Universidad de Buenos Aires
Facultad de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Migración a Plataformas Abiertas - Software Libre
Una propuesta de la gestión de la seguridad de la información en un proyecto de migración a plataformas abiertas - Software Libre.

Autor:
Francisco Silva G.
Director:
Pablo Silberfich

2017
Cohorte 2014

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente (v. 8.7.4) y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firmado.

Ing. Francisco Silva Garcés.

DNI: 95.297.439

Licencia

Resumen

El Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (COESCCI) emitido en diciembre de 2016 por el Gobierno ecuatoriano establece que las instituciones públicas deben diseñar e implementar Planes de Migración a Tecnologías Libres, en sus sistemas y equipamientos informático. En ausencia de un plan para la ejecución de dicho mandato, este trabajo propone establecer un modelo de gestión de procesos de migración a tecnologías libres con una mirada sistémica y tomando de base marcos de referencias y las mejores prácticas establecidas en las normas internacionales de seguridad de la información basadas en el análisis de riesgos, con lo cual se propone estructurar dicho modelo.

Se toma como caso, la migración de escritorios de usuario a tecnologías libres en la que se presenta una serie de consideraciones y acciones a tener en cuenta desde el aspecto técnico y de gestión en la migración, con base a las normas técnicas para la gestión de la seguridad de la información.

Tabla de Contenido

1 Introducción

1.1 Antecedentes

El Gobierno Ecuatoriano, mediante el decreto ejecutivo 1014 publicado en el Registro Oficial 322 del 23 de abril del 2008, estableció como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos.

Posteriormente, mediante Acuerdo Ministerial 166, publicado en el Registro Oficial Suplemento 88 de 25 de septiembre del 2013, la entonces Secretaría Nacional de la Administración Pública expidió el Esquema Gubernamental de Seguridad de la Información (EGSI), en el que dispone a las instituciones de la Administración Pública Central, Institucional y que dependan de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información", las cuales están basadas en las normas internacionales ISO/IEC 27002.

Mediante Acuerdo Ministerial 1063, publicado en el Registro Oficial Suplementario 312 de 28 de abril de 2015, la Secretaría Nacional de la Administración Pública expidió el Plan de Nacional de Gobierno Electrónico, que incluye entre sus principios al de "adecuación tecnológica", por lo cual se garantiza que las administraciones elegirán *"las tecnologías más adecuadas para satisfacer sus necesidades, por lo que se recomienda el uso de estándares abiertos y de software libre en razón de la seguridad, sostenibilidad a largo plazo y la socialización del conocimiento."[1]*

El Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (COESCCI), publicado en Registro Oficial Suplemento No. 899, del viernes 9 de diciembre del 2016, tiene como alcance de implementación a todas las instituciones del sector público, quienes deberán presentar planes de migración a software libre como indica su transitoria décimo tercera.

En consecuencia de la emisión del COESCCI, el decreto 1014 es derogado con Decreto 1425 del 22 de mayo del 2017, el cual además regula la adquisición de software por parte de las entidades contratantes del sector público, en relación al artículo 148 del COESCCI que determina una prelación en la adquisición del software. [2]

A la fecha, las normativas y políticas emitidas no han presentado indicadores ni resultados concretos, lo cual denotan la carencia de un proceso de planificación y de gobernanza para reducirse a un aspecto exclusivamente tecnológico, operativo desligado además de una gestión de la seguridad de la información.

Estado actual

Los procesos de migración a tecnologías libres, desde la publicación del Decreto 1014, han sido impulsados independientemente en ausencia de una gestión centralizada, controlada y alineada a los objetivos nacionales, sobre los cuales se estructure un análisis de riesgos con orientación a los principios de seguridad de la información.

El extinto Ministerio Coordinador de Conocimiento y Talento Humano (MCCTH), inició en el 2016 un proceso de Migración a Software Libre en el sector Conocimiento, el cual coordinaba. Este proceso involucró a 17 instituciones, las cuales tomaron como modelo la implementación realizada en el MCCTH que implica un proceso planificado, considerando el factor humano como eje central del mismo.

Este proceso, por su naturaleza y organización, puede tomarse como base para el presente trabajo para construir un modelo que sirva de guía para todo el Estado alineándolo al Esquema Gubernamental de Seguridad de la Información (EGSI) con una base de análisis de Riesgos.

1.2 Planteo del problema

La falta de un proceso sistémico en los proyectos de migración a tecnologías libres, tal como los sistemas de gestión de seguridad de la información; la ausencia de enfoques en los cuales se considere como fin último el bienestar del ser humano y el cumplimiento de los objetivos nacionales, son problemáticas que de alguna manera pueden encontrarse para construir una propuesta integrada con base a los principios de seguridad de la información y la gestión del riesgo.

Los objetivos de la seguridad de la información, de preservar la integridad, confidencialidad, y disponibilidad ceñidos al cumplimiento normativo ponen de manifiesto carencias de una visión sistémica, al dejar a un lado el componente humano, su desarrollo y su participación dentro de los procesos al tratarse de entidades del sector público. La confidencialidad como uno de los objetivos de seguridad, debe quedar sujeta a consideración del contexto y naturaleza de las entidades públicas, por lo cual deben guardar un equilibrio con principios de transparencia y participación.

En este sentido, la necesidad de establecer un modelo integral para la implementación y mejora continua de un proceso de migración a tecnologías libres en el Estado, se hace latente. La visión sistémica de un marco de trabajo para el Gobierno y la Gestión de Seguridad de la Información podría aportar sustancialmente, complementada con el análisis del riesgo.

1.3 Alcances y limitaciones

Para este trabajo se tendrá como referencia a instituciones públicas del Ecuador, que podría considerarse como modelo. Se tomarán supuestos como elemento de análisis en los procesos involucrados en la migración a tecnologías libre, teniendo como base la experiencia previa del extinto Ministerio Coordinador de Conocimiento y Talento Humano.

Los procesos de migración a tecnologías libres pueden ser muy amplios, por lo cual se tomará para este trabajo exclusivamente los procesos relacionados a la migra-

ción a tecnologías libres de escritorios de usuarios, incluyendo la ofimática, y la infraestructura tecnológica para la gestión centralizada de los mismos.

La metodología definirá una estrategia de acción idónea para el plan de migración, considerando controles de seguridad definidos en el EGSI alineados al proceso de migración y orientados hacia la seguridad informática.

1.4 Objetivos

1.4.1 Generales

Desarrollar un modelo sistémico de gestión de un proyecto de migración a tecnologías libres en entidades del sector público con base a los principios, fundamentos y normas internacionales para la gestión de seguridad de la información y la gestión del riesgo.

1.4.2 Específicos

- Identificar los procesos esenciales en la migración a tecnologías libres de escritorios, su problemática y los riesgos involucrados considerando las normativas y objetivos nacionales.
- Determinar los controles de seguridad aplicables en el proceso de migración a tecnologías libres de escritorios.
- Definir métricas e indicadores que permitan el seguimiento y un proceso de mejora continua de un plan de migración.

1.5 Hipótesis del trabajo

El enfoque de integralidad de la Seguridad del Estado Ecuatoriano, complementada con la coordinación de instituciones públicas y la sociedad civil bajo el principio de eficiencia en el uso de los recursos, supone la anticipación y mitigación de los riesgos y amenazas como parte del proceso de gestión de las políticas públicas. A tal efecto, un modelo de gestión para un proyecto de migración a tecnologías libres con enfoque de gestión de la seguridad informática podría contemplar estos criterios, para garantizar su eficacia y la eficiencia en términos técnicos, económicos y sociales.

1.6 Estructura del trabajo

El presente trabajo parte del contexto ecuatoriano en relación a la normativa acerca del uso de tecnologías libres en el estado, y el marco teórico que hace referencia al marco de trabajo COBIT 5 para la seguridad de la información. Además se consideran las normas internacionales para la gestión del riesgo que fueron analizadas con base a los supuestos que se proponen. El marco teórico finaliza con elementos importantes no tecnológicos para ser considerados en el gobierno de la seguridad para el contexto ecuatoriano en el sector público; de esta manera se propone la base conceptual de este trabajo.

En los capítulos 3 y 4, se formula un Sistema de Gestión de Seguridad de la Información para los proyectos de migración a tecnologías libres definiendo los alcances, límites y el enfoque de evaluación del riesgo. Posteriormente se procede con la identificación, análisis y evaluación de los riesgos para un proyecto de migración a tecnologías libres. El capítulo 4 finaliza proponiendo controles necesarios para el tratamiento de los riesgos del proyecto desde la perspectiva de alto y bajo nivel, es decir, desde el punto de vista de estado e institucional, a los elementos tecnológicos. A continuación se indican cuáles riesgos son aceptables y un protocolo de excepciones que se debe aplicar para casos que pueden quedar excluidos del proceso de migración.

En el capítulo 5, con base a los capítulos anteriores, se procede a proponer un modelo de gestión para proyectos de migración de escritorios de usuarios a tecnologías libres tomando como modelo el marco de trabajo COBIT 5. Para esto se definen los procesos, sus entradas, salidas y sus actividades tomando en cuenta los análisis y controles establecidos en el capítulo 3 y 4.

Finalmente, el modelo de gestión propuesto también tendrá su componente de gestión de riesgos que serán tomados en cuenta, además de las métricas e indicadores para la evaluación y seguimiento del proyecto.

2 Marco Teórico

2.1 COBIT 5 para Seguridad de la Información

Este marco de trabajo provee elementos que permite a las organizaciones alcanzar sus objetivos, y entregar valor a través de una efectiva gobernanza y gestión de las tecnologías de la información.

En la propuesta del modelo de gestión para la migración a tecnologías libres, se utilizará como guía este marco de referencia que se basa en 5 principios de suma relevancia para la Seguridad de la Información, cuya documentación describe como sigue: [3]

1. Satisfacer las necesidades de las partes interesadas. Que se refiere a lograr un equilibrio entre: a) la realización de los beneficios, b) optimización de riesgos, c) optimización de recursos, que además deberán concretarse en metas considerando las metas corporativas, las relacionadas con Tecnologías de la Información (TI), y las de los habilitadores.

2. Cubrir la organización de extremo a extremo. Es decir, no sólo las funciones de TI, sino todas las funciones y procesos que forman parte de la organización. Considerar entonces que todos los habilitadores relacionados con el gobierno y gestión de TI abarquen a toda la organización, incluyendo a todo y a todos, tanto internos como externos relevantes para el gobierno y gestión de la información.

3. Aplicar un marco de referencia único integrado. Que sirva como fuente consistente e integrada de consulta. Una guía en un lenguaje común no técnico y agnóstico a las tecnologías. En este sentido este marco de referencia (Cobit 5) se alinea con estándares y marcos de referencias relevantes.

4. Hacer posible el Enfoque Holístico. En COBIT 5, los habilitadores se dirigen por cascada de metas, por lo tanto las metas de nivel alto de las TI definen lo que los diferentes habilitadores deberían lograr.

5. Separar el Gobierno de la Gestión. Las responsabilidades o funciones se distinguen entre Gobierno y Gestión, como indica la documentación de Cobit 5:

> "*El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.*" [3]
>
> "*La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.*"[3]

En las organizaciones el Gobierno suele ser responsabilidad del consejo de administración o cualquier instancia superior similar, bajo la dirección de una autoridad como por ejemplo su presidente. En cambio la Gestión suele ser responsabilidad de la dirección ejecutiva bajo la dirección del Director General Ejecutivo (Gerente o CEO). Estos roles (gobierno y gestión) pueden identificarse en el modelo de procesos de Cobit 5, como se ilustra a continuación:

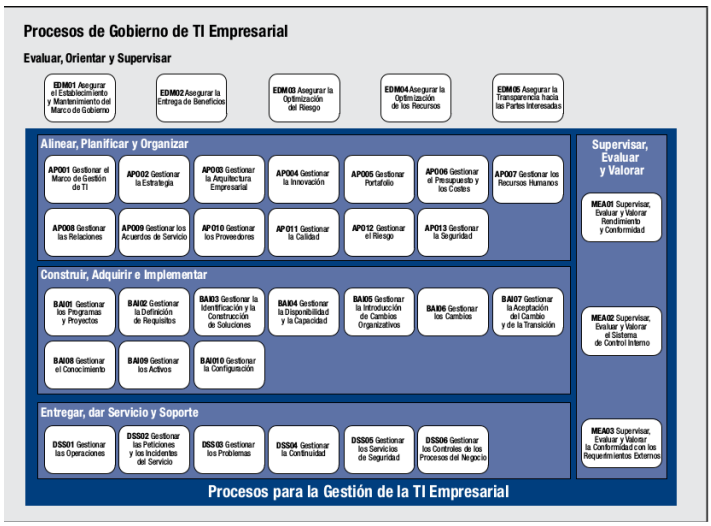

Figura 1: Modelo de Referencia de Procesos de COBIT 5[3]

Los habilitadores que propone COBIT 5, aplicables a la Seguridad de la Información pueden también adaptarse o aplicare a la gestión de la migración a tecnologías libre.

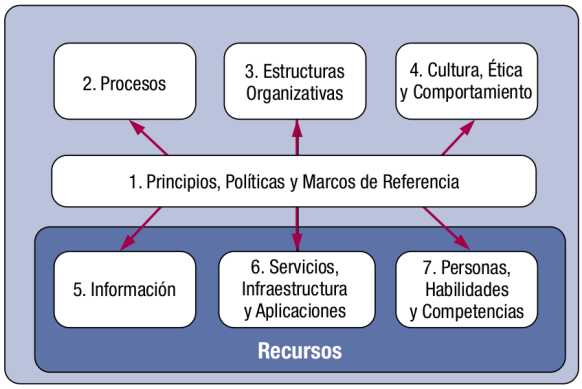

Figura 2: Habilitadores corporativos de COBIT 5[3]

Habilitadores COBIT 5 adaptados para la gobernanza y gestión de migraciones a tecnologías libres.

1. Principios, Políticas y Marcos de Referencia:

Algunas partes interesadas, en el marco del Gobierno Corporativo, definen y establecen las políticas mientras que otras deben alinearse y cumplirlas. La documentación indica que los principios son limitados en números y se deben expresar en un lenguaje claro, sencillo, mientras que las políticas, que tienen un ciclo de vida, expresan una directriz más detallada acerca de cómo se debe llevar a la práctica los principios, es decir, que influyen en cómo se alinean a ellos la toma de decisiones.

La estructura de cómo se puede crear y mantener un conjunto de políticas, está dado por el marco de referencia, el cual además proporciona el ámbito en el que se puede mover dentro o entre ellas. Según las buenas prácticas, el marco de políticas debe definir al menos: [3]

- Las personas que aprueban las políticas de la organización
- Las consecuencias de no cumplir con las políticas
- Los mecanismos para la gestión de las excepciones

- La forma en la que se comprobará y medirá el cumplimiento con la política

Se sugiere adaptar las políticas al entorno de la organización, es decir, principios, objetivos, estrategias, apetito al riesgo, uso responsable de las tecnologías y además considerar factores tales como:

- Regulaciones exclusivas de la organización.
- Requisitos operativos y funcionales del negocio.
- Necesidades de propiedad intelectual y protección de datos sensibles.
- Políticas existentes de alto nivel y la cultura organizacional.
- Diseños únicos de arquitectura TI de la organización.
- Regulaciones gubernamentales.
- Estándares de la industria.

El ciclo de vida de las políticas, implica en su gestión la revisión periódica de las mismas, según los contextos internos o externos en el marco del gobierno.

2. Los Procesos.- incluyen detalles y actividades específicas de la migración a tecnologías libres:

COBIT 5 define a los procesos como *"una colección de prácticas influidas por las políticas y procedimientos de empresa que toma entradas de varias fuentes (incluyendo otros procesos), manipula las entradas y produce salidas (productos, servicios, etc)"[3]*

Los procesos tienen partes interesadas internas y externas, ciclo de vida, y buenas prácticas internas y externas. Estos además, se distinguen entre procesos de gobierno y de gestión.

Los procesos de gobierno se encargan de los objetivos de gobierno de las partes interesadas (proporcionar valor, optimizar riesgos y recursos). Los procesos de gestión involucran prácticas y actividades relacionadas a planificar, construir, ejecutar y supervisar.

3. Las estructuras organizativas.- específicas de la migración a tecnologías libres:

Son los elementos claves en la toma de decisiones de una organización, que involucran: el modelo de estructura organizativas, los roles y estructuras, y responsabilidades.

4. Los factores determinantes de cultura, ética y comportamiento, para el éxito del gobierno y la gestión de la migración a tecnologías libres:

Uno de los factores de éxito en el gobierno y la gestión de la migración a tecnologías libres, es el comportamiento de los individuos y las organizaciones. Por lo cual se debe considerar:

- El modelo cultural: El comportamiento deseado, involucra a toda la organización, ya que los grupos de interés incluso trascienden a grupos externos. Por lo tanto cuando hay que influir en la cultura, deben tenerse en cuenta todos los grupos de interés, es decir, quienes se ocupan de la definición, ejecución, y hacer cumplir los comportamientos deseados; y quienes tienen que alinearse con las reglas y normas definidas.

- El ciclo de vida de la cultura: Las culturas organizativas, los comportamientos individuales, posturas éticas, tienen ciclos de vida. Los cambios necesarios pueden identificarse, y su evolución en el tiempo pueden medirse proporcionando métricas e indicadores para su evaluación.

  Entre las buenas prácticas recomendadas por COBIT para crear, fomentar y mantener un comportamiento podemos encontrar:

  - Comunicar a toda la organización sobre el comportamiento deseado y de los valores corporativos esenciales.
  - Dar a conocer la conducta deseada, por medio del ejemplo de autoridades.
  - Incentivos y recompensas para alentar, y medidas disuasorias para hacer cumplir las actitudes, normas y reglas.
  - Recurrir a líderes que influyan en el comportamiento.
  - Concienciación.

Es importante considerar los distintos factores que influyen el comportamiento, tales como: creencias, etnia, nivel socio económico, experiencias personales, ubicación geográfica, objetivos y ambiciones personales, relaciones interpersonales al interior de la organización. Los comportamientos de todos los miembros de la organización determinan de manera colectiva la cultura organizacional.

- Liderazgo de influyentes en el comportamiento: Los líderes o personas influyentes, son quienes están dispuestos a hablar y servir de ejemplo. Estos pueden ser altos directivos, sin embargo también puede considerarse a miembros del personal mientras sea positivo su aporte y participación activa al cambio y la aplicación de la cultura.

- El comportamiento deseable que debería ser fomentado: Estos podrían ser, entre otros: a) respeto a la importancia de las políticas y principios, b) participación activa en el cambio, c) asumir responsabilidad en el éxito del cambio, d) partes interesadas comprenden los beneficios del cambio y las amenazas que se mitigan, e) directivos colaboran continua y proactivamente con otras funciones en la consecución de los objetivos, f) las autoridades reconocen el valor social de la migración a tecnologías libres.

5. La información de una organización puede ser utilizada para gobernar y gestionar la migración a tecnologías libres:

La dirección puede utilizar la información como base para la toma de decisiones, para esto se analizan varios elementos:

- Modelo de información: Debe identificarse las partes interesadas externas e internas y sus áreas claves de responsabilidad. Los atributos de la información deben considerar desde su uso en el mundo físico (donde los atributos se enlazan con las tecnologías y los medios para capturar, almacenar, procesar, distribuir y presentar) hasta su uso en el mundo social para dar sentido a la información.

- Los Tipos comunes de información: que son habituales en el gobierno y la gestión, dan una idea de cómo el detalle de la migración a tecnologías se extiende en la organización, ejemplo: estrategia, plan, políticas, presupuestos, material de concienciación, informes, inventarios, etc. Es una buena práctica tener una descripción de cada tipo y una estructura modelo.
- Los grupos de interés de la información: Es esencial para optimizar el desarrollo y distribución a través de la organización. Puede estructurarse indicando: la descripción de la parte interesada, el tipo de información, la relación entre la parte interesada y cada tipo de información (Aprobador, Originador, Informado, Usuario).
- El ciclo de vida de la información: Debe ser considerado para asegurar la exactitud y uso óptimo de la información. Se pueden distinguir diferentes fases: Planificar/diseñar/construir/adquirir, Usar/operar, Supervisar, Eliminar.

6. Servicios, Infraestructura y Aplicaciones:

Proporcionan a la empresa información, procesado de la información y servicios, para lo cual se cuenta con los siguientes elementos:

- Modelo de servicios, infraestructura y aplicaciones: Las capacidades de servicio pueden tener partes interesadas externas o internas. Los servicios pueden ser prestados por entidades externas o internas, así mismo, los usuarios de dichos servicios pueden ser internos o externos. Implica además considerar qué servicios y niveles de servicios son más económicos para la organización.
- Los servicios, la infraestructura y las aplicaciones: Los servicios están relacionados a uno o más procesos de COBIT 5, a sus prácticas, actividades y requieren de entradas y salidas. Los servicios no sólo requieren de infraestructuras y aplicaciones, sino también de una combinación de otros habilitadores como procesos, información, estructura organizacional.

7. Personas, habilidades y competencias:

Este habilitador, requiere de los siguientes elementos:

- Modelo de habilidades y competencias: Diferentes partes interesadas pueden asumir diferentes roles en el proyecto de migración, y cada rol requiere un conjunto de habilidades. La organización debe conocer su línea base de habilidades actual y planificar de acuerdo con lo que debe ser. Las habilidades deben ser adquiridas (contratación), desarrolladas (formación) y desplegadas en los diversos roles en la estructura de la organización.
- Habilidades y competencias, relacionadas con la migración a tecnologías libres: Se deben definir los siguientes atributos: a) Definición de habilidades, b) Objetivos, c) Habilitadores relacionados. Una actividad de migración a tecnologías libres debe identificar su línea base de habilidades actual, y alinear esa línea base con el conjunto de habilidades requerido. Las certificaciones pueden ser un valor añadido a los atributos de habilidades y competencias.

2.2 Gestión del Riesgo.

La gestión de riesgos de origen tecnológico tiene como base los estándares ISO/IEC 31000, ISO/IEC 27005 de los cuales se tomaron definiciones y metodologías requeridas para este trabajo. Además se adoptaron e incorporaron en esta propuesta consideraciones o buenas prácticas de la guía para gestión de riesgos NIST SP 800-39.

La NIST en su Norma SP-800-53rv4 (Security and Privacy Controls for Federal Information Systems and Organizations) resalta que *"la selección e implementación de controles de seguridad para sistemas de información y las organizaciones son tareas que pueden tener importantes implicaciones en las operaciones y activos de las organizaciones, así como el bienestar de las personas y del País."[4]*

El daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones; pérdidas financieras, multas o acciones legales; afectación de la imagen de una organización, institución o incluso de un Estado, y además puede causar inconvenientes a nivel operativo, estratégico o afectación a la seguridad de un País.

En general las metodologías consideran importante establecer cuáles son los activos críticos para asociarlos a los procesos respectivos y de allí generar el listado de procesos críticos, que permitan además la identificación de dependencias claves, activos y procesos críticos, amenazas existentes y futuras.

Otro factor importante son los activos de soporte a los procesos analizados. Es decir, se analiza hardware, software, recursos humanos y físicos, con la finalidad de focalizar el estudio sobre los recursos críticos sin extenderse a activos irrelevantes.

Evaluación de Alto Nivel del Riesgo.

Uno de los enfoques que sugiere la norma ISO/IEC 27005[5] de evaluación del Riesgo, tiene como objetivo empezar con una evaluación de alto nivel de las consecuencias en lugar de empezar con un análisis sistémico de amenazas, vulnerabilidades, activos. De este modo se puede abordar una visión más global de la organización, y un análisis de contexto más enfocado en el negocio y el ambiente operativo que en los elementos tecnológicos.

La Norma NIST-SP-800-39 *"Managing information security risk: organization, mission, and information system view"* propone un modelo de gestión del riesgo multi-capa que integra al proceso tres niveles: a) el nivel de organización, b) el nivel de proceso de misión/negocio y c) el nivel de sistema de información. [6]

En el modelo propuesto por este trabajo tomaremos este concepto como base, considerando al Estado como nivel de "organización". Este enfoque implica necesariamente distintos actores involucrados, tanto institucionales como inter-institucionales con intereses comunes de misión y visión, para el cumplimiento de las políticas públicas transversales, que están expresadas en el Plan Nacional de Desarrollo 2017-2021 en tres ejes y 9 objetivos. [7]

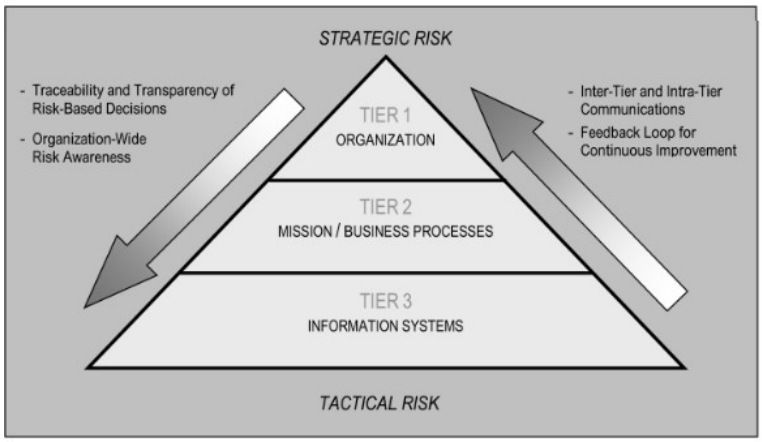

Figura 3: Gestión del Riesgo multi-capa[1]

En relación a la primera capa, a la que llamaremos Estado, podemos encontrar en el anexo A, las normativas y políticas públicas relacionadas que son parte de la gobernabilidad de los proyectos de migración a tecnologías libres. Esta capa proporcionará priorización en cuanto a las decisiones relacionadas a estrategias de financiamiento, y selección de tecnologías consistentes con las metas y objetivos estratégicos y de eficiencia a nivel de Estado que se encuentran en el Plan Nacional de Desarrollo.

La capa nivel 2, estará relacionada a las decisiones que soportarán la misión y los procesos de negocios institucionales. Los procesos de gestión de la seguridad inmersos en las migraciones a tecnologías libres estarán enfocados hacia el cumplimiento de los objetivos institucionales. Estos dos primeros niveles son de interés para la máxima autoridad quien dará aprobación para el inicio del proyecto.

La tercera capa o nivel basará sus decisiones y acciones en función de los dos niveles anteriores, y servirá de insumo para un marco de referencia en la gestión del riesgo institucional.

La identificación del riesgo de alto nivel, será de utilidad como recurso para la presentación del proyecto a la máxima autoridad, ya que este enfoque puede aportar

[1] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

a una lista más limitada de vulnerabilidades y amenazas agrupadas en dominios definidos. Es decir, puede enfocarse en riesgos o escenarios de ataques en lugar de sus elementos, de esta manera las actividades de tratamiento del riesgo intentarán primero proponer y seleccionar controles comunes que sean válidos a través de todo el sistema de gestión.

Ante la situación planteada, en un proyecto específico de migración del software de escritorio a tecnologías libres, es necesario acotar los elementos del análisis de riesgo a los escenarios específico. El enfoque de análisis de alto nivel, mediante tablas sin llegar a ser muy precisas o profundizar en detalles, podrán facilitar la identificación de la importancia relativa no sólo de los activos de información sometidos a las amenazas, sino también de los controles entre las distintas opciones para mitigar los riesgos de análisis.

Tomando como referencia las guías mencionadas, los activos de interés se pueden categorizar, en activos intangibles y tangibles, o activos de valor y activos de soporte.

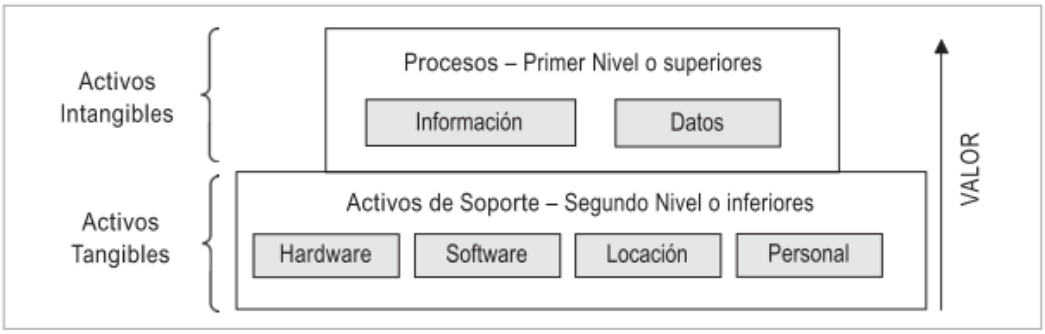

Figura 4: Tipos de Activos[2]

Según la norma ISO/IEC 27005, el plan de comunicación se debe realizar a nivel interno (áreas de la organización, empleados, directivos, socios) y externo (clientes, proveedores, entes reguladores), teniendo en cuenta las definiciones sobre la existen-

[2] A. Ramírez Castro y Z. Ortiz Bayona, «Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad del negocio», Ingeniería, vol. 16, n.o 2, pp. 56-66, 2011.

cia del riesgo, los objetivos de la gestión, el debido informe de los avances del proceso y todo aquello que se considere necesario.

2.3 OSSTMM 3: The Open Source Security Testing Methodology Manual

El Instituto para la Seguridad y Metodologías Abiertas (ISECOM), en enero del 2001 inició el lanzamiento de su Manual de Fuentes Abiertas sobre Metodologías de Pruebas de Seguridad (OSSTMM 3: The Open Source Security Testing Methodology Manual), en la que participaron muchos investigadores que contribuyeron desde distintos campos de estudio, con el objeto de proponer una metodología abierta que no estuviera ceñida a intereses comerciales o agendas geopolíticas.

La metodología se enfoca en darle sentido a la seguridad, de manera que sea aplicable a cualquier ámbito, gobierno, privado, incluso en lo personal, es decir, no sólo se enfoca en los hechos sino en su aplicabilidad al mundo real. Como metodología está diseñada para ser consistente y repetible, y como proyecto de código abierto, da la posibilidad de que cualquier evaluador de seguridad aporte ideas para realizar pruebas de seguridad más precisas, demandable y eficiente.

La Metodología OSSTMM puede abarcar pruebas a distintos canales: Humano, Físico, Inalámbrico, Telecomunicaciones y Redes de Datos, por lo cual lo hace idóneo para testear cloud computing, infraestructuras virtuales, middleware de mensajería, infraestructuras de comunicaciones móviles, localidades de alta seguridad, recursos humanos, informática de alta seguridad y cualquier proceso lógico que cubra múltiples canales y requiera un tipo diferente de pruebas de seguridad.[8]

El propósito esencial es proporcionar una metodología científica para la caracterización precisa de la seguridad operacional mediante la inspección y la correlación de los resultados de las pruebas de una manera coherente y confiable.

El propósito complementario es proveer una guía para asegurar que:

1. Las pruebas sean conducidas a fondo.
2. Las pruebas incluyeron todos los canales necesarios.

3. El punto de visa de las pruebas cumplen con normas legales.
4. Los resultados son medibles de manera cuantificable.
5. Los resultados son consistentes y repetibles.
6. Los resultados sólo contienen hechos derivados de las propias pruebas.

Separar o controlar

Esta metodología proporciona un concepto que será tomado en este trabajo, el cual se centra en una combinación de separación y control, es decir, para que una amenaza sea efectiva, ésta debe interactuar directa o indirectamente con el activo, por lo tanto, separar la amenaza del activo es evitar una posible interacción.

Bajo este criterio, es posible tener mayor seguridad si la amenaza y el activo están completamente separados entre sí, caso contrario, lo que tendríamos es un activo asegurado (safety) por medio de la provisión de controles sobre el activo, o el grado en que se reduzca el impacto de la amenaza.

En el caso de amenazas que no pueden separarse de los activos, la seguridad se deberá tratar de tal manera que las interacciones entre ambas (activo y amenaza) y los efectos de dichas interacciones causen poco o ningún daño.

Entonces, en este contexto la metodología denomina a la "seguridad" (security), como la separación entre un activo y una amenaza; y a "aseguramiento" o protección (safety) al control de una amenaza o sus efectos.

La propuesta metodológica no busca descartar el aseguramiento (safety) por la seguridad (security), sino que ambos conceptos pueden existir independientemente del riesgo y ser plenamente capaz de crear una "seguridad idónea", buscando el equilibrio exacto de "seguridad" (es decir, separación) y controles con operaciones y limitaciones. En este sentido, existen tres maneras lógicas y proactivas de crear esta separación:

1. Mover el activo para crear una barrera física o lógica entre este y la amenaza.
2. Cambiar la amenaza a un estado inofensivo.

3. Destruir la amenaza.

Estos conceptos serán tomados más adelante en este trabajo para el proceso de migración a tecnologías libres, como base para el análisis de riesgo, bajo la premisa de que controlando el entorno se puede controlar todo lo que habita en él.

2.4 Enfoque integral de la Seguridad.

Expandir el concepto de seguridad es una tendencia internacional, que la región ha tomado para sí, y como un caso particular puede mencionarse el enfoque de integralidad construido por Ecuador que llega a formar parte del tejido político estratégico construido desde su Constitución.

La integralidad del concepto de seguridad, plasmada en el documento "Seguridad Integral plan y agendas (2014-2017)", se ve reflejada en cinco ámbitos que se interconectan entre sí y enmarcan su accionar: Defensa y Relaciones Internacionales; Seguridad Ciudadana y Justicia; Gestión de Riesgos y Ambiente; Soberanía Tecnológica y Ciencia e; Inteligencia Estratégica para el fortalecimiento democrático. [9]

En cuanto al ámbito de Defensa y Relaciones Internacionales, uno de los temas centrales se refiere a la soberanía, como concepto que no se limita al ejercicio del poder de decisión sobre un territorio determinado, *"sino que se extiende a todos los campos en los que se desarrolla la vida, para cumplir el rol de protección de los derechos, libertades y garantías de los ciudadanos y ciudadanas."[9]*.

Es decir, que garantizar las soberanías implica, la defensa del Estado y de sus recursos ecológicos, alimentarios, energéticos, económicos, tecnológicos y del conocimiento.

En este sentido, esta integralidad en el nuevo paradigma de seguridad, implica nuevos retos, por ejemplo en el caso de la soberanía tecnológica y del conocimiento, no sólo implica la consolidación de un gobierno eficaz y transparente a través de plataformas tecnológicas, sino que también será indispensable *"desarrollar las capaci-*

dades para proteger a sus ciudadanos y sus intereses vitales de por ejemplo, ataques virtuales."[9].

Para esto, garantizar la seguridad del Estado y sus habitantes, implicará necesariamente contar con las capacidades soberanas en investigación, con el objeto de preservar los intereses nacionales.

América Latina, una región atravesada por la tendencia expansiva de actores imperiales, y como señala Anzelini & Castro, *"requiere de estrategias inequívocamente consistentes en materia de restricción de poder"[10]*. Las tecnologías, son parte de ese poder invisible que aún no ha sido considerado en las agendas de seguridad con la debida seriedad, por lo cual permanecen sin restricción alguna, tomando fuerza cada día estas formas abusivas de poder, expandiéndose sobre la región.

Las nuevas estrategias que se diseñen, en el marco de la arquitectura de seguridad internacional, exige pensar en cómo restringir el poder de los actores hegemónicos, y este no es más que un tema antiguo que viene tomando nuevos escenarios, y nuevos elementos cada vez menos perceptibles, que ponen de manifiesto una necesidad más allá de toda ideología.

Un ejemplo de este poder invisible es el software, que gobierna innegablemente cada equipo electrónico que utilizamos en todas las esferas de nuestras vidas, desde el ámbito personal al militar.

Por esto, las estrategias que vayan dirigidas hacia las restricciones de este poder, deben seguir este enfoque de integralidad que propone el Estado ecuatoriano, para lo cual serán necesario estructuras y procesos, respaldados por un estatus legal y recursos, en todas las instancia gubernamentales que hacen parte de esta integralidad, y que de alguna manera permitan extrapolarlos a la agenda de seguridad regional, mediante la institucionalidad en el sistema internacional.

Esta visión de apropiación de las tecnologías intenta incorporarse en Ecuador, mediante una ley orgánica, tal como el COESCCI (Código Orgánico de la Economía Social del Conocimiento, Creatividad e Innovación), derivada de la Constitución, que en cierto modo se relaciona con otras instituciones como parte del enfoque de integralidad, para aportar a la soberanía tecnológica respecto al software.

2.5 Ciencia, Tecnología y Sociedad (CTS).

Las tecnologías, a veces entendidas como artefactos complejos o futuristas, como "cosas del mañana", son en esencia algo fundamentalmente humano y su historia está inevitablemente ligada a la historia de nuestro futuro. Tecnología podría ser incluso los Estados, los sistemas de educación o tránsito, una forma de organización, y sobre todo podrían ser temas de discusión global en el que todos deberíamos estar inmersos.

Carl Sagan, astrónomo, escritor y divulgador científico afirmaba que *"vivimos en una sociedad profundamente dependiente de la ciencia y la tecnología y en la que nadie sabe nada de estos temas. Ello constituye una fórmula segura para el desastre"*. Las tecnologías no son, ni deben ser, ajenas a nosotros sino que son parte esencial de nuestra cultura, sin embargo su omnipresencia entre nuestras vidas nos hace difícil acercarnos a ellas para comprenderlas. [11]

Dedicamos poco tiempo a reflexionar sobre las tecnologías, seguramente porque las herramientas intelectuales para razonar sobre ellas, sus usos no declarados o su impacto social, son escasas como para llegar incluso a proyectar sus consecuencias.

Las tecnologías están en constante evolución, y ante este torrente de constantes innovaciones, se vuelve un gran desafío poder pensar, reflexionar, usar, criticar, hacer, transformar y evaluar la tecnología todo al mismo tiempo. Es decir, desarrollar esa capacidad de ver a través de las tecnologías, es una tarea que implica hurgar en la historia y la construcción social de la que surgen.

El Dr. Melvin Kranzberg, un profesor de historia de la tecnología en el Instituto de Tecnología de Georgia, entre los años de 1970 y 1980, afirmaba que *"El Ingeniero debería comprender que sus actividades profesionales afectan a todos los elementos de nuestra cultura, que un puente o un teléfono satisfacen necesidades económicas y sociales, y poseen valores estéticos y culturales, así como elementos tecnológicos. [...] Todo el que esté algo interesado en comprender el pasado, en aprender cómo llegó a ser el presente tal como es, o en especular sobre el futuro – y ello debería incluir a todo hombre pensante -, debe preocuparse por la evolución de la tecnología y su relación con la sociedad y la cultura." [12]*

Esta cita fue una nota introductoria del Dr. Kranzberg al primer número de la revista "Technology and Culture", una publicación de la Society for the History of Technology (SHOT) a inicio de los años 1960.

Kranzberg formuló las leyes de la relación entre tecnología y sociedad, que derivan de profundizar en el estudio del desarrollo de las tecnologías y sus interacciones con los cambios socio-culturales. Dos de sus leyes fundamentales indican que "*La tecnología no es ni buena, ni mala, ni neutral"* y que "*Aunque la tecnología puede ser un elemento primordial en muchos temas de interés público, los asuntos no técnicos son el factor primordial en cuanto a decisiones en políticas tecnológicas*"[13]

Esto implica que incluso como simples usuarios de las tecnologías debemos tener una mirada multidimensional al momento de evaluarlas, no sólo desde sus aspectos técnicos o artefactualistas sino también sobre su impacto en la construcción o selección de las mismas.

Hoy estamos frente a una nueva realidad que va más allá de lo tecnológico o económico, sino que también remite a lo socio-cultural e incluso político, que inevitablemente impacta en lo didáctico y metodológico vinculado a lo profesional.

Las revelaciones de Edward Snowden en el 2013[14], marcaron un hito en este sentido respecto a la conciencia social en el uso de las tecnologías al evidenciar usos

no declarados de tecnologías y artefactos omnipresentes en nuestras vidas. Sin embargo la didáctica queda develada como una necesidad importante para la comprensión de estas nuevas dimensiones, las cuales a pesar de las evidencias públicas siguen estando ocultas al entendimiento incluso de profesionales del ámbito de la informática y especialmente de la seguridad.

Las instituciones educativas juegan un rol importante en este cambio de paradigmas, en el que la inclusión de las CTS en los diseños curriculares, no sólo en las carreras de ingeniería sino incluso desde las escuelas, permitan a la sociedad abordar las múltiples dimensiones de las tecnologías.

Es decir, no sólo cubrir necesidades tecno-económicas o sociales (aplicación de principios científicos para fines prácticos), sino también la selección misma de estas tecnologías para cubrir dichas necesidades. Para esto es necesario que la formación en la problemática tecnológica tenga su vinculación con la sociedad desde la concepción misma de las tecnologías.

Este enfoque de las CTS aunque aparentemente irrelevante en el que hacer profesional en nuestras carreras ingenieriles, tiene décadas de discusión y de generación de políticas públicas, y son parte innegable de este trabajo.

3 Gestión de la Seguridad

La migración a tecnologías libres como cualquier proyecto informático debe seguir su ciclo, normas, controles, buenas prácticas y considerar además procesos para la gestión de la seguridad de la información relativos al proyecto.

Para esto se tomará como referencia la norma ISO/IEC 27001, que proporciona una guía para la implementación de un Sistema de Gestión de la Seguridad de la Información, que lleva a cabo las medidas necesarias para proteger los activos informáticos, por medio de políticas, procesos, objetivos, y una estructura organizacional.

La norma establece los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI, dentro del contexto de los riesgos del negocio global de la organización.

Para establecer un SGSI[15], es necesario los siguientes pasos:

a) Definir alcance y límites.
b) Definir la política.
c) Definir el enfoque de evaluación de riesgo de la organización.
d) Identificar los riesgos.
e) Analizar y evaluar los riesgos.
f) Identificar y evaluar opciones para el tratamiento de los riesgos.
g) Seleccionar los objetivos de control, y los controles para el tratamiento de los riesgos.
h) Obtener la aprobación gerencial de los riesgos residuales propuestos.
i) Obtener la autorización gerencial para implementar y operar el SGSI.
j) Preparar una declaración de aplicabilidad.

En este trabajo nos enfocaremos en los pasos desde la a) hasta la g).

3.1 Definir alcance y límites.

Los alcances y límites definidos en el capítulo 1.3 y 5.1 de este trabajo, determinan una migración a tecnologías libres de los escritorios de usuarios y los sistemas de gestión centralizada de estos escritorios, en instituciones públicas que cumplen ciertas condiciones.

3.2 Definir la política

Podemos encontrar un detalle de las políticas, marcos normativos, nacionales e institucionales en el anexo A. Este marco normativo será el que regirá a las partes interesadas, involucradas tanto internas como externas de los proyectos de migración a tecnologías libres.

Se recomienda además, definir una política institucional acerca del uso, desarrollo e impulso de las tecnologías libres tomando como marco regulatorio el COESCCI. Esto puede emitirse a través de un Acuerdo Ministerial, o una Resolución dependiendo del tipo de institución pública.

3.3 Definir el enfoque de evaluación del riesgo.

La metodología que se implemente deberá considerar, la situación actual de la institución tomando como referencia los supuestos definidos en el capítulo 5.1. Además deberá tener en cuenta el componente altamente humano, que implica este tipo de migraciones al estar enfocado directamente a los usuarios.

Se deberá considerar que al tratarse de instituciones públicas, estas en su accionar deben estar ligadas a los objetivos institucionales y los nacionales tomando como referencia el Plan Nacional de Desarrollo (PND) y el COESCCI. De esta mantera el análisis debe considerar los riesgos al cumplimiento o no de objetivos nacionales detallados en el anexo F, y el cumplimiento normativo detallado en el anexo A.

El siguiente cuadro recopila los objetivos nacionales (PND, COESCCI, Constitución, Ley de Seguridad Pública y del Estado) que están relacionados en los procesos

de migración a tecnologías libres en las instituciones públicas. Estos serán parte del análisis y evaluación del riesgo de alto nivel.

Objetivos Nacionales relacionados	**Referencia**
- Fortalecer la dolarización, evitar salida de dividas. - Incrementar valor agregado ecuatoriano en las compras públicas.	Objetivo 4, PND
- Promover, capacitación, investigación, transferencia tecnológica.	Objetivo 5, PND
- Dar preferencia al software de Tecnologías Libres en las compras públicas, con servicios ecuatorianos.	Art. 148, COESCCI
- Promover desarrollo de la ciencia, tecnología, innovación. - Incentivar producción de conocimiento.	Art. 3, COESCCI
- Garantizar la soberanía que en el ámbito de la seguridad del Estado implica la protección y control de los riesgos tecnológicos y científicos.	Art 3, Constitución Art 1, Ley de Seguridad Pública y del Estado,

En el capítulo 4 se desarrollará la identificación, análisis y evaluación del riesgo y las opciones de controles para el tratamiento de los mismos.

4 Identificación, análisis y evaluación de los riesgos.

Con base a la normativa y políticas nacionales, la migración no es una opción que pueda no considerarse, por lo tanto el análisis y evaluación del riesgo determinará su factibilidad el cual delimitará su alcance.

4.1 Identificación del riesgo.

Como primer paso se debe identificar los activos involucrados en el proceso de migración, y las amenazas posibles al proceso relacionado con dichos activos. En este proceso se pensará en las amenazas que impidan el cumplimiento de los objetivos institucionales y nacionales.

4.1.1 Objetivos institucionales – Identificación de activos y amenazas.

Tipo de Activo	Activo	Amenazas
Hardware	Computadores de escritorios o portátiles de los usuarios.	- Incompatibilidad parcial o total con el Sistema Operativo.
	Servidores para los sistemas de gestión centralizada de escritorios.	
Software	Sistema Operativo.	- Incompatibilidad con el hardware. - Ataque de virus/malware/spyware.
	Software institucional.	- Incompatibilidad con el Sistema Operativo. - Incompatibilidad de formatos de datos. - Ausencia de alternativas de Software Libre. - Ataque de virus/malware/spyware. - Acceso no autorizado.
	Ofimática y herramientas de colaboración.	
	Software de escritorio complementario – micro-informátca.	
	Software de escritorio especializado.	
Información	Para procesos sustantivos.	- Incompatibilidad de formato de archivos, documentos. - Pérdida de datos/documentos. - Acceso no autorizado.
	Para procesos adjetivos.	
	Archivos de usuario.	
Personas	Servidores públicos con habilidades o conocimiento especializado.	- Cambio de herramientas. - Cambio de modo de trabajo.

	Servidor público administrativo.	- No disponer de las herramientas adecuadas para la realización de su trabajo.
	Servidor público del jerárquico superior.	
	Máximas autoridades.	
Procesos	Procesos sustantivos.	- Afectación al cumplimiento de los objetivos.
	Procesos adjetivos.	- Desconocimiento del usuario sobre las nuevas herramientas. - Mala predisposición del usuario para aceptar el cambio de las herramientas.
	Para el cumplimiento de normativa.	- Desconocimiento del usuario sobre la normativa y políticas.

Estos activos pueden clasificarse en "activos críticos" y "activos de apoyo". Entre los activos críticos podemos identificar: Información y Procesos. Es decir, que las amenazas identificadas afectarían en concreto a la información y a la consecución de los objetivos de los procesos institucionales, ya sea de manera directa o a través de sus activos de apoyo.

4.1.2 Objetivos nacionales – Identificación de las amenazas y su impacto.

Se describen tres casos para este análisis: la situación actual; y dos opciones de remediación. La situación actual (caso 1), se refiere al mantener los 1000 equipos de escritorio de usuarios con su software sin licencias, exceptuando el antivirus que se mantiene actualizado. Las dos opciones de remediación se describen como: regularizar las licencias (caso 2), o migrar a tecnologías libres (caso 3).

Amenazas	**Impacto**		
	Caso 1	**Caso 2**	**Caso 3**
Incumplimiento con la Norma de Control Interno 410: mantener el software con sus licencias en situación regular.	Alto	Bajo	Bajo
Incumplimiento con el COESCCI: Iniciar estudio de factibilidad para la migración a tecnologías libres.	Alto	Alto	Bajo
Problemas judiciales por violación a los derechos de autor.	Alto	Bajo	Bajo
Incumplimiento con Decreto Ejecuto 135: Austeridad y control de gasto.	Bajo	Alto	Bajo
Afectación al cumplimiento de los Objetivos del PND: generación de salida de divisas (2.04 millones de dólares en 4 años), promover capacitación y transferencia tecnológica.	Alto	Alto	Bajo
Afectación a los Objetivos institucionales generado por el cambio de herramientas a los usuarios.	Bajo	Bajo	Alto

4.2 Análisis y evaluación del riesgo.

De la lista anterior podemos determinar un grupo de amenazas que son de particularidad del proceso de migración a tecnologías libres, consecuencia de un cambio de herramientas en los usuarios finales; y un grupo de amenazas comunes ya sea para una migración o no.

Para la evaluación se establecerá la siguiente escala: Bajo (1), Medio (2), Alto (3). El análisis se enfocará en las amenazas con impacto Alto y Medio.

Amenazas en consecuencia del proceso de migración, con impacto Alto o Medio.

Amenaza	Activo	Probabilidad
- Incompatibilidad parcial o total con el Sistema Operativo.	Computadores de escritorio	Alto
	Portátiles	Alto
	Servidores para gestión centralizada	Bajo
- Incompatibilidad de formatos de datos	Software institucional	Bajo
	Software especializado de escritorio	Alto
- Ausencia de alternativas de Software Libre.	Software institucional	Bajo
	Ofimática y herramientas de colaboración	Bajo
	Software especializado de escritorio	Alto
- Incompatibilidad de formato de archivos, documentos.	para procesos sustantivos	Medio
- Cambio de herramientas y modo de trabajo.	Servidores públicos con habilidades o conocimiento especializado	Alto
	Servidor público del jerárquico superior	Alto
	Máximas autoridades	Alto
- No disponer de las herramientas adecuadas para la realización de su trabajo.	Servidores públicos con habilidades o conocimiento especializado	Alto
	Servidor público administrativo	Bajo
	Servidor público del jerárquico superior	Alto
	Máximas autoridades	Alto
- Desconocimiento del usuario sobre las nuevas herramientas.	procesos sustantivos	Alto
- Mala predisposición del usuario para aceptar el cambio de las herramientas.	procesos sustantivos	Alto

Amenazas comunes situación actual (caso 1) y migración (caso 3), con impacto Alto.

Amenaza	Activo	Probabilidad	
		Caso 1	Caso 3
- Ataque de virus/malware/spyware.	Sistema Operativo	Alto	Bajo
	Software institucional	Alto	Bajo
	Ofimática y herramientas de colaboración	Alto	Bajo
	Software especializado de escritorio	Alto	Bajo
- Acceso no autorizado.	Sistema Operativo	Alto	Bajo
	Documentos y datos de usuarios	Alto	Bajo
- Pérdida de datos/documentos.	para procesos sustantivos	Alto	Medio
- Afectación al cumplimiento de los objetivos.	procesos sustantivos	Bajo	Alto

Evaluación del riesgo

Un análisis complementario para la evaluación del riesgo, podría ser utilizando la matriz propuesta en el modelo de impacto del riesgo de GTAG11[3]. En el anexo H podemos encontrar la matriz GTAG11 para el caso 1 (situación actual, previo a la migración), y el caso 3 (migración a tecnologías libres). En dicho análisis se puede concluir que el mantener la situación actual (caso 1) representa un riesgo mayor.

En resumen, el proceso de migración representa un alto riesgo al cumplimiento de objetivos institucionales:

- Por el cambio a la adopción de nuevas tecnologías, que implican adaptación al cambio.
- La afectación al acceso, disponibilidad de documentos de ofimática críticos por compatibilidad, o a los datos de aplicativos especializados de usuario.

En cambio el no migrar, y mantener la situación actual o regular las licencias, representan un alto riesgo al cumplimiento de los objetivos nacionales.

[3] Developing the IT Audit Plan - GTAG 11

4.3 Tratamiento de riesgos

En esta etapa se recomiendan los controles adecuados para mitigar los riesgos identificados para el proceso de migración de escritorios a tecnologías libres, además de determinar los riesgos residuales y su posible aceptación.

Todas estas amenazas descritas representan un impacto alto, con una probabilidad media o alta de ocurrencia, debido a la naturaleza del proyecto que implica un cambio de herramientas y en la manera de trabajar con ellas por parte de los usuarios. Por lo tanto todas estas amenazas deberán ser remediadas.

Controles propuestos para mitigación del riesgo.

Amenazas	**Controles**
- Incompatibilidad parcial o total con el Sistema Operativo.	Levantar inventario de equipos de usuarios, determinar marcas y modelos existentes. Realizar comprobación de compatibilidad mediante: - Verificar con fuentes de información públicas de compatibilidad. - Pruebas de laboratorio. - Seleccionar distribución GNU/Linux de mayor compatibilidad.
- Incompatibilidad de formatos de datos	Levantar inventario de documentos para procesos sustantivos, y comprobar compatibilidad de los documentos con la ofimática libre para categorizarlos. Determinar procedimientos para subsanar inconveniente por medio de un protocolo de migración que determine la excepciones.
- Ausencia de alternativas de Software Libre.	Levantar inventario de software de escritorio, y categorizar según posibilidad de migración. Determinar procedimientos para subsanar inconveniente por medio de un protocolo de migración que determine la excepciones.
- Cambio de herramientas y modo de trabajo	Coordinar procesos de capacitación, definiendo los mecanismos y recursos idóneos, para llegar a la totalidad de los usuarios.
- No disponer de las herramientas adecuadas para la realización de su trabajo.	Levantar inventario de software de escritorio, y categorizar según posibilidad de migración. Utilizar criterios de selección del sofware alternativo. Determinar procedimientos para subsanar inconveniente por medio de un protocolo de migración que determine la excepciones.
- Desconocimiento del usuario sobre las nuevas herramientas.	Coordinar procesos de capacitación, definiendo los mecanismos y recursos idóneos, para llegar a la totalidad de los usuarios.
- Mala predisposición del	Coordinar procesos de sensibilización, definiendo los mecanis-

usuario para aceptar el cambio de las herramientas.	mos y recursos idóneos, para llegar a la totalidad de los usuarios.
- Acceso no autorizado.	Implementar sistema de gestión centralizada de autenticación y aprovisionamiento de configuraciones, paqueterías y software.
- Pérdida de datos/documentos.	Definir política y protocolo de respaldo de datos de los usuarios previo a la implementación.

Con base al Plan Nacional de Desarrollo 2017-2021 estructurado en 9 objetivos[7] se definen los siguientes ejes estratégicos que serán fundamentales en todo proceso de migración a tecnologías libres (ver anexo F):

- Soberanía: relativo a la soberanía y autodeterminación respecto a las tecnologías y el control de las mismas.
- Sostenibilidad: en relación al mediano y largo plazo que implican el soporte, mantenimiento, desarrollo de capacidades respecto a las tecnologías, y su sostenibilidad económica a lo largo del tiempo contribuyendo además a la sostenibilidad y fortalecimiento de la dolarización.
- Inclusión y Desarrollo: respecto a ampliar las posibilidades de oportunidad y de generación de emprendimientos, de la mano con el desarrollo de capacidad tecnológica.
- Transparencia: relativo a la posibilidad de incluir a las comunidades y demás grupos sociales en la determinación de las tecnologías, promoviendo la participación y control social sobre las políticas establecidas y las tecnologías seleccionadas.

Estos ejes estratégicos serán la base de los criterios de selección de las Tecnologías Libres que se proponen en el anexo E. Las tecnologías seleccionadas deberán cumplir también con lo establecido en el EGSI.

El Esquema Gubernamental de la Seguridad de la Información (EGSI), basado en la norma ISO/IEC 27002:2005 propone 133 controles, repartidos entre 11 dominios. De estos controles se tomarán en cuenta 12 (ver tabla siguiente) relacionados al proyecto de migración a tecnologías libres de escritorios de usuarios, que servirán de insumo para la selección de las tecnologías a emplear.

Dominio	Control	Hitos
6. Gestión de Comunicación y Operaciones	6.10 Controles contra código malicioso	b) d) i)
	6.24 Transacciones en línea	b) c) d) f)
	6.26 Registros de auditoría	a) b) c) d) e) f) g) h) i) j) k)
	6.27 Monitoreo del uso del sistema	a) b) c) d) e)
7. Control de Acceso	7.6 Uso de contraseñas	b) c) d)
	7.7 Equipo de usuario desatendido	a)
	7.12 Protección de los puertos de configuración y diagnóstico remoto	b)
	7.16 Procedimiento de registro de inicio seguro	a) c) d) e) i) j)
8. Adquisición, desarrollo y mantenimiento de sistemas de información	8.1 Análisis y especificaciones de los requerimientos de seguridad.	a) b) c)
	8.4 Integridad del mensaje	a)
	8.6 Política sobre el uso de controles criptográficos	a) b) d) e) f) h)
11. Cumplimiento	11.8 Verificación del cumplimiento técnico	d)

Los hitos están detallados en el EGSI[4] y corresponde al desglose de requerimientos que las instituciones públicas deben cumplir para cada control.

Como control adicional, se deberá considerar los criterios de selección del software de tecnologías libres. Cada criterio de selección tendrá un nivel de criticidad en la selección (ver anexo E), y le corresponderá su respectivo nivel de cumplimiento con dicho criterio, por ejemplo:

Criterio	Criticidad	Condiciones que debe cumplir
Soporte	Alta	1. Rapidez de respuesta de la comunidad: 2. Presencia internacional de empresas especializada: 3. Presencia local de empresas especializada:

En el caso ecuatoriano, distribuciones GNU/Linux basadas en Ubuntu o CentOS, la herramienta de ofimática LibreOffice, y los sistemas de gestión centralizada de los escritorios de usuarios, cumplen con las tres condiciones, por lo tanto tendrán un nivel de cumplimiento Alto favorable para su selectividad.

[4] SNAP. (2013). Acuerdo 166: EGSI - Esquema Gubernamental de Seguridad de la Información. Recuperado de http://www.educarecuador.gob.ec/anexos/correo/Acuerdo_166.pdf

4.4 Aceptación del riesgo.

Una de las amenazas identificadas es el ataque de virus/malware a los equipos de usuarios que podrían poner en riesgo la información de la institución.

Casos internacionales de poder y control a través de las tecnologías, ponen la alerta sobre los recursos tecnológicos sobre todo en el sector público y estratégico. Entre estos casos podemos citar el sabotaje producido por el virus StuxNet[5] diseñado para Irán, el apagón en Ucrania[6] [7], entre otros, además de las filtraciones de los documentos de la NSA en el 2013[8]. Estos casos representan un conjunto de amenazas reales que se pueden categorizar como ciber-operaciones.

Empresas especializadas en ciberseguridad reconocen y afirman una tendencia que avanza hacia los dispositivos de usuario, e infraestructura crítica.[16] El 2017 fue escenario de múltiples ransomware y malware dirigido hacia usuarios de todo tipo, las estadísticas son claras en cuanto a la afectación y tipos de sistemas atacados. Más de 54 mil modificaciones de ransomware y 62 familias nuevas detectadas en 2016[17], y más de 96 mil modificaciones y 38 nuevas familias detectadas en el 2017[18]. Los sistemas operativos privativos son el blanco fácil y apetecido por este tipo de amenazas.

Un caso reciente de malware, descubierto por investigadores de FireEyes.com, es el virus Zyklon que explota 3 vulnerabilidades de Microsoft Office, de los cuales uno de ellos (CVE-2017-11882) es un fallo que tiene 17 años y permite la ejecución de código malicioso[19]. No basta con reforzar la seguridad de los sistemas, hay que procurar separar los sistemas de las amenazas.

[5] Silva, Francisco. "StuxNet – El sotware como herramienta de control geopolítico". https://www.-migralab.ec/2017/08/11/stuxnet-el-software-como-herramienta-de-control-geopolitico/

[6] UNAM. «Malware Industroyer está relacionado con el corte eléctrico en Kiev», n.o Junio 14 (2017). https://www.seguridad.unam.mx/malware-industroyer-relacionado-en-kiev.

[7] Leyden, John. «Move over, Stuxnet: Industroyer malware linked to Kiev blackouts», n.o Junio 12 (2017). https://www.theregister.co.uk/2017/06/12/industroyer_malware/.

[8] Rafael, Bonifaz. «Universidad de Buenos Aires Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería». Universidad de Buenos Aires, 2017. https://rafael.bonifaz.ec/blog/wp-content/uploads/2017/11/La-NSA-Según-las-Revelaciones-de-Snowden-Final.pdf.

Los computadores de escritorio de usuario al ser instalados con sistemas operativos de tecnologías libres como GNU/Linux, estarían siendo prácticamente aislados de estas amenazas tipo malware que en un 90% atacan a equipos con sistemas operativos privativos. Los efectos secundarios en caso de infección en sistemas GNU/Linux serían mínimos y controlables, por lo cual no tendría sentido la utilización de antivirus.

Es decir, que los riesgos derivados por la no utilización de antivirus sobre sistema operativo GNU/Linux son bajos, por lo tanto aceptables, al aplicar el concepto de separación entre las amenazas y el activo, para evitar interacción entre ellos. Esto implica atención en la implementación de controles.

4.5 Protocolo de excepciones.

Se determinarán excepciones, según la dificultad de migración de los documentos de ofimática o de los equipos de computación. Las excepciones estarán determinadas con base a una política que establecerá las condiciones para considerarse tales, y su tratamiento se dará en fases posteriores. Las excepciones deberán ser autorizadas por un Comité, con base a las políticas establecidas, como se sugiere a continuación:

Para documentos de ofimática

- Usuarios que manejen hojas de cálculos con elementos complejos, tales como:
  - Tablas dinámicas que no puedan portarse o migrase a LibreOffice, sin sufrir cambios importantes en su estructura y contenido.
  - Uso de herramienta “Solver”.
  - Uso de programación en “Macros”.
- Usuarios que necesiten intercambiar documentos de hoja de cálculo con otras instituciones; siempre y cuando el formato o funcionalidad del documento se vea afectado al abrirse con LibreOffice.
- Usuarios que manejen documentos de textos en ofimática privativa que incluyan programación en Macros.

La excepciones se aplicarán siempre sobre sistemas operativos de software libre, no sobre sistemas privativos. Es decir, que se considerarán mecanismo para acce-

der a la ofimática privativa desde el sistema operativo de tecnologías libres basado en GNU/Linux.

- Como una de las alternativas, las excepciones deberán ser servidas mediante Servicio de Escritorio Remoto (RDS). Es decir, la ofimática privativa podrá ser servida por RDS, sobre GNU/Linux utilizando un cliente RDS como "remmina"[9] o similar.
- Otra alternativa podría considerarse emuladores como Wine; o también WPS Office, una suite de ofimática privativa sobre GNU/Linux, cuya versión sin costo mantiene las funcionalidades esenciales.

Para aplicativos de escritorios

- Todo software privativo que no tenga alternativa en tecnologías libres, deberá ser servido mediante Servicio de Escritorio Remoto (RDS) sobre GNU/Linux.
- Serán excepciones todo caso que no pueda ser servido por Servicio de Escritorio Remoto, los cuales podrán mantener el sistema operativo privativo, tales como:
  - Dispositivos especiales de hardware de laboratorios científicos u otros que no tengan soporte en sistemas operativos GNU/Linux.
  - Dispositivos para registro de huellas para asistencia, cuyos controladores no tengan alternativa en sistemas operativos GNU/Linux.
  - Dispositivos de firma electrónica (token) cuyos controladores no tengan soporte para sistema operativo GNU/Linux.
  - Cualquier otro caso que sea analizado y determinado por equipo técnico de la Institución, bajo aprobación del Comité.

Para los controles de gestión centralizada de autenticación, configuración, actualización y aprovisionamiento se seleccionarán herramientas que cumplas con los criterios antes mencionados (anexo E) y los controles del EGSI. En el anexo G se puede encontrar alternativas de tecnologías libres que soporten estos controles.

[9] Remmina es un aplicativo para escritorios remotos (Remote Desktop Application) para Linux. Soporta RDP, VNC, SSH, NX, entre otros protocolos: http://www.remmina.org/wp/
Su código fuente puede encontrarse en: https://github.com/FreeRDP/Remmina

5 Propuesta de Modelo de Gestión de Actualización de escritorio de usuario a Tecnologías Libres.

Una vez analizado y evaluado los riegos relacionados al proyecto de migración a tecnologías libres, se procede a la construcción de una propuesta de modelo de gestión para la migración de escritorios de usuarios a tecnologías libres tomando en cuenta los controles propuestos.

Además se tomarán en cuenta las buenas prácticas o recomendaciones sobre la materia, emitidas en el informe "lecciones aprendidas" del Instituto de Análisis de la Defensa[10] (IDA). (ver Anexo I).

5.1 Supuestos de Trabajos

La propuesta se basa en instituciones públicas en las que tienen en común un marco normativo transversal acorde a un conjunto de políticas públicas ya establecidas que las rigen, sin embargo, como suele ser común las autoridades no necesariamente acuerdan un criterio homogéneo en cuanto a las acciones que se deben tomar para la ejecución de dichas políticas.

Por tal motivo, para este trabajo se deberán considerar los siguientes supuestos:

1. No todos los servidores públicos tienen experiencia en actividades de gestión.
2. Las máximas autoridades en las instituciones, no necesariamente darán apoyo inicial a los proyectos de migración, por lo cual deberá proporcionarse información necesaria para la toma de decisiones.
3. Las instituciones tienen presupuestos y recurso humano limitado.
4. La migración de los sistemas de escritorio no suponen modificación en los aplicativos de core de las instituciones.

[10] El Instituto de Análisis de la Defensa (IDA del inglés Institute for Defense Analyses) es una corporación sin ánimo de lucro de Estados Unidos financiada por el gobierno de Estados Unidos. Es un centro de investigación y desarrollo del gobierno y, como tal, sólo trabaja para él. En particular trabaja principalmente para el Departamento de Defensa de los Estados Unidos aunque a veces trabaja para otras entidades del gobierno como el Departamento de Estado de los Estados Unidos y la Agencia Central de Inteligencia.
https://www.ida.org/

5. En general los procesos de migración suponen un cambio de tecnologías, que no necesariamente implican un paso de transición controlado.
6. El término "migración" como tal, en países como el nuestro donde la historia ha dejado un marcado significado con mucha carga negativa por las migraciones de ciudadanos a finales de los 90s que implicaron desmembramiento de las estructuras sociales, es percibido como un proceso de impacto negativo. Por tal motivo en este trabajo se tomará el término "Actualización" que supone en general la percepción de algo nuevo, mejorado con implicaciones positivas.
7. Las instituciones mantienen sus sistemas operativos de usuario y ofimática sin licencias (software pirata).
8. Se asume el caso de una institución con 1000 funcionarios en una sola localidad, a los que se les actualizará sus equipos a tecnologías libres.

5.2 Habilitadores COBIT 5 adaptados al Modelo de Gestión propuesto.

Tomando como referencia el Marco de Trabajo COBIT 5 para la Seguridad de la Información, se construirá un marco de referencia para el modelo de gestión de actualización a tecnologías libres para las instituciones públicas. Es decir, se aplicará el enfoque holístico de COBIT 5 para construir el modelo de gobierno y gestión de procesos de Actualización a Tecnologías Libres institucional, centrado a escritorios de usuarios.

Las siete categorías de habilitadores (ver capítulo 2.1) aplicables a este modelo, serán adaptadas para la presente propuesta:

1. Principios, políticas y marcos de referencias:

Para el modelo que se propone podemos encontrar un detalle de las políticas, marcos normativos, en el anexo A. Este marco normativo será el que regirá a las partes interesadas, involucradas tanto internas como externas de los proyectos de Actualización a Tecnologías Libres.

Siguiendo las buenas prácticas propuestas en COBIT 5, para el marco de políticas generales, estas tendrán una estructura jerárquica:

a) Principios Generales:
    - Centrarse en el core de negocio institucionales.
    - Cumplir con requisitos legales y regulatorios nacionales.
    - Evaluar impacto del proceso de Actualización a Tecnologías Libres.
    - Promover mejora continua del proceso de Actualización a Tecnologías Libres.
    - Adoptar estrategia basada en el riesgo, considerando además el impacto hacia los objetivos nacionales (Plan Nacional de Desarrollo, COESCCI).
    - Fomentar una cultura positiva de Actualización a Tecnologías Libres.
b) Políticas Institucionales:
    - Marco normativo institucional.
    - Políticas institucionales como: políticas de seguridad de la información, acuerdos ministeriales, entre otras.
c) Adaptar las políticas al entorno institucional. Se deberá tomar en cuenta:
    - Requisitos operativos y funcionales de la institución: reglamentos, manuales del orgánico funcional, etc.
    - Políticas existentes de alto nivel y cultura organizacional.
    - Regulaciones gubernamentales (por ejemplo: Norma de Control Interno 410 de contraloría, COESCCI, ESGI, Decreto 1425[11]).
    - Estándares de la industria (ISO/IEC 27002, EGSI, ISO/IEC 27005).
    - Restricciones presupuestarias (Decreto Ejecutivo 135[12]).
    - Innovación, buenas prácticas y creación de valor.
d) Ciclo de vida de las políticas: considerar los cambios regulatorios y los giros o proyectos establecidos por las políticas públicas que podrían implicar modificación de políticas internas.

[11] Decreto 1425 "Reglamento para la adquisición de software por parte de las entidades contratantes del sector público"

[12] Decreto Ejecutivo 135 de "optimización y austeridad del gasto público", emitido el 1 de septiembre del 2017

2. Procesos:

Los procesos de gobierno se encargarán de proporcionar valor, optimizar riesgos y recursos, esto implicará además la evaluación de opciones estratégicas que proporcionarán dirección al proceso de Actualización a Tecnologías Libres. Para la generación del modelo de gestión se han seleccionado los siguientes procesos de gobierno:

Código	Descripción
EDM01	Asegurar el establecimiento y mantenimiento del Marco de Gobierno
EDM02	Asegurar la Entrada de Beneficios
EDM03	Asegurar la Optimización del Riesgo
EDM04	Asegurar la Optimización de Recursos.

Los procesos de gestión involucran prácticas y actividades para la planificación, construcción, ejecución y supervisión. Los procesos que se tomarán de base para la presente propuesta, son los que siguen:

Código	Descripción
APO01	Gestionar el marco de gestión de Tecnologías Libres
APO02	Gestionar la Estrategia
APO04	Gestionar la Innovación
APO12	Gestionar el Riesgo

Los procesos seleccionados del marco de trabajo son los utilizados para la generación del modelo de gestión, sin embargo no son los únicos. En el anexo D se puede encontrar una adaptación de estos procesos en el marco de la Gestión de la Actualización de escritorios de usuarios a tecnologías libres.

3. Estructura Organizativa

Involucra las partes interesadas como primer componente, que pueden separarse en dos categorías:

a) Roles y estructuras específicas: Internas a la función de la Dirección de Tecnologías de la Información y Comunicación.
    - Director DTIC

- Jefes de las áreas de: Infraestructura, Soporte a usuario, Seguridad Informática.

b) Roles y estructuras relacionadas: Internas a la organización relativas a la función de otras áreas de la institución que contribuirán al desarrollo exitoso del proyecto de Actualización a Tecnologías Libres:
   - Servidores públicos a quienes se actualizarán sus escritorios a tecnologías libres.
   - Director de Talento Humano o delegado.
   - Director de Planificación o delegado.
   - Director de Comunicación o delegado.
   - Director de Gestión del Cambio y Cultura Organizacional o delegado.
   - Delegado de la máxima autoridad.

   Externas a la organización, relativas a las instituciones de control o regulación:
   - Ministerio de Telecomunicaciones y de la Sociedad de la Información: Institución encargada de conocer los planes de migración/actualización a tecnologías libres.
   - Contraloría General del Estado: Institución encargada de velar por el cumplimiento de las normas de control interno.

c) Responsabilidad sobre el proyecto de Actualización a Tecnologías Libres: Entre las distintas alternativas de este rol, se sugiere que sea un delegado de la máxima autoridad quien lidere el proyecto.

4. Cultura, ética y comportamiento

Este es un factor de éxito clave para el gobierno y gestión del proyecto, y deberá tomarse en cuenta los siguientes elementos:

a) Modelo cultural: Trasciende a toda la institución, esto incluye e inicia con la máxima autoridad y las personas y áreas involucradas directamente con la gestión del proyecto. Es decir, debe tomarse en cuenta el grupo que se encargará de gestionar el proyecto y moldear los comportamientos deseados, además del grupo que debe simplemente alinearse con las reglas y normas definidas.

   Debe vincularse con la ética de la organización, la ética individual y los comportamientos individuales. Por lo tanto, se debe considerar las siguientes buenas prácticas:

   - Comunicación a toda la institución de los comportamientos deseados.
   - Conocimiento de la conducta deseada (reforzado y apoyado por el ejemplo de las autoridades y líderes o "agentes del cambio").
   - Incentivos para alentar y medidas disuasorias para hacer cumplir las actitudes, normas y reglas.

b) El ciclo de vida de la cultura: La medición en el tiempo del comportamiento de las partes interesadas dará una visión correcta de la cultura. Estas mediciones permitirán construir indicadores, lo cual no sería posible con datos estáticos y no aportarían mayor valor. Por lo tanto se debe evaluar su evolución en el tiempo, antes, durante y después del proyecto, de esta manera se podrá proporcionar por medio de estas métricas un mecanismo de evaluación consistente de la cultura y su evolución.

c) Liderazgo o "agentes del cambio" que puedan influir en el comportamiento: Los líderes o agentes del cambio son personas de la institución que están dispuestas a hablar y servir de ejemplo para otros. Estos serán servidores públicos de la institución que proporcionarán soporte para el cambio y aplicación de la cultura, incluso para el levantamiento de información inicial entre otras tareas técnicas menores.

   En este grupo se puede considerar a:

   - Las autoridades de cada área.
   - Un delegado por las autoridades de cada área.

- Personas con predisposición al cambio, y afinidad a las tecnologías y los principios del proyecto.

d) <u>El comportamiento deseable. Se puede identificar los siguientes:</u>
   - Las personas comprenden y respetan la importancia de las políticas y principios relacionados a las tecnologías libres.
   - Se les proporciona directrices suficientes y detalladas, además se les fomenta su participación activa en el cambio de la situación actual.
   - Todo el mundo es responsable por lograr los beneficios institucionales y nacionales que implica el proyecto, acorde al Plan Nacional de Desarrollo y el COESCCI, y garantizar su éxito.
   - Las partes interesadas saben cómo identificar y mitigar los riesgos que pudiera suponer la implementación del proyecto.
   - La máxima autoridad comprende, reconoce, apoya y soporta las directrices establecidas, y el valor que suponen a nivel institucional, como Estado y como país, acorde al Plan Nacional de Desarrollo y el COESCCI.

5. Información

En el marco del contexto de gobierno y gestión para un proyecto de Actualización a Tecnologías Libres, se pueden enumerar los siguientes tipos de información:

- Estrategias de Actualización a Tecnologías Libres, estudio de factibilidad.
- Presupuesto POA / PAC.
- Procesos sustantivos (agregadores de valor), procesos adjetivos (de apoyo) de la institución.
- Plan de Actualización a Tecnologías Libres, Plan de Comunicación, Plan de Capacitación.
- Políticas y Marco Normativo, institucionales y nacionales.
- Plantillas de aprovisionamiento de equipos de escritorios.
- Material para la Concienciación (Insumo para el Plan de Comunicación).
- Registro y análisis de riesgos, de alto y bajo nivel.
- Análisis de amenazas.

- Informe de evaluación de vulnerabilidades.
- Catálogo de procesos y servicios afectados.
- Inventarios de hardware, software y documentos de ofimática.
- Métricas e indicadores de evaluación de predisposición al cambio.
- Métricas e indicadores de beneficios e impactos.

En el anexo B se podrá encontrar un detalle de los tipos de información, y las partes interesadas.

El ciclo de vida de la información, está vinculado a la gestión del conocimiento para garantizar la exactitud de la misma. En el modelo propuesto toda información generada como parte integral de un proyecto de Actualización a Tecnologías Libres deberá incluir las siguientes fases: a) Planificar, diseñar, construir, adquirir; b) Usar/operar (almacenar, compartir, usar); c) Supervisar; e) Eliminar.

Haciendo referencia a las recomendaciones sugeridas en el capítulo 3.1 “desafíos y oportunidades”, los manuales y demás documentación producida que generen conocimiento, deberán ser liberados con licencias Creative Commons para su libre acceso de otras instituciones, y que además sirvan para la documentación de casos de éxito y contribuyan a la generación de comunidades.

6. Servicios, infraestructuras y aplicaciones

La propuesta se centra en procesos de Actualización a Tecnologías Libres de escritorios de usuarios, por lo cual este habilitador estará enfocado a las aplicaciones e infraestructura tecnológica necesaria para el cumplimiento de las funciones de los usuarios institucionales y los servicios institucionales involucrados.

Los servicios están directamente relacionados con otros habilitadores como procesos, información, estructura organizativa. Esta relación será importante en la priorización que se aplica en la planificación estratégica para la implementación de la Actualización a Tecnologías Libres. Para esto se deberá contar con un inventario de procesos institucionales sustantivos (agregadores de valor) y adjetivos (de apoyo), software, hardware y sus dependencias entre estos.

Este trabajo no pretende hacer un análisis de las tecnologías específicas, puesto que el marco de referencia COBIT 5 es agnóstico a las mismas, sin embargo se determinarán criterios de selección, que se pueden encontrar en el anexo E, para evaluar las tecnologías libres que se vayan a emplear.

7. Personas, habilidades y competencias

Una de las metas que se deberán alcanzar está relacionada a la comprensión y predisposición hacia las tecnologías libres, y el conocimiento técnico y operativo que este implique según las competencias de cada rol.

Como parte del ciclo de vida de este habilitador se considera al conocimiento de la línea base de habilidades, y la re-definición de la misma para alcanzar los objetivos. Un proyecto de Actualización a Tecnologías Libres deberá considerar el desarrollo de las habilidades necesarias mediante formación, certificaciones, y la definición de políticas en las contrataciones de personal que incluyan estas habilidades. Esta línea base deberá ser evaluada periódicamente, en función de las políticas públicas y la evolución de las tecnologías libres.

Se puede definir la línea base de manera horizontal y específica, como se muestra en el cuadro siguiente:

Alcance	**Rol**	**Ámbito**	**Habilidades / competencias**
Horizontales	Servidores públicos en general	Operativo	Uso de: Sistemas Operativos y Ofimática de Tecnologías Libres.
		Conceptual	Tecnologías libres, CTS, aceptación al cambio.
Específicas	Soporte Técnico	Técnico	Sysadmin nivel medio, en sistemas operativos GNU/Linux.
	Infraestructura Tecnológica	Técnico	Sysadmin nivel avanzado en sistemas operativos GNU/Linux.
			Tecnologías libres específicas para la gestión de los escritorios de usuario.

De manera horizontal, implicará un alcance para todo servidor público para quienes se deberán incluir certificaciones sobre conocimientos generales y conceptuales en tecnologías libres y su impacto social (CTS).

Siempre se deberá tener en cuenta un nivel óptimo a alcanzar, aunque la realidad de los resultados pueda que no represente a estos niveles. Un valor añadido a este habilitador pueden ser las certificaciones en perfiles de la Secretaría Técnica del Sistema Nacional de Cualificaciones Profesionales[13] (SETEC).

En el caso de los usuarios finales, estas habilidades estarían orientadas hacia la aceptación al cambio y nuevos paradigmas, además del manejo y uso de herramientas básicas como sistema operativo y ofimática libre. En el caso de técnicos especialistas de las áreas de informática éstas deben centrarse en operadores y administradores de sistemas operativos libres, para escritorios y servidores (sysadmin).

5.3 Factores de Éxito.

Tomando como referencia las recomendaciones de COBIT 5, los factores claves de éxito para la implementación de un proyecto de Actualización a Tecnologías Libres deben incluir al menos lo siguiente:

- Debe haber apoyo continuo y visible de la máxima autoridad de la institución, incluso a nivel de Estado. La dirección y el mandato para la iniciativa debe venir desde la máxima autoridad, con base del marco normativo.
- Los objetivos institucionales y nacionales deben ser comprendidos por la iniciativa del proyecto.
- Procurar resultados rápidos y priorizados (éxitos tempranos, metodologías ágiles), tomando en cuenta las área más sencillas de implementar o que generan el menor impacto posible de cara al servicio que se ofrece al ciudadano.
- Comprometer los recursos y financiación priorizada, en caso de ser necesario.
- Contar con el talento humano adecuadamente preparado para la implementación de las distintas fases.

[13] La SETEC es una Institución ecuatoriana que impulsa y gestiona el Sistema Nacional de Cualificaciones Profesionales, y además promueve la capacitación y certificación para fortalecer y reconocer las competencias del talento humano en el Ecuador.

- Vincular a la Academia, Redes de Investigación, sector empresarial y a las Comunidades de Tecnologías Libres en el proceso. Esto incluye prácticas pre-profesionales universitarias.

En un contexto institucional en el que no exista comprensión y apoyo directo por parte de la máxima autoridad, será necesario la evaluación de alto nivel del riesgo, el impacto y los beneficios institucionales y nacionales involucrados que servirán de insumo para presentar el proyecto a la máxima autoridad y conseguir su apoyo.

Es necesario que el compromiso y la adhesión de la partes interesadas principales se solicite desde el nacimiento del proyecto, por tal motivo los objetivos y beneficios deben expresarse claramente relacionados al marco normativo, los objetivos institucionales, y los objetivos nacionales estipulados en el Plan Nacional de Desarrollo.

La gestión del cambio de manera eficaz es otro factor de éxito, el cual no deberá enfocarse exclusivamente en elementos tecnológicos, sino también humanos y sociales.

5.4 Modelo de Gestión.

Siguiendo el ciclo de Edwards Deming o PDCA (Plan-Do-Check-Act por sus siglas en inglés), se describe a continuación los procesos que se deben considerar como parte de la propuesta de este trabajo.

5.4.1 Planificación

Esta fase es de vital importancia para garantizar la consecución de las fases posteriores. Todo el esfuerzo invertido en la fase de Planificación derivarán en el éxito o fracaso de la fase de Implementación, y le corresponde a todas las áreas involucradas en un trabajo conjunto, colaborativo.

Esta fase inicia con la identificación del contexto institucional, que entre otras cosas deberá determinar si se cuenta o no con el apoyo de la máxima autoridad. En los

supuestos de trabajo planteados, se asume que será necesario convencer a la máxima autoridad para lo cual se recurre a un análisis de riesgos que deberá generar la información necesaria para la toma de decisión de la máxima autoridad para dar inicio a la planificación del proyecto.

Una vez que se tiene la autorización de la máxima autoridad, entonces se procede a dar inicio a los procesos de esta fase, como se describen a continuación:

Conformación del Comité/Comisión de ASL (P01)

En este proceso, se realizan todas las actividades relacionadas a la conformación del comité interno de Actualización a Tecnologías Libres. El comité deberá estar conformado al menos de las siguientes unidades:

- Talento Humano
- Comunicación
- Gestión del Cambio
- Planificación
- Tecnologías de la Información y Comunicación

Convocatoria desde la máxima autoridad		**P01-01**
Actividades	**Entrada**	**Salida**
- Debe realizarse desde la máxima autoridad, por medios oficiales, dirigida a los Directores de las Unidades Administrativas que la conformarán. - Asignar un delegado de la máxima autoridad para el Comité.	Estructura orgánico/funcional. Marco normativo: - COESCCI, - Constitución, - Decreto 1425, - Decreto 135	Documento y comunicación oficial de Convocatoria.

Reunión 0 Esta será la primera reunión del comité/comisión que tendrá un fuerte componente de concienciación.		**P01-02**
Actividades	**Entrada**	**Salida**
La primera reunión, producto de la convocatoria, deberá tener al menos la siguiente agenda:	P01-01 Hoja de ruta	Acta Reunión Documento de Compromisos.

• Sensibilización a los directivos • Socialización de hoja de ruta • Resolución de dudas sobre el proyecto. • Establecer compromisos • Asignar tareas y delegados	Marco normativo: - COESCCI, - Constitución, - Decreto 1425, - Decreto 135	

Guía de la agenda:

Sensibilización a los directivos: Se sugiere inducciones acerca de: ¿Qué es software libre?, ¿Porqué Actualizarnos a Software Libre?, La importancia de utilizar formatos de documentos con estándares abiertos en el Gobierno. El Marco Normativo Nacional que impulsa a las entidades públicas a la actualización a tecnologías libres. Los mitos y verdades acerca de las tecnologías libres. La importancia del estudio de factibilidad, para determinar alcance y excepciones de la Actualización a Tecnologías Libres.

Socialización de hoja de ruta: Se expone la hoja de ruta, y se hace una explicación general de la misma.

Resolución de dudas (sobre el proyecto): Surgirán dudas sobre la hoja de ruta, y sobre el proceso de actualización, las cuales deberán ser resultas, sin profundizar en detalles.

Establecer compromisos: Se explica el apoyo que corresponde a cada unidad administrativa desde sus competencias, en relación a canalizar esfuerzos y recursos, incluso en los procesos de sensibilización.

Asignar funciones y delegados: Se explica de manera general las funciones que estarán delegadas a cada unidad:

- Comunicación:
  - Difusión externa de iniciativas.
  - Difusión externa de logros.
- Gestión del Cambio:
  - Mediciones ex-ante y ex-post de predisposición al cambio.
  - Campañas para sensibilización interna.
  - Campañas de difusión interna de iniciativa y logros.
  - Campañas de difusión de ventajas y beneficios.
  - Campañas de difusión del marco normativo
- Tecnología:
  - Presidir el Comité. (podría ser también unidad de Planificación).
  - Realizar levantamiento de información y laboratorios técnicos.
  - Apoyar procesos de capacitación con recursos de personal técnicos y tecnológicos.
  - Planificar y Ejecutar la migración de los Equipos de Escritorios.
- Talento Humano:
  - Gestionar capacitación personal no técnico (usuario final).
  - Gestionar capacitación personal técnico.
  - Coordinar con el comité recursos para capacitación.
  - Coordinar con Comunidad y Academia apoyo para realización de Talleres.
- Planificación:
  - Priorizar presupuestos y recursos para la migración.
  - Detener recursos para licenciamiento de software, que no cumplan con el COESCCI y el Decreto1425.
  - Coordinar con el comité las autorizaciones de licencias de software.

Oficializar/Institucionalizar conformación del comité desde la máxima autoridad		P01-03
Actividades	**Entrada**	**Salida**
- Elaboración y firma de Resolución / Acuerdo Ministerial para instrumentar el Comité Interno y la definición de políticas institucionales de base para el Proceso de Actualización de Tecnologías Libres. Este documento debe ser firmado por la máxima autoridad.	P01-02	Instrumento del conformación oficial del Comité/Comisión (Resolución/Acuerdo Ministerial), firmado y enviado.

Asignación de Tareas (P02)

Se revisan las plantillas/estructuras de los documentos de Planes de Actualización a Tecnologías Libres, Comunicación y Capacitación y se resuelven las dudas que se presenten. Esta mesa debe ser llevada por el delegado de la máxima autoridad. Se comunican las responsabilidades de cada área con cada Plan, y la siguiente tarea (Diagnóstico). Se oficializan los compromisos adquiridos de los delegados de cada área con sus responsabilidades, y el cronograma macro (borrador de los Planes).

Convocatoria desde la autoridad del comité para Reunión 01		P02-01
Actividades	**Entrada**	**Salida**
- Realizar convocatoria desde la autoridad del Comité/Comisión, delegada por la máxima autoridad de la Institución, hacia los miembros del comité/comisión.	P01-02 P01-03	Comunicado de convocatoria a las partes interesadas.

Reunión 01 Esta sería la primera reunión de planificación conjunta donde se da a conocer con más profundidad el proyecto.		P02-02
Actividades	**Entrada**	**Salida**
La reunión deberá tener al menos la siguiente agenda: • Presentar al detalle la estructura de formato del documento de los Planes de Actualización a Tecnologías Libres, Comunicación, Capacitación. • Resolución de dudas sobre los documentos de los Planes. • Delegar los Planes respectivos a las áreas correspondientes. • Establecer cronogramas macro de trabajo.	P01-02 P01-03	Acta de Reunión. Cronograma macro.
Guía de la Agenda		
Presentar al detalle la estructura del documento de los Planes: Se deberá presentar y expli-		

car los elementos de los modelos de Planes (Actualización, Capacitación, Comunicación). Esto estará a cargo del especialista de Tecnologías Libres delegado por la máxima autoridad.

Resolución de dudas sobre los documentos modelo de los Planes: Toda inquietud o duda sobre los modelos de Planes y su operatividad, deberá ser resuelta por el especialista de Tecnologías Libres delegado por la máxima autoridad.

Delegar los Planes respectivos a las áreas correspondientes:

- Plan de Comunicación:
  - Comunicación Interna (concienciación), dependiendo del caso, podrá estar a cargo de las áreas: Comunicación, Gestión del Cambio o Talento Humano.
  - Comunicación externa, estará a cargo de la unidad de Comunicación.
- Plan de Capacitación: estará a cargo de la unidad de Talento Humano.
- Plan de Actualización: estará a cargo de la unidad de Tecnologías de Información y Comunicación.

Establecer cronogramas macro de trabajo: Se acuerda el cronograma de entrega del primer borrador de los Planes por cada área.

Oficializar los compromisos.		**P02-03**
Actividades	**Entrada**	**Salida**
- Los compromisos deberán estar registrados en el acta de la reunión, al cuál el Comité/Comisión deberá hacer seguimiento de su efectivo cumplimiento. Tanto el acta, como los informes del seguimiento deberán remitirse a la máxima autoridad.	P02-02	Carta de Compromiso

Diagnóstico (Análisis y recopilación) (P03)

Es necesario el levantamiento de toda la información relevante de cada unidad de la institución, para el proceso de Actualización a Tecnologías Libres.

Se realizan inventarios, encuestas, evaluaciones. Se ejecutan las encuestas para efectos de medición inicial (ex-ante). Se socializan los resultados del relevamiento para efectos de elaborar los estudios de factibilidad con la participación de la comunidad.

Inventario		**P03-01**
Actividades	**Entrada**	**Salida**
Se debe realizar al menos los siguientes inventarios:	Alcance del proyecto.	Documentos de inventario pre-categori-

• Inventario de Hardware de escritorio. • Inventario de Software de escritorio. • Inventario de modelos de documentos de ofimática de los usuarios. • Inventario de procesos institucionales.	Plantillas de inventarios de hardware. Plantillas de inventarios de software. Plantillas de inventarios de documentos.	zado por unidad administrativa.
Guía del inventario		
• Inventario de Hardware de escritorio: Se debe obtener el inventario de equipos de escritorio, incluyendo equipos portátiles, impresoras y scanners, y cualquier equipo adicional de escritorio que utilicen los usuarios y que interactúen con sistemas operativos de escritorio. Este inventario luego serán categorizados según su factibilidad de actualizarse a tecnologías libres, por compatibilidad de hardware, según las pruebas de laboratorio. • Inventario de Software de escritorio: Se debe obtener el inventario de todo software utilizado por los servidores públicos para sus actividades. Esto implica sistemas operativos, utilitarios, aplicativos institucionales, registrándose además si los aplicativos institucionales son cliente servidor o arquitectura web. Estos inventarios deben ser categorizados según su factibilidad de actualizarse a tecnologías libres, con base a las pruebas de laboratorio. • Inventario de modelos de documentos de ofimática de usuarios: Se debe obtener el inventario de las plantillas/modelos de documentos de ofimática, es decir, documentos tipos que son utilizados con frecuencia para las actividades de las unidades administrativas, inclusive documentos que interactúan con instituciones externas. Estos documentos luego serán categorizados según su factibilidad de actualizarse a tecnologías libres, en las pruebas de laboratorio. • Inventario de procesos institucionales: Se deberá obtener el inventario de los procesos sustantivos y adjetivos de la institución, los cuales deberán ser categorizados según su nivel de criticidad e importancia.		

Determinación de conocimientos técnicos.		**P03-02**
Actividades	**Entrada**	**Salida**
Evaluar, determinar las habilidades técnicas y experticia de los funcionarios: • Unidad TICs • Usuarios finales	P02-02 P02-03 Marco normativo. Modelo de encuestas Modelo de evaluaciones.	Resultado de evaluación técnica.
Guía de las actividades		
Unidad TICs: Se determina las habilidades técnicas respecto a sistemas operativos GNU/Linux. • TICs Linux nivel medio para equipo de soporte a usuario. • TICs Linux SysAdmin nivel avanzado para equipo de infraestructura tecnológica. Usuarios finales: • Se determina las habilidades que tengan los usuarios finales en el manejo de herramientas de ofimática (independientemente que sea libre o no). Herramientas: • Se puede recurrir a evaluaciones, encuestas, información histórica de las mismas.		

Determinación de niveles de sensibilización y conceptualización.		P03-03
Actividades	**Entrada**	**Salida**
Dirigido a todos los servidores públicos, especialmente a los no tecnológicos. Se debe considerar al menos: • Expectativa. • Conocimiento conceptuales. • Sensibilización y niveles de predisposición al cambio.	P02-02 P02-03 Marco Normativo. Modelo de encuestas. Modelo de evaluaciones.	Resultado de encuestas, sobre los niveles de conocimiento y predisposición al cambio.
Guía de las actividades		
El objetivo es determinar los niveles de conocimientos conceptuales (no técnicos) sobre tecnologías libres, y los niveles de predisposición al cambio. Esto se puede realizar por medio de encuestas, en donde se abarcarán al menos las siguientes dimensiones: Expectativa: Sobre el marco normativo, y el proyecto de Actualización a Tecnologías Libres. Conocimiento conceptuales: Acerca del marco normativo, las Tecnologías Libres, Soberanía Tecnológica, Apropiación del Conocimiento. Sensibilización y niveles de predisposición al cambio: Se tocarán temas como: Cambio de paradigmas, Tecnologías como construcción social, situación actual de la industria local de software, la economía social de los conocimientos y la creación de una real industria de tecnologías.		

Elaborar estudios de factibilidad técnica.		P03-04
Actividades	**Entrada**	**Salida**
Una vez obtenido los inventarios, se realiza la categorización del mismo según los niveles de complejidad de actualización a tecnologías libres. • Actualización de Software. • Drivers de Hardware. • Documentos de ofimática.	P03-01	Estudio de factibilidad.
Guía de las actividades		
Actualización del software: • Se determina las opciones en alternativas libres que podrían reemplazar a las privativas. • Se clasifica al software con al menos las siguientes categorías:		

- Actualizable: existe una alternativa en tecnologías libres para reemplazo inmediato, junto con el sistema operativo.
- No actualizable: no existe una alternativa libre, e impide actualizar al sistema operativo a tecnologías libres.
- Portable: no existe alternativa libre, sin embargo hay mecanismo para que la herramienta corra sobre sistema operativo libre o mediante acceso remoto tipo RDS.

Drivers Hardware:

- Se deberá probar por cada marca y modelo de equipo (PC, laptop, impresora, scanner, etc) su funcionamiento en la distribución Linux elegida.
- Se deberá probar las distros GNU/Linux idónea para el caso particular de la institución, en relación al hardware que se dispone.
- Se deberá categorizar según los resultados de las pruebas, al menos de la siguiente manera:
  - Compatible totalmente.
  - Compatible parcialmente: pero deberá existir una alternativa de solución para el componen no compatible.
  - Incompatible: no hay manera que pueda operar establemente en sistemas operativos GNU/Linux.

Documentos ofimática:

- Debe hacerse pruebas con un software de ofimática en tecnologías libres de las plantillas de documentos que fueron inventariadas.
- Se debe categorizar al menos con los siguientes criterios:
  - Documento Actualizable: al manipular con Ofimática Libre este no presenta problema alguno de compatibilidad.
  - Documento no Actualizable: documentos que típicamente incluyen macros, o tablas dinámicas muy grandes con más de 50 mil registros, que tomaría tiempo adaptarlos u optimizarlos.
  - Documentos Actualizables re-haciéndolos: documentos que tienen cierta incompatibilidad con estilos o formatos en tablas u otros elementos no estándares que se solucionan rehaciendo el documento en la herramienta de Ofimática Libre.

Procesos institucionales:

- Los procesos sustantivos y adjetivos categorizados deberán evaluarse en conjunto con los niveles de complejidad de migración de documentos, hardware y software.
- Se deberá elaborar una matriz para visualizar los niveles de criticidad y por lo tanto la priorización para migrar, conjugando todos los elementos (procesos, documentos, hardware y software).

Revisión, coordinación y aprobación de cronogramas (P04)

Se revisan los borradores de los planes, estudio de factibilidad, la información relevada, y se trazan estrategias de acción para cada área. Se determinan cronograma de las actividades de cada Plan.

Convocatoria desde la autoridad del comité		P04-01
Actividades	**Entrada**	**Salida**
- Realizar convocatoria desde la autoridad del Comité/Comisión, delegada por la máxima autoridad de la Institución, hacia los miembros del comité/comisión.	Marco Normativo. P03-04	Comunicado de convocatoria a las partes interesadas.

Reunión 02 Esta es una reunión para seguimiento y definición de estrategias con base al diagnóstico.		**P04-02**
Actividades	**Entrada**	**Salida**
- Deberá tener al menos la siguiente agenda: • Revisión del Estudio de factibilidad. • Revisar cronogramas de cada plan. • Revisión de medición de predisposición al cambio. • Definir estrategias de acción.	P03-03 P03-04	Acta de Reunión. Estudio de factibilidad actualizado. Cronogramas actualizados. Planes actualizados.

Guía de la Agenda

Revisión del Estudio de factibilidad técnica: Servirá de base para discutir los puntos críticos y definir las estrategias.

Revisar cronogramas de cada plan: Cada Plan deberá tener su cronograma. En esta etapa deberá ser una primera propuesta general del mismo.

Definir estrategias de acción:

- Definir estrategia de implementación: En base al diagnóstico (P03) se determina en conjunto con las demás unidades del comité, la estrategia de implementación, que deberá contemplar por ejemplo:
  - Las unidades criticas.
  - Las unidades administrativas piloto con quienes se empezará (usualmente unidades menos complejas o menos críticas).
  - Los niveles de criticidad determinará las unidades de inicio y fin.
  - Las tecnologías que son más complejas de implementar podrían quedar al final.
- Definir estrategia de respaldo de datos: Esto debe definirse principalmente por la unidad de TIC, en conjunto con la unidad de Talento Humano o Procesos.
- Definir estrategia comunicacional: Esta estrategia debe considerar tanto la comunicación interna (concienciación), como la comunicación externa, en función de la evaluación ex-ante de predisposición al cambio.
- Definir estrategia de capacitación: Deberá ser coordinada según estrategia de implementación.

Oficializar aprobación del cronograma.		P04-03
Actividades	**Entrada**	**Salida**
- Debe hacerse público, tanto al interior de la institución como a las entidades rectoras y la comunidad, del cronograma y las estrategias determinadas, ya que permitirá mejor coordinación del apoyo tanto de la comunidad como de la entidad reguladora.	P04-02	Documento oficial de aprobación.

Laboratorios (P05)

Este proceso involucra a todas las actividades técnicas para la realización de los laboratorios con el apoyo del personal técnico de la unidad de TICs, proveedores, la academia, incluso la comunidad de software libre.

Se realizarán actividades de capacitación técnica, formal o informal, y en los espacios físicos y electrónicos de colaboración interinstitucional para la resolución de dudas, novedades, en el montaje de los laboratorios.

La entidad reguladora y/o la comunidad podrá recurrir a herramientas tales como foros, listas de correo, call center, manuales, videos, guías de laboratorio, talleres, etc.

Talleres Técnicos TICs		P05-01
Actividades	**Entrada**	**Salida**
Se debe gestionar para el equipo TICs talleres, workshop, cursos, etc. al menos en los siguientes temas: Para área de Soporte a usuario: • Taller Linux nivel Medio. Para área de Informaciones de TI • Taller Linux nivel Avanzado. • Taller Sistemas de Gestión centralizada de: ◦ Autenticación. ◦ Configuraciones, políticas, aprovisionamiento. Workshop Tecnologías Varias.	Marco Normativo. Manuales técnicos, guías, tutoriales. Plan de Capacitación. P03-02	Actas de capacitación Resultado de evaluaciones. Registros de asistencias a talleres, eventos, etc.

Pruebas de Laboratorio		P05-02
Actividades	**Entrada**	**Salida**
Las pruebas de laboratorio deberán enfocarse a los requerimientos del proyecto, explorando las tecnologías libres disponibles para los efectos. • Sistemas Operativos de escritorios. • Ofimática Libre. • Sistemas de Gestión centralizada: ◦ Autenticación. ◦ Configuraciones, políticas, aprovisionamiento.	Marco Normativo. Manuales técnicos, guías, tutoriales. P03-01 P03-04	Actualización estudio de factibilidad. Actualización Plan de Actualización y cronogramas. Manuales y tutoriales.
Guía de las actividades		
Las pruebas deberán dirigirse para lograr los siguientes objetivos: • Sistemas Operativos de escritorios: Determinar distribución de Linux acorde a la realidad del parque tecnológico de la institución y los niveles de predisposición al cambio. • Ofimática Libre: realizar pruebas con los documentos inventariados para determinar y categorizarlos por los niveles de complejidad para Actualizarlos a Tecnologías Libres. • Sistemas de Gestión centralizada ◦ Autenticación: Para sistemas operativos privativos y basados en Linux. Se debe considerar que la implementación será progresiva. ◦ Configuraciones, políticas, aprovisionamiento: Se debe considerar el esfuerzo para las tecnologías libres enfocadas a la gestión de sistemas operativos libres.		

Presentación y Aprobación de Planes (P06)

Ese proceso contempla las actividades de revisión de los pre-release de los Planes, estrategias, cronogramas. Se aceptan y se aprueban los Planes. Se oficializa la aprobación de los Planes, sus cronogramas y el inicio de su ejecución.

Se realiza la comunicación internar y externa del inicio de la ejecución del Plan y su conformidad.

Convocatoria desde la autoridad del Comité		P06-01
Actividades	**Entrada**	**Salida**
- La convocatoria debe ser realizada por la máxima autoridad del Comité/Comisión con el objeto de presentar y aprobar los documentos finales de los Planes respectivos.	Marco Normativo	Comunicado oficial de convocatoria.

Reunión 03 Esta reunión es de revisión y aprobación de los documentos finales de planes.		**P06-02**
Actividades	**Entrada**	**Salida**
La reunión deberá tener al menos la siguiente agenda: • Revisión de Planes. • Resolución de dudas. • Aceptación / Aprobación de los Planes.	P06-01 Plan de Actualización. Plan de Comunicación. Plan de capacitación.	Acta de Reunión. Actualización, firma y aprobación d ellos Planes.
Guía de Agenda		
Revisión de Planes: Se realiza la presentación, revisión de los planes, sus cronogramas y las estrategias. Resolución de dudas: Se solventas todas las dudas que puedan surgir de los planes, los cronogramas, sus actividades y estrategias. Aceptación / Aprobación de los Planes: Se da sentado por acta la aprobación de los Planes y sus fechas de inicio de ejecución.		

Oficializar y socializar la aprobación de los Planes.		**P06-03**
Actividades	**Entrada**	**Salida**
Por medio de documento oficial, los Planes aprobados y firmados por los representantes de las unidades que conforman el Comité, se oficializan y se adjunta a dicho documento. Tanto el documento oficial como el documento de los Planes se socializa con la entidad reguladora y la comunidad.	P06-02	Instrumentación oficial de inicio de ejecución, y socialización.

5.4.2 Implementación

La implementación estará basada en los Planes generados, pero debe tomarse en cuenta que en el orden lógico de ejecución, el componente técnico siempre será el último. Es decir, ser recomienda el siguiente orden de implementación:

- Plan de Concienciación.
- Plan de Capacitación.
- Plan de Actualización.

Podrá ejecutarse en paralelo los planes, desarrollándose pequeñas etapas iterativas de implementación, sin embargo siempre el orden deberán ser incluso en dichas etapas: concienciación, capacitación, implementación.

Implementación del Plan de Concienciación (E01)

Despliegue de campaña		**E01-01**
Actividades	**Entrada**	**Salida**
- Se implementa el Plan de Comunicación, en base a las estrategias definidas. - Se recurre a los distintos medios, y fases de la campaña que se debió detallar en el plan de comunicación.	Plan de Comunicación. Marco Normativo. Contenido recabado sobre el estado del arte en tecnologías libres, a nivel social.	Contenidos. Programa de despliegue. Respaldos de boletines, mail, memes enviados. Actas de participación. Registro gráfico.
Guía de las actividades		
Se sigue el plan, las actividades, estrategias y cronogramas para la ejecución de actividades como estas: Envío de boletines: por medio de correo electrónico a los servidores públicos. Difusión de memes: por medio de correo electrónico a los servidores públicos, y/o redes sociales para difusión hacia afuera, o cualquier otro social-media. Tipos de Contenidos: • Marco normativo: Como parte de las campañas debe socializarse elementos puntuales del marco normativo en relación al cumplimiento de los procesos de actualización a tecnologías libres, y de adquisición del software. • Casos de éxito: de otras instituciones públicas en Ecuador, o en a nivel Internacional. • Tendencia, noticias internacionales sector público: Iniciativas en el sector público de distintos países, incluyendo la Región. • Tendencia, noticias internacionales sector privado: Iniciativas, apoyo, inversión, proyectos conjuntos del sector privado en proyectos de software libre. Charlas de concienciación segmentada, convocadas desde la máxima autoridad: • Para autoridades. • Para servidores públicos, personal de apoyo. • Para unidad TICs. Entrega de certificados de participación en las Charlas		

Evaluación Concienciación		E01-02
Actividades	**Entrada**	**Salida**
Esta evaluación se debe realiza después de impartidas las charlas, con el objeto de medir el nivel de predisposición al cambio que pudiera haber incidido las charlas.	Plan de Comunicación. E01-01	Resultados de encuestas. Actualización de Comunicación.
Guía de las actividades		
Deberán considerarse al menos las siguientes actividades: • Diseño de encuestas. • Envío de encuesta. • Medir resultados. • Retroalimentar procesos de concienciación.		

Implementación del Plan de Capacitación (E02)

La capacitación más fuerte será la centrada al personal TICs, como responsables de la infraestructura tecnológica, y la continuidad de su operación.

Despliegue de programas de capacitación		E02-01
Actividades	**Entrada**	**Salida**
La unidad de Talento Humano deberá tener a cargo la ejecución del Plan de Capacitación como documento guía y el Comité deberá dar seguimiento al mismo.	Plan de Capacitación. Cronogramas	Actas de participación
Guía de las actividades		
Deberán tenerse en cuenta al menos las siguientes actividades: • Gestionar recursos y medios para la realización de las capacitaciones necesarias. • Coordinar grupo, fecha, hora, lugar, instructores. • Convocatoria oficial desde autoridad del Comité/Comisión. • Realizar capacitación de manera presencial o medios virtuales. • Registro de participación y resultados. • Entrega de certificados. Las capacitaciones técnicas deberán estar orientadas a lo siguiente: • Marco Normativo. • Capacitación sobre Ofimática Libre. • Escritorio del Sistema Operativo Libre seleccionado. • Herramientas Libres para Gestión centralizada de Autenticación/Configuración y aprovisionamiento.		

Evaluación del programa de capacitación		E02-02
Actividades	**Entrada**	**Salida**
Debe realizarse, antes, durante y al final de las mismas, considerando: • Temáticas y personal estimado a recibir capacitación. • Personal inscrito que están recibiendo capacitación. • Personal que ha finalizado y aprobado las capacitaciones.	E02-01	Informe de evaluación
Guía de la Actividad		
- La Unidad de Talento Humano: • Deberá llevar registro del personal que inscrito en los cursos de capacitación, sean estos presenciales o virtuales. Deberá llevar también un registro de quienes han culminado y aprobado los cursos. • Deberá gestionar la entrega de certificados de aprobación de los cursos e incluirlos en el historial de los servidores públicos. • Deberá realizar capacitaciones y evaluaciones periódicas hasta asegurarse la completitud de los cursos y su aprobación, de la totalidad de los servidores públicos involucrados, incluyendo a quienes se van incorporando a la institución. - Certificaciones: • Los servidores públicos podrán certificarse mediante entidades certificadoras avaladas por la SETEC, para dar acreditación formal de sus conocimientos.		

Implementación del Plan de Actualización (E03)

Despliegue del Plan de Actualización		E03-01
Actividades	**Entrada**	**Salida**
Se realiza la instalación de los elementos de infraestructura para la gestión centralizada de las estaciones de trabajo (equipos de usuario).	Plan de Actualización. P04-02	Modificaciones o ajustes al Plan de Actualización a Tecnologías Libres.
Guía de las actividades		
Puesta en producción de la infraestructura: Antes de iniciar el despliegue de los equipos de usuarios es necesario iniciar la puesta en producción de Infraestructura, que comprende: • Sistemas de Autenticación para Sistemas Operativos Libres y su integración con sistemas no libres. • Sistema de Gestión centralizada de configuraciones y aprovisionamiento para sistemas con tecnologías libres. Puesta en producción de sistemas de escritorio: El despliegue de la actualización de los equipos de escritorios, debe empezar por un Grupo Piloto que debió determinarse en la definición de estrategias. Se deberá tomar en cuenta las normativas en relación a la seguri-		

dad de la información, para la salvaguarda de los documentos de los usuarios. Despliegue por fases: Se estima como fase 0 el grupo piloto, a posterior surgirán distintas fases consecutivas según la estrategia definida, tomando en cuenta que siempre será un proceso progresivo.

Evaluación del despliegue		**E03-02**
Actividades	**Entrada**	**Salida**
La evaluación del despliegue, como un proceso constante, debe tener en cuenta al menos las siguientes actividades: • Registro de soporte solicitado. • Registro de incidentes. • Determinación, documentación de soluciones. • Socialización de soluciones a incidentes o soporte solicitado.	E03-01 E03-02	Documentos de soluciones y recomendaciones. Modificaciones o mejoras a los Planes.
Guía de las actividades		
Desde las pruebas de laboratorio hasta la fase de implementación se deberán registrar y actualizar la documentación de solución de incidentes. Debe asignarse un equipo para ello, el cual entrará una vez que se ha realizado el despliegue de un grupo o fase. Esta actividad puede estar a cargo de personal de apoyo como prácticas pre-profesionales o pasantías, coordinadas por persona de la unidad de Tecnología de la institución.		

5.4.3 Evaluación y Mejoras

Presentación de Informes y evaluación. (C01)

Convocatoria desde la máxima autoridad del Comité.		**C01-01**
Actividades	**Entrada**	**Salida**
Esta última convocatoria, debe realizarse desde la autoridad del Comité, con el objeto de evaluar y cerrar la etapa de implementación. Se dará inicio a nuevas etapas o nuevos proyectos de Actualización a Tecnologías Libres.	E03-02	Comunicado de convocatoria.
Guía de las actividades		
Se deberá convocar a los miembros del comité o sus delegados que deberán informar sobre los avances.		

Reunión 04		C01-02
Actividades	**Entrada**	**Salida**
La reunión deberá tener al menos la siguiente agenda: • Presentar resultados de la implementación de los Planes. • Determinar continuidad de los Planes. • Determinar nuevos proyectos de Actualización a Tecnologías Libres.	E03-02	Acta de Reunión. Informe de Cierre. Recomendaciones para mejora continuación.
Guía de las actividades		
Se debe contar con todos los informes, y sustentos de ejecución del proyecto. • Avances de la implementación, avances de capacitación y evaluaciones, avances de los procesos de concienciación y evaluaciones. • Informe de excepciones con sus autorizaciones. • Registro de novedades e inconvenientes y acciones tomadas. • Registro de procesos institucionales que pudieran automatizarse para no depender de ofimática. • Nuevas etapas sugeridas para la continuidad del proyecto de actualización a tecnologías libres.		

Socializar resultados y Oficializar siguiente etapa		C01-03
Actividades	**Entrada**	**Salida**
Se socializa a las autoridades y entidad rectora, además de la comunidad los resultados del proyecto. Se determina los nuevos proyectos y etapas futuros, los cuales también se socializan.	C01-01 C01-02 E03-02	Acta de inicio de siguiente etapa.
Guía de las actividades		
Se oficializa a través de Acta la programación de las etapas subsiguientes del proyecto de Actualización a Tecnologías Libres de la Institución. Se consideran y estiman los recursos monetarios y no monetarios. La socialización de los resultados se realizará por los medios de comunicación establecidos, que podrían ser: • redes sociales, • sitio web, • comunidades de tecnologías libres, • entidad rectora.		

5.5 Gestión del Riesgo

Tomando el enfoque de la metodología OSSTMM se buscará el balance adecuado entre "seguridad" (security) y "controles" (safety) basada en la separación entre activo y las posibles amenazas.

En este sentido, existen tres maneras lógicas y proactivas de crear esta separación entre el activo y las posibles amenazas (ver capítulo 2.3). De estas, las dos primeras son aplicables en el proceso de Actualización a Tecnologías Libres.

Es decir, que más del 90% del malware existente para sistemas operativos de escritorio es creado para sistemas privativos[20], y el impacto en los sistemas libres es sustancialmente menor que en los privativos[21], lo cual indica que estaríamos moviendo las amenazas por malware a un estado inofensivo, y al cambiar el sistema operativo de escritorio privativo por Libre, estaríamos creando una barrera físico/lógica entre el activo y la amenaza.

Los controles son un medio para influir en el impacto de las amenazas y sus efectos cuando se requiere interacción con el activo. El hecho de que no se pueda controlar directamente la amenaza, no significa que no se la pueda controlar. Es decir, la máxima es "controla el entorno y controlas todo lo que hay en él".

En este sentido, las políticas de seguridad y la gestión centralizada de autenticación, aprovisionamiento, configuraciones y actualizaciones son parte de los controles a implementar para cubrir el margen restante de posibilidad de ataque por malware, basado en la norma nacional NTE INEN-ISO/IEC 27002. recomendada por el EGSI.

El modelo multi-capas establece que los enfoques basados en el riesgo para la selección y especificación del control de seguridad deben considerar no solo la eficacia y la eficiencia, sino también las restricciones debido a leyes nacionales aplicables, las órdenes ejecutivas, directivas, políticas, regulaciones, normas y directrices.

Evaluación de alto nivel del riesgo para presentar el proyecto.

Considerando el enfoque multi-nivel, la evaluación del Riesgo deberá centrarse en las dos capas superiores, esto es, en el cumplimiento de los objetivos nacionales (anexo F) y los objetivos institucionales.

Es decir, se deberán analizar las implicaciones entre: a) mantener situación actual (software pirata), b) regularizar adquisición de licencias, c) decidir iniciar proyecto de Actualización a Tecnologías Libres.

Se plantean a continuación dos ejemplos de escenarios de riesgos, en relación a sostener situación actual:

IMPACTO	AMENAZA	VULNERABILIDAD
ESCENARIO 1		
Afectación a la imagen institucional y política.	- Demanda judicial. - Observación de ente de regulación y control.	- Sistema operativo y ofimática sin licencias (software pirata)
ESCENARIO 2		
Afectación al servicio al ciudadano (misión).	- Ataques de virus, malware, demás software malicioso como ransomware, spyware, etc	- Sistemas operativos y ofimática crackeado con antivirus.

Se plantean a continuación dos ejemplos de escenarios de riesgos, en relación a la adquisición de licencias:

IMPACTO	AMENAZA	VULNERABILIDAD
ESCENARIO 1		
Afectación a la economía, y a la imagen institucional y política.	- Observación del ente de regulación y control por incumplimiento COESCCI, y objetivos nacionales del Plan Nacional de Desarrollo. - Alto porcentaje (85%) del costo de las licencias corresponde a salida de divisas.	- Sistema económico dolarizado y en recesión.
ESCENARIO 2		
Afectación a la soberanía.	- Alianzas de Agencias internacionales de seguridad con empresas de sistemas masivos (sistemas operativos), para espionaje global.	- Se está utilizando sistemas operativos y ofimática privativos de empresas que colaboran con espionaje global, que además está crackeado.

Evaluación del Riesgo en la ejecución del proyecto.

A continuación se presenta un ejemplo de cómo de podría evaluar el riesgo para el proyecto de Actualización a Tecnologías Libres de escritorios de usuarios, en función de las amenaza, vulnerabilidades listados en el anexo C.

Se identifican como activos primarios:

- Los procesos: Institucionales sustantivos, los que dependan de tecnología privativa.
- La información: documentos de ofimática necesarios para los procesos sustantivos, documentos que dependan de formatos privativos no interoperables, información confidencial.

Se identifican como activos de apoyo:

- Computadores de escritorio, impresoras y escaneadores.
- Software necesario para la ejecución de procesos institucionales: sistema operativo, ofimática y software complementario de escritorio, aplicativos institucionales.

Identificación de consecuencias

Escenario: Mala predisposición al cambio que afecte a la operatividad institucional.

Amenaza: Desinformación que produce poca o nula predisposición al cambio.

Vulnerabilidad: poca conciencia sobre tecnologías libres, y sobrecarga laboral.

En Ecuador, la desinformación acerca de las tecnologías libres es un hecho que se ha reflejado en los debates del COESCCI en la Asamblea. Esta desinformación ha tocado incluso a las autoridades, y no han tenido más espacios de debate público. La poca conciencia sobre las tecnologías en los usuarios y la ciudadanía en general, es un tema crítico para estos procesos.

ESCENARIO									
PROBABILIDAD AMENAZA	**BAJA**			**MEDIA**			**ALTA**		
EXPLOTACIÓN VULNERABILIDAD	B	M	A	B	M	A	B	M	**A**
VALOR PROBABILIDAD ESCENARIO	0	1	2	1	2	3	2	3	**4**

La predisposición al cambio, que podrá determinarse en las encuestas de evaluación inicial previo a los procesos de concienciación, indicarán el nivel de impacto a la operatividad que se podría esperar. En caso de una mala predisposición por desconocimiento de las motivaciones del proyecto y sus beneficios nacionales podrían generar un fuerte impacto.

ESCENARIO	PROB.	MB	B	M	A	MA
IMPACTO	MB	0	1	2	3	4
	B	1	2	3	4	5
	M	2	3	4	5	6
	A	3	4	5	6	7
	MA	4	5	6	7	8

En consecuencia, será necesario poner mucho esfuerzo en los controles orientado a los procesos de concienciación y capacitación de los usuarios en las etapa adecuadas, para mitigar el riesgo de afectación a la operatividad institucional.

5.6 Métricas e Indicadores

Proceso	Métrica	Indicador
PLANIFICACIÓN		
Conformación del Comité/Comisión de ASL (P01)	Documento de oficialización del Comité/Comisión	Ejecutado
Asignación de Tareas (P02)	$\frac{[docs(salida)entregados]}{[total\,docs(salida)]}$	% Ejecución 100% esperado.
Diagnóstico (Análisis y recopilación) (P03)	$\frac{[docs(salida)entregados]}{[total\,docs(salida)]}$	% Ejecución 100% esperado.
	$\frac{\#\,usuarios\,afines\,al\,cambio}{Total\,usuarios}$	% Aceptación al cambio: 0%-10% crítico, 10%-30% esperable,

		30%-50% aceptable, 50%-100% idóneo.
Revisión, coordinación y aprobación de cronogramas (P04)	$\frac{[docs(salida)entregados]}{[totaldocs(salida)]}$	% Ejecución 100% esperado.
Laboratorios (P05)	$\frac{Participantes\ capaciación}{Total\ servidores\ públicos\ TIC}$	% asistentes 80% aceptable
	$\frac{cantidad\ servicio\ probados}{Total\ servicio}$	% pruebas 100% esperado.
Presentación y Aprobación de Planes (P06)	Documento oficial de aprobación	Ejecutado
EJECUCIÓN		
Implementación del Plan de Concienciación (E01).	$\frac{campañas\ desplegadas}{Total\ campañas}$	% Ejecución 100% esperado.
	$\frac{participantes}{Total\ servidores\ públicos}$	% Ejecución 100% esperado.
	$\frac{\#\ usuarios\ afines\ al\ cambio}{Total\ usuarios}$	% Aceptación al cambio: 0%-30% crítico, 30%-60% aceptable, 60%-100% idóneo.
	$\frac{\%\ aceptación\ ex-post}{\%\ aceptación\ ex-ante}-1$	% incremento aceptación
Implementación del Plan de Capacitación (E02)	$\frac{Aprobados}{Participantes}$	% aprobados 0%-50% critico 50%-80% aceptable 80%-100% idóneo
	$\frac{Participantes}{Total\ servidores\ públicos}$	% participantes 80%-100% aceptable
	Informe estadísticas	Entregado
Implementación del Plan de Actualización (E03)	$\frac{Equipos\ actualizados}{Total\ equipos}$	% equipos actualizados
CONTROL Y SEGUIMIENTO		
Presentación de Informes y evaluación. (C01)	Realizado	Realizad

6 Conclusiones

Una migración a cualquier tecnología no debe considerarse un proceso plug-and-play; entre otras cosas se debe tener en cuenta el componente humano en mayor o menor grado según el tipo y alcance del proyecto. Este trabajo ha presentado una guía para aplicar las buenas prácticas documentadas en modelos y marcos de referencia de gestión de la seguridad de la información aceptados internacionalmente, para garantizar un buen camino en este tipo de proyectos, especialmente los de migración a tecnologías libres.

Se hace énfasis en observar los elementos tecnológicos como un componente más, no como un fin en sí mismo; sobre todo en ambientes gubernamentales en los que debe congeniarse lo tecnológico con los objetivos nacionales y los marcos de referencia de gestión de seguridad de la información.

Se tomó el modelo de implementación para un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, como elemento importante para el proyecto de migración, teniendo como uno de sus componentes la implementación y operación de controles para el manejo de los riesgos relacionados y los programas de concienciación y entrenamiento.

Con un enfoque desde la perspectiva de procesos, el marco de trabajo COBIT 5 para la Seguridad de la Información, y las normas técnicas para establecer un SGSI, fueron elementos de referencia que permitieron como resultado proponer un Modelo de Gestión para un proyecto de Actualización a Tecnologías Libres de escritorios de usuarios.

Para el análisis de riesgos, el modelo multi-capas de la norma NIST SP-800-39, que sugiere una perspectiva desde una dimensión de nivel superior que en este trabajo se ha denominado como "Estado", permitió considerar los impactos a nivel de país. A su vez, el enfoque de alto nivel propuestos por la norma ISO/IEC 27005 basado en escenarios fue considerado como recurso para la toma de decisiones de la máxima autoridad con el objeto de conseguir su autorización y patrocinio, incorporando el marco normativo y los objetivos nacionales expresado en la Constitución y el Plan Nacional de Desarrollo.

De esta manera se propone considerar no sólo los escenarios de incidentes relacionados a la institución en aspectos tecnológicos sino también los relacionados al país para alcanzar los objetivos nacionales, en aspectos sociales y de seguridad integral; acotando los escenarios al alcance del proyecto, es decir, considerando los activos, amenazas, vulnerabilidades y consecuencias exclusivamente enmarcados en la migración de escritorios de usuarios.

Aunque es posible la aplicación del modelo para cualquier proceso de Actualización a Tecnologías Libres en el sector público, debe tenerse en cuenta que en el caso de escritorios de usuarios implica enfoques distintos de procesos de concienciación. En el caso de infraestructura tecnológica, el impacto al cambio podría ser menor, ya que todos los esfuerzos estarían reducidos al personal de TI.

En la actualización de escritorios el impacto es sobre todo al usuario final, que son los encargados de la ejecución de los procesos que dan la vida a la organización. Por lo tanto, en una institución de cientos o miles de funcionarios con un débil proceso de gestión del cambio podría ser extremadamente contraproducente para la operatividad de la institución, afectando gravemente a la imagen y al servicio al ciudadano, por tal motivo es importante observar el énfasis en la cultura organizacional y la gestión del cambio en toda la institución.

Se puede inferir que en un ambiente gubernamental, la gobernabilidad de proyectos de Actualización a Tecnologías Libres debería ser coordinada y liderada por una

entidad estatal que dé institucionalidad, además de coherencia en la alineación de los objetivos institucionales y nacionales que deriven en procesos horizontales de actualización a tecnologías libre y programas de concienciación; con el objeto de alcanzar una gestión óptima de recursos, y la generación y control de indicadores de gestión globales.

7 Anexos

7.1 Anexo A: Marco Normativo Nacional[14]

Ley, Plan, Acuerdo, Decreto, Resolución
Constitución de la República del Ecuador
Plan de Gobierno Electrónico
Esquema Gubernamental de la Seguridad de la Información
Ley de Seguridad Pública y del Estado.
Ley Orgánica de Transparencia y Acceso a la Información Pública.
Ley Orgánica del Sistema Nacional de Contratación Pública
Codificación de Resoluciones del SERCOP
Código Orgánico de Planificación y Finanzas Públicas.
Código Orgánico de la Economía Social de los Conocimientos Creatividad e Innovación.
Declaración sobre el Derecho al Desarrollo
Decreto Ejecutivo 1425 (22 mayo 2017)
Decreto Ejecutivo 5 (24 mayo 2017) – Supresión de la SNAP y atribuciones a MINTEL
Decreto Ejecutivo 64 (6 Julio 2017) – Planes de factibilidad de migración a tecnologías libres
Decreto Ejecutivo 135 (1 septiembre 2017) – Optimización y austeridad del gasto público.
Decreto Ejecutivo 163 (18 septiembre 2017) - Reforma DE 149, 1384, 1425 Plazos y competencias.

[14] Un detalle del articulado relevante de las normas puede encontrarse en: https://www.migralab.ec/resumen-marco-normativo/

7.2 Anexo B: Activos y Tipos de Información

TIPO	CATEGORÍA	ACTIVOS
Primarios	Procesos y actividades del negocio	Procesos, servicios internos (adjetivos)
		Procesos, servicios al ciudadano (sustantivos)
	información	Datos, documentos del servidor público
Apoyo	Hardware	Computadores de escritorio
		Computadores portátiles
		Impresoras
		Scanner
	Software	Sistema Operativo de escritorio
		Software de administración
		Software base complementario de escritorio
		Aplicativos institucionales
		Software de ofimática
	Personas	Autoridades
		Funcionarios
		Apoyo TIC
	Infraestructura	Servidor de Gestión de Autenticación y Políticas
		Servidor de Gestión de Configuraciones
		Servidor de Monitoreo

Grupos de Interés relacionados al proyecto de ASL												
Aprobador, **O**riginador, **I**nformado, **U**suario.	**Parte Interesada**											
Tipo de Información	**Comisión/Comité**	**Unidad Planificación**	**Unidad Talento Humano**	**Unidad Gestión del Cambio**	**Unidad de Comunicación**	**Unidad Tecnología**	**Máxima Autoridad**	**Soporte TI**	**Infraestructura TI**	**Todas las unidades Administrativas**	**Usuarios**
• Estrategias de Actualización a Software Libre	**A**	**O**	**O**	**O**		**O**	**I**	**O**	**O**		
• Presupuesto POA / PAC	**A**	**O**	**O**	**O**		**O**	**A**	**U**	**U**		
• Plan de Actualización a Software Libre	**A**					**O**					
• Plan de Comunicación	**A**				**O**						
• Plan de Capacitación	**A**		**O**								
• Políticas y Marco Normativo	**I**	**U**	**U**	**U**	**U**	**U**	**U**	**U**	**U**		**U**
• Plantillas de aprovisionamiento de equipos de escritorios			**I**	**I**		**A**			**O**		
• Material para la Concienciación (Insumo para el Plan de Comunicación)	**A**			**O**		**O**				**U**	**U**
• Registro y análisis de riesgos	**O**						**A**				
• Análisis de amenazas	**A**					**O**					
• Informe de evaluación de vulenrabilidades	**A**					**O**					
• Catálogo de procesos y servicios afectados	**A**		**O**				**A**				
• Inventarios de hardware y software	**A**					**I**		**O**	**O**		
• Métricas e indicadores de evaluación de predisposición al cambio	**A**			**O**							
• Métricas e indicadores de beneficios e impactos.	**I**			**O**		**O**	**A**				

7.3 Anexo C: Amenazas y vulnerabilidades

Amenazas

La siguiente tabla muestra un conjunto de amenazas en la situación actual, previo a iniciar un proyecto de Actualización a Tecnologías Libres.

AMENAZAS	PROBABILIDAD OCURRENCIA	SUSTENTO
Poca disponibilidad de recursos económicos.	ALTA	- Se ha emitido Decreto Ejecutivo 135 de austeridad y optimización de los recursos.
Acceso externo no autorizado a información crítica de los equipos.	ALTA	- No tener acceso al código fuente imposibilita su auditoria/escrutinio, quedando el control en el proveedor o dueño del software. - Los procesos de desarrollo colaborativo, y sus controles minimizan posibilidad de inclusión de puertas traseras. - Casos como StuxNet[15] y los documentos revelados por Edward Snowden en el 2013 evidencian incorporación de puertas traseras por diseño.[16]
Inclusión de puertas traseras o defectos por diseño	ALTA	
Espionaje remoto	ALTA	
Manipulación con software	ALTA	
Desinformación que produce poca o nula predisposición al cambio	ALTA	- Existe posibilidad que partes adversas al proceso de cambio genera desinformación sobre calidad/confianza en el software de tecnologías libres. Esto se ha evidenciado en el país por parte de los representantes de la industria local.
Ataque de virus, spyware, malware al sistema operativo	ALTA	- Estadísticas indican que menos de 1% de los casos de ataques de virus son a sistemas operativos basados en Linux. - La publicación del código fuente facilita su auditoria/escrutinio y un rápido ciclo de desarrollo y actualizaciones. - Los procesos de desarrollo colaborativo, y sus controles minimizan posibilidad de inclusión de puertas traseras, lo que no sucede con software privativo.
Liberación lenta de actualización o parches.	MEDIA	- La liberación de parches/actualizaciones se hace casi inmediatamente encontrado las vulnerabilidades en el caso de tecnologías libres.

[15] Virus informático que atacó infraestructura crítica del programa nuclear Iraní. Estudios indican que el virus fue creado entre Estados Unidos e Israel para sabotear el programa nuclear Iraní. Investigaciones posteriores dan información que el virus atacó vulnerabilidades zero day del sistema operativo en los equipos objetivos, vulnerabilidades destinadas a facilitar la entrada del virus. Más información puede encontrarse en el artículo: https://www.migralab.ec/2017/08/11/stuxnet-el-software-como-herramienta-de-control-geopolitico/

[16] En el 2013 Edward Snowden filtró documentos de la NSA en la que, entre otras cosas, se daba a conocer las alianzas con grandes multinacionales tecnológicas para la colaboración en el espionaje masivo mundial. Más información puede encontrarse en este artículo: https://rafael.bonifaz.ec/blog/2017/11/la-nsa-segun-las-revelaciones-de-snowden/

		Las actualizaciones son frecuentes. - El software privativo tiene tiempos más largos de liberación de parches. En muchas ocasiones la divulgación de una vulnerabilidad inmediata puede representar impactos económicos en la empresa dueña del software.[17]
Difusión de software malicioso	ALTA	- Las estadísticas indican que la probabilidad de infección de un sistema operativo basado en Linux es menor al 1%, y su propagación aún menor. - Las instituciones mantiene los sistemas operativos de escritorio sin licencia, sin recursos para poder adquirirlas, lo cual implica crackear los sistemas exponiéndolos a software malicioso.
Falla en funcionamiento de dispositivos por incompatibilidad	BAJA	- Los sistemas operativos privativos usualmente funcionan con la mayoría de dispositivos.

La siguiente tabla muestra un conjunto de amenazas en relación al proyecto de Actualización a Tecnologías Libres.

AMENAZAS	PROBABILIDAD OCURRENCIA	COMENTARIO
Acceso no autorizado al equipo	BAJA	- La arquitectura de los sistemas Linux o basados en Unix permiten mejor seguridad nativa que otros sistemas comerciales. - Se mantienen controles combinando la arquitectura de los sistemas operativos basados en Linux con un IDM, sistemas de gestión de políticas y auditoría.
Sobrecarga de tareas	ALTA	- La carga operativa de los servidores públicos podría acumularse y ser excesiva en caso de fallos en los equipos, o durante los procesos de migración producto del cambio y adaptación.
Falla en proceso de capacitación continua	MEDIA	- Es necesario procesos de capacitación previo a implementar la migración, caso contrario podría afectar a la operatividad.
Corrupción de los datos	BAJA	- Los casos de corrupción de datos pueden darse por ausencia de controles, no por fallas del sistema operativo.
Saturamiento de los sistemas en el equipo de escritorio	BAJA	- Es improbable que los equipos sufran sobrecarga de trabajo por efectos de virus o malware que colapsen el sistema.

[17] Telang, Rahul, y Sunil Wattal. «An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price» 33, n.o 8 (2007): 544-57. https://www.heinz.cmu.edu/~rtelang/tse_published.pdf.

Vulnerabilidades.

La siguiente tabla muestra las vulnerabilidades que pueden ser explotadas por las amenazas, para el caso de tecnologías libres y software privativo.

VULNERABILIDAD	AMENAZAS	*LIBRE*	*NO LIBRE*
Falta de actualizaciones o parches del sistema operativo	Ataque de virus, spyware, malware al sistema operativo	BAJA	MEDIA
software crakeado (copia ilegal del software)	Difusión de software malicioso Desinformación que produce poca o nula predisposición al cambio	BAJA	ALTA
software no autorizado	Difusión de software malicioso	BAJA	ALTA
antivirus sobre sistema operativo crackeado	Difusión de software malicioso Desinformación que produce poca o nula predisposición al cambio	BAJA	ALTA
Incompatibilidad de drivers	Falla en funcionamiento de dispositivos por incompatibilidad	MEDIA	BAJA
Imposibilidad de auditoría del código fuente.	Inclusión de puertas traseras o defectos por diseño	BAJA	ALTA
Perfil de usuario no limitado.	Falla en proceso de capacitación continua	MEDIA	BAJA

La siguiente tabla muestra las vulnerabilidades que pueden ser explotadas por las amenazas en el caso específico de Actualización a Tecnologías Libres.

VULNERABILIDAD	AMENAZAS	*LIBRE*	*NO LIBRE*
Desconocimiento de normativas	- Desinformación que produce poca o nula predisposición al cambio	ALTA	BAJA
Falta de concienciación sobre tecnologías libres			
Pobre cultura organizacional			
Uso poco eficiente de las herramientas	- Falla en proceso de capacitación - Poca disponibilidad de recursos económicos. - Sobre cargas de tareas	ALTA	BAJA
Falta de conocimiento ofimática libre y escritorio linux.			

7.4 Anexo D: Procesos COBIT 5 para la Seguridad de la Información, de base adaptados.

Tomando el modelo de procesos de COBIT 5 para la seguridad de la información, podemos realizar una adaptación reduciéndolo a lo que es relevante para la propuesta del presente trabajo. En esta adaptación se han mantenido los mismos códigos de procesos para un fácil relacionamiento con los procesos originales del modelo de procesos de COBIT 5.

Procesos de Gobierno

Asegurar el establecimiento y mantenimiento del Marco de Gobierno (EDM01)

Este proceso proporciona un enfoque consistente e integrado con el enfoque de gobierno institucional, para garantizar que las decisiones respecto a las tecnologías libres estén alineadas a los objetivos institucionales y nacionales.

Métricas:

- Número de procesos de negocio y de TI en los que las tecnologías libres están integradas.

Evaluar el Sistema de Gobierno Identificar a las partes interesadas (áreas involucradas) y comprometerlas. Realizar estimación actual y futura de la gobernabilidad del proyecto.		**EDM01-01**
Prácticas y Actividades	**Entrada**	**Salida**
- Evaluar el grado en que las tecnologías libres cumplen con las necesidades institucionales.	- Marco Normativo Nacional. - Marco Normativo Institucionales. - Principios Fundamentales de las Tecnologías Libres.	Principios que rigen la utilización de tecnologías l ibres en el Estado.

Orientar el Sistema de Gobierno Informar a la máxima autoridad institucional y de las áreas involucradas, y obtener apoyo de la máxima autoridad. Definir la información necesaria para la toma de decisiones.		**EDM01-02**
Prácticas y Actividades	**Entrada**	**Salida**
- Obtener compromiso de la máxima autoridad.	EDM01-01	Cultura y entorno favorable para la Actualización a Tec-

- Asignar un comité/comisión para el proyecto, con funciones de alcance global. - Alinear estrategia a los objetivos institucionales y nacionales. - Fomentar el entorno y cultura favorables.	AP002-05	nologías Libres.

Supervisar el Sistema de Gobierno Analizar si el sistema de gobernabilidad y los mecanismos implementados operan adecuadamente y proporcionan supervisión apropiada a TI y el cumplimiento de las directrices.		**EDM01-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Supervisar los mecanismos para garantizar que las tecnologías seleccionadas cumplen con los marcos normativos nacionales, institucionales.	- Marco Normativo Nacional - Marco Normativo Institucionales. EDM01-01	Evaluación del cumplimiento.

Asegurar la Entrada de Beneficios (EDM02)

Este proceso tiene como meta asegurar que los beneficios, costos, riesgos de las inversiones o recursos (sean estas en términos monetarios o recursos internos), para los proyectos de Actualización a Tecnologías Libres son equilibradas, gestionadas y además contribuyen en su valor óptimo.

Métricas:

- Nivel de satisfacción de las partes interesadas con las medidas relativas a tecnologías libres existentes, basado en encuestas.

Evaluar la Optimización de Valor Evaluar continuamente los servicios, activos, inversiones, recursos para poder determinar la probabilidad de alcanzar los objetivos institucionales y nacionales.		**EDM02-01**
Prácticas y Actividades	**Entrada**	**Salida**
- Identificar y registrar requisitos de las partes interesadas y aportar valor por medio del proyecto de Actualización a Tecnologías Libres.	Evaluación del alineamiento estratégico.	Portafolio actualizado.

Orientar la Optimización de Valor Orientar principios y prácticas de gestión de valor respecto a las tecnologías y demás recursos institucionales.		**EDM02-02**
Prácticas y Actividades	**Entrada**	**Salida**
- Establecer un método para demostrar el valor del proyecto de Actualización a Tecnologías Libres, para el uso eficiente de los recursos. - Asegurar el uso de medidas financieras y no financieras para describir el valor aportado. - Usar métodos enfocados a los objetivos institucionales y nacionales para la comunicación del valor aportado por las iniciativas.	Tipos y criterios de decisión respecto a las tecnologías y demás recursos institucionales.	Tipos y criterios de decisión respecto a las tecnologías y demás recursos institucionales, actualizados.

Supervisar la Optimización de Valor Supervisar indicadores claves y sus métricas para determinar el grado en que la institución, y el País está obteniendo el valor y los beneficios esperados.		**EDM02-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Seguir los resultados de las iniciativas en relación al proyecto de Actualización a Tecnologías Libres y compararlos con las expectativas para asegurar la entrega de valor frente a los objetivos institucionales y nacionales.		Retroalimentación sobre el valor aportado por las iniciativas.

Asegurar la Optimización del Riesgo (EDM03)

La gestión del Riesgo asociado al proyecto de Actualización a Tecnologías Libres debe formar parte de las decisiones institucionales, y de la gestión general de los riesgos institucionales y nacionales.

Métricas:

- Porcentaje del riesgo de la Actualización a Tecnologías Libres en relación con el riesgo institucional global.

- Porcentaje de riesgos institucionales mitigados con tecnologías libres en relación con los riesgos mitigados con tecnologías no libres.

Evaluar la Gestión del Riesgo Examinar y evaluar permanentemente el efecto del riesgo sobre la situación previa y posterior al proyecto de Actualización a Tecnologías Libres. Considerar el apetito al riesgo institucional y si este es el adecuado, identificado y gestionado.		**EDM03-01**
Prácticas y Actividades	**Entrada**	**Salida**
- Determinar el apetito al riesgo. - Medir el nivel de integración de la gestión del riesgo con el modelo general de gestión de riesgo institucional.	- indicadores clave del riesgo institucional. (KRI) - Orientación sobre el apetito al riesgo.	Alineamiento de los KRI de la institución con los del proyecto. Nivel aceptable del riesgo.

Orientar la Gestión del Riesgo Orientar la elaboración de prácticas de la gestión del riesgo del proyecto para que no exceda el apetito del riesgo.		**EDM03-02**
Prácticas y Actividades	**Entrada**	**Salida**
- Integrar la gestión del riesgo del proyecto con el modelo general de gestión de riesgo institucional.	EDM03-01	Políticas de gestión del riesgo actualizadas.

Supervisar la Gestión del Riesgo Supervisar los objetivos y las métricas claves de los procesos de gestión de riesgo.		**EDM03-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Supervisar el perfil del riesgo del proyecto o el apetito de riesgo, para lograr un equilibrio óptimo entre riesgos y oportunidades institucionales. - Incluir los resultados de los procesos de gestión del riesgo del proyecto a la gestión de riesgo institucional.	EDM03-01 AP001-03	Acciones correctivas para solventar desviaciones en la gestión del riesgo.

Asegurar la Optimización de Recursos. (EDM04)

Asegurar que las necesidades de talento humano y recursos, sean estos procesos o tecnologías, son cubiertas de un modo óptimo, y que los costos en tecnologías son optimizados e incrementan la posibilidad de obtener beneficios.

Métricas:

- Estudio comparativo del gasto a largo plazo en soluciones con tecnologías libres en relación a las alternativas privativas.
- Cuantía de la desviación respecto al presupuesto asignado para tecnologías libres.
- Porcentaje de reutilización de soluciones de tecnologías de la información.

Evaluar la Gestión de Recursos Examinar y evaluar continuamente la necesidad actual y futura de los recursos tecnológicos.		**EDM04-01**
Prácticas y Actividades	**Entrada**	**Salida**
- Evaluar la eficacia de los recursos tecnológicos en términos de: suministro, formación, concienciación y competencias de los recursos en relación con las necesidades institucionales.	Plan de recursos aprobado.	Recursos tecnológicos actualizados.

Orientar la Gestión de Recursos Asegurar la adopción de principios de gestión de recursos asociados a los principios institucionales y nacionales.		**EDM04-02**
Prácticas y Actividades	**Entrada**	**Salida**
- Asegurar que la gestión de los recursos tecnológicos estén alineados con las necesidades del negocio.	Asignación de responsables para la gestión de recursos.	Recursos tecnológicos actualizados.

Supervisar la Gestión de Recursos Supervisar los objetivos y métricas de los procesos de gestión de recursos. Establecer cómo serán identificados, seguidos e informados para resolución de problemas o desviaciones.		**EDM04-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Medir la eficacia, eficiencia y capacidad de los recursos respectos a las necesidades institucionales.		Acciones correctivas para solventar las desviaciones en la gestión de recursos.

Procesos de Gestión

Gestionar el marco de gestión de Tecnologías Libres (APO01)

Implementar y mantener mecanismos y autoridades para la gestión y uso de las tecnologías libres para apoyar los objetivos de gobierno institucionales y nacionales.

Métricas

- Porcentaje de actividades de apoyo respecto a las tecnologías libres que resultan alineadas con la estrategia institucional y nacional.
-

Definir la estructura organizativa		**APO01-01**
Prácticas y Actividades	**Entrada**	**Salida**
- Establecer una estructura organizativa interna (Comité/Comisión)	EDM01-01 Normativas institucionales y nacionales.	Estructura y mandato oficial.
Establecer roles y responsabilidades		**APO01-02**
Prácticas y Actividades	**Entrada**	**Salida**
- Establecer, acordar y comunicar roles y responsabilidades de las partes interesadas, incluso del personal de TI.	Normativas institucionales y nacionales. Políticas de Talento Humano.	Definición de los puestos, roles y responsabilidades.
Mantener los habilitadores del sistema de gestión.		**APO01-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Considerar el entorno interno (cultura, tolerancia al riesgo, valores éticos, código de conducta, etc). Alinearse con la normativa nacional e institucional. - Desarrollar políticas específicas en relación al proyecto.	Normativas institucionales y nacionales. Políticas de Talento Humano.	Políticas relacionadas.
Comunicar los objetivos y la dirección de gestión.		**APO01-04**
Prácticas y Actividades	**Entrada**	**Salida**
- Definir las expectativas en relación al proyecto y las tecnologías libres. Elaborar un programa de concienciación. - Establecer métricas para medir los comportamientos en relación al proyecto y las tecnologías libres.	EDM01-01 AP002-06 DSS05-01,02,03	Programa de formación y concienciación en tecnologías libres.
Optimizar la ubicación de la función de las Tecnologías Libres		**APO01-05**

Prácticas y Actividades	Entrada	Salida
- Definir la función de la Actualización a Tecnologías Libres y sus actividades en la institución. - Obtener acuerdos de todas las partes.		Definición de la función de la Actualización a Tecnologías Libres y su ubicación en la institución.
Definir la propiedad de la información (datos) y los sistemas.		**APO01-06**
Prácticas y Actividades	**Entrada**	**Salida**
- Definir la propiedad de los datos y sistemas en el proceso de Actualización a Tecnologías Libres. - Asignar custodio de seguridad de los datos.	APO01-05	Roles y responsabilidades de seguridad de los datos y sistemas. Directrices de clasificación de datos.
Gestionar la mejora continua de los procesos		**APO01-07**
Prácticas y Actividades	**Entrada**	**Salida**
- Considerar mecanismo de mejora de la eficiencia de los equipos TIC (formación, documentación, automatización, certificación)	Planes de acciones correctivas actualizados. MEA01-04	- Documentación sobre procesos, tecnologías, normalización. - Formación/certificación del equipos TICs.
Mantener el cumplimiento de las políticas y procedimientos		**APO01-08**
Prácticas y Actividades	**Entrada**	**Salida**
- Planificar y realizar evaluaciones periódicas para determinar el cumplimiento de las políticas y procedimientos de Actualización a Tecnologías Libres.	APO02-05 APO02-06 Objetivos institucionales, nacionales. Marco normativo institucional y nacional.	Evaluación del cumplimiento.

Gestionar la Estrategia (APO02)

Proporciona una mirada holística hacia la misión de la institución y del entorno de TI, y las iniciativas requeridas para lograr la Actualización a Tecnologías Libres. Alinear el Plan de Actualización con los objetivos institucionales y nacionales.

Métricas:

- Datos de las encuestas de satisfacción de los grupos de interés sobre la eficacia de la estrategia de implementación de tecnologías libres.

- Porcentaje de iniciativas/proyectos de tecnologías libres en que los requisitos son promovidos por la máxima autoridad.

Comprender la misión/visión institucional.		**APO02-01**
Prácticas y Actividades	**Entrada**	**Salida**
- Comprender cómo las tecnologías libres apoyan los objetivos institucionales y nacionales, gestionando los riesgos y el cumplimiento. - Identificar las deficiencias potencialess de seguridad.	EDM01-01	Prioridades para los cambios y fuentes de alto nivel.
Evaluar el entorno, capacidades y rendimientos actuales		**APO02-02**
Prácticas y Actividades	**Entrada**	**Salida**
- Definir unas capacidades básicas en relación a las tecnologías libres. - Crear criterios en la selección de tecnologías libres.	APO01-08 APO02-01	Capacidades en tecnologías libres.
Definir las capacidades objetivo en Tecnologías Libres.		**APO02-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Garantizar que los requisitos normativos respecto a las tecnologías libres se incluyan en las capacidades objetivo de TI - Definir el estado objetivo respecto a las tecnologías libres. - Definir y consensuar el impacto de los requisitos normativos respecto a tecnologías libres en los objetivos institucionales y nacionales.	APO02-02	Necesidades de tecnologías libres en las capacidades objetivo de TI.
Definir el plan estratégico y la hoja de ruta		**APO02-05**
Prácticas y Actividades	**Entrada**	**Salida**
- Definir la estrategia de la implementación de tecnologías libres, alineado a la estrategia institucional. - Crear plan de acción con una planificación tentativa, métricas, objetivos que se relacionen con los beneficios institucionales y nacionales.	EDM01-01	Estrategia de implementación Hoja de ruta estratégica.
Comunicar la estrategia y la dirección del proyecto de		**APO02-06**

Tecnologías Libres.		
Prácticas y Actividades	**Entrada**	**Salida**
- Definir el Plan de Actualización a Tecnologías Libres, identificando las consecuencias prácticas de su no implementación. - Comunicar la estrategia y el Plan de Actualización a Tecnologías Libres, a las partes interesadas. - Crear conciencia y compresión de los objetivos del proyecto de Actualización a Tecnologías Libres, como se encuentra reflejada en los objetivos institucionales y nacionales.	APO01-04	Comunicación de los objetivos de Actualización a Tecnologías Libres. Plan de Actualización a Tecnologías Libres.

Gestionar la Innovación (APO04)

Mantener un conocimiento de las tecnologías libres y las tendencias relacionadas con el servicio y los objetivos institucionales, identificar oportunidades de innovación y planificar la manera de beneficiarse de ella en relación con los objetivos institucionales y nacionales.

Métricas:

- Porcentaje del presupuesto asignado a investigación, desarrollo, e implementación de tecnologías libres.
- Número de puestos con perfil de Tecnologías Libres y que incluyen aspectos de innovación con tecnologías libres.

Crear entorno favorable para la innovación		APO04-01
Prácticas y Actividades	**Entrada**	**Salida**
- Establecer vínculos con comunidades de tecnologías libres y universidades. - Mantener políticas y principios establecidos por el órgano público de Investigación e Innovación.	- Marco normativo institucional y nacional.	Plan de innovación en tecnologías libres.

Mantener un entendimiento del entorno institucional		APO04-02
Prácticas y Actividades	**Entrada**	**Salida**

- Determinar los efectos e impactos de las innovaciones en tecnologías libres, identificando oportunidades y limitaciones.	Investigación externa	Evaluaciones de impacto institucionales y nacionales de nuevas iniciativas

Supervisar y explorar el entorno tecnológico		**APO04-03**
Prácticas y Actividades	**Entrada**	**Salida**
- Llevar a cabo investigación, explorando además el entorno externo para identificar tendencias emergentes en tecnologías libres. - Fomentar la realimentación con las partes interesadas sobre innovación en tecnologías libres.	Investigación externa.	Tendencias emergentes identificadas en tecnologías libres.

Evaluar el potencial de las Tecnologías Libres emergentes y las ideas innovadoras.		**APO04-04**
Prácticas y Actividades	**Entrada**	**Salida**
- Evaluar las innovaciones identificadas en tecnologías libres - Apoyar las actividades de prueba de concepto para iniciativas de innovación.	APO02-02 APO02-06	Evaluación del cumplimiento de los requisitos de las tecnologías libres exploradas.

Recomendar iniciativas apropiadas adicionales		**APO04-05**
Prácticas y Actividades	**Entrada**	**Salida**
- Proporcionar asesoramiento respecto a tecnologías libres, a partir de los resultados de las pruebas de concepto	APO02-06 APO04-04	Recomendaciones de tecnologías libres a partir de los resultados de pruebas de concepto.

Supervisar la implementación y uso de la innovación		**APO04-06**
Prácticas y Actividades	**Entrada**	**Salida**
- Medir los beneficios y riesgos para la operatividad durante las pruebas de concepto y otras actividades de innovación.	APO04-01	Planes de Innovación ajustados.

7.5 Anexo E: Criterios de selección de Tecnologías Libres.

La CTIC (Consejo para las Tecnologías de Información y Comunicación) de Bolivia, emitió en diciembre 2016 un documento de alternativas para la selección de software libre, para lo cual presenta criterios de selección que permiten realizar comparaciones de manera objetiva entre soluciones tecnológicas.[22] Se tomaron algunos criterios y se categorizaron según los ejes estratégicos.

Ejes estratégicos	Criterio	Condición(es)	criticidad
Inclusión y Desarrollo	Número de paquetes u opciones	La capacidad del software de ser extendido con nuevas características o funcionalidades.	Medio
	Generación de Tecnología	Tiene la capacidad de promover la generación de tecnologías, cuando proporciona las herramientas para estudiar y aprender el funcionamiento del software (Ejemplo; facilita manuales, aportes de la comunidad.) Además el proyecto está dispuesto a recibir aportes y contribuciones por parte de la comunidad en forma libre.	Alto
Soberanía	Soberanía Tecnológica[18]	Pueden suceder tres condiciones: 1) software depende de una empresa, 2) software depende de una comunidad, 3) software depende de una comunidad y propone un contrato social.	Alto
Sostenibilidad	Soporte	La capacidad de brindar canales de comunicación que permitan mejorar la usabilidad del software, resolver problemas, y proveer actualizaciones. Esto incluye la rapidez de respuesta de la comunidad, y la presencia de empresas especializadas y desarrolladores locales.	Alto
	Madurez	El año de inicio del proyecto, permite describir el grado de antigüedad del software. La Fecha de última versión, junto al año de inicio puede dar una idea de la vitalidad y madurez del proyecto.	Alto
	Especialización	Si se trata de un software de uso general o específico que incluyen tareas generales o altamente específicas.	Bajo
	Curva de aprendizaje	El grado de facilidad de aprendizaje del software tanto técnicamente como a nivel de usuario final.	Medio
Transparencia	Compatibilidad	Capacidad de ser compatible con el hardware (sistemas operativos) o de comprender o ser comprendido por otros programas, y formatos de datos.	Alto
	Licencia	Software debe ser publicado bajo licencias libres, conforme a las aceptadas por la FSF (Free Software Foundation)[19]	Alto
	Seguridad	En relación a la cantidad de vulnerabilidad y su rápida resolución, en relación al tiempo de vida del software.	Alto

[18] Es la facultad de cada pueblo, país, nación, para definir sus propias políticas hacia una independencia tecnológica. Es la condición que permite potenciar la economía de un país y avanzar hacia la economía social de los conocimientos estimulando además la innovación e investigación.

[19] https://www.gnu.org/philosophy/free-sw.es.html

7.6 Anexo F: Ejes estratégicos y objetivos nacionales

PLAN NACIONAL DE DESARROLLO 2017-2021		
Políticas	**Objetivos**	**Ejes**
EJE ESTRATÉGICO MIGRACION: INCLUSIÓN Y DESARROLLO		
1.2 Generar capacidades y promover oportunidades en condiciones de equidad para todas las personas a lo largo del ciclo de vida.	1. Garantizar una vida con iguales oportunidades para todas las personas.	**1. Derechos para todos durante toda la vida**
1.4 Fortalecer los sistemas de atención integral a la infancia con el fin de estimular las capacidades de las niñas y niños, considerando los contextos territoriales, la interculturalidad y el género.		
4.7 Incentivar la inversión productiva privada en sus diversos esquemas, incluyendo mecanismos de asociatividad y alianzas público-privadas, fortaleciendo el tejido productivo, con una regulación previsible y simplificada.	4. Consolidar la sostenibilidad del sistema económico social y solidario, afianzar la dolarización.	**2. Economía al servicio de la sociedad**
4.8 Incrementar el valor agregado nacional en la compra pública, garantizando mayor participación de la MIPYMES y actores de la economía popular y solidaria.		
5.2 Diversificar la producción nacional, a fin de aprovechar nuestras ventajas competitivas, comparativas y las oportunidades identificadas en el mercado interno y externo, para logar un crecimiento económico sostenible y sustentable.	5. Impulsar la productividad y competitividad para el crecimiento económico sustentable de manera redistributiva y solidaria.	
5.3 Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, en articulación con las necesidades sociales, para impulsar el cambio de la matriz productiva.		
5.4 Fortalecer y fomentar la asociatividad, los circuitos alternativos de comercialización, las cadenas productivas y el comercio justo, priorizando la Economía Popular y Solidaria, para consolidar de manera redistributiva y solidaria la estructura productiva del país.		
7.5 Consolidar una gestión estatal y gubernamental eficiente y democrática que opere en sociedad, impulsando las capacidades ciudadanas e integrando las acciones sociales.	7. Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía.	**3. Más sociedad, mejor Estado**
EJE ESTRATÉGICO MIGRACIÓN: SOBERANÍA		
9.3 Crear y fortalecer los vínculos políticos, sociales, económicos, turísticos, ambientales, académicos y culturales, y las líneas de cooperación para la transferencia tecnológica, con socios estratégicos de Ecuador.	9. Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo.	**3. Más sociedad, mejor Estado**
EJE ESTRATÉGICO: SOSTENIBILIDAD		

4.2 Canalizar los recursos hacia el sector productivo promoviendo fuentes alternativas de financiamiento y la inversión a largo plazo, en articulación entre la banca pública y el sistema financiero privado, y el popular y solidario.	4. Consolidar la sostenibilidad del sistema económico social y solidario, afianzar la dolarización.	**2. Economía al servicio de la sociedad**
4.5 Profundizar la progresividad, calidad y oportunidad del gasto público optimizando la asignación de recursos y en el contexto de un manejo sostenible del financiamiento público.		
4.6 Fortalecer la dolarización promoviendo un mayor ingreso neto de divisas y fomentando la oferta exportable no petrolera que contribuyan a la sostenibilidad de la balanza de pagos.		
7.8 Fortalecer las capacidades de los gobiernos autónomos descentralizados para el cumplimiento de los objetivos nacionales, la gestión de sus competencias, la sostenibilidad financiera y la prestación de servicios públicos a su cargo, con énfasis en agua y saneamiento.	7. Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía.	**3. Más sociedad, mejor Estado**
EJE ESTRATÉGICO MIGRACIÓN: TRANSPARENCIA		
8.2 Fortalecer la transparencia de las políticas públicas y la lucha contra la corrupción, con mejor acceso a información pública de calidad, optimizando las políticas de rendición de cuentas y promoviendo la participación y el control social.	8. Promover la transparencia y la corresponsabilidad para una nueva ética social.	**3. Más sociedad, mejor Estado**

7.7 Anexo G: Alternativa Tecnología Libre para gestión centralizada de equipos de escritorio.

Las siguientes son tecnologías que cumplen con requerimientos estipulados en el EGSI del gobierno ecuatoriano, y los criterios de selección de tecnologías libres:

Tecnología	Descripción
FreeIPA[20]	Proyecto de software libre mantenida por el Proyecto Fedora, patrocinada por RedHat, que provee una interfaz segura y sencilla para administración de: • Identidades (IDM basado en 389 Directory Server). • NTP para sincronización horaria. • Integración de certificados CA, RA (DogTag). • DNS (Bind). • Integración con Active Directory mediante Cross Forest Trusts (Samba4).
Foreman + Katello[21]	Es una herramienta para la gestión del ciclo de vida para servidores físicos y virtuales. Permite la automatización de tareas repetibles y el rápido despliegue de aplicativos y configuraciones. El plug-in Katello, orientado a sistemas basados en rpm/yum, le agrega la capacidad de gestión de contenedores de repositorios/paquetes, y configuraciones para este tipo de sistemas.
Foreman + Ansible[22]	Es una herramienta para la gestión del ciclo de vida para servidores físicos y virtuales. Permite la automatización de tareas repetibles y el rápido despliegue de aplicativos y configuraciones. El plug-in Ansible le agrega la funcionalidad de aprovisionamiento y gestión de configuraciones desatendida, de cualquier tipo de sistema operativo GNU/Linux, basados en .rpm o .deb

[20] Sitio y documentación: https://www.freeipa.org/page/Main_Page
Código fuente puede encontrarse en: https://github.com/freeipa/freeipa

[21] Sitio y documentación: https://theforeman.org/plugins/katello/
Código fuente puede encontrarse en: https://github.com/theforeman/forklift/

[22] Sitio y documentación: https://theforeman.org/plugins/foreman_ansible/1.x/index.html
Código fuente puede encontrarse en: https://github.com/theforeman/foreman_ansible

7.8 Anexo H: Matriz modelo GTAG11

Caso 1: Situación actual previo a la migración a tecnologías libres

AREA / OBJETIVOS DE CONTROL	Impacto Financiero		Riesgos IT										Puntaje y niveles	
			Calidad de Controles Internos		Rotación Unidad de Auditoría		Disponibilidad		Integridad		Confiden-cialidad			
	P	I	P	I	P	I	P	I	P	I	P	I		
1. Control de código malicioso	3	3	3	3	2	3	3	3	3	3	3	3	51	H
2. Tansacciones en línea seguras	2	3	2	3	2	3	2	3	2	3	3	3	39	H
3. Registros de auditoría	3	2	3	3	2	3	2	2	1	2	2	2	31	M
4. Monitoreo del uso del sistema	1	2	3	3	2	3	2	2	2	2	2	2	29	M
5. Gestión de acceso del usuario	2	3	3	3	3	3	2	3	2	3	2	3	42	H
6. Control de acceso al sistema operativo	2	2	3	3	2	3	2	3	2	3	3	3	40	H
7. Control de acceso a los aplicativos	2	3	3	3	2	3	2	3	2	3	2	3	39	H
8. Protección de los puertos de configuración y diagnóstico remot	2	2	3	3	2	3	2	3	2	2	2	3	35	H
9. Política de uso de controles criptográficos	1	2	3	2	2	3	1	3	3	3	3	3	35	H
10. Continuidad del negocio	2	3	3	3	2	3	2	3	2	3	2	3	39	H
11. Accesibilidad agenda y correos electrónicos	2	3	2	3	2	3	2	3	2	3	2	3	36	H
12. Control de licencias de software	3	3	3	3	2	3	3	3	3	3	3	3	51	H
												total suma de puntajes	467	
Puntaje Bajo	6-19													
Puntaje Medio	20-34		total máximo de puntaje: 12x54 = 648											
Puntaje Alto	35-54													

Caso 3: Migración de escritorios a tecnologías libres

AREA / OBJETIVOS DE CONTROL	Impacto Financiero		Riesgos IT										Puntaje y niveles	
			Calidad de Controles Internos		Rotación Unidad de Auditoría		Disponibilidad		Integridad		Confiden-cialidad			
	P	I	P	I	P	I	P	I	P	I	P	I		
1. Control de código malicioso	1	1	1	3	2	3	1	3	1	3	1	3	19	L
2. Tansacciones en línea seguras	1	3	1	3	2	3	1	3	1	3	1	3	21	M
3. Registros de auditoría	1	2	1	3	2	3	1	2	1	2	1	2	17	L
4. Monitoreo del uso del sistema	1	2	2	3	2	3	1	2	1	2	1	2	20	M
5. Gestión de acceso del usuario	2	3	1	3	2	3	1	3	1	3	1	3	24	M
6. Control de acceso al sistema operativo	1	2	1	3	1	3	1	3	1	3	1	3	17	L
7. Control de acceso a los aplicativos	1	2	1	3	1	3	1	3	1	3	1	3	17	L
8. Protección de los puertos de configuración y diagnóstico remo	1	2	1	3	2	3	1	2	1	2	1	2	17	L
9. Política de uso de controles criptográficos	1	2	2	2	2	3	1	3	1	3	1	3	21	M
10. Continuidad del negocio	2	3	3	3	2	3	2	3	2	3	2	3	39	H
11. Accesibilidad agenda y correos electrónicos	2	2	2	3	2	3	2	3	2	3	2	3	34	M
12. Control de licencias de software	1	3	1	2	2	3	1	1	1	1	1	1	14	L
												total suma de puntajes	260	
Puntaje Bajo	6-19													
Puntaje Medio	20-34		total máximo de puntaje: 12x54 = 648											
Puntaje Alto	35-54													

Para cualquiera de los casos la suma máxima posible de puntajes llegaría a 648 (54 x 12) que se calcula asumiendo que cada uno de los 12 objetivos de control dieron un puntaje del máximo valor posible (54). Podemos notar que para el Caso 1, la suma total de puntajes da 467, y para el Caso 2 suma 260, que representan el 72% y 40% respectivamente del máximo posible, Es decir, mantener la situación actual represente un riesgo mayor.

7.9 Anexo I: Desafíos y Oportunidades

En agosto del 2013, el Institute for Defense Analyses (IDA) junto con la George Tech Research Institute (GTRI) de Los Estados Unidos, emitieron un documento de "lecciones aprendidas" que identifica desafíos y oportunidades en la aplicación del software de tecnologías libres en el gobierno. Este documento proporciona recomendaciones valiosas para todo proceso de adopción o migración a tecnologías libres, las cuales contribuirán en el diseño de los planes de concienciación y por ende a la mitigación de riesgos.

Dicho documento recoge algunas entrevistas realizadas a expertos, proveedores y potenciales usuarios quienes expresaron sus opiniones, sugerencias, inconvenientes, que compiladas en dicho documento están expresadas como retos y oportunidades.

El documento afirma que para maximizar el uso de los recursos limitados, los Estados Unidos debe abordar estos retos, que permitirían mitigar barreras o impedimentos innecesarios al uso o desarrollo de software de tecnologías libres en el gobierno, los cuales han sido agrupados en las siguiente categorías: [23]

1. Uso y desarrollo existentes de Tecnologías Libres en el Estado. (generar casos de estudio). Es decir, crear y distribuir las historias de éxito, como casos de estudio para que otras instituciones puedan valerse de ese conocimiento.
2. Inercia. Contrarrestar la resistencia al cambio, publicando casos de estudio, disminuyendo el costo de transición haciendo énfasis en la modularidad y en los estándares.
3. Temor sobre baja calidad o malware en el software. Asegurarse que el gobierno y sus proveedores comprendan que las tecnologías libres puede asegurar alta calidad de una manera más transparente y que además existen diversas manera para evaluar a las tecnologías libres.
4. Preocupación sobre soporte comercial o garantías. Hacer comprender y asegurarse de que los servidores públicos tanto de las áreas técnicas como las de

compras estén conscientes que existen muchas maneras para dar soporte y garantías a tecnologías libres, y esto incluye el soporte propio.

5. Adquisición y Comunidad. Incentivar la creación de comunidades colaborativas y el compartir el código por medio de programas de gobierno o los contratistas. El gobierno por default debe requerir compartir y liberar el software como tecnologías libres, si este fue desarrollado con fondos públicos.
6. Certificación y Acreditación (C&A), Gestión del Riesgo y Participación. Asegurarse que todas las partes relevantes, incluyendo los proveedores de tecnologías libres, se involucren cuando el gobierno esté desarrollando especificaciones relacionadas.
7. Estándares / Interoperabilidad. Cambiar los formatos y protocolos propietarios por sistemas modulares y estándares abiertos, ya que permiten la transición a software alternativo, incluyendo las tecnologías libres.
8. Retos para liberar el código fuente del Estado. Cuando el gobierno libera nuevos proyectos de Tecnologías Libres al público, debe utilizar repositorios colaborativos públicos existentes, cuando sea necesario. El gobierno necesita apoyar una amplia participación de programadores y un activo desarrollo.
9. Necesidad de Guías / Manuales. Crear guías para la evaluación de tecnologías libres, los cuales deben incluir el impacto de las licencias para la contribución hacia las comunidades, y para poder liberar nuevos proyectos financiados por el gobierno como Tecnología Libre.
10. Necesidad de Educación. Proveer educación sobre tecnologías libres en general, por ejemplo en licencias y propiedad intelectual del software para servidores públicos y tecnológicos y de áreas de compras; en compra pública para proveedores potenciales; y en certificaciones y acreditaciones. También debe considerar a los servidores públicos no tecnológicos para los procesos de concienciación.

Las entrevistas fueron realizadas en el 2011 como parte del proyecto Tecnología Abierta de Seguridad Nacional (HOST por sus siglas en inglés) del Consejo de Ciencia y Tecnología (S & T por sus siglas en inglés) del Departamento de Seguridad Nacional (DHS por sus siglas en inglés).[23]

8 Bibliografía

8.1 Fuentes primarias

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). NIST 800-55 Rev1: Measurement Guide for Information Security, (July), 80. Retrieved from http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152183

Popolna, D. (2016). Metodología de Migración a Software Libre y Seguridad Digital. Retrieved from http://www.ctamlibre.org/documentacion-en-linea/metodologias/metodologia-migracion-debian

OGC. (2008). Alineando Cobit 4.1, ITIL V3e, ISO/IEC 27002, en beneficio del negocio.

INEN (2009) NTE INEN-ISO/IEC 27002:2009, Tecnología de la Información. Técnicas de la Seguridad. Código de Práctica para le Gestión de la Seguridad de la Información.

NIST (2012) Special Publication 800-30 Revision1: Guide for Conducting Risk Assessments, Risk Management Guide for Information … 95. Recuperado de http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:NIST+Special+Publication+800-30#0

Bowen, P., Hash, J., & Wilson, M. (2006). NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers.

SOMAP (2006) Open Information Security Risk Assessment Guide. (2006), 1–35.

Metric, O. S. (2003). Security: Linux versus Windows. Retrieved from http://regmedia.co.uk/2004/10/22/security_report_windows_vs_linux.pdf

Franch, X., Susi, A., & Annosi, M. (2013). Managing Risk in Open Source Software Adoption. … . Conf. on Software …. Retrieved from http://www.manolodominguez.com/content/common/pdf/cv/publications/RisksInOSS-icsoft-2013.pdf

ISACA. (2012). COBIT 5: para Seguridad de la Información.

NIST Security Guidelines. (2011), 329. http://doi.org/10.1016/B978-1-59749-645-2.00020-3

MCCTH. (2016) Plan de Actualización a Software Libre. https://www.migralab.ec/wp-content/uploads/2017/11/P0210-PLAN-ACTUALIZACION-V1.5.odt

CMSI. Informe Final de la Fase de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información, 9Secretaría Ejecutiva de la CMSI 1–66 (2004). Retrieved from https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0009!R1!PDF-S.pdf

CMSI. Informe de la Fase de Túnez de la Cumbre Mundial sobre la Sociedad de la Información, 9WSIS-05/TUNIS/DOC/9(Rev.1)-S 1–65 (2006). Retrieved from https://www.itu.int/net/wsis/docs2/tunis/off/9rev1-es.pdf

Pillay, N. (2011). La Declaración de las Naciones Unidas sobre el derecho al desarrollo cumple 25 años. Retrieved from http://www.ohchr.org/Documents/Issues/Development/RTDInfonNote_sp.pdf

ONU. (1986). Declaración sobre el Derecho al Desarrollo, (Book, Whole). Recuperado de http://www.ohchr.org/Documents/Issues/Development/DeclarationRightDevelopment_sp.pdf

Plan Nacional para el Buen Vivir 2013-2017 (2013). Ecuador. Recuperado de http://www.buenvivir.gob.ec/versiones-plan-nacional;jsessionid=9547688AF53E99105B54203121C0F55C

Asamblea. Ley de Seguridad Pública y del Estado (2009) (2009). Ecuador. Recuperado de http://www.seguridad.gob.ec/wp-content/uploads/downloads/2012/07/01_LEY_DE_SEGURIDAD_PUBLICA_Y_DEL_ESTADO.pdf

SNAP. Plan Nacional de Gobierno Electrónico (2014). Ecuador. Recuperado de http://www.gobiernoelectronico.gob.ec/wp-content/uploads/2015/02/PlanGobierNoElectronicoV1.pdf

SNAP. (2013). Acuerdo 166: EGSI - Esquema Gubernamental de Seguridad de la Información. Recuperado de http://www.educarecuador.gob.ec/anexos/correo/Acuerdo_166.pdf

Asamblea. Constitución de la República del Ecuador 2008 (2008). Ecuador.

MICS. Seguridad Integral plan y agendas 2014-2017 (2014). Ecuador. Retrieved from http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/03/plan_nacional_seguridad_integral2014_2017v2.pdf

Contraloria. (2010). Norma de Control Interno 410 - Tecnología de la Información.

CEPAL. (2015). La cadena del software en Ecuador: Diagnóstico , visión estratégica y lineamientos de política (resumen). Recuperado de http://www.vicepresidencia.gob.ec/wp-content/uploads/2015/07/Resumen-Cadena-Software.pdf

Monk, L. (2013). El rol del cooperativismo: soberanía tecnológica y cooperativismo. Revista Caras Y Caretas, diciembre(2289), 1. Recuperado de http://gcoop.coop/soberania-tecnologica-y-cooperativismo

Rodríguez Echeverría, R. (2007). Penetración del Software Libre en la Administración Pública Extremeña. Recuperado de https://observatorio.iti.upv.es/resources/report/145

UNAM. «Malware Industroyer está relacionado con el corte eléctrico en Kiev», n.o Junio 14 (2017). https://www.seguridad.unam.mx/malware-industroyer-relacionado-en-kiev.

Leyden, John. «Move over, Stuxnet: Industroyer malware linked to Kiev blackouts», n.o Junio 12 (2017). https://www.theregister.co.uk/2017/06/12/industroyer_malware/.

Maggiore, Marcia L. «Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio». Universidad de Buenos Aires, 2014.

8.2 Referencias

[1] SNAP, *Plan Nacional de Gobierno Electrónico*. Ecuador, 2014.

[2] *Decreto 1425: Reglamento para la adquisición de software por parte de las entidades contratantes del sector público*. 2017, p. 6.

[3] ISACA, *COBIT 5: para Seguridad de la Información*. 2012.

[4] NIST, *NIST 800-53r4: Security and Privacy Controls for Federal Information Systems and Organizations*. 2013, p. 462.

[5] L. Rajchel, M. Takahashi, W. Fumy, M. De Soete, E. J. Humphreys, T. Chikazawa, K. Rannenberg, y E. Andrukiewicz, *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management*. 2011.

[6] J. Task y F. Transformation, *NIST SP 800-39 Managing information security risk: organization, mission, and information system view*, n.º March. 2011, p. 88.

[7] SENPLADES, *Plan Nacional para el Buen vivir 2017-2021*. 2017, p. 159.

[8] P. Herzog, *OSSTMM 3: The Open Source Security Testing Methodology Manual*. 2010.

[9] MICS, *Seguridad Integral plan y agendas 2014-2017*. Ecuador, 2014, p. 264.

[10] L. Anzelini y S. Castro, «Los Estados medianos y la arquitectura de seguridad internacional: apuntes estratégicos para el caso argentino», *Rev. POSTData*, vol. 17, n.º 2, pp. 37-85, 2012.

[11] M. Perez Comisso, «(Re)definiendo tecnología», p. 13, 2016.

[12] K. C. Ferrando, «Importancia de la inclusión de contenidos CTS en la formación de ingenieros», *VII Jornadas Sociol.*, p. 15, 2007.

[13] M. Kranzberg, «Leyes de Melvin Kranzberg sobre tecnología».

[14] R. Bonifaz, «The NSA Surveillance Capabilities According to the Snowden Documents», *IX Congr. Iberoam. Segur. informática CIBSI2017*, pp. 26-33, 2017.

[15] IRAM, *IRAM-ISO/IEC 27001 - Sistemas de gestión de la seguridad de la información (SGSI)*. Argentina, 2007, p. 44.

[16] ADACSI, «¿Qué ciberataques nos esperan para el 2018?», *isaca.org.ar*, n.º diciembre 7, 2017.

[17] M. Garnaeva, F. Sinitsyn, y Y. Namestnikov, «ESTADÍSTICAS GENERALES DE 2016», 2016.

[18] K. Lab, «Estadísticas generales de 2017», 2017.

[19] S. Patil y Y. Londhe, «Microsoft Office Vulnerabilities Used to Distribute Zyklon Malware in Recent Campaign», *fireeye.com*, n.º enero 17, 2018.

[20] AV-TEST, «Security Report 2016/17», 2017.

[21] Syssec, *Red book: A Roadmap for Systems Security Research*. 2013.

[22] CTIC, *Alternativas para la selección de software libre Índice general*. Bolivia, 2016.

[23] E. L. Morgan, *Open Source Software in Government: Challenges and Opportunities*, n.º August. 2013.