realizar una revisión exhaustiva del mismo.	

Anexo AL: Valoración de Riesgos por A/V del Activo R15

ID	Activos de información	Amenazas	Vulnerabilidades	Probabilidad de Riesgo	Impacto	Riesgo	
R.15	**Docs (Alfresco)**	A. Fuga de información sensible (documentos de los clientes).	A.1 Acceso a la información por parte de funcionarios no autorizados.	2+1+2	8	**R.15.1**	**40**
		B. Fuga de información - Documentación e información depositada en Alfresco.	B.1 Que no se firmen acuerdos de confidencialidad con los proveedores del servicio.	2+1+1		**R.15.2**	**32**
		C. Fallo a la hora de realizar los cambios en Alfresco (aplicación).	C.1 Ausencia de versionamiento de software.	2+2+2		**R.15.3**	**48**

Anexo AM: Tareas a realizar en Activo R15 – Riesgo Residual

Opción de tratamiento del riesgo	Control	ID Riesgo	Tarea a realizar/Evidencia	Riesgo residual
Transferir/ Mitigar	A.1 Firmas de acuerdo de confidencialidad para los administradores, capacitación del personal administrativo de la herramienta. Monitorear control de acceso y logs.	R.15.1	A.1 Realizar capacitaciones, la institución deberá garantizar la firma de acuerdos de confidencialidad, se deberán realizar e implementar procedimientos para logs y control de acceso, destinar un servidor independiente para almacenamiento de logs (que no sea manejado por el administrador).	**24**
	B.1 Firma de acuerdos de confidencialidad del proveedor.	R.15.2	B.1 Acuerdo de confidencialidad entre empresas.	
	C.1 Establecer un procedimiento de control de versionamiento del Alfresco	R.15.3	C.1 Verificar el control de versionamiento del Alfresco.	

Anexo AN: EGSI-SCRUM

Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Producto
EGSI-SCRUM	**266 días**	**lun 01/06/15**	lun 06/06/16		
Implementación Fase 1	**71 días**	**lun 01/06/15**	**lun 07/09/15**		
Sprint 1	**11 días**	**lun 01/06/15**	**lun 15/06/15**		
Reunión de Planificación	2 horas	**lun 01/06/15**	lun 01/06/15	Oficial de Seguridad	
1.1.1.- (*) EJECUCIÓN: Implementación del EGSI en la institución dispuesta por la máxima autoridad.	20 horas	lun 01/06/15	vie 05/06/15	Viceministro	Documentación de la Implementación del EGSI
2.1.3.- (*) EJECUCIÓN: Comité de Gestión de la Seguridad de la Información oficialmente Conformado	20 horas	lun 01/06/15	vie 05/06/15	Viceministro	Comité conformado
2.2.1.1.- (*) EJECUCIÓN: Oficial de Seguridad de la Información quien actuará como coordinador del CSI oficialmente designado.	20 horas	lun 01/06/15	vie 05/06/15	Viceministro	Oficial designado
DEFINICIÓN: Acuerdo de implementación del Esquema Gubernamental de Seguridad de la Información emitido	20 horas	lun 01/06/15	vie 05/06/15	Viceministro	Generación de Acuerdo Ministerial
1.1.2.- (*) EJECUCIÓN: Política de seguridad de la información de referencia o propia de la institución difundida	15 horas	lun 01/06/15	jue 04/06/15	Coordinador General de TIC'S	Políticas Establecidas y Difundidas.
3.1.2.1.- (*) EJECUCIÓN: inventario de Equipos móviles: teléfono inteligente (Smartphone), teléfono	10 horas	lun 01/06/15	mié 03/06/15	Coordinador General de Auditoría Interna	Inventarios

celular, tableta, computador portátil, asistente digital personal (PDA), etc. realizado					
6.26.1.- (*) EJECUCIÓN: Accesos y tipos de acceso registrados	18 horas	lun 01/06/15	vie 05/06/15	Director de Infraestructura y Operaciones TI	Esquemas definidos y aplicados
5.1.1.- (*) EJECUCIÓN: Área definida de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio	15 horas	lun 01/06/15	jue 04/06/15	Director Administrativo	Áreas Establecidas
2.5.2.- (*) EJECUCIÓN: Acuerdos de confidencialidad de la información, documento físico o electrónico firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción	10 horas	lun 01/06/15	mié 03/06/15	Director de Administración de Talento Humano	Acuerdos firmados
2.5.3.- (*) EJECUCIÓN: Acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos custodiados/archivados	10 horas	lun 01/06/15	mié 03/06/15	Director de Asuntos Legales de Gestión Interna	Acuerdos firmados/archivados
7.8.1.- (*) EJECUCIÓN: Lineamientos de resguardo de Información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina implementado/ejecutado	15 horas	lun 01/06/15	jue 04/06/15	Director de Comunicación Social	Lineamientos establecidos
6.10.1.- (*) EJECUCIÓN: Prohibir el uso de software no autorizado por la	10 horas	lun 01/06/15	mié 03/06/15	Director de Desarrollo TI	Elaboración de listado de SOFTWARE no permitido e

institución. Listado del software autorizado elaborado.					Informes de monitoreo
5.3.2.- (*)EJECUCIÓN: Impresoras, copiadoras, etc. ubicadas en un área protegida	10 horas	lun 01/06/15	mié 03/06/15	Director de Documentos y Servicios	Informes de Ubicación de las Impresoras
6.12.1.- (*) EJECUCIÓN: Procedimientos determinado para el resguardo y contención de la información por parte de los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información.	20 horas	lun 01/06/15	vie 05/06/15	Director de Gestión y Servicios	Procedimientos establecidos y aplicados
2.5.5.- (*) EJECUCIÓN: Aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros realizados/ejecutados	15 horas	lun 01/06/15	jue 04/06/15	Director de la Gestión Documental y Archivo	Generación de Acuerdos/Firma de Acuerdos
2.1.2.- (*) EJECUCIÓN: La difusión, capacitación y sensibilización del contenido del EGSI dispuesta	12 horas	lun 01/06/15	mié 03/06/15	Director de Seguridad Informática TI	Área Tecnológica
3.3.1.- (*) EJECUCIÓN: Uso de correo electrónico institucional reglamentado	12 horas	lun 01/06/15	mié 03/06/15	Director de Servicio y Soporte al Usuario	Reglamento de uso de correo electrónico institucional
4.4.1.- (*)EJECUCIÓN: Funciones y las responsabilidades respecto a la seguridad de la información explicadas y definidas,	12 horas	lun 01/06/15	mié 03/06/15	Director de Servicios, Procesos y Calidad	Acta de funciones entregadas y firmadas a la firma del contrato

antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles					
SCRUM diario	15 mins	mar 02/06/15	mar 02/06/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 03/06/15	mié 03/06/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 04/06/15	jue 04/06/15	Oficial de Seguridad	
6.26.4.- (*) EJECUCIÓN: Sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS) activados y desactivados	15 horas	jue 04/06/15	mar 09/06/15	Director de Desarrollo TI	Registro de Configuración
2.5.1.- (*) EJECUCIÓN: Acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI elaborados y aprobados	12 horas	jue 04/06/15	lun 08/06/15	Director de Seguridad Informática TI	Acuerdos elaborados
3.3.2.- (*) EJECUCIÓN: Acceso y uso de la Internet y sus aplicaciones/servicios reglamentado	12 horas	jue 04/06/15	lun 08/06/15	Director de Servicio y Soporte al Usuario	Reglamento de acceso y uso de internet, aplicaciones y servicios
SCRUM diario	15 mins	vie 05/06/15	vie 05/06/15	Oficial de Seguridad	
2.1.1.- (*) EJECUCIÓN: Seguimiento de la puesta en marcha de las normas EGSI realizado	10 horas	vie 05/06/15	mar 09/06/15	Coordinador General de TIC'S	Informes de seguimiento de todas las unidades
Revisión del Sprint	2 horas	lun 08/06/15	lun 08/06/15	Oficial de Seguridad	

3.1.2.2.- (*) EJECUCIÓN: Inventario de Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc. realizado	10 horas	lun 08/06/15	mié 10/06/15	Coordinador General de Auditoría Interna	Inventarios
6.26.2.- (*) EJECUCIÓN: Direcciones y protocolos de red registrados	18 horas	lun 08/06/15	vie 12/06/15	Director de Infraestructura y Operaciones TI	Registro de direcciones y protocolos de red
SCRUM diario	15 mins	mar 09/06/15	mar 09/06/15	Oficial de Seguridad	
6.10.2.- (*) EJECUCIÓN: Software de antivirus y contra código malicioso instalado y actualizado periódicamente	15 horas	mar 09/06/15	vie 12/06/15	Director de Seguridad Informática TI	Informes de monitoreo
3.3.3.- (*) EJECUCIÓN: Uso de los sistemas de video-conferencia reglamentado	12 horas	mar 09/06/15	jue 11/06/15	Director de Servicio y Soporte al Usuario	Reglamento de uso de los sistemas de video-conferencia
SCRUM diario	15 mins	mié 10/06/15	mié 10/06/15	Oficial de Seguridad	
2.2.1.2.- (*) EJECUCIÓN: Responsable de seguridad del área de Tecnologías de la Información oficialmente designado.	10 horas	mié 10/06/15	vie 12/06/15	Coordinador General de TIC'S	Director Designado
6.30.3.- (*) EJECUCIÓN: Registro de fallas esté habilitado	15 horas	mié 10/06/15	lun 15/06/15	Director de Desarrollo TI	Registro de Configuración
SCRUM diario	15 mins	jue 11/06/15	jue 11/06/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 12/06/15	vie 12/06/15	Oficial de Seguridad	
Retrospectiva del	1,5	lun	lun	Oficial de	

Sprint	horas	15/06/15	15/06/15	Seguridad	
Sprint 2	**11 días**	**lun 15/06/15**	**lun 29/06/15**		
Reunión de Planificación	1,5 horas	**lun 15/06/15**	lun 15/06/15	Oficial de Seguridad	
3.1.2.3.- (*) EJECUCIÓN: Inventario de Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc. realizado	10 horas	lun 15/06/15	mié 17/06/15	Coordinador General de Auditoría Interna	Inventarios
6.6.2.- (*) EJECUCIÓN: Reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos analizados	20 horas	lun 15/06/15	vie 19/06/15	Coordinador General de TIC'S	Resultados de evaluaciones y análisis de reportes
5.2.1.- (*) EJECUCIÓN: Hora y fecha de ingreso y salida de permanencia de visitantes en las áreas restringidas registradas y supervisadas.	5 horas	lun 15/06/15	mar 16/06/15	Director Administrativo	Proceso de Registro
4.1.1.- (*) EJECUCIÓN: Candidatos verificados, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida.	10 horas	lun 15/06/15	mié 17/06/15	Director de Administración de Talento Humano	Proceso de Verificación Implementado
7.16.6.- (*) EJECUCIÓN: Identificadores de aplicación controlados para que no muestren identificadores de aplicación ni de sistema,	20 horas	lun 15/06/15	vie 19/06/15	Director de Desarrollo TI	Registro de Configuración

hasta que el proceso de registro se haya completado exitosamente.					
5.7.1.- (*) EJECUCIÓN: Directrices establecidas para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información	12 horas	lun 15/06/15	mié 17/06/15	Director de Documentos y Servicios	Elaboración y Formalización de la Directriz
6.8.1.- (*) EJECUCIÓN: Proyecciones realizadas de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos	20 horas	lun 15/06/15	vie 19/06/15	Director de Gestión y Servicios	Planificación de compras o contrataciones relacionadas
5.8.1.- (*) EJECUCIÓN: 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 identificados	20 horas	lun 15/06/15	vie 19/06/15	Director de Infraestructura y Operaciones TI	Informe de Funcionamiento de UPS
3.4.1.- (*) EJECUCIÓN: Información clasificada como pública o confidencial	20 horas	lun 15/06/15	vie 19/06/15	Director de la Gestión Documental y Archivo	Informes de Cumplimiento del Hito
6.14.1.- (*) EJECUCIÓN: Tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red incorporada/implementada	20 horas	lun 15/06/15	vie 19/06/15	Director de Seguridad Informática TI	Informes de implementación y monitoreo
6.1.1.- (*) EJECUCIÓN: Contactos de soporte, necesarios en	10 horas	lun 15/06/15	mié 17/06/15	Director de Servicio y Soporte al	Elaboración de listado de Contactos

caso de incidentes documentados				Usuario	
5.2.2.- (*) EJECUCIÓN: Código de uso de una identificación visible para todo el personal y visitantes y de acompañamiento de visitas a áreas restringidas implementado.	5 horas	lun 15/06/15	mar 16/06/15	Director de Servicios, Procesos y Calidad	Proceso de Uso de Identificación
SCRUM diario	15 mins	mar 16/06/15	mar 16/06/15	Oficial de Seguridad	
2.5.4.- (*) EJECUCIÓN: Firma de los acuerdos de confidencialidad vinculados/anexados a los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción	5 horas	mar 16/06/15	mié 17/06/15	Director de Asuntos Legales de Gestión Interna	Generación de Acuerdos/Firma de Acuerdos
SCRUM diario	15 mins	mié 17/06/15	mié 17/06/15	Oficial de Seguridad	
5.3.1.- (*) EJECUCIÓN: Instalaciones claves protegidas de acceso a personal no autorizado	20 horas	mié 17/06/15	mar 23/06/15	Director Administrativo	Implementación de Control de Acceso
SCRUM diario	15 mins	jue 18/06/15	jue 18/06/15	Oficial de Seguridad	
3.1.2.4.- (*) EJECUCIÓN: Inventario de Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc. realizado	10 horas	jue 18/06/15	lun 22/06/15	Coordinador General de Auditoría Interna	Inventarios
7.16.1.- (*) EJECUCIÓN: Usuarios	20 horas	jue 18/06/1	mié 24/06/1	Director de Servicio y	Registro de Configuración e

autorizados autenticados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada		5	5	Soporte al Usuario	informes periódicos de usuarios autenticados
SCRUM diario	15 mins	vie 19/06/15	vie 19/06/15	Oficial de Seguridad	
Revisión del Sprint	2 horas	lun 22/06/15	lun 22/06/15	Oficial de Seguridad	
6.6.3.- (*) EJECUCIÓN: 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	18 horas	lun 22/06/15	vie 26/06/15	Coordinador General de TIC'S	Resultados de evaluaciones y auditorias contratadas
7.16.7.- (*) EJECUCIÓN: Cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos	15 horas	lun 22/06/15	jue 25/06/15	Director de Desarrollo TI	Registro de Configuración
5.9.1.- (*) EJECUCIÓN: Diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc. identificados/documentados	20 horas	lun 22/06/15	vie 26/06/15	Director de Infraestructura y Operaciones TI	Entrega de Diagramas de Conexión
6.14.2.- (*)EJECUCIÓN: Soluciones implementadas que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de	20 horas	lun 22/06/15	vie 26/06/15	Director de Seguridad Informática TI	Informes de implementación y monitoreo

firewalls, antivirus, etc.					
SCRUM diario	15 mins	mar 23/06/15	mar 23/06/15	Oficial de Seguridad	
3.1.2.5.- (*) EJECUCIÓN: Inventario de Periféricos y dispositivos de almacenamiento realizado	10 horas	mar 23/06/15	jue 25/06/15	Coordinador General de Auditoría Interna	Inventarios
SCRUM diario	15 mins	mié 24/06/15	mié 24/06/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 25/06/15	jue 25/06/15	Oficial de Seguridad	
7.16.2.- (*) EJECUCIÓN: Registro de definición documentado para el uso de privilegios especiales del sistema	10 horas	jue 25/06/15	lun 29/06/15	Director de Servicio y Soporte al Usuario	Protocolo definido
SCRUM diario	15 mins	vie 26/06/15	vie 26/06/15	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 29/06/15	lun 29/06/15	Oficial de Seguridad	
Sprint 3	**11 días**	**lun 29/06/15**	**lun 13/07/15**		
Reunión de Planificación	1,5 horas	**lun 29/06/15**	lun 29/06/15	Oficial de Seguridad	
3.1.2.6.- (*) EJECUCIÓN: Inventario de Periféricos de comunicaciones realizado	10 horas	lun 29/06/15	mié 01/07/15	Coordinador General de Auditoría Interna	Inventarios
7.6.5.- (*)EJECUCIÓN: Revisiones periódicas de la gestión de usuarios generadas y documentadas incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información	12 horas	lun 29/06/15	mié 01/07/15	Coordinador General de TIC'S	Informe de revisión periódica

5.4.2.- (*) EJECUCIÓN: Mantenimientos en los sistemas de climatización y ductos de ventilación realizados / ejecutados	15 horas	lun 29/06/15	jue 02/07/15	Director Administrativo	Cronogramas e Informes de mantenimiento
4.1.2.- (*) EJECUCIÓN: Funciones y responsabilidades entregados formalmente a los funcionarios.	12 horas	lun 29/06/15	mié 01/07/15	Director de Administración de Talento Humano	Funciones entregadas a la firma del contrato
7.16.8.- (*) EJECUCIÓN: Tiempo de dilación limitado antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica	15 horas	lun 29/06/15	jue 02/07/15	Director de Desarrollo TI	Registro de Configuración
6.12.3.- (*) EJECUCIÓN: Extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución definida	15 horas	lun 29/06/15	jue 02/07/15	Director de Documentos y Servicios	Esquemas definidos y aplicados
5.4.1.- (*) EJECUCIÓN: Mantenimientos de las instalaciones eléctricas y UPS realizados	15 horas	lun 29/06/15	jue 02/07/15	Director de Infraestructura y Operaciones TI	Cronogramas e Informes de mantenimiento
6.10.3.- (*) EJECUCIÓN: Los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles	15 horas	lun 29/06/15	jue 02/07/15	Director de Seguridad Informática TI	Informes de monitoreo
7.16.5.- (*) EJECUCIÓN: Tiempo definido de conexión de los usuarios, considerando las necesidades de la institución	18 horas	lun 29/06/15	vie 03/07/15	Director de Servicio y Soporte al Usuario	Esquema de tiempos de conexión por usuarios
SCRUM diario	15 mins	mar 30/06/1	mar 30/06/1	Oficial de Seguridad	

		5	5		
SCRUM diario	15 mins	mié 01/07/15	mié 01/07/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 02/07/15	jue 02/07/15	Oficial de Seguridad	
3.1.2.7.- (*) EJECUCIÓN: Inventario de Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc. realizado	10 horas	jue 02/07/15	lun 06/07/15	Coordinador General de Auditoría Interna	Inventarios
9.1.2.3.- (*) EJECUCIÓN: Incidentes de Seguridad de la Información de la institución notificados al Oficial de Seguridad	12 horas	jue 02/07/15	lun 06/07/15	Coordinador General de TIC'S	Notificación de los Incidentes
SCRUM diario	15 mins	vie 03/07/15	vie 03/07/15	Oficial de Seguridad	
5.6.1.- (*) EJECUCIÓN: Código de acceso al área de despacho y carga, únicamente a personal identificado y autorizado implementado	15 horas	vie 03/07/15	mié 08/07/15	Director Administrativo	Implementación de Sistema de Acceso
7.17.2.- (*) EJECUCIÓN: Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, definido y documentado	20 horas	vie 03/07/15	jue 09/07/15	Director de Desarrollo TI	Registro de Configuración
5.5.1.- (*) EJECUCIÓN: Código de uso equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos	10 horas	vie 03/07/15	mar 07/07/15	Director de Infraestructura y Operaciones TI	Elaboración, entrega e implementación del procedimiento de uso

móviles, etc., implementado					
6.27.1.- (*) EJECUCIÓN: Accesos autorizados, incluyendo registrados	12 horas	vie 03/07/15	mar 07/07/15	Director de Seguridad Informática TI	Registros de perfiles de acceso
Revisión del Sprint	2 horas	lun 06/07/15	lun 06/07/15	Oficial de Seguridad	
SCRUM diario	15 mins	mar 07/07/15	mar 07/07/15	Oficial de Seguridad	
7.18.2.- (*) EJECUCIÓN: Contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad cambiados	15 horas	lun 06/07/15	jue 09/07/15	Director de Servicio y Soporte al Usuario	Esquemas de definición y uso de claves para personal de TICS
3.1.2.8.- (*)EJECUCIÓN: Inventario de Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc. realizado	10 horas	mar 07/07/15	jue 09/07/15	Coordinador General de Auditoría Interna	Inventarios
9.1.2.4.- (*) EJECUCIÓN: Incidentes clasificados de acuerdo al tipo de servicio afectado y al nivel de severidad	12 horas	mar 07/07/15	jue 09/07/15	Coordinador General de TIC'S	Clasificación de los Incidentes
SCRUM diario	15 mins	mié 08/07/15	mié 08/07/15	Oficial de Seguridad	
6.12.2.- (*) EJECUCIÓN: Procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención definido	12 horas	mié 08/07/15	vie 10/07/15	Director de Infraestructura y Operaciones TI	Respaldos realizados, etiquetados y almacenados
6.27.2.- (*) EJECUCIÓN: Operaciones privilegiadas	12 horas	mié 08/07/15	vie 10/07/15	Director de Seguridad Informática TI	Reportes de monitoreo

monitoreadas					
SCRUM diario	15 mins	jue 09/07/15	jue 09/07/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 10/07/15	vie 10/07/15	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 13/07/15	lun 13/07/15	Oficial de Seguridad	
Sprint 4	**11 días**	**lun 13/07/15**	**lun 27/07/15**		
Reunión de Planificación	1,5 horas	**lun 13/07/15**	lun 13/07/15	Oficial de Seguridad	
3.1.3.1.- (*) EJECUCIÓN: Inventario de Sistemas operativos realizado	10 horas	lun 13/07/15	mié 15/07/15	Coordinador General de Auditoría Interna	Inventarios
9.1.2.5.- (*) EJECUCIÓN: Incidentes priorizados en el caso de que se produjeran varios en forma simultanea	12 horas	lun 13/07/15	mié 15/07/15	Coordinador General de TIC'S	Priorización del Incidente
7.17.3.- (*) EJECUCIÓN: Uso de usuarios genéricos restringido	18 horas	lun 13/07/15	vie 17/07/15	Director de Desarrollo TI	Registro de Configuración
6.26.3.- (*) EJECUCIÓN: Alarmas originadas por el sistema de control de acceso definidas	20 horas	lun 13/07/15	vie 17/07/15	Director de Infraestructura y Operaciones TI	Informes de implementación y monitoreo
6.27.3.- (*) EJECUCIÓN: Intentos de acceso no autorizados monitoreados	8 horas	lun 13/07/15	mar 14/07/15	Director de Seguridad Informática TI	Reportes de monitoreo
7.25.1.- (*) EJECUCIÓN: Exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo registrados/controlados	15 horas	lun 13/07/15	jue 16/07/15	Director de Servicio y Soporte al Usuario	Control de ubicación de los equipos portátiles/informe
SCRUM diario	15 mins	mar 14/07/1	mar 14/07/1	Oficial de Seguridad	

		5	5		
SCRUM diario	15 mins	mié 15/07/15	mié 15/07/15	Oficial de Seguridad	
6.27.4.- (*) EJECUCIÓN: Alertas o fallas del sistema revisados	8 horas	mié 15/07/15	jue 16/07/15	Director de Seguridad Informática TI	Análisis de alertas o fallas
SCRUM diario	15 mins	jue 16/07/15	jue 16/07/15	Oficial de Seguridad	
3.1.3.2.- (*) EJECUCIÓN: Inventario de Software de servicio, mantenimiento o administración realizado	10 horas	jue 16/07/15	lun 20/07/15	Coordinador General de Auditoría Interna	Inventarios
9.1.2.7.- (*) EJECUCIÓN: Incidentes escalados, en el caso que el funcionario en turno no pueda solucionarlo	12 horas	jue 16/07/15	lun 20/07/15	Coordinador General de TIC'S	Escalamiento del incidente
SCRUM diario	15 mins	vie 17/07/15	vie 17/07/15	Oficial de Seguridad	
6.29.1.- (*) EJECUCIÓN: Hora en la que ocurrió el evento registrados	8 horas	vie 17/07/15	lun 20/07/15	Director de Seguridad Informática TI	Reportes de monitoreo
7.26.1.- (*) EJECUCIÓN: Uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución reportado/registrado.	15 horas	vie 17/07/15	mié 22/07/15	Director de Servicio y Soporte al Usuario	Control de ubicación de los equipos portátiles/informe
Revisión del Sprint	2 horas	lun 20/07/15	lun 20/07/15	Oficial de Seguridad	
7.18.3.- (*) EJECUCIÓN: Lineamientos de cambio de contraseña obligatorio en el primer registro de acceso o inicio de sesión implementado	15 horas	lun 20/07/15	jue 23/07/15	Director de Desarrollo TI	Lineamientos establecidos
7.10.1.- (*)	15	lun	jue	Director de	Estrategias o

EJECUCIÓN: Mecanismos generados/implementados para asegurar la información transmitida por los canales de conexión remota	horas	20/07/15	23/07/15	Infraestructura y Operaciones TI	protocolos definidos
SCRUM diario	15 mins	mar 21/07/15	mar 21/07/15	Oficial de Seguridad	
3.1.3.3.- (*)EJECUCIÓN: Inventario de Paquetes de software o software base realizado	10 horas	mar 21/07/15	jue 23/07/15	Coordinador General de Auditoría Interna	Inventarios
6.29.2.- (*) EJECUCIÓN: Información sobre el evento registrados	8 horas	mar 21/07/15	mié 22/07/15	Director de Seguridad Informática TI	Reportes de monitoreo
SCRUM diario	15 mins	mié 22/07/15	mié 22/07/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 23/07/15	jue 23/07/15	Oficial de Seguridad	
6.29.3.- (*) EJECUCIÓN: Cuenta de administrador y operador que estuvo involucrado registrados	8 horas	jue 23/07/15	vie 24/07/15	Director de Seguridad Informática TI	Reportes de monitoreo
7.8.4.- (*) EJECUCIÓN: Información sensible retirada una vez que ha sido impresa	10 horas	jue 23/07/15	lun 27/07/15	Director de Servicio y Soporte al Usuario	Informes de implementación o informes de incidentes
SCRUM diario	15 mins	vie 24/07/15	vie 24/07/15	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 27/07/15	lun 27/07/15	Oficial de Seguridad	
Sprint 5	**11 días**	**lun 27/07/15**	**lun 10/08/15**		
Reunión de Planificación	1,5 horas	**lun 27/07/15**	lun 27/07/15	Oficial de Seguridad	

3.1.3.4.- (*) EJECUCIÓN: Inventario de Aplicativos informáticos del negocio realizado	10 horas	lun 27/07/15	mié 29/07/15	Coordinador General de Auditoría Interna	Inventarios
7.12.1.- (*) EJECUCIÓN: Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, eliminados o deshabilitados	20 horas	lun 27/07/15	vie 31/07/15	Director de Infraestructura y Operaciones TI	Informes de implementación
6.30.1.- (*) EJECUCIÓN: Registros realizados de fallas o errores del sistema revisados	8 horas	lun 27/07/15	mar 28/07/15	Director de Seguridad Informática TI	Reportes de monitoreo
7.16.4.- (*) EJECUCIÓN: Mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios utilizados/ejecutados	15 horas	lun 27/07/15	jue 30/07/15	Coordinador General de TIC'S	Reportes periódicos
7.7.1.- (*) EJECUCIÓN: Medidas implementadas para que, en un determinado tiempo, 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	12 horas	lun 27/07/15	mié 29/07/15	Director de Servicio y Soporte al Usuario	Informes de implementación
7.6.2.- (*) EJECUCIÓN: Lineamientos de generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta	20 horas	lun 27/07/15	vie 31/07/15	Director de Desarrollo TI	Lineamientos establecidos

implementados					
SCRUM diario	15 mins	mar 28/07/15	mar 28/07/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 29/07/15	mié 29/07/15	Oficial de Seguridad	
3.1.4.1.- (*) EJECUCIÓN: Inventario de Cables de comunicaciones realizado	10 horas	mié 29/07/15	vie 31/07/15	Coordinador General de Auditoría Interna	Inventarios
6.30.2.- (*)EJECUCIÓN: Medidas correctivas realizadas para garantizar que no se hayan vulnerado los controles revisados	15 horas	mié 29/07/15	lun 03/08/15	Director de Seguridad Informática TI	Informes de implementación de recomendaciones y observaciones
SCRUM diario	15 mins	jue 30/07/15	jue 30/07/15	Oficial de Seguridad	
7.8.5.- (*) EJECUCIÓN: Información sensible retirada, como las claves, de sus escritorios y pantallas	10 horas	jue 30/07/15	lun 03/08/15	Director de Servicio y Soporte al Usuario	Informes de implementación o informes de incidentes
SCRUM diario	15 mins	vie 31/07/15	vie 31/07/15	Oficial de Seguridad	
7.17.1.- (*) EJECUCIÓN: Actividades evidenciadas de las personas responsables de administraciones críticas de la institución, rastreados utilizando los identificadores de usuario	15 horas	vie 31/07/15	mié 05/08/15	Coordinador General de TIC'S	Reportes de actividades de personas responsables de administraciones criticas
Revisión del Sprint	2 horas	lun 03/08/15	lun 03/08/15	Oficial de Seguridad	
3.1.4.2.- (*) EJECUCIÓN: Inventario de Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo	10 horas	lun 03/08/15	mié 05/08/15	Coordinador General de Auditoría Interna	Inventarios

terminal de datos, etc.) realizado					
7.13.1.- (*) EJECUCIÓN: Evaluación de riesgos realizada para identificar los segmentos de red donde se encuentren los activos críticos para la institución	20 horas	lun 03/08/15	vie 07/08/15	Director de Infraestructura y Operaciones TI	Informes de evaluación de riesgos relacionados
7.6.3.- (*) EJECUCIÓN: Lineamientos para contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables implementadas	15 horas	lun 03/08/15	jue 06/08/15	Director de Desarrollo TI	Lineamientos establecidos
SCRUM diario	15 mins	mar 04/08/15	mar 04/08/15	Oficial de Seguridad	
7.16.3.- (*) EJECUCIÓN: 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 documentados	15 horas	mar 04/08/15	vie 07/08/15	Director de Seguridad Informática TI	Reporte de monitoreo
9.1.2.- (*) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden	18 horas	mar 04/08/15	lun 10/08/15	Director de Servicio y Soporte al Usuario	Procedimiento Implementado
SCRUM diario	15 mins	mié 05/08/15	mié 05/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 06/08/15	jue 06/08/15	Oficial de Seguridad	
3.1.4.3.- (*) EJECUCIÓN: Inventario	10 horas	jue 06/08/1	lun 10/08/1	Coordinador General de	Inventarios

de Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc. Realizado		5	5	Auditoría Interna	
6.29.4.- (*) EJECUCIÓN: Procesos que estuvieron implicados registrados	8 horas	jue 06/08/15	vie 07/08/15	Director de Seguridad Informática TI	Reportes de monitoreo
SCRUM diario	15 mins	vie 07/08/15	vie 07/08/15	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 10/08/15	lun 10/08/15	Oficial de Seguridad	
Sprint 6	**11 días**	**lun 10/08/15**	**lun 24/08/15**		
Reunión de Planificación	1,5 horas	**lun 10/08/15**	lun 10/08/15	Oficial de Seguridad	
3.1.4.4.- (*) EJECUCIÓN: Inventario de Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc. Realizado	10 horas	lun 10/08/15	mié 12/08/15	Coordinador General de Auditoría Interna	Inventarios
7.26.2.- (*) EJECUCIÓN: Protección de antivirus y reglas del Firewall definidas/ reguladas	20 horas	lun 10/08/15	vie 14/08/15	Director de Desarrollo TI	Registro de Configuración
7.15.1.- (*) EJECUCIÓN: Políticas de control de acceso configuradas para el enrutamiento en la red, basándose en los requerimientos de la institución	20 horas	lun 10/08/15	vie 14/08/15	Director de Infraestructura y Operaciones TI	Registro de Configuración
6.6.1.- (*) EJECUCIÓN: Niveles de desempeño de los servicios monitoreados	18 horas	lun 10/08/15	vie 14/08/15	Director de Seguridad Informática TI	Evaluación de informes y reportes de implementación y

para verificar el cumplimiento de los acuerdos					monitoreo
9.1.1.- (*) EJECUCIÓN: Procedimiento formal instaurado/implementado para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente	15 horas	lun 10/08/15	jue 13/08/15	Coordinador General de TIC'S	Procedimiento Implementado
7.6.1.- (*) EJECUCIÓN: Procedimiento de accesos documentado donde se indique las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados	20 horas	lun 10/08/15	vie 14/08/15	Director de Servicio y Soporte al Usuario	Registro de claves por usuarios
SCRUM diario	15 mins	mar 11/08/15	mar 11/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 12/08/15	mié 12/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 13/08/15	jue 13/08/15	Oficial de Seguridad	
7.11.1.- (*) EJECUCIÓN: Equipos que se encuentran en las redes documentados e identificados	8 horas	jue 13/08/15	vie 14/08/15	Coordinador General de Auditoría Interna	Reportes periódicos
SCRUM diario	15 mins	vie 14/08/15	vie 14/08/15	Oficial de Seguridad	
Revisión del Sprint	2 horas	lun 17/08/15	lun 17/08/15	Oficial de Seguridad	
7.17.4.- (*) EJECUCIÓN: Métodos alternos utilizados a la contraseña, como los	20 horas	lun 17/08/15	vie 21/08/15	Coordinador General de Auditoría Interna	Inventario de medios alternativos de autenticación y

medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación					políticas de uso
7.4.1.- (*)EJECUCIÓN: Proceso formal para la asignación y cambio de contraseñas establecido	20 horas	lun 17/08/15	vie 21/08/15	Director de Desarrollo TI	Registro de Configuración
7.18.1.- (*) EJECUCIÓN: Política de accesos implementada donde se indica la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible	12 horas	lun 17/08/15	mié 19/08/15	Director de Seguridad Informática TI	Política de accesos definida e implementada
7.8.3.- (*) EJECUCIÓN: Copiadoras bloqueadas y control de acceso especial dispuesto para horario fuera de oficinas	15 horas	lun 17/08/15	jue 20/08/15	Director de Servicio y Soporte al Usuario	Informes de implementación
7.6.4.- (*) EJECUCIÓN: Cambio periódico de contraseñas de los usuarios controlados	12 horas	lun 17/08/15	mié 19/08/15	Director de Infraestructura y Operaciones TI	Registro de Configuración
SCRUM diario	15 mins	mar 18/08/15	mar 18/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 19/08/15	mié 19/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 20/08/15	jue 20/08/15	Oficial de Seguridad	
9.1.2.2.- (*) EJECUCIÓN: 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	10 horas	jue 20/08/15	lun 24/08/15	Director de Seguridad Informática TI	Registro del los Incidentes

descripción del incidente registrados.					
SCRUM diario	15 mins	vie 21/08/15	vie 21/08/15	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 24/08/15	lun 24/08/15	Oficial de Seguridad	
Sprint 7	**11 días**	lun 24/08/15	**lun 07/09/15**		
Reunión de Planificación	1,5 horas	**lun 24/08/15**	lun 24/08/15	Oficial de Seguridad	
7.8.5.- (*) EJECUCIÓN: Información sensible retirada, como las claves, de sus escritorios y pantallas	10 horas	lun 24/08/15	mié 26/08/15	Director de Servicio y Soporte al Usuario	Informes de implementación o informes de incidentes
8.1.1.- (*) EJECUCIÓN: Requerimientos de seguridad definidos. Por ejemplo: criptografía, control de sesiones, etc.	15 horas	lun 24/08/15	jue 27/08/15	Director de Desarrollo TI	Procesos de seguridad definidos
9.1.2.6.- (*) EJECUCIÓN: Diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causa, realizado	12 horas	lun 24/08/15	mié 26/08/15	Director de Seguridad Informática TI	Diagnostico del Incidente
SCRUM diario	15 mins	mar 25/08/15	mar 25/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 26/08/15	mié 26/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 27/08/15	jue 27/08/15	Oficial de Seguridad	
9.1.2.1.- (*)	20	jue	mié	Director de	Informe de

EJECUCIÓN: Incidentes Identificados	horas	27/08/15	02/09/15	Servicio y Soporte al Usuario	Identificación del incidente
9.1.2.8.- (*) EJECUCIÓN: Causas Investigadas y diagnosticadas en forma definitiva las por las cuales se produjo el incidente	12 horas	jue 27/08/15	lun 31/08/15	Director de Seguridad Informática TI	Informe de causas de incidentes
SCRUM diario	15 mins	vie 28/08/15	vie 28/08/15	Oficial de Seguridad	
8.1.2.- (*) EJECUCIÓN: Controles apropiados definidos, tanto automatizados como manuales	15 horas	vie 28/08/15	mié 02/09/15	Director de Desarrollo TI	Procesos de seguridad definidos
Revisión del Sprint	2 horas	lun 31/08/15	lun 31/08/15	Oficial de Seguridad	
SCRUM diario	15 mins	mar 01/09/15	mar 01/09/15	Oficial de Seguridad	
9.1.2.9.- (*) EJECUCIÓN: 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 resueltos y restaurados	15 horas	mar 01/09/15	vie 04/09/15	Director de Seguridad Informática TI	Registro de la Solución
SCRUM diario	15 mins	mié 02/09/15	mié 02/09/15	Oficial de Seguridad	
CIERRE: Reporte de ejecución de primera fase finalizada.	12 horas	mié 02/09/15	vie 04/09/15	Coordinador General de TIC'S	Reporte de primera fase
SCRUM diario	15 mins	jue 03/09/15	jue 03/09/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 04/09/15	vie 04/09/15	Oficial de Seguridad	
Retrospectiva del	1,5	lun	lun	Oficial de	

Sprint	horas	07/09/15	07/09/15	Seguridad	
Implementación Fase 2	**191 días**	lun 14/09/15	lun 06/06/16		
Sprint 1	**11 días**	lun 14/09/15	**lun 28/09/15**		
Reunión de Planificación	1,5 horas	lun 14/09/15	lun 14/09/15	Oficial de Seguridad	
1.2 Revisión de la Política	10 horas	lun 14/09/15	mié 16/09/15	Viceministro	
2.2 Coordinación de la Gestión de la Seguridad de la Información	11 horas	lun 14/09/15	mié 16/09/15	Área de Servicios Generales	
4.1 Funciones y responsabilidades	5 horas	lun 14/09/15	mar 15/09/15	Área de Recursos Humanos	
6.3 Distribución de funciones	10 horas	lun 14/09/15	mié 16/09/15	Área Tecnológica	
SCRUM diario	15 mins	mar 15/09/15	mar 15/09/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 16/09/15	mié 16/09/15	Oficial de Seguridad	
4.2 Selección	8 horas	mié 16/09/15	jue 17/09/15	Área de Recursos Humanos	
SCRUM diario	15 mins	jue 17/09/15	jue 17/09/15	Oficial de Seguridad	
2.3 Asignación de responsabilidades para la seguridad de la información	10 horas	jue 17/09/15	lun 21/09/15	Área de Servicios Generales	
6.4 Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción	20 horas	jue 17/09/15	mié 23/09/15	Área Tecnológica	
SCRUM diario	15	vie	vie	Oficial de	

	mins	18/09/15	18/09/15	Seguridad	
4.3 Términos y condiciones laborales	15 horas	vie 18/09/15	mié 23/09/15	Área de Recursos Humanos	
Revisión de Sprint	2 horas	lun 21/09/15	lun 21/09/15	Oficial de Seguridad	
SCRUM diario	15 mins	mar 22/09/15	mar 22/09/15	Oficial de Seguridad	
2.4 Proceso de autorización para nuevos servicios de procesamiento de la información	10 horas	mar 22/09/15	jue 24/09/15	Área de Servicios Generales	
SCRUM diario	15 mins	mié 23/09/15	mié 23/09/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 24/09/15	jue 24/09/15	Oficial de Seguridad	
6.5 Presentación del servicio	5 horas	jue 24/09/15	vie 25/09/15	Área Tecnológica	
SCRUM diario	15 mins	vie 25/09/15	vie 25/09/15	Oficial de Seguridad	
6.6 Monitoreo y revisión de los servicios, por terceros.	5 horas	vie 25/09/15	lun 28/09/15	Área Tecnológica	
Retrospectiva del Sprint	1,5 horas	lun 28/09/15	lun 28/09/15	Oficial de Seguridad	
Sprint 2	**11 días**	lun 28/09/15	**lun 12/10/15**		
Reunión de Planificación	1,5 horas	lun 28/09/15	lun 28/09/15	Oficial de Seguridad	
2.6 Contacto con las autoridades	10 horas	lun 28/09/15	mié 30/09/15	Área de Servicios Generales	
4.4 Responsabilidades de la dirección a cargo del	14 horas	lun 28/09/15	jue 01/10/15	Área de Recursos Humanos	

funcionario					
6.8 Gestión de la capacidad	10 horas	lun 28/09/15	mié 30/09/15	Área Tecnológica	
SCRUM diario	15 mins	mar 29/09/15	mar 29/09/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 30/09/15	mié 30/09/15	Oficial de Seguridad	
2.7 Contactos con grupos de interés especiales	10 horas	mié 30/09/15	vie 02/10/15	Área de Servicios Generales	
SCRUM diario	15 mins	jue 01/10/15	jue 01/10/15	Oficial de Seguridad	
6.9 Aceptación del Sistema	10 horas	jue 01/10/15	lun 05/10/15	Área Tecnológica	
SCRUM diario	15 mins	vie 02/10/15	vie 02/10/15	Oficial de Seguridad	
4.5 Educación formación y sensibilización en seguridad de la información	20 horas	vie 02/10/15	jue 08/10/15	Área de Recursos Humanos	
Revisión de Sprint	2 horas	lun 05/10/15	lun 05/10/15	Oficial de Seguridad	
2.8 Revisión independiente de la seguridad de la información	10 horas	lun 05/10/15	mié 07/10/15	Área de Servicios Generales	
SCRUM diario	15 mins	mar 06/10/15	mar 06/10/15	Oficial de Seguridad	
6.10 Controles contra código malicioso	20 horas	mar 06/10/15	lun 12/10/15	Área Tecnológica	
SCRUM diario	15 mins	mié 07/10/15	mié 07/10/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 08/10/15	jue 08/10/15	Oficial de Seguridad	

2.9 Identificación de los riegos relacionados con las partes externas	10 horas	jue 08/10/15	lun 12/10/15	Área de Servicios Generales	
SCRUM diario	15 mins	vie 09/10/15	vie 09/10/15	Oficial de Seguridad	
4.7 Responsabilidades de la terminación de contrato	5 horas	vie 09/10/15	lun 12/10/15	Área de Recursos Humanos	
Retrospectiva del Sprint	1,5 horas	lun 12/10/15	lun 12/10/15	Oficial de Seguridad	
Sprint 3	11 días	lun 12/10/15	lun 26/10/15		
Reunión de Planificación	1,5 horas	lun 12/10/15	lun 12/10/15	Oficial de Seguridad	
2.10 Consideraciones de la seguridad cuando se trata de ciudadanos o clientes	10 horas	lun 12/10/15	mié 14/10/15	Área de Servicios Generales	
4.6 Proceso disciplinario	14 horas	lun 12/10/15	jue 15/10/15	Área de Recursos Humanos	
6.1 Documentación de los procedimientos de Operación	10 horas	lun 12/10/15	mié 14/10/15	Área Tecnológica	
SCRUM diario	15 mins	mar 13/10/15	mar 13/10/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 14/10/15	mié 14/10/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 15/10/15	jue 15/10/15	Oficial de Seguridad	
2.11 Consideraciones de la seguridad de los acuerdos con terceras partes	10 horas	jue 15/10/15	lun 19/10/15	Área de Servicios Generales	
6.2 Gestión del cambio	8 horas	jue 15/10/15	vie 16/10/15	Área Tecnológica	
SCRUM diario	15 mins	vie 16/10/1	vie 16/10/1	Oficial de Seguridad	

		5	5		
4.8 Devolución de activos	5 horas	vie 16/10/15	lun 19/10/15	Área de Recursos Humanos	
6.7 Gestión de los cambios en los servicios ofrecidos por terceros	5 horas	vie 16/10/15	lun 19/10/15	Área Tecnológica	
Revisión de Sprint	2 horas	lun 19/10/15	lun 19/10/15	Oficial de Seguridad	
3.2 Responsable de los activos	2 horas	lun 19/10/15	lun 19/10/15	Área de Servicios Generales	
SCRUM diario	15 mins	mar 20/10/15	mar 20/10/15	Oficial de Seguridad	
3.3 Uso aceptable de los activos	5 horas	mar 20/10/15	mié 21/10/15	Área de Servicios Generales	
4.9 Retiro de los privilegios de acceso	5 horas	mar 20/10/15	mié 21/10/15	Área de Recursos Humanos	
6.11 Controles contra códigos móviles	10 horas	mar 20/10/15	jue 22/10/15	Área Tecnológica	
SCRUM diario	15 mins	mié 21/10/15	mié 21/10/15	Oficial de Seguridad	
3.4 Directrices de clasificación de la información	2 horas	mié 21/10/15	mié 21/10/15	Área de Servicios Generales	
SCRUM diario	15 mins	jue 22/10/15	jue 22/10/15	Oficial de Seguridad	
3.5 Etiquetado y manejo de la información	10 horas	jue 22/10/15	lun 26/10/15	Área de Servicios Generales	
SCRUM diario	15 mins	vie 23/10/15	vie 23/10/15	Oficial de Seguridad	
6.15 Gestión de los medios removibles	5 horas	vie 23/10/15	lun 26/10/15	Área Tecnológica	
Retrospectiva del Sprint	1,5 horas	lun 26/10/15	lun 26/10/15	Oficial de Seguridad	

Sprint 4	11 días	lun 26/10/15	lun 09/11/15		
Reunión de Planificación	1,5 horas	lun 26/10/15	lun 26/10/15	Oficial de Seguridad	
3.1 Inventario de activos	32 horas	lun 26/10/15	mié 04/11/15	Área de Servicios Generales	
11.1 Identificación de la legislación aplicable	6 horas	lun 26/10/15	mar 27/10/15	Área de Recursos Humanos	
6.12 Establecer controles criptográficos para autenticar de forma única el código móvil.	15 horas	lun 26/10/15	jue 29/10/15	Área Tecnológica	
SCRUM diario	15 mins	mar 27/10/15	mar 27/10/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 28/10/15	mié 28/10/15	Oficial de Seguridad	
11.2 Derechos de propiedad intelectual	15 horas	mié 28/10/15	lun 02/11/15	Área de Recursos Humanos	
SCRUM diario	15 mins	jue 29/10/15	jue 29/10/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 30/10/15	vie 30/10/15	Oficial de Seguridad	
6.13 Controles de la redes	15 horas	vie 30/10/15	mié 04/11/15	Área Tecnológica	
Revisión de Sprint	2 horas	lun 02/11/15	lun 02/11/15	Oficial de Seguridad	
SCRUM diario	15 mins	mar 03/11/15	mar 03/11/15	Oficial de Seguridad	
11.3 Protección de registros en cada entidad	15 horas	mar 03/11/15	vie 06/11/15	Área de Recursos Humanos	
SCRUM diario	15 mins	mié 04/11/15	mié 04/11/15	Oficial de Seguridad	

SCRUM diario	15 mins	jue 05/11/15	jue 05/11/15	Oficial de Seguridad	
5.1 Perímetro de la seguridad física	8 horas	jue 05/11/15	vie 06/11/15	Área de Servicios Generales	
6.14 Seguridad de los servicios de la red	10 horas	jue 05/11/15	lun 09/11/15	Área Tecnológica	
SCRUM diario	15 mins	vie 06/11/15	vie 06/11/15	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 09/11/15	lun 09/11/15	Oficial de Seguridad	
Sprint 5	11 días	lun 09/11/15	lun 23/11/15		
Reunión de Planificación	1,5 horas	lun 09/11/15	lun 09/11/15	Oficial de Seguridad	
5.2 Controles de acceso físico	8 horas	lun 09/11/15	mar 10/11/15	Área de Servicios Generales	
6.16 Eliminación de los medios	10 horas	lun 09/11/15	mié 11/11/15	Área Tecnológica	
11.4 Protección de los datos y privacidad de la información personal	8 horas	lun 09/11/15	mar 10/11/15	Área de Recursos Humanos	
SCRUM diario	15 mins	mar 10/11/15	mar 10/11/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 11/11/15	mié 11/11/15	Oficial de Seguridad	
5.3 Seguridad de oficinas, recintos e instalaciones	8 horas	mié 11/11/15	jue 12/11/15	Área de Servicios Generales	
6.17 Procedimiento para el manejo de la información	5 horas	mié 11/11/15	jue 12/11/15	Área Tecnológica	
11.5 Prevención del uso inadecuado de servicios de procesamiento de	15 horas	mié 11/11/15	lun 16/11/15	Área de Recursos Humanos	

información					
SCRUM diario	15 mins	jue 12/11/15	jue 12/11/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 13/11/15	vie 13/11/15	Oficial de Seguridad	
5.4 Protección contra amenazas externas y ambientales	8 horas	vie 13/11/15	lun 16/11/15	Área de Servicios Generales	
6.19 Políticas y procedimientos para el intercambio de información	10 horas	vie 13/11/15	mar 17/11/15	Área Tecnológica	
Revisión de Sprint	2 horas	lun 16/11/15	lun 16/11/15	Oficial de Seguridad	
SCRUM diario	15 mins	mar 17/11/15	mar 17/11/15	Oficial de Seguridad	
5.5 Trabajo en áreas seguras	10 horas	mar 17/11/15	jue 19/11/15	Área de Servicios Generales	
11.6 Reglamentación de controles criptográficos	10 horas	mar 17/11/15	jue 19/11/15	Área de Recursos Humanos	
SCRUM diario	15 mins	mié 18/11/15	mié 18/11/15	Oficial de Seguridad	
6.21 Medios físicos en tránsito	15 horas	mié 18/11/15	lun 23/11/15	Área Tecnológica	
SCRUM diario	15 mins	jue 19/11/15	jue 19/11/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 20/11/15	vie 20/11/15	Oficial de Seguridad	
5.6 Áreas de carga, despacho y acceso público	5 horas	vie 20/11/15	lun 23/11/15	Área de Servicios Generales	
Retrospectiva del Sprint	1,5 horas	lun 23/11/15	lun 23/11/15	Oficial de Seguridad	
Sprint 6	11 días	lun 23/11/1	lun 07/12/1		

		5	5		
Reunión de Planificación	1,5 horas	lun 23/11/15	lun 23/11/15	Oficial de Seguridad	
5.7 Ubicación y protección de los equipos	10 horas	lun 23/11/15	mié 25/11/15	Área de Servicios Generales	
6.18 Seguridad de la documentación del sistema	8 horas	lun 23/11/15	mar 24/11/15	Área Tecnológica	
11.7 Cumplimiento con las políticas y normas de la seguridad	8 horas	lun 23/11/15	mar 24/11/15	Área de Recursos Humanos	
SCRUM diario	15 mins	mar 24/11/15	mar 24/11/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 25/11/15	mié 25/11/15	Oficial de Seguridad	
6.22 Mensajería electrónica	12 horas	mié 25/11/15	vie 27/11/15	Área Tecnológica	
11.8 Verificación del cumplimento técnico	8 horas	mié 25/11/15	jue 26/11/15	Área de Recursos Humanos	
SCRUM diario	15 mins	jue 26/11/15	jue 26/11/15	Oficial de Seguridad	
5.10 Mantenimiento de los equipos	18 horas	jue 26/11/15	mié 02/12/15	Área de Servicios Generales	
SCRUM diario	15 mins	vie 27/11/15	vie 27/11/15	Oficial de Seguridad	
11.9 Control de auditoría de los sistemas de Información	8 horas	vie 27/11/15	lun 30/11/15	Área de Recursos Humanos	
Revisión de Sprint	2 horas	lun 30/11/15	lun 30/11/15	Oficial de Seguridad	
6.23 Sistemas de información del negocio	15 horas	lun 30/11/15	jue 03/12/15	Área Tecnológica	
SCRUM diario	15 mins	mar 01/12/15	mar 01/12/15	Oficial de Seguridad	

11.10 Protección de las herramientas de auditoría de los sistemas de Información	8 horas	mar 01/12/15	mié 02/12/15	Área de Recursos Humanos	
SCRUM diario	15 mins	mié 02/12/15	mié 02/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 03/12/15	jue 03/12/15	Oficial de Seguridad	
5.11 Seguridad de los equipos fuera de las instalaciones	12 horas	jue 03/12/15	lun 07/12/15	Área de Servicios Generales	
SCRUM diario	15 mins	vie 04/12/15	vie 04/12/15	Oficial de Seguridad	
6.27 Monitoreo del uso del sistema	5 horas	vie 04/12/15	lun 07/12/15	Área Tecnológica	
Retrospectiva del Sprint	1,5 horas	lun 07/12/15	lun 07/12/15	Oficial de Seguridad	
Sprint 7	11 días	lun 07/12/15	lun 21/12/15		
Reunión de Planificación	1,5 horas	lun 07/12/15	lun 07/12/15	Oficial de Seguridad	
5.8 Servicios de suministro	10 horas	lun 07/12/15	mié 09/12/15	Área de Servicios Generales	
6.20 Acuerdos para el intercambio	8 horas	lun 07/12/15	mar 08/12/15	Área Tecnológica	
SCRUM diario	15 mins	mar 08/12/15	mar 08/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 09/12/15	mié 09/12/15	Oficial de Seguridad	
6.25 Información disponible al público	8 horas	mié 09/12/15	jue 10/12/15	Área Tecnológica	
SCRUM diario	15 mins	jue 10/12/15	jue 10/12/15	Oficial de Seguridad	

5.9 Seguridad del cableado	15 horas	jue 10/12/15	mar 15/12/15	Área de Servicios Generales	
SCRUM diario	15 mins	vie 11/12/15	vie 11/12/15	Oficial de Seguridad	
6.26 Registros de auditorías	8 horas	vie 11/12/15	lun 14/12/15	Área Tecnológica	
Revisión de Sprint	2 horas	lun 14/12/15	lun 14/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	mar 15/12/15	mar 15/12/15	Oficial de Seguridad	
6.28 Protección del registro de la información	10 horas	mar 15/12/15	jue 17/12/15	Área Tecnológica	
SCRUM diario	15 mins	mié 16/12/15	mié 16/12/15	Oficial de Seguridad	
5.12 Seguridad de la reutilización o eliminación de los equipos	10 horas	mié 16/12/15	vie 18/12/15	Área de Servicios Generales	
SCRUM diario	15 mins	jue 17/12/15	jue 17/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 18/12/15	vie 18/12/15	Oficial de Seguridad	
6.31 Sincronización de relojes	5 horas	vie 18/12/15	lun 21/12/15	Área Tecnológica	
Retrospectiva del Sprint	1,5 horas	lun 21/12/15	lun 21/12/15	Oficial de Seguridad	
Sprint 8	11 días	lun 21/12/15	lun 04/01/16		
Reunión de Planificación	1,5 horas	lun 21/12/15	lun 21/12/15	Oficial de Seguridad	
6.24 Transacciones en línea	15 horas	lun 21/12/15	jue 24/12/15	Área Tecnológica	
5.13 Retiro de	10	lun	mié	Área de	

activos de la propiedad	horas	21/12/15	23/12/15	Servicios Generales	
SCRUM diario	15 mins	mar 22/12/15	mar 22/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 23/12/15	mié 23/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	jue 24/12/15	jue 24/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	vie 25/12/15	vie 25/12/15	Oficial de Seguridad	
7.1 Política de control de acceso	5 horas	vie 25/12/15	lun 28/12/15	Área Tecnológica	
Revisión de Sprint	2 horas	lun 28/12/15	lun 28/12/15	Oficial de Seguridad	
7.2 Registro de usuarios	5 horas	lun 28/12/15	mar 29/12/15	Área Tecnológica	
SCRUM diario	15 mins	mar 29/12/15	mar 29/12/15	Oficial de Seguridad	
SCRUM diario	15 mins	mié 30/12/15	mié 30/12/15	Oficial de Seguridad	
7.8 Política de puesto de trabajo despejado y pantalla limpia	5 horas	mié 30/12/15	jue 31/12/15	Área Tecnológica	
SCRUM diario	15 mins	jue 31/12/15	jue 31/12/15	Oficial de Seguridad	
7.9 Política de uso de los servicios de red	5 horas	jue 31/12/15	vie 01/01/16	Área Tecnológica	
SCRUM diario	15 mins	vie 01/01/16	vie 01/01/16	Oficial de Seguridad	
7.21 Limitación del tiempo de conexión	5 horas	vie 01/01/16	lun 04/01/16	Área Tecnológica	
Retrospectiva del	1,5	lun	lun	Oficial de	

Sprint	horas	04/01/16	04/01/16	Seguridad	
Sprint 9	11 días	lun 04/01/16	lun 18/01/16		
Reunión de Planificación	1,5 horas	lun 04/01/16	lun 04/01/16	Oficial de Seguridad	
7.3 Gestión de privilegios	8 horas	lun 04/01/16	mar 05/01/16	Área Tecnológica	
SCRUM diario	15 mins	mar 05/01/16	mar 05/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 06/01/16	mié 06/01/16	Oficial de Seguridad	
7.5 Revisión de los derechos de accesos de los usuarios	8 horas	mié 06/01/16	jue 07/01/16	Área Tecnológica	
SCRUM diario	15 mins	jue 07/01/16	jue 07/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 08/01/16	vie 08/01/16	Oficial de Seguridad	
7.10 Autenticación de usuarios para conexiones externas	12 horas	vie 08/01/16	mar 12/01/16	Área Tecnológica	
Revisión de Sprint	2 horas	lun 11/01/16	lun 11/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	mar 12/01/16	mar 12/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 13/01/16	mié 13/01/16	Oficial de Seguridad	
7.14 Control de conexión a las redes	12 horas	mié 13/01/16	vie 15/01/16	Área Tecnológica	
SCRUM diario	15 mins	jue 14/01/16	jue 14/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 15/01/1	vie 15/01/1	Oficial de Seguridad	

		6	6		
Retrospectiva del Sprint	1,5 horas	lun 18/01/16	lun 18/01/16	Oficial de Seguridad	
Sprint 10	11 días	lun 18/01/16	lun 01/02/16		
Reunión de Planificación	1,5 horas	lun 18/01/16	lun 18/01/16	Oficial de Seguridad	
7.11 Identificación de los equipos en las redes	18 horas	lun 18/01/16	vie 22/01/16	Área Tecnológica	
SCRUM diario	15 mins	mar 19/01/16	mar 19/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 20/01/16	mié 20/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 21/01/16	jue 21/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 22/01/16	vie 22/01/16	Oficial de Seguridad	
Revisión de Sprint	2 horas	lun 25/01/16	lun 25/01/16	Oficial de Seguridad	
7.15 Control del enrutamiento en la red	12 horas	lun 25/01/16	mié 27/01/16	Área Tecnológica	
SCRUM diario	15 mins	mar 26/01/16	mar 26/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 27/01/16	mié 27/01/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 28/01/16	jue 28/01/16	Oficial de Seguridad	
7.16 Procedimiento de registro de inicio seguro	10 horas	jue 28/01/16	lun 01/02/16	Área Tecnológica	
SCRUM diario	15 mins	vie 29/01/16	vie 29/01/16	Oficial de Seguridad	

Retrospectiva del Sprint	1,5 horas	lun 01/02/16	lun 01/02/16	Oficial de Seguridad	
Sprint 11	11 días	lun 01/02/16	lun 15/02/16		
Reunión de Planificación	1,5 horas	lun 01/02/16	lun 01/02/16	Oficial de Seguridad	
7.12 Protección de los puertos de configuración y diagnóstico remoto	20 horas	lun 01/02/16	vie 05/02/16	Área Tecnológica	
SCRUM diario	15 mins	mar 02/02/16	mar 02/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 03/02/16	mié 03/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 04/02/16	jue 04/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 05/02/16	vie 05/02/16	Oficial de Seguridad	
Revisión de Sprint	2 horas	lun 08/02/16	lun 08/02/16	Oficial de Seguridad	
7.18 Sistema de gestión de contraseñas	10 horas	lun 08/02/16	mié 10/02/16	Área Tecnológica	
SCRUM diario	15 mins	mar 09/02/16	mar 09/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 10/02/16	mié 10/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 11/02/16	jue 11/02/16	Oficial de Seguridad	
7.19 Uso de las utilidades del sistema	10 horas	jue 11/02/16	lun 15/02/16	Área Tecnológica	
SCRUM diario	15 mins	vie 12/02/16	vie 12/02/16	Oficial de Seguridad	

Retrospectiva del Sprint	1,5 horas	lun 15/02/16	lun 15/02/16	Oficial de Seguridad	
Sprint 12	11 días	lun 15/02/16	lun 29/02/16		
Reunión de Planificación	1,5 horas	lun 15/02/16	lun 15/02/16	Oficial de Seguridad	
7.13 Separación en las redes	25 horas	lun 15/02/16	mar 23/02/16	Área Tecnológica	
SCRUM diario	15 mins	mar 16/02/16	mar 16/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 17/02/16	mié 17/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 18/02/16	jue 18/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 19/02/16	vie 19/02/16	Oficial de Seguridad	
Revisión de Sprint	2 horas	lun 22/02/16	lun 22/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	mar 23/02/16	mar 23/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 24/02/16	mié 24/02/16	Oficial de Seguridad	
7.24 Aislamiento de sistemas sensibles	15 horas	mié 24/02/16	lun 29/02/16	Área Tecnológica	
SCRUM diario	15 mins	jue 25/02/16	jue 25/02/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 26/02/16	vie 26/02/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 29/02/16	lun 29/02/16	Oficial de Seguridad	
Sprint 13	11	lun	lun		

	días	29/02/16	14/03/16		
Reunión de Planificación	1,5 horas	lun 29/02/16	lun 29/02/16	Oficial de Seguridad	
7.25 Computación y comunicaciones móviles	10 horas	lun 29/02/16	mié 02/03/16	Área Tecnológica	
SCRUM diario	15 mins	mar 01/03/16	mar 01/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 02/03/16	mié 02/03/16	Oficial de Seguridad	
7.26 Trabajo remoto	10 horas	mié 02/03/16	vie 04/03/16	Área Tecnológica	
SCRUM diario	15 mins	jue 03/03/16	jue 03/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 04/03/16	vie 04/03/16	Oficial de Seguridad	
Revisión de Sprint	2 horas	lun 07/03/16	lun 07/03/16	Oficial de Seguridad	
8.3 Control de procesamiento interno	15 horas	lun 07/03/16	jue 10/03/16	Área Tecnológica	
SCRUM diario	15 mins	mar 08/03/16	mar 08/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 09/03/16	mié 09/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 10/03/16	jue 10/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 11/03/16	vie 11/03/16	Oficial de Seguridad	
8.4 Integridad del mensaje	5 horas	vie 11/03/16	lun 14/03/16	Área Tecnológica	
Retrospectiva del Sprint	1,5 horas	lun 14/03/1	lun 14/03/1	Oficial de Seguridad	

		6	6		
Sprint 14	11 días	lun 14/03/16	lun 28/03/16		
Reunión de Planificación	1,5 horas	lun 14/03/16	lun 14/03/16	Oficial de Seguridad	
7.17 Identificación y autenticación de usuarios	8 horas	lun 14/03/16	mar 15/03/16	Área Tecnológica	
SCRUM diario	15 mins	mar 15/03/16	mar 15/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 16/03/16	mié 16/03/16	Oficial de Seguridad	
7.20 Tiempo de inactividad de la sesión	8 horas	mié 16/03/16	jue 17/03/16	Área Tecnológica	
SCRUM diario	15 mins	jue 17/03/16	jue 17/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 18/03/16	vie 18/03/16	Oficial de Seguridad	
7.22 Control de accesos a las aplicaciones y a la información	8 horas	vie 18/03/16	lun 21/03/16	Área Tecnológica	
Revisión de Sprint	2 horas	lun 21/03/16	lun 21/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	mar 22/03/16	mar 22/03/16	Oficial de Seguridad	
7.23 Restricciones de acceso a la información	8 horas	mar 22/03/16	mié 23/03/16	Área Tecnológica	
SCRUM diario	15 mins	mié 23/03/16	mié 23/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 24/03/16	jue 24/03/16	Oficial de Seguridad	
8.12 Revisión técnica de las	8 horas	jue 24/03/1	vie 25/03/1	Área Tecnológica	

aplicaciones después de los cambios en el sistema operativo		6	6		
SCRUM diario	15 mins	vie 25/03/16	vie 25/03/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 28/03/16	lun 28/03/16	Oficial de Seguridad	
Sprint 15	11 días	lun 28/03/16	lun 11/04/16		
Reunión de Planificación	1,5 horas	lun 28/03/16	lun 28/03/16	Oficial de Seguridad	
8.13 Restricción del cambio de paquetes de software	10 horas	lun 28/03/16	mié 30/03/16	Área Tecnológica	
SCRUM diario	15 mins	mar 29/03/16	mar 29/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 30/03/16	mié 30/03/16	Oficial de Seguridad	
8.14 Fuga de información	10 horas	mié 30/03/16	vie 01/04/16	Área Tecnológica	
SCRUM diario	15 mins	jue 31/03/16	jue 31/03/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 01/04/16	vie 01/04/16	Oficial de Seguridad	
Revisión de Sprint	2 horas	lun 04/04/16	lun 04/04/16	Oficial de Seguridad	
8.15 Desarrollo de software contratado externamente	5 horas	lun 04/04/16	mar 05/04/16	Área Tecnológica	
SCRUM diario	15 mins	mar 05/04/16	mar 05/04/16	Oficial de Seguridad	
8.16 Control de las vulnerabilidades técnicas	15 horas	mar 05/04/16	vie 08/04/16	Área Tecnológica	
SCRUM diario	15	mié	mié	Oficial de	

	mins	06/04/16	06/04/16	Seguridad	
SCRUM diario	15 mins	jue 07/04/16	jue 07/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 08/04/16	vie 08/04/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 11/04/16	lun 11/04/16	Oficial de Seguridad	
Sprint 16	11 días	lun 11/04/16	lun 25/04/16		
Reunión de Planificación	1,5 horas	lun 11/04/16	lun 11/04/16	Oficial de Seguridad	
8.1 Análisis y especificaciones de los requerimientos de seguridad	4 horas	lun 11/04/16	lun 11/04/16	Área Tecnológica	
SCRUM diario	15 mins	mar 12/04/16	mar 12/04/16	Oficial de Seguridad	
8.9 Protección de los datos de prueba del sistema	12 horas	mar 12/04/16	jue 14/04/16	Área Tecnológica	
SCRUM diario	15 mins	mié 13/04/16	mié 13/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 14/04/16	jue 14/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 15/04/16	vie 15/04/16	Oficial de Seguridad	
8.10 Control de acceso al código fuente de los programas	12 horas	vie 15/04/16	mar 19/04/16	Área Tecnológica	
Revisión de Sprint	2 horas	lun 18/04/16	lun 18/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	mar 19/04/16	mar 19/04/16	Oficial de Seguridad	
SCRUM diario	15	mié	mié	Oficial de	

	mins	20/04/16	20/04/16	Seguridad	
8.11 Procedimiento de control de cambios	12 horas	mié 20/04/16	vie 22/04/16	Área Tecnológica	
SCRUM diario	15 mins	jue 21/04/16	jue 21/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 22/04/16	vie 22/04/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 25/04/16	lun 25/04/16	Oficial de Seguridad	
Sprint 17	11 días	lun 25/04/16	lun 09/05/16		
Reunión de Planificación	1,5 horas	lun 25/04/16	lun 25/04/16	Oficial de Seguridad	
8.2 Validación de datos de entrada	10 horas	lun 25/04/16	mié 27/04/16	Área Tecnológica	
SCRUM diario	15 mins	mar 26/04/16	mar 26/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 27/04/16	mié 27/04/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 28/04/16	jue 28/04/16	Oficial de Seguridad	
8.5 Validación de datos de salidas	5 horas	jue 28/04/16	vie 29/04/16	Área Tecnológica	
SCRUM diario	15 mins	vie 29/04/16	vie 29/04/16	Oficial de Seguridad	
Revisión de Sprint	2 horas	lun 02/05/16	lun 02/05/16	Oficial de Seguridad	
8.7 Gestión de claves	15 horas	lun 02/05/16	jue 05/05/16	Área Tecnológica	
SCRUM diario	15 mins	mar 03/05/1	mar 03/05/1	Oficial de Seguridad	

		6	6		
SCRUM diario	15 mins	mié 04/05/16	mié 04/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 05/05/16	jue 05/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 06/05/16	vie 06/05/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 09/05/16	lun 09/05/16	Oficial de Seguridad	
Sprint 18	11 días	lun 09/05/16	lun 23/05/16		
Reunión de Planificación	1,5 horas	lun 09/05/16	lun 09/05/16	Oficial de Seguridad	
8.6 Política sobre el uso de controles criptográficos	12 horas	lun 09/05/16	mié 11/05/16	Área Tecnológica	
10.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	8 horas	lun 09/05/16	mar 10/05/16	Viceministro	
SCRUM diario	15 mins	mar 10/05/16	mar 10/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 11/05/16	mié 11/05/16	Oficial de Seguridad	
10.2 Continuidad del negocio y evaluación de riesgos	10 horas	mié 11/05/16	vie 13/05/16	Viceministro	
SCRUM diario	15 mins	jue 12/05/16	jue 12/05/16	Oficial de Seguridad	
8.8 Control de software operativo	12 horas	jue 12/05/16	lun 16/05/16	Área Tecnológica	
SCRUM diario	15 mins	vie 13/05/16	vie 13/05/16	Oficial de Seguridad	
Revisión de Sprint	2	lun	lun	Oficial de	

	horas	16/05/16	16/05/16	Seguridad	
10.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	10 horas	lun 16/05/16	mié 18/05/16	Viceministro	
SCRUM diario	15 mins	mar 17/05/16	mar 17/05/16	Oficial de Seguridad	
9.2 Reporte sobre las debilidades en la seguridad	8 horas	mar 17/05/16	mié 18/05/16	Área Tecnológica	
SCRUM diario	15 mins	mié 18/05/16	mié 18/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	jue 19/05/16	jue 19/05/16	Oficial de Seguridad	
9.5 Recolección de evidencias	8 horas	jue 19/05/16	vie 20/05/16	Área Tecnológica	
SCRUM diario	15 mins	vie 20/05/16	vie 20/05/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 23/05/16	lun 23/05/16	Oficial de Seguridad	
Sprint 19	11 días	lun 23/05/16	lun 06/06/16		
Reunión de Planificación	1,5 horas	lun 23/05/16	lun 23/05/16	Oficial de Seguridad	
9.1 Reporte sobre los eventos de seguridad de la información	6 horas	lun 23/05/16	mar 24/05/16	Área Tecnológica	
10.4 Estructura para la planificación de la continuidad del negocio	12 horas	lun 23/05/16	mié 25/05/16	Viceministro	
SCRUM diario	15 mins	mar 24/05/16	mar 24/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 25/05/16	mié 25/05/16	Oficial de Seguridad	

SCRUM diario	15 mins	jue 26/05/16	jue 26/05/16	Oficial de Seguridad	
9.3 Responsabilidades y procedimientos	15 horas	jue 26/05/16	mar 31/05/16	Área Tecnológica	
SCRUM diario	15 mins	vie 27/05/16	vie 27/05/16	Oficial de Seguridad	
10.5 Pruebas, mantenimiento y revisión de los planes de continuidad del negocio.	11 horas	vie 27/05/16	mar 31/05/16	Viceministro	
Revisión de Sprint	2 horas	lun 30/05/16	lun 30/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	mar 31/05/16	mar 31/05/16	Oficial de Seguridad	
SCRUM diario	15 mins	mié 01/06/16	mié 01/06/16	Oficial de Seguridad	
9.4 Aprendizaje debido a los incidentes de seguridad de la información	15 horas	mié 01/06/16	lun 06/06/16	Área Tecnológica	
SCRUM diario	15 mins	jue 02/06/16	jue 02/06/16	Oficial de Seguridad	
SCRUM diario	15 mins	vie 03/06/16	vie 03/06/16	Oficial de Seguridad	
Retrospectiva del Sprint	1,5 horas	lun 06/06/16	lun 06/06/16	Oficial de Seguridad	

BIBLIOGRAFÍA

[1] Castillo Peñaherrera Cristhian, Esquema Gubernamental de Seguridad de la Información, http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf, fecha de consulta abril 2015.

[2] Meucci Mateo, Guía de Pruebas OWASP, https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf, fecha de consulta abril 2015.

[3] Schwaber Ken y Sutherland Jeff, La Guía de SCRUM, http://www.scrumguides.org/docs/scrumguide/v1/Scrum-Guide-ES.pdf, fecha de consulta abril 2015.

[4] SNAP, RANKING DE ENTIDADES PÚBLICAS DEL CUMPLIMIENTO DE LA IMPLEMENTACIÓN DEL EGSI, fecha de consulta abril 2015.

[5] MREMH, Organigrama Cancillería, http://www.cancilleria.gob.ec/wp-content/uploads/2012/10/organigrama-cancilleria-octubre-2013.jpg, fecha de consulta abril 2015.

[6] MTOP, Organigrama Ministerio de Transporte y Obras Públicas,

http://www.obraspublicas.gob.ec/wp-content/uploads/2012/10/2012organigrama_ministerio_transporte_obras_publicas.png, fecha de consulta abril 2015.

[7] SENAGUA, Organigrama Secretaría Nacional del Agua, http://www.agua.gob.ec/wp-content/uploads/2012/10/organigrama.jpg, fecha de consulta abril 2015.