FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ESCUELA DE TECNOLOGÍA EN REDES Y TELECOMUNICACIONES

ELABORACIÓN DE POLÍTICAS INTERNAS PARA EL MINISTERIO DE CULTURA Y PATRIMONIO SOBRE EL BUEN USO DE INTERNET, CORREO, CONTRASEÑAS, ESCRITORIO LIMPIO, BASADAS EN LA NORMA DE CONTROL INTERNO Y NORMATIVA ITIL.

TRABAJO DE TITULACIÓN PRESENTADO EN CONFORMIDAD CON LOS REQUISITOS ESTABLECIDOS PARA OPTAR POR EL TITULO DE "TECNÓLOGO EN REDES Y TELECOMUNICACIONES"

Profesor guía: José Luis Rodríguez Añazco

Autor: Paúl Andrés Mero García.

Quito-Ecuador

2016

DECLARACIÓN PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación

---

Ing. José Luis Rodríguez Añazco

C.I. 1716909450

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado fuentes correspondientes y que en su ejecución, se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Paúl Andrés Mero García

C.I.1715006928

AGRADECIMIENTO

Al culminar una parte importante en mi vida, quiero dejar asentado mi más profundo agradecimiento a mi Esposa, Padres, Hermano y Familia por ser parte fundamental de este proceso, ya que sin su apoyo y comprensión no hubiera logrado culminar con éxito la meta propuesta.

A la Universidad de las Américas, noble institución que me acogió como estudiante y me supo enriquecer de conocimientos y valores que ahora forman parte de mi personalidad en los ámbitos intelectual como humano.

A mis compañeros y amigos que con sus criterios y conocimientos supieron fortalecer y dar palabras de aliento para conseguir una meta propuesta.

DEDICATORIA

Este trabajo lo dedico a todas las personas que en el transcurso de este periodo de aprendizaje han empujado y fortalecido mis ánimos de seguir adelante.

RESUMEN

En nuestros tiempos donde los servicios tecnológicos son más frecuentes es necesario tener normativas, políticas, estándares que garanticen los tres requerimientos de mayor importancia para la protección de la información que son confidencialidad, integridad, disponibilidad, así se puede garantizar la calidad y la satisfacción del cliente en la entrega de servicios. Estas buenas prácticas las están adoptando Organizaciones que van de la mano con la Norma de Control Interno de la Contraloría General del Estado Ecuatoriano, ITIL, que son aceptados y reconocidos para la gestión de servicios TI. Este proyecto de investigación está enfocado en generar políticas de correo, buen uso de internet, contraseñas, escritorio limpio, basadas en dichas normativas para evaluar una mesa de servicios TI de una Organización y particularmente la del Ministerio de Cultura y Patrimonio, determinando las gestiones, insumos y requerimientos mínimos que deberá cumplir.

ABSTRACT

In our times where technological services are more frequent you need to have regulations, policies, standards that guarantee the three most important requirements for information protection are confidentiality, integrity, availability , and you can ensure quality and satisfaction customer service delivery . These best practices being adopted by organizations that go together with the Statement of Internal Control of the Comptroller General of Ecuador, ITIL and COBIT, which are accepted and recognized for IT service management. This research project is focused on generating mail policies, good use of internet, passwords, clean desk , based on these standards to evaluate a table of IT services of an organization and particularly the Ministry of Culture and Heritage , determining the arrangements , inputs and minimum requirements to be met

ÍNDICE DEL CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El avance tecnológico y los grandes cambios en la producción y procesos en las Organizaciones a nivel mundial, han hecho que muchas de dichas Organizaciones deseen adoptar e implementar en su organización marcos de referencia y buenas prácticas en búsqueda de la calidad y la satisfacción del cliente en la entrega de servicios, en el caso del Ministerio de Cultura y Patrimonio esto ha nacido desde el área de Tecnología de la Información y Comunicación y específicamente en las áreas de Mesa de Servicios de TI, Infraestructura, Desarrollo, Seguridad Informática, quienes mantienen contacto hacia el usuario interno, demandando más y mejores servicios.

El presente proyecto de investigación está enfocado en generar una guía para la elaboración de Políticas Internas, poder evaluar y mejorar los servicios TI en una Organización y particularmente la del Ministerio de Cultura y Patrimonio, determinando las gestiones, insumos y requerimientos mínimos que deberá cumplir por disposición de la Contraloría General del Estado el cual solicita la implementación de la normativa de control interno para no incurrir en faltas, el proyecto también verificara e implementara el enfoque de dicha norma con las buenas prácticas de los servicios como lo indica ITIL.

Cabe mencionar que las fases para una auditoría realizada por cualquier ente regulador son: planeación, ejecución e informe, el proyecto a desarrollarse se centra en la fase de planeación para obtener documentos, reglamentos, normativas que puedan ser adaptables al Ministerio de Cultura y Patrimonio, al final se realizara las políticas como si fuese un documento formal, mediante la aplicación de marcos de referencia y buenas prácticas basadas en ITIL, mismos que son aceptados y reconocidos mundialmente para la gestión de servicios TI.

Localmente se aplica la Norma de Control Interno de la Contraloría General del Estado, la cual es de uso obligatorio para empresas del sector público en el Ecuador.

CAPÍTULO I

1. ITIL y Norma de Control Interno

1.1 Marco Teórico

Antecedentes del estado del arte

Para el presente proyecto se generará políticas internas para mejorar los niveles de servicio brindados por las diferentes áreas en la Unidad de Tecnologías de la Información y Comunicación del MCYP o cualquier Entidad pública dentro del territorio ecuatoriano, con respecto a la elaboración de las políticas, se ha encontrado documentos legales en la contraloría, reglamentos, leyes y guías de fundamentos de ITIL que serán evaluados para la gestión de servicios TI basados en buenas prácticas, evaluaciones de distintas organizaciones, alineaciones, ITIL y otros estándares enfocados a la gestión integral entre TI y el Negocio.

1.2 Marco Referencial

En nuestra actualidad todas las Organizaciones necesitan recurrir a nuevos procesos para poderlos implementar y así alinearse a la utilización de estándares y buenas prácticas reconocidas a nivel mundial, esto lo realizan para aplicarlas en sus actividades diarias y así ir a la par de un mundo más globalizado, bajo este enfoque los dos estándares y prácticas establecidos en este caso de estudio desempeñan un papel vital, la Norma de Control Interno que se alinea con la estructura de COBIT, establecen **lo que debe** hacerse, e ITIL proporciona **el cómo** hacer para los aspectos de la gestión de servicios TI.

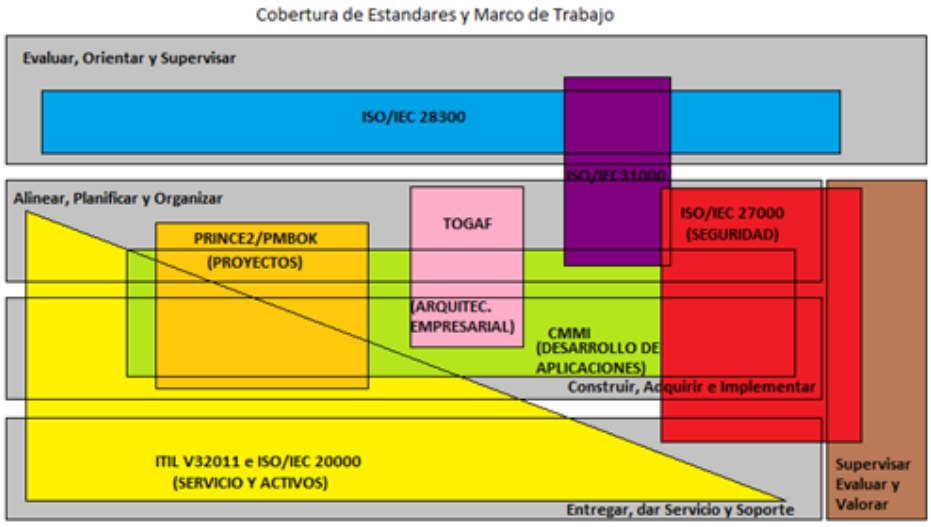

Figura 1. Resumen de un mapeo cobertura de COBIT 5 de otros estándares y Marcos de Trabajo.

Tomado de: (EXACTA-COBIT, 2013)

1.3 ITIL

1.3.1 Historia de ITIL

En la década 1980 debido a la calidad de los servicio de TI en empresas internas y externas la Agencia Central de Telecomunicaciones actualmente Ministerio de Comercio, OCG, recibió el encargo de desarrollar una metodología la cual hoy en día se llama ITIL, la patentó y en la actualidad posee todos los derechos.(New Horizon, 2010)

Desde 1990, ITIL ha dejado de ser un marco teórico para convertirse en una metodología compartida por varios países para ser utilizada en la práctica.(New Horizon, 2010)

ITIL tuvo comienzo en 1986, en la versión I, ITIL contaba con 31 libros dentro de un proyecto inicialmente dirigido por Peter Skinner y John Stewart, se tituló GovernmentInformationTechnologyInfrastructureMethod (‘Métodode Infraestructura de la Tecnología de Información del Gobierno’, GITM) (New Horizon, 2010)

Luego de ello apareció la Versión 2 de ITIL, y los libros fueron agrupados y como resultado de ello quedó reducida a 10 libros. En el año 2007 se desarrolló y salió la tercera versión de ITIL y la versión II mantuvo un periodo de transición que acabo en el 2008, la diferencia es que versiones anteriores ha sido durante años una pieza clave para la divulgación de ideas sobre ITIL y la Gestión de Servicios de TI, la principal diferencia entre la versiones 2 y 3 está en la visión del Ciclo de Vida del Servicio que fue introducida en la versión 3 mientras que en la versión dos, encontramos el enfoque que se le dio a las practicas más sencillas en Provisión, Soporte y Seguridad cuando se agrupo la versión 3 se pudo ya tener en cuenta el Ciclo de Vida por lo que así estuvo completo el servicio. Consta de 5 libros los cuales conforman una estructura muy articulada en torno al ciclo de vida del servicio de TI.(New Horizon, 2010)

ITIL fue desarrollada al reconocer el nivel de dependencia tecnológica de las personas y empresas, se necesita conseguir un buen equilibrio y las metodologías orientadas a procesos exige métodos de extremo a extremos centrados en el usuario, para entenderlos se puede decir que al usuario no le sirve de nada saber si los servidores o equipos están en funcionamiento, lo que les interesa en tener el servicio óptimo y que así puedan cumplir con sus labores accediendo a la información en su lugar de trabajo y así cumplir sus objetivos. Por lo que las ITIL lo que busca es Alinear la Tecnología con el negocio por medio de la gestión de servicios.(MOLINA, Introducción a la Gestión de Servicios de TI, 2006)

Por ese motivo ITIL es cierto modo no es una norma, no son reglas y no es una metodología, la madurez de una organización no puede limitarse al proveedor de servicio. ITIL el objetivo es alinear la Tecnología con el Negocio, y se hace mediante guías y consejos de aquellas prácticas que han demostrado ser más efectivas que otras, pero no es mandatorio, no son obligatorias. (MOLINA, Gestión de Servicios de TI, 2008)

En la versión 3 de ITIL recurre a conceptos importantes para determinar el valor de un servicio, el valor no solo se aprecia en los resultados del negocio del cliente, sino también depende de la percepción de cliente, esto es consecuencia de la diferencia entre valor económico y percepción económica, la percepción depende de diferentes factores como la imagen, los atributos de valor y la experiencia personal del cliente. Se debe tener claro la definición y diferenciación del valor.(MOLINA, Gestión de Servicios de TI, 2008)

El valor económico no siempre corresponde con las percepciones económicas del cliente.

Por consecuencia la versión 3 de ITIL depende del punto de vista del cliente donde el efecto positivo en la "funcionalidad" de un servicio, mientras de la "garantía" es lo que garantiza dicho servicio, el valor de servicio es la mezcla entre las dos la funcionalidad y la garantía.(MOLINA, Gestión de Servicios de TI, 2008)

Para ITIL la funcionalidad se define como la adecuación a un propósito y la garantía es la adecuación a un uso.

La funcionalidad es lo que el cliente recibe, mientras que la garantía reside en cómo se proporciona. Para explicar los pasos de creación de valor se muestra en la siguiente Fig. 2.

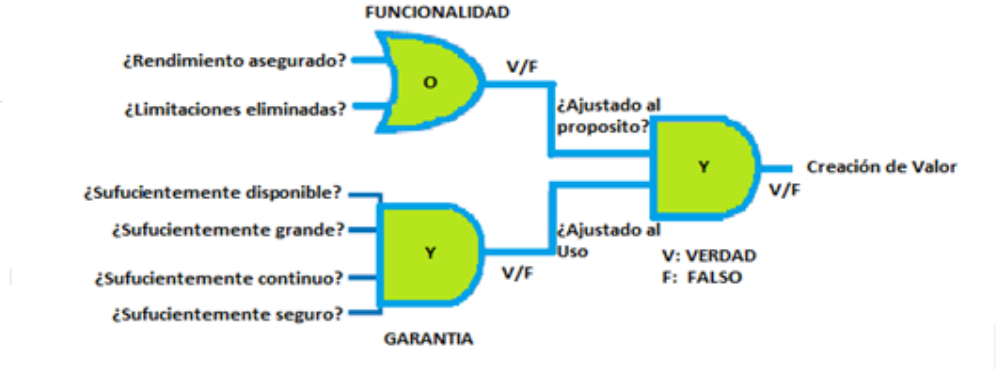

Figura 2: Creación de valor

Tomado de:(MOLINA, 2008)

1.3.2 Principios de ITIL

Para el estudio de ITIL existen 4 principios que son los pilares de ITIL:

Procesos: Sirven para poder acoplar el negocio y la gestión de servicios TI, esto se lo realiza mediante una mejora constante de los procesos dejando de lado el enfoque en la tecnología.(MOLINA, 2008)

Calidad: Se toma como base los procesos y mediante las mejoras de ellos se alinean con las Normas de Calidad lo cual ayuda a la misma. Adicionalmente toma como base otros estándares de calidad como los ISO 9000 y la Calidad Total como EFQM.(MOLINA, 2008)

Cliente: Es el único beneficiario de la mejora de los servicios.

Independencia: Mantiene buenas prácticas independientes de fabricantes, marcas, metodologías y compañías de servicio.”(MOLINA, 2008)

1.3.3Proceso y Fases

1.3.3.1 Proceso

Un proceso son actividades estructuradas diseñadas para cumplir objetivos específicos, al final dan como resultado un cambio orientado hacia un objetivo utilizan la retroalimentación para tener auto mejoras y autocorrecciones.(MOLINA, 2008)

1.3.3.2 Ciclo de Vida del Servicio

El ciclo de vida de ITIL consta de 5 fases las cuales en cada una de ellas se describe el proceso tanto antiguo como nuevo a seguir y mediante ellos se describe los cambios que se producen en el ciclo de vida por cada fase.

- **Estrategia de Servicio:** Es la fase de diseño, en esta se desarrolla e implementa la Gestión del Servicio como un recurso estratégico.
- **Diseño de Servicio:** Es la fase de diseño para poder desarrollar el servicio de TI apropiados, incluyendo arquitectura, procesos, políticas y documentos, el objetivo principal del diseño es cumplir requerimientos presentes y futuros de la empresa.(MOLINA, 2008)
- **Transición de Servicio:** Es la fase en la cual se desarrolla y se mejora de capacidades dando el paso a producción de servicios nuevos y modificados.(MOLINA, 2008)
- **Operación de Servicios:** Es la fase que garantiza la efectividad y eficacia en la provisión y el soporte de servicios con ello genera valor para el cliente y el proveedor del servicio.(MOLINA, 2008)
- **Mejora continua en el Servicio:** Es la fase en la genera y mantiene el valor para el cliente esto lo consigue mediante la mejora del diseño y la introducción y Operación del Servicio. (MOLINA, 2008).

La fase de Estrategia del Servicio es el eje motor para las demás fases del Ciclo de Vida del Servicio ya que giran en torno a ella; es la fase de definición de políticas y objetivos**.** Las fases de Diseño del Servicio, Transición del Servicio y Operación del Servicio ponen en práctica esta estrategia a través de ajustes y cambios, la fase de Mejora Continua del Servicio consiste en el aprendizaje y mejora, abarca todas las fases del ciclo ya que en esta fase inicia los proyectos y programas de mejora asignándoles prioridades en función de los objetivos estratégicos de la organización.(MOLINA, 2008)

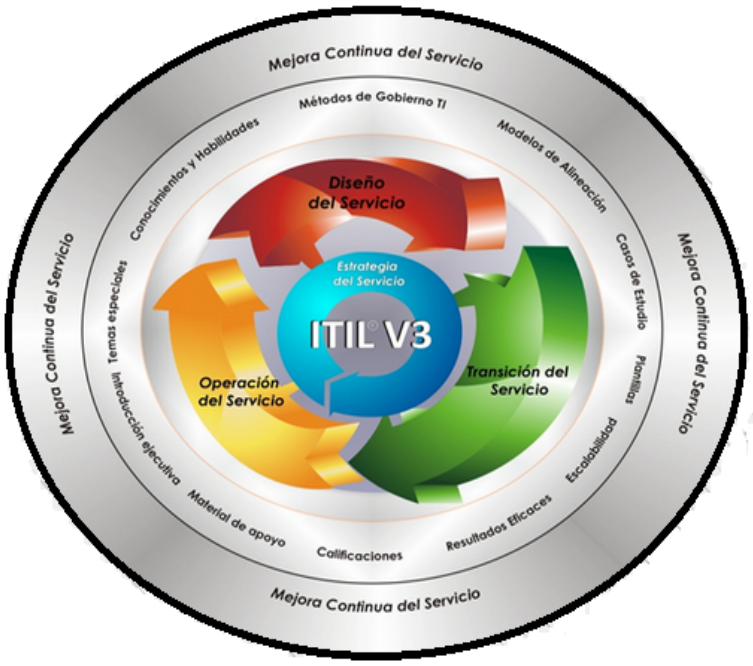

Figura 3. Ciclo de Vida del Servicio de ITIL

Tomado de: (COBIT, 2007)

Tabla 1.Procesos de ITIL V3

Volumen	Procesos
Estrategia del Servicio	Gestión Financiera, Gestión de Portafolio de Servicios, Gestión de la Demanda
Diseño del Servicio	Gestión de Catálogo de Servicios, Gestión de Niveles de Servicio, Gestión de la Capacidad, Gestión de Continuidad de Servicios TI, Gestión de la Disponibilidad, Gestión de Seguridad, Gestión de Proveedores.
Transición del Servicio	Gestión de Configuración, Gestión del Conocimiento, Gestión de Cambios, Gestión de liberaciones de nuevas versiones en plantaciones
Operación del Servicio	Gestión de Incidentes, Gestión de Peticiones, Gestión de Problemas, Gestión de Eventos, Gestión de Acceso a los servicios TI
Mejora Continua del Servicio	Evaluación de Servicios y Evaluación de Procesos, Definición de Iniciativas de Mejoramiento y Monitorización

Adaptado de :(OSIATIS ITIL v3, 2011)

1.3.4. Ventajas

La utilización de ITIL y de sus buenas prácticas para la gestión de servicios tecnológicos, se logra conseguir beneficios como los siguientes:

- ✓ Reducir los costos externos y internos.
- ✓ Mejor utilización de los recursos de la empresa.
- ✓ Mejorar trato del cliente por lo que mejora el servicio.
- ✓ Alinear TI con el Negocio.
- ✓ Mejor comunicación y flujo de información entre todos los empleados.
- ✓ Mejorar la productividad y desarrollo.(MOLINA, 2008)

1.4 COBIT 5

1.4.1 Historia

El proyecto COBIT(Control Objetives for Information and related Tecnology) es una herramienta de gobierno de las Tecnologías de la Información se emprendió por primera vez en el año 1995, se lo realizo con el fin de crear un mayor producto global que tenga un impacto duradero en los campos de los negocios y tener control sobre los sistemas de información que consta los negocios.(EXACTA-COBIT, 2013)

La primera edición de COBIT fue desarrollada y publicada 1996 y se lo realizo en 98 países comenzó como herramienta de Auditoría, la segunda edición se publicó en Abril de 1998 y desarrolla y mejora lo que tenía la versión anterior mediante un mayor número de referencias y documentos que fueron revisados de manera detallada por lo que intensifican las líneas de Auditoria en esta etapa llega el Control, ya anteriormente es aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que implica, se utiliza para controlar, planear, implementar y evaluar el gobierno sobre TIC[1], que permite a la Gerencia cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgo de negocios.(EXACTA-COBIT, 2013)

La tercera versión aparece en el 2000 con la evolución de la Gestión (la versión online estuvo disponible en el 2003), la cuarta versión aparece en diciembre de 2005 donde se toma en cuenta por separado estándares como son Risk IT(2009), Val IT 2.0(2008) y BMIS(2010) igual que en la versión 4.1 que salió en mayo del 2007, y la versión 5 y vigente desde abril del 2012 los estándares utilizados por separados en las versiones anteriores se acoplan en uno solo para así tener hasta la actualidad el Gobierno TI. (EXACTA-COBIT, 2013)

[1] TIC: Tecnologías de la Información y la Comunicación (Information Technology and Communication)

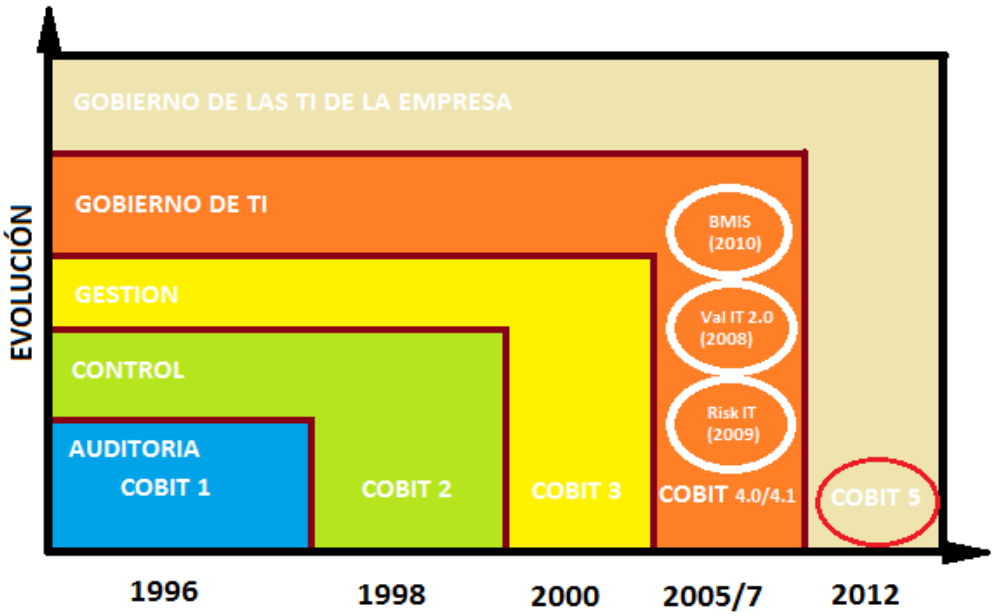

Figura 4.Evolución de Cobit

Tomado de: (EXACTA-COBIT, 2013)

La motivaciones para el desarrollo de un marco de referencia es que proporcionan una guía en la Arquitectura Empresarial en la Gestión de activos y servicios, modelos emergentes de organización y internalización/internalización.(EXACTA-COBIT, 2013)

Las necesidades de las empresas para el desarrollo de dicho marco son que necesitan lograr mayor creación de valor, obtener satisfacción del usuario de negocios, lograr el cumplimiento de las leyes pertinentes**,** reglamentos y políticas, mejorar la relación entre negocio y TI entre otras, esto se debe a gran parte a que la información tienen un ciclo de vida vital ya que es creada, usada, conservada, revelada y destruida, la tecnología desempeña un rol clave en estas acciones ya que ella penetra todos los aspectos del negocio y de la vida personal, cualquier tipo de empresa necesita ser capaz de poder confiar en información de calidad para así poder apoyar las decisiones ejecutivas.(EXACTA-COBIT, 2013)

COBIT 5 no es simplemente para las TI ni tampoco para grandes negocios, es gobernar y administrar información, cualquiera que sea el medio que se utilice y eso se lo realiza en negocios globales, multinacionales, Gobierno nacional y local, Organizaciones de beneficencia y para las empresas sin fines de lucro, empresas pequeñas a medianas, clubes y asociaciones.(EXACTA-COBIT, 2013)

COBIT5 proporciona un marco de referencia amplio, que ayuda a las empresas a alcanzar su metas y ofreces valor , a través de una gobernabilidad y gestión eficaz, define el punto de partida, crea una visión más holística y crea un lenguaje común entre TI (EXACTA-COBIT, 2013)

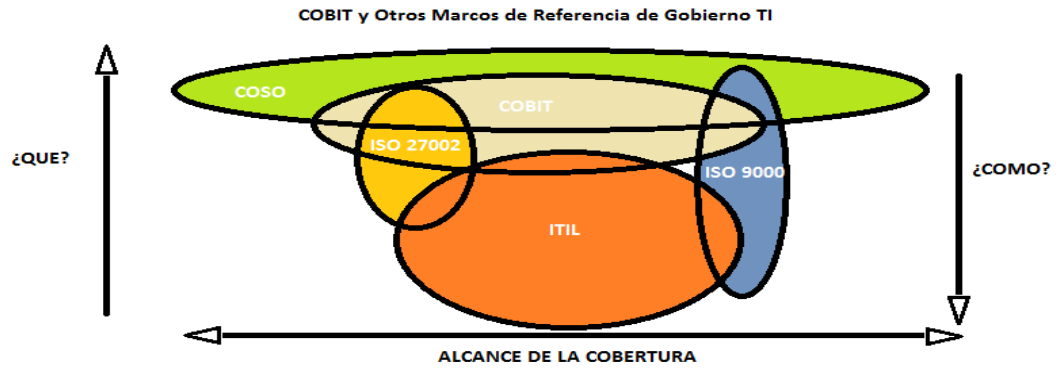

Figura 5. COBIT y Otro Marcos de Referencia de Gobierno de TI

Tomado de : (EXACTA-COBIT, 2013)

1.4.2 Principios de COBIT

Existen cinco principios:

- Satisfacer las Necesidades de las Partes Interesadas.
- Cubrir la Empresa Extremo a Extremo.
- Aplicar en Marco de Referencia Único Integrado.
- Hacer posible un Enfoque Holístico.
- Separar el Gobierno de la Gestión.(EXACTA-COBIT, 2013)

1.4.3 Dominios

Según ISACA, “El modelo de referencia de proceso de COBIT 5 es sucesor del modelo de proceso de COBIT 4.1, con los modelos de proceso de Risk IT [2] y Val IT [3] también integrados. El mismo que tiene 5 Dominios y 37 procesos de gobierno y gestión:

- ✓ Evaluar, Orientar y Supervisar
- ✓ Alinear, Planificar y Organizar
- ✓ Construir, Adquirir e Implementar
- ✓ Entregar, dar Servicio y Soporte
- ✓ Supervisar, Evaluar y Valorar” (EXACTA-COBIT, 2013)

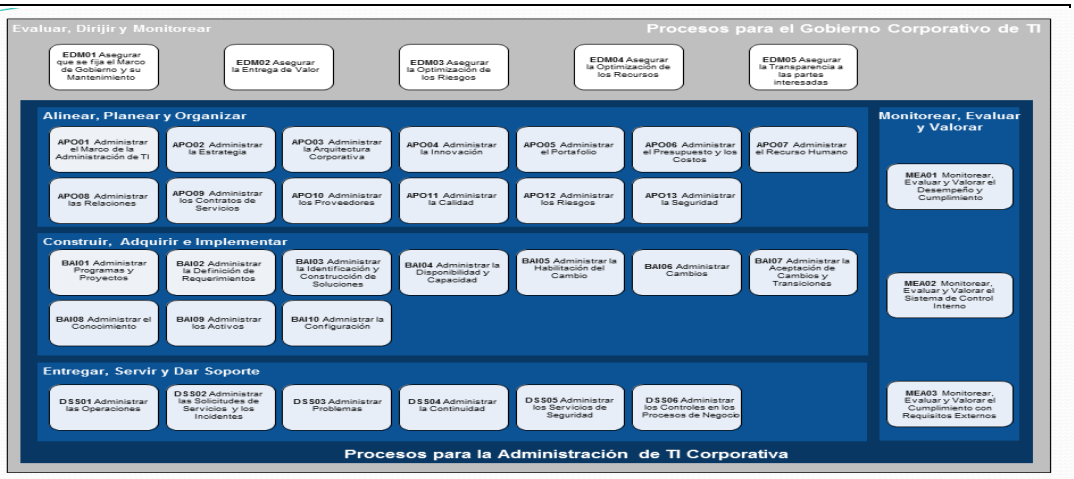

Figura 6. Dominios de Cobit

Tomado de :(EXACTA-COBIT, 2013)

El modelo de COBIT 5, no es una ordenanza o no debe ser cumplido de manera obligatoria pero radica a que varias organizaciones empresariales implementen una gestión de los procesos para que de esta forma las áreas claves estén cubiertas.(EXACTA-COBIT, 2013)

[2]RISKIT: Riesgos Relacionados con la tecnología de la información
[3]VALIT: Valor de las Inversiones de TI

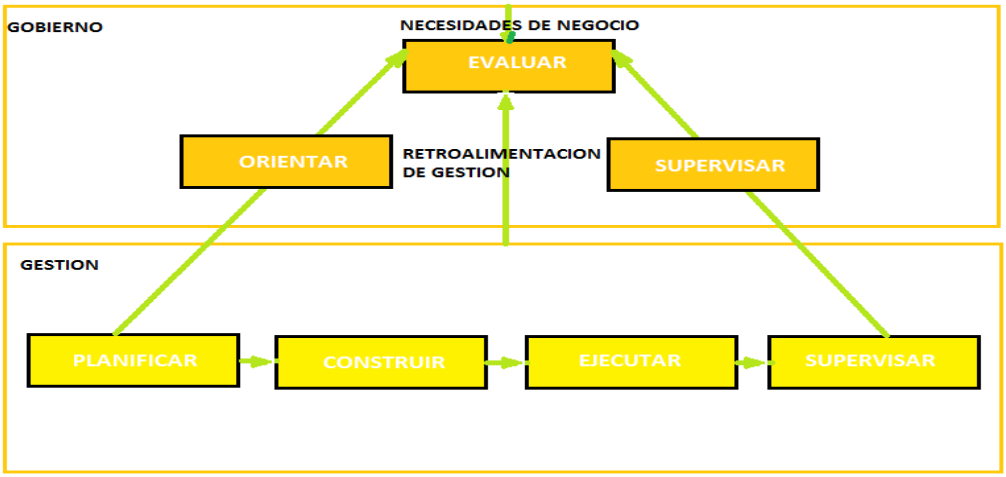

Figura 7. Modelo de Cobit 5

Tomado de : (EXACTA-COBIT, 2013)

1.4.4 Matriz RACI

En la última versión de COBIT se indica y se emplea matriz RACI que sirve y ayuda para describir las funciones y responsabilidades de tal forma que ayuda a tener una mejor visión, más detalle, claridad del negocio y el rol que desempeña sus funciones, para cada práctica de manejo.(ISACA, 2013)

Matriz RACI DSS02																									
Prácticas Clave de Gestión	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.						I					I	I									A		R			I
DSS02.03 Verificar, aprobar y resolver peticiones de servicio.						R												I		R	R		A			

Figura 8. Matriz RACI

Tomado de : (ISACA, 2013)

1.4.5 Ventajas

Las ventajas de usar COBIT 5 son:

- ✓ “Incremento de la creación de valor a través un gobierno y gestión efectiva de la información y de los activos tecnológicos. La función de TI se vuelve más enfocada al negocio
- ✓ Incremento de la satisfacción del usuario con el compromiso de TI y sus servicios prestados – TI es visto como facilitador clave.
- ✓ Incremento del nivel de cumplimiento con las leyes regulaciones y políticas relevantes
- ✓ Las personas que participan son más proactivas en la creación de valor a partir de la gestión de TI”. (ISACA, 2013)

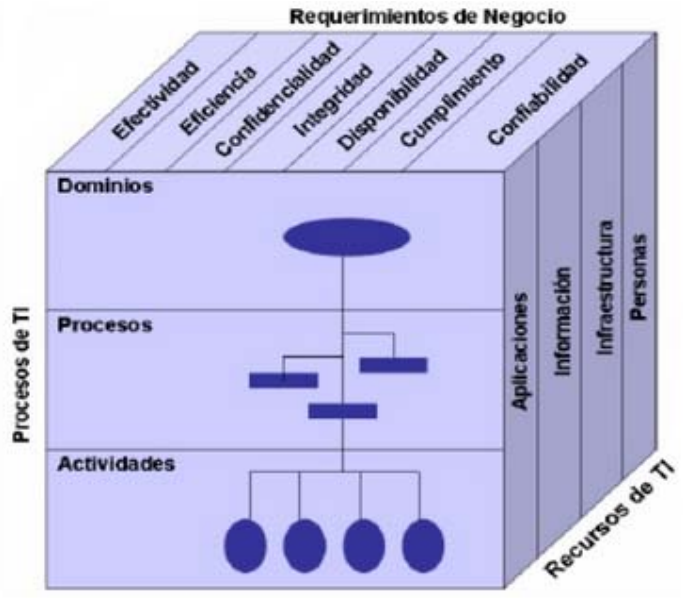

Figura 9. Cubo COBIT

Tomado de :(ISACA-COBIT, 2013)

1.5 Norma de Control Interno de Contraloría General del Estado

1.5.1 Historia

Mediante Acuerdo 000971, la Contraloría General del Estado expidió las primeras Normas Técnicas de Control Interno conjuntamente con las Políticas de Contabilidad, Normas Técnicas de Contabilidad y Políticas de Auditoría del Sector Público. Esta normatividad fue actualizada en abril de 1994, con la expedición del Acuerdo 017-CG.(CONTRALORÍA GENERAL DEL ESTADO, 2009)

Con el propósito de asegurar la correcta y eficiente administración de los recursos y bienes de las entidades y organismos del sector público ecuatoriano, en el año 2002, la Contraloría General del Estado emitió las

Normas de Control Interno, que constituyen lineamientos orientados al cumplimiento de dichos objetivos.

La norma vigente y actualmente utilizada por instituciones es la publicada en el 2009 mediante Acuerdo 039 - CG - 2009 (16/11/2009) R.O. 78 (01-12-2009) Y SUPLEMENTO R.O. 87 (14/12/2009).

El organismo encargado del control de los ingresos públicos en el Ecuador es la Contraloría General del Estado, quién se encuentra inmersa en el proceso estratégico de cambio que tiende a mejorar los servicios que brinda al Estado, orientando su accionar sobre la base de políticas que se enmarcan en la dinámica de la planificación, dirigida a la obtención de resultados óptimos en el control del uso de los recursos públicos que coadyuven en la toma de decisiones adecuadas por parte de los administradores públicos. (CONTRALORÍA GENERAL DEL ESTADO, 2009)

Es así como la Auditoría en el Sector Público se constituye en un examen objetivo, sistemático, independiente, constructivo y selectivo de evidencias, efectuadas a la gestión institucional en el manejo de los recursos públicos, con el objeto de determinar la razonabilidad de la información, el grado de cumplimiento de los objetivos y metas así como respecto de la adquisición, protección y empleo de los recursos humanos, materiales, financieros, tecnológicos, ecológicos y de tiempo y, si estos, fueron administrados con eficiencia, efectividad, economía, eficacia y transparencia. (CONTRALORÍA GENERAL DEL ESTADO, 2009)

1.5.2 Normas

Las Normas de Control Interno se encuentran agrupadas por áreas, sub-áreas y títulos. Las áreas de trabajo constituyen campos donde se agrupan un

conjunto de normas relacionadas con criterios afines y se clasifican según la Contraloría General del Estado en:

- ✓ “Normas generales de control interno
- ✓ Normas de control interno para el área de administración financiera gubernamental
- ✓ Normas de control interno para el área de recursos humanos
- ✓ Normas de control interno para el área de sistemas de Información computarizados: la misma que contiene lineamientos en el capítulo 410 Tecnología de la Información que permite a las organizaciones establecer controles de sus recursos tecnológicos.
- ✓ Normas de control interno para el área de inversiones en Proyectos y programas”. (CONTRALORÍA GENERAL DEL ESTADO, 2009)

1.5.3 Ventajas

- ✓ Permite controlar la utilización de los recursos estatales de todos los organismos públicos.
- ✓ Proporciona una seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.
- ✓ Cumple con el ordenamiento jurídico, técnico y administrativo, promoviendo la eficiencia y eficacia de las operaciones de la Entidad y garantizar la confiabilidad y oportunidad de la información.
- ✓ Son normas publicadas por la Contraloría General del Estado que rigen de forma mandatorio sobre el sector público. (CONTRALORÍA GENERAL DEL ESTADO, 2009)

CAPÍTULO II

2. Herramientas informáticas, su función, uso y alcance

2.1 Definiciones, usos y alcance de: internet, contraseñas, escritorio limpio, correo

2.1.1 Internet

El Internet es una red desarrollada en toda la extensión del Globo Terráqueo que interconecta equipos tecnológicos y ofrece varios servicios a sus usuarios, lo cual permite la comunicación instantánea con cualquier ordenador del mundo, a la vez que nos permite compartir recursos. Todos los servicios que ofrece Internet son llevados a cabo por ordenadores encendidos y conectados a Internet, el objetivo primordial es que los usuarios soliciten servicios.(RAMÍREZ, 2011)

2.1.1.1 Breve historia del Internet

El internet nace en el año 1969 y se lo realiza con fines únicamente militares para defensa estadounidense, consistió en crear una red de comunicación segura ARPANET (Red de Agencia de Proyectos de Investigación Avanzada, que conectó unos 60.000 ordenadores dispersos).Luego de ello a finales de 1989, el informático británico Timothy Berners Lee, desarrolla la World Wide Web para la CERN (Organización Europea para la Investigación Nuclear). Después de ello saliendo ya del ámbito estrictamente militar Arpanet creció en Estados Unidos conectando gran cantidad de universidades y centros de investigación. Tanto avanzó este desarrollo que en diferentes lugares del mundo se conectaron, llegando a conocerlo como la gran telaraña mundial (World Wide Web). En 1990, Arpanet fue sustituida por la Red NSFNET (Red de la Fundación Nacional para la

Ciencia) para conectar sus supercomputadoras con las redes regionales. En la actualidad, la NSFNET funciona como el núcleo de alta velocidad de Internet. No es hasta 1994 cuando Internet comienza a parecerse a lo que hoy conocemos: una puerta al mundo accesible para cualquiera. (Ministerio del Interior- Chile, 2016)

2.1.1.2 Ventajas y riesgos

Existen varios hitos importantes en lo cual el internet se fundamenta tanto en ventajas y riesgos:

Acceso anónimo: En este aspecto el eje primordial es que los usuarios pueden esconderse detrás del anonimato y esto hace que se sientan libres de realizar acciones o acceder a informaciones que no la realizarían si se le exigiese una autenticación.(Ministerio del Interior- Chile, 2016)

Acceso permanente: El tener un acceso al Internet las 24 horas al día por ancho de banda y costos relativamente bajos hace que los riesgos aumenten si no se controla la información ingresada o el tipo de uso que se lo puede dar tanto en para trabajadores, educadores o padres a sus hijos que corre riesgos permanentes, el acceso permanente debe ir de la mano con buenas prácticas de uso del internet. (Ministerio del Interior- Chile, 2016)

Facilidad de acceso a la información: El internet tiene disponibilidad a varios recursos gratuitos, servicios y de acceso rápido que no siempre son recomendados tanto en lugares de trabajo causando robo de información o en usuarios jóvenes que están en las primeras etapas formativas.(Ministerio del Interior- Chile, 2016)

Facilidad en la transmisión de la información: El internet en un medio multiplicador y un eficiente medio de transmisión de la información, esto lleva a que se trasmita tanto los aspectos positivos como los negativos.(UTE, 2013)

Facilidad de relación interpersonal: Elteneranonimato en ciertos usuarios malintencionados con el que se mueven los internautas permite que

no se conozca las personalidades y se enmascaren actitudes perversas que quedarían de manifiesto con la presencia física. Para lograr tener una facilidad de comunicación se requiere siempre una madurez y capacidad de discernimiento de la que no todos los usuarios disponen. (Ministerio del Interior-Chile, 2016)

2.1.1.3Ventajas

- El uso del internet no se lo puede catalogar como bueno o malo depende mucho del uso que los usuarios se lo den y de los objetivos que se persigan al acceder. Se va a enumerar algunas ventajas que tiene el internet.(UNIVERSIDAD ECOTEC)
- Ayuda a la socialización. El fácil acceso a Internet y la utilización de algunos de sus servicios (chats, juegos en red, video conferencias ...) ayuda en los negocios o las intercomunicación entre usuarios lo cual facilita muchos procesos de socialización, esto hace que se refuerce el sentido de pertenencia al grupo así como sus habilidades para comunicarse con el resto del grupo utilizando estos servicios basados en las TIC.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)
- Ayuda a que exista canales de información y comunicación en territorios cada vez más alejados, pueblos, que llevan consigo a entregar información como ciencia, cultura.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)
- Permite que se pueda desarrollar nuevas maneras de aprendizaje en personas con discapacidad o problemas de movilidad que puedan proseguir con su aprendizaje y sigan siendo de gran aporte a la humanidad.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)
- Acceso a gran cantidad de información de cualquier tipo. Noticias, eventos, prensa electrónica, bibliotecas on-line, información cultural, información científico-técnica, etc. Es importante recalcar que existe una

cultura informática, lo cual colectivamente se ayuda en beneficio de todos. Esto ayuda al crecimiento intelectual más rápido y eficaz, pero no siempre se debe manejar las páginas de consulta como fuentes reales que promueven información si no solo como fuente de guía.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

- Permite un mejor seguimiento por parte de los usuarios a sus trabajos o de los jefes a los recursos y documentos de sus colaboradores realizando seguimiento a las funciones diarias, se mantiene un contacto más frecuente con personas que ayuden a este tipo de trabajos o de colaboradores para requerir información; recibir indicaciones y sugerencias relativas a la formación profesional, así como mantenerse informados de disposiciones, etc. (DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

2.1.1.4 Riesgos

Debido a la facilidad que se puede conectar con el internet y a las ventajas que esto representa, es necesario conocer información que nos ayuden a verificar los riesgos y lograr aprender la manera de manejarlos y realizar un responsable, útil y constructivo de la red. (DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

a) Relativos al acceso a la información.

Siempre es importante hacer una serie de consultas para verificar si la información es adecuada y que nos ayuden o aporten seguridad verificar su origen y si está actualizada. Pero se debe tener encuentra de la búsqueda de información puede conllevar una pérdida de tiempo importante y así mismo la propia navegación puede dispersar la atención. La mayoría de veces , al navegar se va pasando de una página a otra olvidando el objetivo inicial de la visita. (DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

b) Relativos al tipo de información.

Ayuda a facilitar el acceso a información que en nuestros tiempos es inadecuada para todos los usuarios, esto es porque el contenido de la información es de violencia, terrorismo, pornografía, sectas, etc., o es presentada de forma inadecuada teniendo comportamientos y actitudes socialmente reprobables. Debido a lo complicado de la red se hace imposible poderla manejar o tener un control sobre todas las publicaciones de usuarios, autores, gente anónima para poder penalizar en caso de información no adecuada. (DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

c) Relativos a relaciones personales.

En nuestra actualidad las relaciones entre usuarios se facilita con la llegada del internet y en la mayoría de veces produce que dichos usuarios tengan comportamiento desinhibidos para causar otra imagen de lo que no son con su realidad, pero en el otro extremo también puede causar que los usuarios tengan comportamientos de aislamiento por no poder interactuar o socializar de manera adecuado con otras personas. (DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

- Se puede producir una pérdida de intimidad: Existen varios tipos de servicio adecuados e inadecuados los cuales para poder acceder los usuarios necesitan ingresar información personal a terceros o desconocidos, con riesgo de no saber de manera óptima lo que realizaran con dicha información.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

- Amistades no convenientes: A través de chats o redes sociales los usuarios contactan con personas de dudosa reputación, de carácter violento e intenciones no muy claras que enmascaran, todo ello, bajo la apariencia de amistad y entretenimiento.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

- Adicciones: No lograr tener un control(referida a control temporal) de Internet puede provocar que los usuarios dependiendo su criterio, perfiles o las circunstancias personales por las que estén atravesando se enfoquen en búsquedas de información, juegos de red, chats, pornografía que los encierre en circunstancias o desordenes.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

d) Relativos a la comunicación.

El tener la necesidad de estar comunicados con los demás hace que no podamos ver los riesgos que corremos con servicios que trabajamos día a día, estos riesgos se producen en servicios implicados, como son el correo electrónico, cuentas bancarias, redes sociales, los blogs, chats, foros, etc. En nuestra actualidad ya es común encontrar problemas en todas las empresas de robo de información derivados de la recepción masiva de correos basura (spam), el hackeo o bloqueo de nuestras cuentas al recibir y abrir correos con archivos adjuntos que gran tamaño, la entrega de información en chats y foros a los que nos requieren información personal que se utilizada de manera inadecuada. (DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

e) Relativos al propio funcionamiento de Internet.

Internet no es una red segura. Se tiene muchos errores de seguridad lo cual produce situaciones de alarma, esto se debe a agujeros o errores que tiene la tecnología que la sustenta. Para entenderlo por ejemplo los virus y gusanos que dañan y destruyen los equipos, problemas de saturación que dificulta la navegación y los accesos por personas no autorizadas por nosotros a los recursos de nuestras maquinas.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

2.1.2 Contraseñas

Las contraseñas o password en cualquier sistema computacional, redes sociales, internet,etc., sirve para autentificar a un usuario, es utilizada para la verificación de identidad asegurando que sea una persona la que se encuentra al otro lado de la conexión.(CÁRDENAS, 2012)

Si otras personas lograran tener acceso a nuestras contraseñas pueden ser utilizadas con fines perjudiciales o de robo de información .Las contraseñas es la manera de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.(CÁRDENAS, 2012)

La lengua inglesa tiene dos denominaciones para las contraseñas password(palabra de acceso) y pass code (código de acceso), no necesariamente la primera implica usar alguna palabra existente pero en la mayoría de claves se les coloca palabras que sean fácil de recordar para el usuario.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

2.1.2.1 Breve historia

El uso de contraseñas tiene origen en la antigüedad donde los centinelas que vigilaban una posición especifica en algún paramo o sector solicitaban a la gente que circulaba el "santo y seña" para que puedan pasar. Únicamente se permitía el acceso a aquella persona que conoce la seña. (WIKIPEDIA, 2013)

En la época actual o desde comienzos de la era tecnológica con el nacimiento del internet con fines militares, se introdujeron las contraseñas para proteger la información de carácter confidencial, debido al alto número de secretos militares o personales en el mundo las contraseñas se han adaptado a políticas de seguridad para tener cifrados, complejidad, caracteres, etc., lo cual ayuda a protegernos de personas que desea violentar dicha información.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

Las contraseñas son comúnmente para controlar el acceso a los sistemas operativos, teléfonos celulares, decodificadores, cables personales de cajeros automáticos, etc.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

Las contraseñas comúnmente va asociadas a códigos alfanuméricos (también llamados PIT- Personal Identification Text). La segunda frecuentemente se liga a la utilización de un códigoalfanumérico(así mismo se llama PIN-Personal Identification Number), esto también se maneja en el idioma español ya que clave y contraseña se usan indistintamente.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

2.1.2.2 Ventajas y riesgo

Ventajas

- Fácil de implementar
- Bajo costo (no requiere software sofisticados)
- Fácil de usar(al menos que se olvide lacontraseña)
- Debe existir mejores prácticas para el uso de contraseñas como son la longitud, complejidad
- Protege la seguridad de nuestros documentos de la red
- Nos ayuda verificar que la persona que ingrese a herramientas o servicios de la web sea real un usuario cabe recalcar que no siempre la identidad es la verdadera.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

Riesgos

- Fácil de adivinar si la contraseña no es compleja

- Puede ser infiltrados o utiliza fuerza bruta

- Los usuarios en la mayoría de ocasiones olvidad sus contraseñas o incluso anotan en documentos lo que causa que deje de ser privado y se convierta en publico

- Posibles robos informáticos en cuentas bancarias o recursos.

2.1.3 Escritorio Limpio

El escritorio limpio aparece como tema de seguridad informática, donde en la actualidad se lo estableció como política, un puesto de trabajo que tiene un escritorio desordenado es propenso y vulnerable, esto es porque entre los escritorios existe información personal y profesional confidencial que pueden ser potencialmente peligrosas para nuestro trabajo.(Auditoria-MCYP, 2011)

2.1.3.1Breve historia

Desde siempre el ser humano debido a los distintos trabajos tanto gubernamentales como privados maneja información o genera información que son importante para los lugares donde se trabaja, debido al alto crecimiento de la tecnología los documentos donde antes se archivaba en bodegas de seguridad o archivos internos de cada empresa son cada vez más extensos y vulnerables por lo que se los guarda en los computadores o archivos físicos de cada usuario, al hablar de escritorio limpio no solo se habla aparentemente de ser organizado si no solo se habla de documentos en la mesas de trabajo, celulares, agendas, pantallas del computador desbloqueadas, papeles adhesivos con información personal y incluso contraseñas de servicios, documentos olvidados en la impresora, documentos con información encontrados en el tacho de la basura, llaves, tarjetas de acceso, etc.(CSI, 2013)

El mantener un escritorio limpio tiene solamente ventajas ya que las desventajas no ocurren al mantener nuestra información con cuidado, por lo que es importante fomentar el buen uso de todos los recursos que forman parte de nuestros escritorios y de todo nuestros entornos más cercano, con esto se logra evitar riesgos de ambiente externo que puedan afectar a los activos de la información personales y de la empresa.(CSI, 2013)

2.1.3.2 Ventajas

- Es fundamental el orden y la limpieza para tener una organización que permita trabajar más eficientemente con ello se puede lograr mayor productividad y aprovechar los tiempos libres de mejor manera.

- Mantener organizadores que realice que sobre nuestros escritorios no exista información sensible expuesta, causa que no exista perdida de información.

- Se evita dejar información sensible a disposición de personas no autorizadas.

- Guardar bajo llave documentación sensible o secreta nos ayuda mantenerla alejado de personas no autorizadas.

- Procurar no trabajar con USB o pendrives, CDs que contengas información vulnerables nos ayuda evitar que si se deja en lugares visibles y fácilmente accesibles sean robadas o extraviadas.

- El no tener documentos encima de los escritorios con contraseñas y usuarios, o números de cuenta corriente nos protege del robo de los mismos.

- Dejar apagado nuestro computador hace que ahorremos energía y si por algún motivo existe un corte del mismo no se pierda documentos en los que estemos trabajando.(CSI, 2013)

2.1.4Correo electrónico

El correo electrónico es un servicio comúnmente gratuitito en el que usuarios en todo el mundo pueden enviar y recibir mensajes, imágenes, archivos, de manera instantánea a través del internet; trabaja en el protocolo SMTP, aunque por extensión también se lo puede ver aplicado en sistemas análogos que usen otras tecnologías.(CSI, 2013)

2.1.4.1 Breve historia del correo electrónico

La manera de comunicarse de las personas ha trascendido durante muchísimos años, las sociedades cada vez más han evolucionado al tener contacto con otras personas. Debido al crecimiento de las poblaciones el comercio y la comunicación ha sido el eje fundamental para dichos procesos. Por ello se puede decir que la comunicación entre las personas es tan remota como nuestra propia historia, siendo los mensajeros uno de los personajes más antiguos y importantes hasta en nuestra actualidad.(AVILA, 2016)

Aunque la comunicación provenga de un pasado sumamente antiguo en si el correo aparece en España y se debe a los romanos.El cursus publicus, como se lo conocía, era una larga red de caminos los cuales recorrían toda la geografía Hispania portando mensajes para el ejército o los administradores romanos.(AVILA, 2016)

Luego de ello durante la Edad Media numerosos reinos crearon sus propios sistemas de correo donde los mandaderos iban de una corte a otra llevando información que los Reyes mandaban.(AVILA, 2016)

Durante el siglo XI, la evolución del servicio de correo se convirtió en revolución tras la construcción del ferrocarril en España, estohizo que mejore notablemente la entrega de cartas y sobres con documentos a cualquier lugar o persona es esa región.(AVILA, 2016)

En nuestra actualidad con el crecimiento de nuevas tecnologías el correo se ha consolidado en todos los ámbitos tanto en rapidez como confianza, pero con la aparición del internet es necesario conocer como se lo implemento, el correo electrónico fue creado en 1971 por Ray Tomlinson, él fue un ingeniero de Bolt Beranek and Newman, esta fue la empresa encargada de poner en marcha Arpanet. Tomlinson nunca considero haber realizado un experimento importante y a pesar de que no existía manera de enviar mensajes a otra persona de una red, lo que logro fue una difusión de servicios para chequear una cuenta POP desde cualquier navegador.(AVILA, 2016)

Se presume que uno de los primeros mensajes enviados fue "QUIEJKDHNC" que fueron teclas usadas al azar por motivos de pruebas, esto lo indico el inventor, el cual fue enviado por un programa que el invento y que se llamaba SNDMSG.Cuando el experimento se acababa en 1971 los EEUU deciden contratar Bol Beranek la empresa de Tomlinson para crear una red Arpanet se les ocurrió la idea de crear un sistema para enviar y recibir mensajes por la red.(AVILA, 2016)

Tomlison había escrito un programa para los desarrolladores de la Arpanet y que ellos se dejaran mensajes en sus ordenadores que compartían(15 en toda la red nacional),investigando con otros protocolos para transferir archivos entre las maquinas el noto que juntos podían usarse para acceder a todas las casillas de correo.(AVILA, 2016)

2.1.4.2Ventajas

- Facilita la vida comunicacional de las personas y de las empresas

- Mejora en tiempo y distancias entre las personas para su comunicación.
- Se puede enviar cualquier tipo de archivos de audio, video, documentos, en diferentes tipos de programas.
- Se pude revisar en cualquier lugar del mundo que tenga conexión a internet.
- La rapidez con que llega la información es casi inmediata.
- Es económico
- Se puede enviar mensajes sin importar la hora o el día.
- Ayuda a mejorar en medio ambiente.(AVILA, 2016)

2.1.4.3Desventajas

- Los correos son propensos a recibir virus
- Se recibe gran cantidad de SPAM que hace que nuestro correo este más lento y nos hace perder el tiempo.
- Debido al crecimiento tecnológico no existe problema en recibir correos si se tiene una conexión a internet pero aun existe sectores en el mundo donde no tienen dichas conexiones lo que puede ser complicado en la mayoría de los casos para comunicarse.(DIAGO, 2010)
- Si no se tiene un poco de conocimiento tecnológico se hace sumamente complicado manejar un correo.
- Debido a la gran cantidad de información que almacenamos en nuestros correos muchas veces tenemos información crucial como contraseñas o

cuentas bancarias o documentos confidenciales, lo que hace propenso para usuarios externos que desean robar y ocupar nuestra información con fines maliciosos.(DIAGO, 2010)

2.2 Uso del Internet, correo, escritorio limpio, contraseñas en el MCYP

El Ministerio de Cultura y Patrimonio debido a que ejerce rectoría del Sistema Nacional de Cultura para fortalecer la Identidad Nacional y Interculturalidad lo cual protege y promueve la diversidad cultural, artística, musical en el País utiliza las herramientas informáticas para distintos factores en su ciclo de negocio.

En la actualidad no existe políticas definidas regularizadas para poder solventar los requerimientos de los usuarios para el buen uso del Internet, correo, escritorio limpio, contraseñas, pero en base a disposición general de la Contraloría General del Estado con la Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos se establece lineamientos que deben ser cumplidos.

Dicha norma establece varios hitos que necesitan cumplirse a cabalidad, por lo que es un causante para el desarrollo de este documento, la norma explica que las entidades y organismos del sector público deben estar acopladas en un marco de trabajos para procesos de tecnología de la información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

Dicha norma, entre varios hitos expuestos habla de que debe existir un Plan informático estratégico de tecnología para administrar y dirigir todos los

recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de Gobierno.

La Contraloría General del estado en su hito 410-04 sobre Políticas y procedimientos establece que la máxima autoridad de la entidad aprobara las políticas y procedimientos que permitan organizar el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

Mediante dichas disposiciones el MCYP ha realizado cambios en su infraestructura tecnológica desde el 2013 para cumplir con las normas y sistemas de seguridad de la información mínimos para garantizar la eficacia, eficiencia y disponibilidad de todos los servicios tecnológicos de la Institución, en la actualidad se ha fortalecido los servicios y equipos y ya se puede proceder con las políticas establecidas.

La información de años anteriores para el buen uso de internet, contraseñas, escritorio limpio, correo nunca estuvo disponible y no existe documentos formales sobre elaboración de políticas o de la estructura de la red o los servicios no estuvieron claros.

En el 2014 se logró desarrollar los diagramas y servicios disponibles de la Institución teniendo un panorama más claro para el estudio de este proyecto para lo cual se gráfica y se explicara lo siguiente:

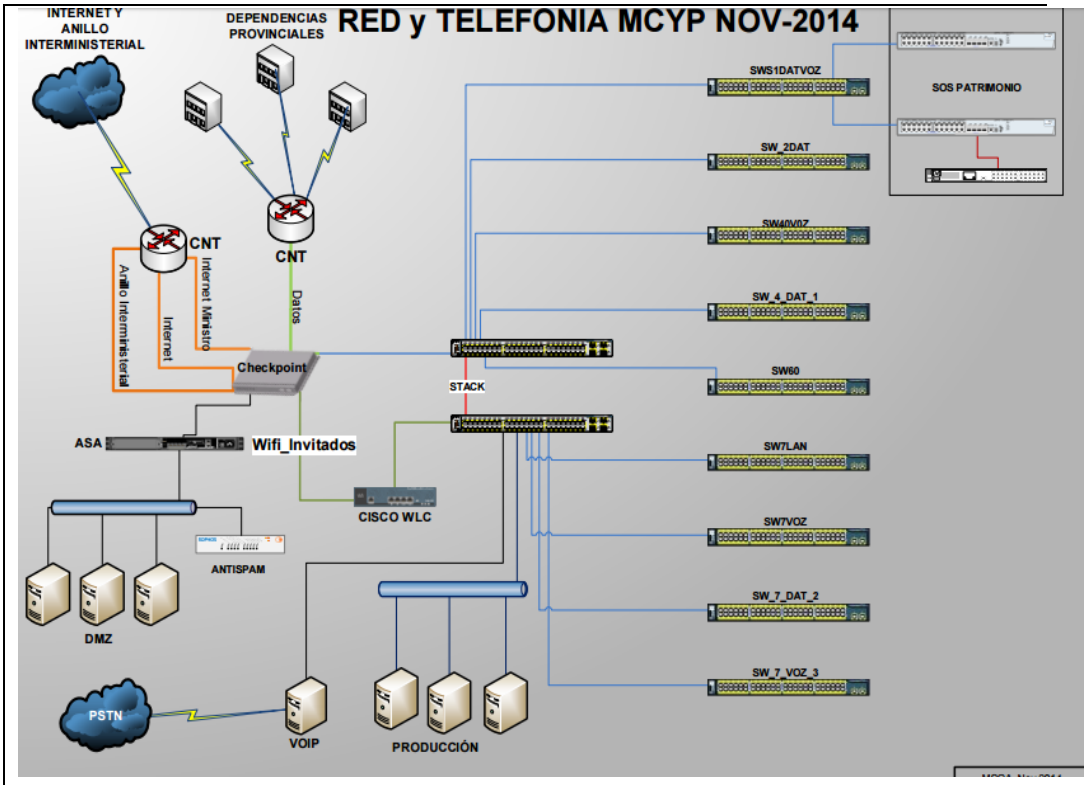

Figura 10. Red y telefonía MCYP Nov-2014

2.2.1Uso de Internet.

El MCYP tiene equipos de seguridad y servicios, además posee herramientas tecnológicas para corregir y monitorear la red, por ello es necesario implementar servicios de acceso a internet para el trabajo diario,

El equipo de mayor relevancia para dar servicio de internet con diferentes blades, los cuales realizan bloqueos, monitoreos, analizan la red, implementa políticas, se denomina CheckPoint el es la base estructural y primordial para brindar servicio de Internet.

El modelo del equipo es SmartDashboard R77.30 el cual protege y maneja toda la red del MCYP, entre sus blade está el Firewall, Application&URL Filtering, Data Loss Prevention, IPS, Threat Prevention, Anti-

Spam & Mail, Movile Acces, IPsec VPN, entre otros, el equipo está diseñado para cumplir ciertas reglas que vienen por default y nuevas que coloca el administrador de la red según sus necesidades y requerimientos, en base a la elaboración de políticas para el buen uso del internet, mismas que podrán ser implementadas en dicho equipo.

El equipo tiene paneles de logs, mensajes y acciones de posibles vulnerabilidades que se alinean a estándares como son la ISO27001,ISO27002, mismas que se acoplan a los marcos de referencia que expone la normativa COBIT y que para el tema de políticas nos guía en que se debe utilizar la normativa ISO.

Debido a que no existen políticas alineadas al buen uso del Internet el equipo en la actualidad cuenta con reglas que el administrador ha analizado y colocado según la necesidad y que el proveedor sugirió cuando realizaron la implementación.

El equipo por el momento contiene 3 perfiles principales para acceso a la red y perfiles secundarios para casos específicos, se debe tener en cuenta que todos los usuarios que no estén en dichos perfiles, el equipo los ubica en un grupo de perfiles básicos quienes deben cumplir todas las restricciones del administrador, esto puede ser modificado según los requerimientos del negocio, los perfiles son:

PRINCIPALES

VIP (Acceso total, excepciones en páginas como ejemplo pornografía, en este perfil se coloca solo usuarios de Jerárquico Superior)

Sistemas:(Acceso total, con restricciones como ejemplo juegos, pornografía), este perfil se coloca usuarios solo de sistemas que necesiten accesos a servidores o herramientas para el desarrollo o investigación de los servicios

Redes Sociales:(Acceso parecido a un perfil de carácter Normal a excepción que se da permiso a redes sociales, este perfil se coloca usuarios que tengan pedido por escrito de autorización del Jerárquico Superior)

SECUNDARIOS

Youtube(Acceso de perfil Normal y con habilitación solo Youtube, se coloca usuarios que realizan temas investigativos como por ejemplo, el MCYP cuenta con la reserva de videoteca y musicoteca ecuatoriana más grande en el país, esto hace que exista muchos videos de investigación y edición de dichos archivos, la herramienta facilita el trabajo del usuario.)

Teamviewer(Existe una cantidad reducida de usuarios que necesitan la comunicación vía remota a los archivos en sus computadores, esto se debe a que hay varios usuarios de campo que están constantemente en provincias desarrollando alguna actividad. En el 2015 el equipo de Sistemas del MCYP, trabajo en la implementación de VPN para 50 usuarios remotos con la instalación de un nuevo blade llamado Mobile Access, esto aun no está en producción pese a que ya está probado y en funcionamiento)

Debido a que no existe aun la implementación de políticas, no han sido regularizados varios de los servicios de internet con los que trabaja el MCYP, entre algunos se puede mencionar la autorización a redes sociales, bloqueo y desbloqueo de páginas web, informes mensuales de usuarios que tengan alguna violación a la seguridad o restricción a páginas y que constantemente desean ingresar, lo que probablemente se interprete como una violación a la intimidad pero en el caso de los administradores de red, da una señal de si está bien estructurado las políticas en el equipo y además que posiblemente el usuario tenga algún tipo de virus malicioso en su equipo lo que produce tráfico a la red o ataques para violentar la seguridad del equipo.

Muchos de los servicios de internet en los lugares de trabajo son violentados por el mismo usuario esto también se produce en el MCYP, ya que

debido a la influencia que tiene los usuarios de Jerárquico Superior, autoriz... el acceso a todos los servicios, redes sociales, desbloqueo de páginas, a usuarios que en su gran mayoría no necesitan el desbloqueo total a internet y al existir un monitoreo de la red por parte del administrador encuentra un gran trafico verificando por ejemplo que los usuarios se encuentran escuchando música desde Youtube.

Mediante las políticas que se elabora como guía en este documento, servirán para mejorar los servicios y corregir todo tipo de falencias y como indica la norma de control interno de la Contraloría General del Estado serán aprobadas por la Máxima Autoridad, lo cual será un agravante para sanciones e indicaciones de que se debe dar un buen uso de internet y cumplir con lo establecido en los documentos, bajo la Normativa ITIL se lograra saber cómo poder cumplir los procedimientos de manera óptima para brindar un buen servicio.

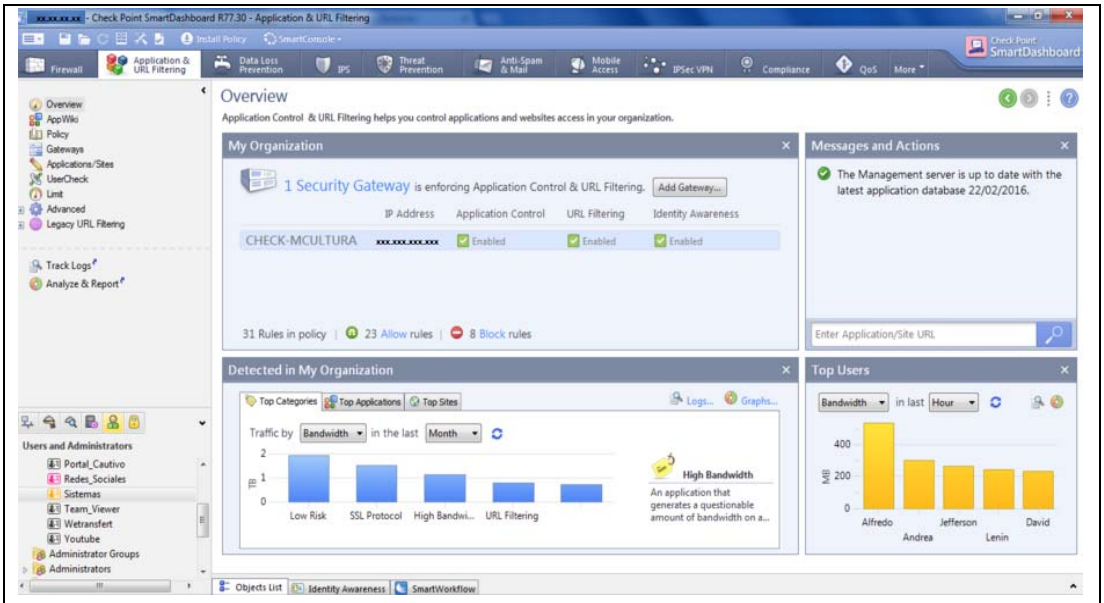

Figura 11. Equipo CheckPoint

Adaptado de: Equipo CheckPoint.

2.2.2Uso de contraseñas

Bajo lo expuesto anteriormente en MCYP tiene varios servidores informáticos, entre los cuales se encuentra el Active Directory, este equipo de seguridad que es fundamental para brindar servicio de internet debido a que es el DNS del MCYP, su réplica se encuentra en el edificio Aranjuez, el equipo es el que permite la administración de los usuarios.El MCYP en el 2014 realizo un despliegue para que todos sus equipos y servicios sean parte de un dominio único el cual es MCYP.LOCAL, dicho trabajo permitió tener en su gran mayoría un control de los equipos informáticos de la red. Active Directory permite muchas funcionalidades, entre las más importantes para este estudio es el tema de permisos a los usuarios, en la instalación o desinstalación de programas en sus equipos con perfiles de administradores o usuarios normales, como también el uso de contraseñas para ingresar a los computadores, permisos como ya vimos anteriormente de perfiles de internet y se acopla al uso del correo electrónico Zimbra. En cuanto a las contraseñas que maneja el MCYP, utiliza una sola para todos los servicios internos institucionales lo cual produce un gran avance de seguridad y que mediante el uso de buenas prácticas se puede lograr mantener una manera organizada del uso de dicha contraseña.

Debido a lo señalado anteriormente, se puede elaborar políticas de contraseñas cumpliendo ciertas normas de longitud, caracteres, periodo de validez, etc. En la actualidad el MCYP, tiene ciertas normas para el uso de sus contraseñas como son caracteres mínimos(8), el uso de mayúsculas y minúsculas, entre otros, pero ya que no existe regularización de la política no se puede exigir temas como periodo de validez. La normativa de control interno y el EGSI que se centra en la estructura de COBIT manejando la ISO27002, entre otros estándares de seguridad exigen que las contraseñas sean cambiadas durante un periodo de tiempo, lo cual se indicará más adelante, pero al no cumplir con el estándar de cambio de contraseña, los usuarios ocasionan a que las cuentas del MCYP sean violentadas y comienzan a existir

spam, es por ello que por más que se tenga un procedimiento para el bloqueo de la cuenta, verificación y cambio de contraseñas no se puede encontrar la mejor manera de monitorear las mismas.

Esto se puede evidenciar cuando las cuentas son expuestas en cybers o lugares con niveles de seguridad bajo, o como sabemos correos maliciosos que solicitan el ingreso de información. Estos correos vienen por ejemplo de la siguiente manera *"Su cuenta esta próxima a expirar, por favor ingrese su contraseña actual y su contraseña nueva caso contrario su cuenta será bloqueada "* y muchas veces acompañadas de logos de la institución, etc.

En MCYP en la actualidad ha trabajado con el Oficial de Seguridad que exige el SNAP (Secretaria Nacional de Administración Pública) para solventar dichos problemas, por lo que en la actualidad falta plasmar en documentos los temas de seguridad y en base a ITIL tener los mejores procedimientos para el uso de las contraseñas lo que se lo verá en los capítulos siguientes.

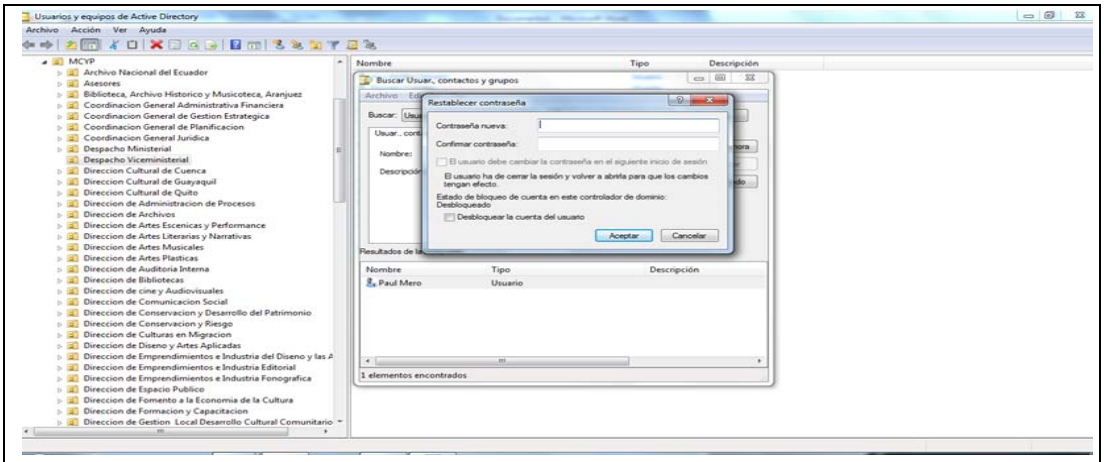

Figura12. Servidor Active Directory

2.2.3 Uso del Correo

El MCYP tiene un servidor correo electrónico propio llamado ZIMBRA, dicho servicio es colaborativo y libre, existe tanto para clientes como para

empresas por lo que el MCYP desde su inicio, adquirió licencias para la implementación de este servicio.

En la actualidad existe una cantidad aproximada de 700 cuentas activas en dicho servidor, y 40 listas para el envío de correos masivos.

El correo tiene un uso primordial para el trabajo diario en el MCYP, el cual es expuesto a violaciones de seguridad como por ejemplo el uso del mismo para envío o recibo de documentos que no tengan que ver con el rol del negocio, o para crear servicios web como ejemplo Amazon entre otros y arriesgar el uso del correo de la Institución por cualquier eventualidad que pueda ocurrir.

El servidor de correo tiene almacenado cuentas de usuarios que ya no pertenecen a la institución, este procedimiento exige el EGSI conjuntamente con el oficial de Seguridad que debe almacenarse por un periodo de 5 años los correos de todo el personal que labora o laboro en la Institución, el MCYP en la actualidad cuenta con servidores de respaldo, en el 2015 se realizó el procedimiento para la compra de un storage para el almacenaje de este tipo de servicios lo cual sigue en proceso hasta la presente fecha.

Bajo la normativa ITIL de buenas prácticas, el MCYP está trabajando en brindar un uso adecuado de los servicios, por lo que a inicios del 2015 se trabajó en el despliegue para la implementación en todos los equipos de los Usuarios del software Thunderbirt, esta herramienta sincroniza con los servicios de Zimbra pero con la gran ventaja de que almacena los correos electrónicos en los ordenadores de los Usuarios, pudiendo así archivar sin tener que eliminar los correos de sus bandejas esto debido a los perfiles que se maneja en el MCYP de capacidad máxima de almacenamiento las cuales son:

Jerárquico Superior (2 Gb)Usuarios (500 Mb)

Esto necesita una capacitación del uso y del buen manejo del mismo ha... poder implementar un servidor de almacenamiento.

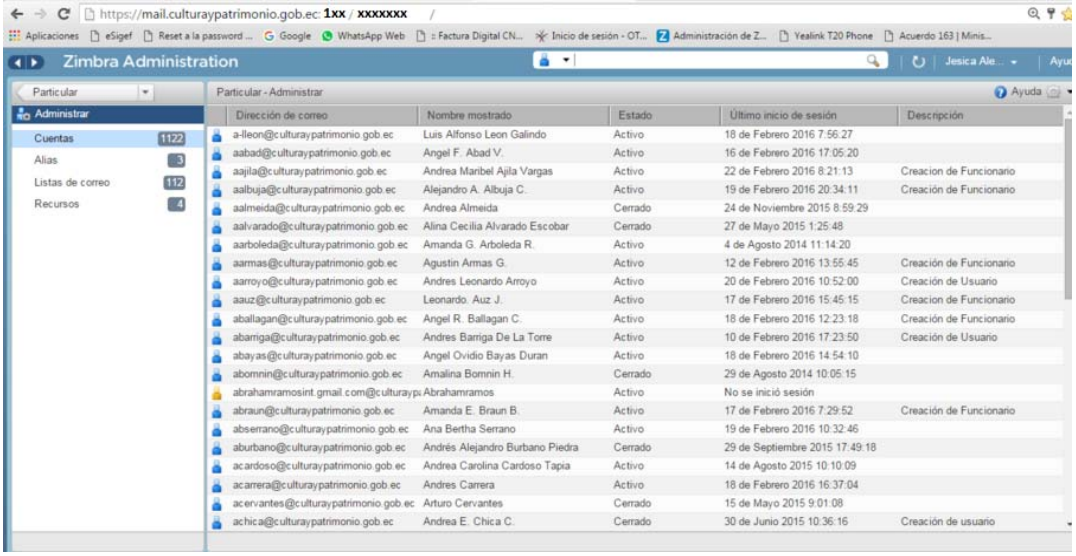

Figura 13. Servidor Zimbra

2.2.4 Uso de Escritorio Limpio

El MCYP no tiene ningún mecanismo en la actualidad para poder solventar el inconveniente que ocurre en todo tipo de entidades privadas y públicas, la política de escritorio limpio debe ser elaborada bajo la norma de control interno pero se debe analizar si puede intervenir ITIL para verificar temas de servicio u otra norma y realizar los despliegues necesarios para la definición particularmente de esta política.

La Coordinación General de Gestión Estratégica del Ministerio de Cultura y Patrimonio poseen entre algunas Unidades incluida TICs, la de Cambio y Cultura Organizacional, al hablar de Escritorio limpio como ya se indicó anteriormente no se está hablando de ser ordenando, se habla de tener un cambio organizacional de todos los recursos que se utiliza a diario sea estos

USB, pantallas desbloqueadas, papeles en la impresora, claves en nuestros escritorios, billeteras, celulares, etc.

En la actualidad la gran mayoría de Entidades Públicas poseen con documentación de suma importancia para el desarrollo del país al igual que con una serie de desperdicios de documentos que no son analizados y incurren en faltan grabes a las instituciones.

El 25 de Noviembre del 2011, se expidió la Ley de Fomento Ambiental y Optimización de Ingresos del Estado, entre algunas de las propuestas también se trabaja hasta la actualidad en una campaña denominada CERO PAPELES, este proyecto está basado en que se debe dejar de incurrir en el desperdicio de recursos naturales incluidos papel, botellas y demás, que se debe reciclar todo tipo de materia usado, el MCYP en el año 2014 ya procedió a fomentar dicha idea, pero en la parte tecnológica muchos usuarios imprimen o manejan su información inadecuadamente, impidiendo que se dé el cambio organizacional implementado y adecuado a los a los riegos de TICs adecuados.

Existe un exceso de trámites que manejan las instituciones públicas y existe la necesidad de evaluarlos. El proceso “Cero papeles” muestra un significativo avance a través de la gestión que realizan varias entidades, al igual que debe adaptarse políticas para mejorar el uso de dichos documentos e información de riesgos que tenemos en nuestros escritorios a diario. Con ello podemos adaptarnos al Plan de Desarrollo Nacional para el Buen Vivir.

Para optimizar los recursos se deben implementar por ejemplo claves a las impresoras para verificar el uso de documentos, pero además debe existir un mejor manejo de nuestro escritorio de trabajo.

El tener dispositivos de almacenamiento extraíble, donde se guarda información crítica y que pueda ser extraviada o equipos de uso personales como celulares incurren en faltas graves a la seguridad informática ya que en

ellos no solo se guarda información personal sino muchas veces de la empresa y en algunos casos claves de servicio entre otros.

2.3Alcance de los usos de los servicios en el MCYP

Para mejorar la confidencialidad, integridad y disponibilidad de los servicios tecnológicos en el MCYP es necesario implementar Políticas que ayuden a regularizar y establecer lineamientos a estos servicios.

Mediante normas como el EGSI(Esquema Gubernamental de Seguridad de la Información) que son normas para mejorar la calidad de los servicios institucionales tanto públicos como privados y que se alinean a COBIT el cual expresa el manejo de la ISO y mediante las normas de control interno dictado por la contraloría general del estado y que son de carácter obligatorio, que mediante Acuerdo Ministerial 804 y 837 del 29 de agosto de 2011,respectivamente, la Secretaria Nacional de Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de Administración Pública Central e Institucional.

Estos Acuerdos indica que es necesario adoptar políticas, estrategias, normas, procesos, procedimientos y medios necesarios para mantener la seguridad en la información que se genera y custodia en las diferentes medios y formatos de las entidades de la Administración Pública Central Institucional y que dependen de la Función Ejecutiva.(Auditoria-MCYP, 2011)

Las tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional por lo que debe cumplir estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

El EGSI es elaborado en base a la norma NTE INEN-ISO/IEC 27C__ "Código de Práctica para la Gestión de la Seguridad de la Información(En base a la estructura de COBIT para el manejo de Seguridad Informática aplica la Norma ISO por ello es que el EGSI se basa en dicha norma)"

Mediante ello el MCYP también debe trabajar no solo en la Norma de Control Interno sino también al sistema Gubernamental EGSI y ajustarse los estándares internacionales del cómo se va a hacer cumplir esas normas y con ITIL para tener mejores prácticas.

2.4Estadísticas del uso del Internet en el MCYP

Debido a que no existe aún políticas ni temas de seguridad estandarizados en el MCYP no se puede tener 100%estadísticas de todos los servicios Institucionales, pero se tiene herramientas como CheckPoint que pueden guiarnos como está actualmente los servicios en el MCYP.

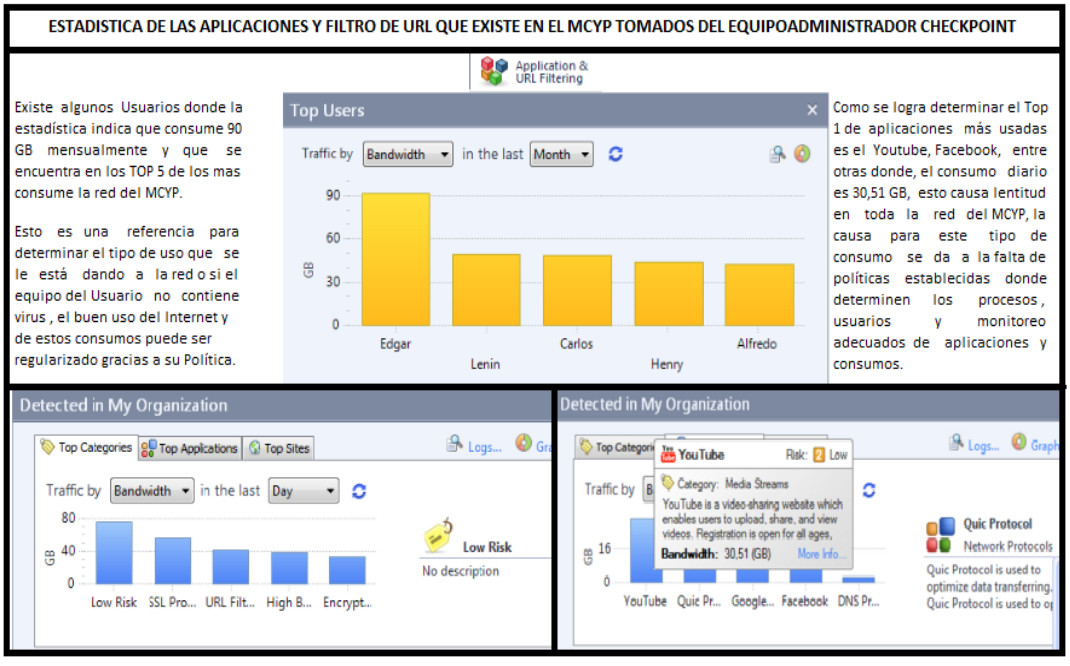

Figura 14. Estadísticas equipo CheckPoint

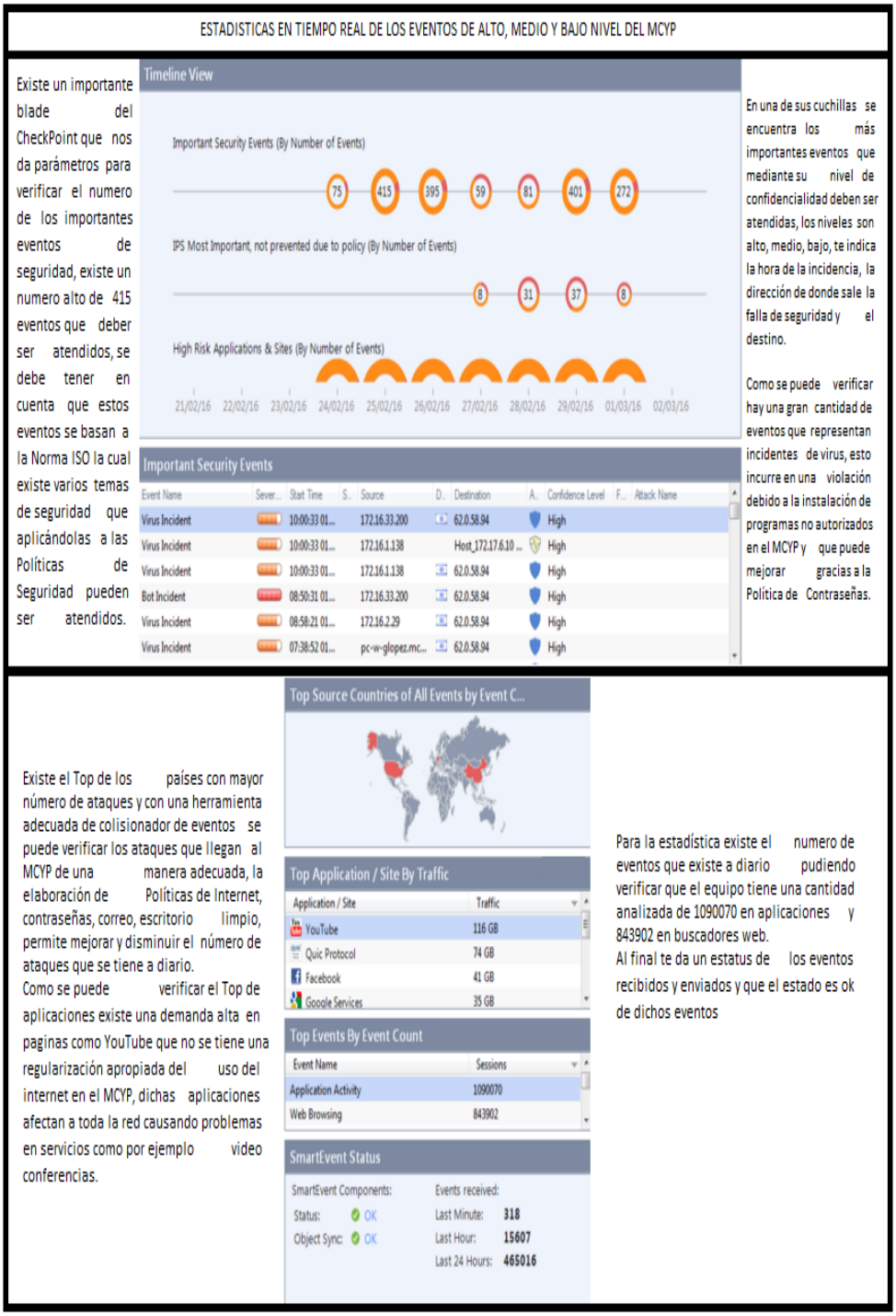

Figura 15. Estadísticas equipo CheckPoint

Tomado de: Equipo CheckPoint

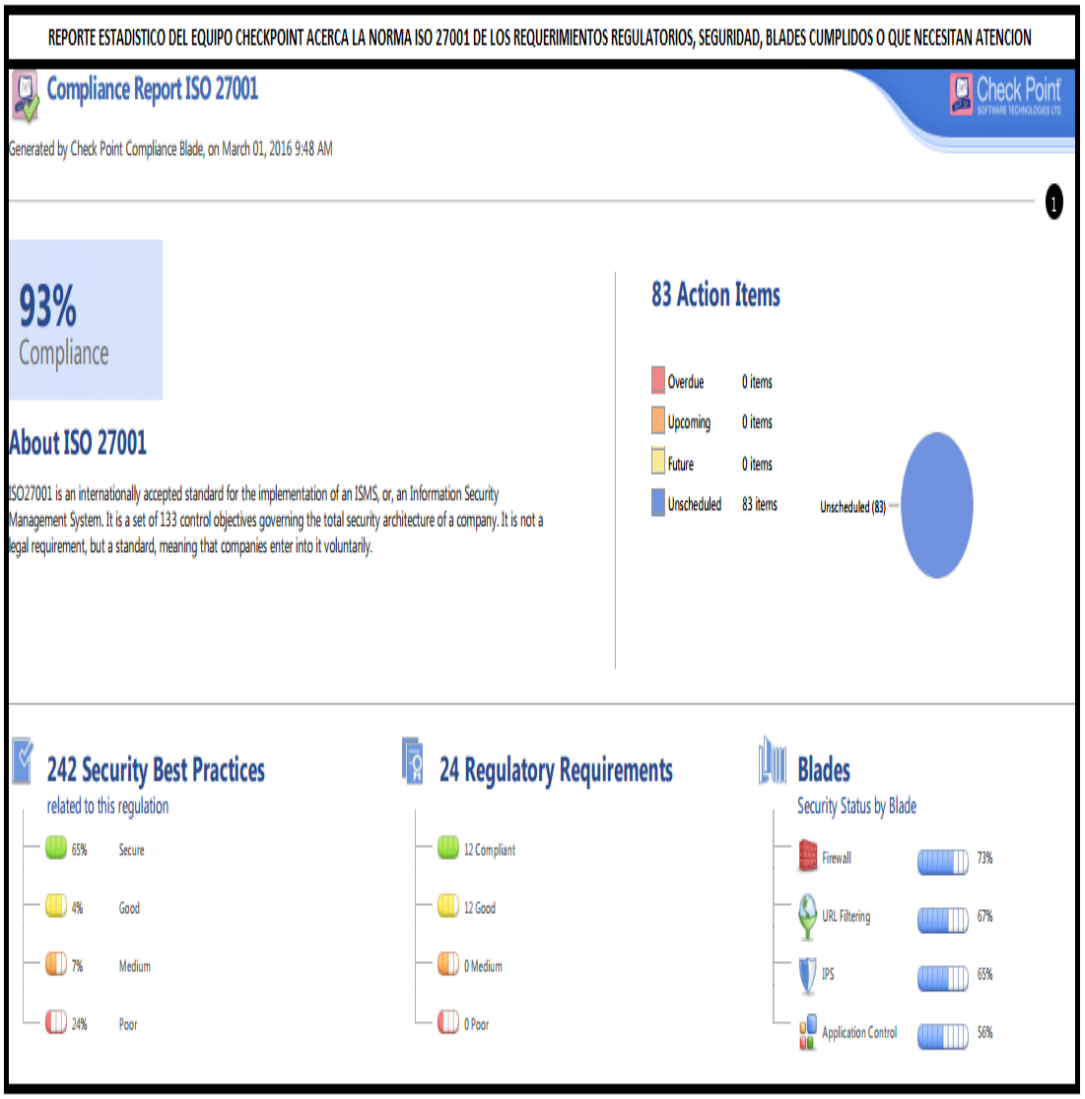

Figura 16. Estadísticas equipo CheckPoint

Tomado de: Equipo CheckPoint

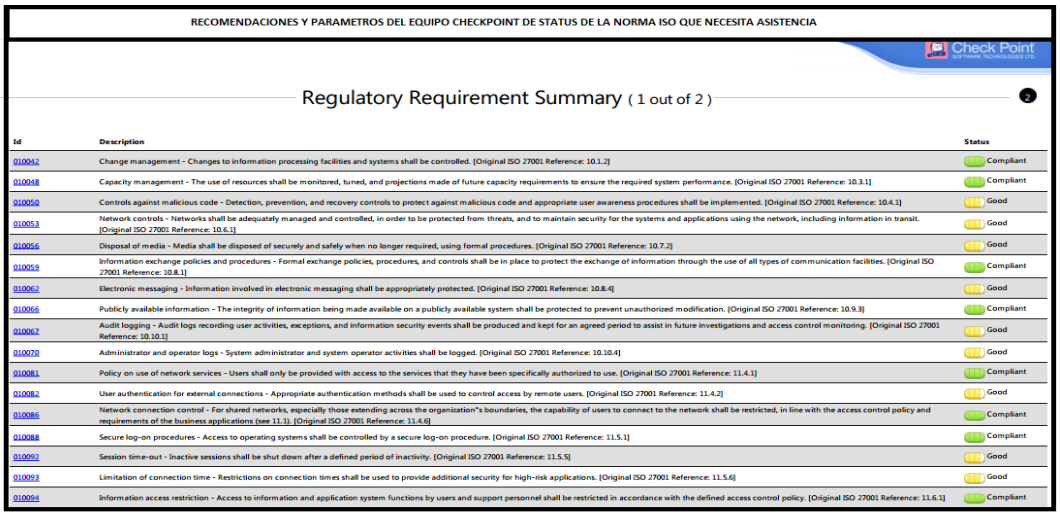

Figura 17. Estadísticas equipo CheckPoint

Tomado de : Equipo CheckPoint

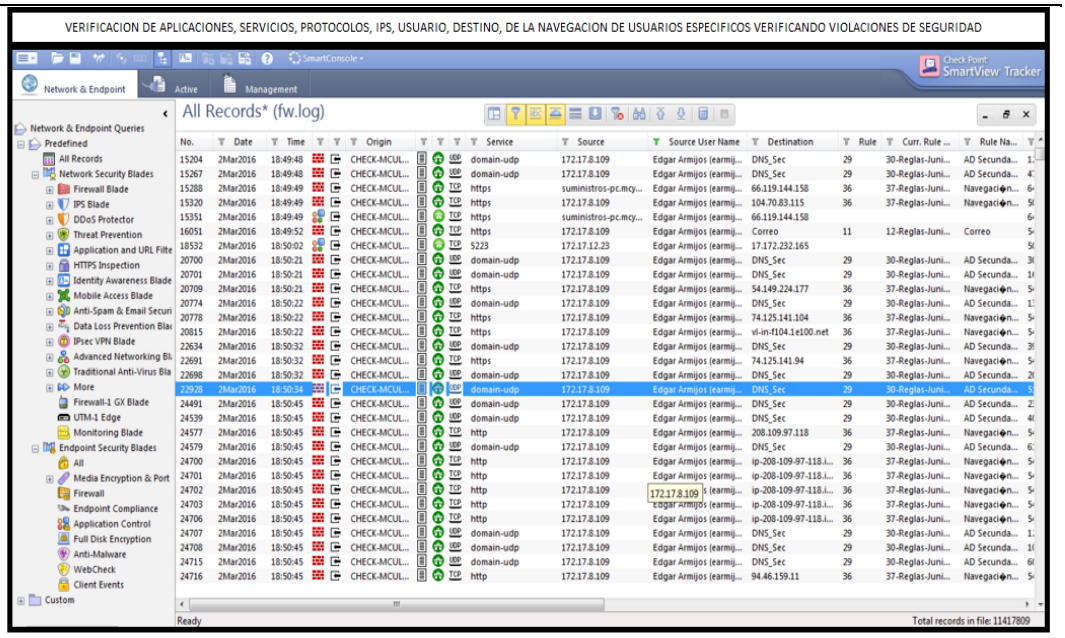

Figura 18. Estadísticas equipo CheckPoint

Tomado de: Equipo CheckPoint

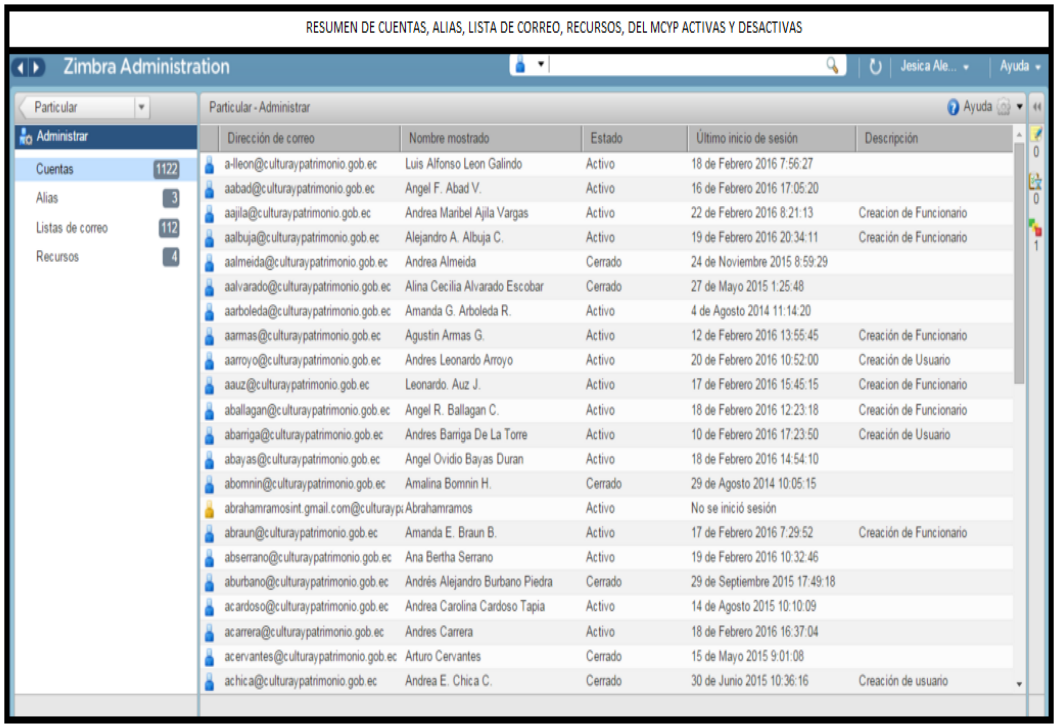

Figura 19. Estadísticas equipo Zimbra

Tomado de: Equipo Zimbra

2.5Verificación de políticas y normas de control interno establecidas para TICS

En base a la verificación de normativas y para el estudio de este proyecto se verificó que para la elaboración de políticas y normas establecidas para TICs existe dos ejes fundamentales; el primero es la Norma de Control Interno y el segundo bajo recomendaciones del Oficial de Seguridad del MCYP, se establece trabajar con el EGSI.

Cabe recalcar que la Unidad de Tecnologías de la Información y Comunicación tiene actualmente ningún seguimiento a políticas o disposiciones, las dos normativas exigen de manera obligatoria hitos que deben ser cumplidos a cabalidad y entre ellos está el desarrollo de políticas, las

normas no solo lo establecen de manera general, entre sus hitos esta desmenuzado ciertos factores que son de utilidad para la elaboración de las políticas y que será expuesta más adelante.

Una unidad Administrativa del MCYP, es la Dirección de Auditoría Interna, que se encarga de la regularización de todos los proyectos y procesos que se realiza a diario, en dicha Dirección cada año se establece requerimientos de solicitudes a cada área para verificar el cumplimiento de varios temas, entre ellos la Normativa de Control Interno que exige la Contraloría General del Estado, entre otros, bajo los comunicados expuestos se verifica que el área de Auditoría Interna emitió el documento DAI-003-201, en el que se solicitó realice la Evaluación Integral del Sistema de Control Interno del Ministerio de Cultura y Patrimonio, por el periodo comprendido entre el 1 de noviembre de 2011 y el 31 de octubre de 2012, pidiendo a todas las áreas indicar el estado de las recomendaciones de Contraloría, cuyo documento formal se encuentra ubicado en la página web de dicha entidad, pero para nuestro estudio el tema de Políticas aún no ha sido regularizado.

Entre algunos de los hitos de la Norma de Control Interno, ya que es destinado para todas las áreas está NCI 410 TECNOLOGÍA DE LA INFORMACIÓN que se explica a continuación:

NCI 410-03 Plan informático estratégico de tecnología

"No está creada la estructura organizacional de la Coordinación General de Gestión Estratégica y no se elabora un Plan estratégico de Tecnologías de Información y Comunicación."(Auditoria-MCYP, 2011)

Recomendaciones.

Al Coordinador General Administrativo Financiero

- ✓ Crear la Coordinación General de Gestión Estratégica con su titular y el dirigirá las funciones de la Unidad de Tecnologías de la Información y Comunicación.

Este proceso ya fue realizado y en la actualidad cuenta con la Estructura de la Coordinación de Gestión Estratégica quien a su vez tiene tres áreas a su cargo las cuales son Cambio y Cultura Organizacional, Dirección de Procesos y la Unidad de Tecnologías de la Información y Comunicación.

- ✓ Al Coordinador General de Planificación e Inversión

Elaborará conjuntamente con el responsable de la Unidad de Tecnologías de Información y Comunicación los planes de tecnología entre los cuales incluirá la estructura interna, procesos, infraestructura, las estrategias de migración, los riesgos y su mitigación, la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia, estos planes deben estar alineados con el Plan Informático Estratégico Institucional.

Desde la recomendación en el 2011 han existido diferentes cambios de Ministros que ha retardado los procesos requeridos, desde el 2013 se comenzó a trabajar en los planes operativos, proyectos entre otros requisitos que solicitó Auditoría, SNAP y Contraloría, los proyectos entre los más relevantes fue el cambio de tecnología en los servidores de MCYP al igual que herramientas para solventar los requerimientos de los Usuarios , el ingreso al dominio de todas las maquinas a nivel Nacional, el licenciamiento de software de los servidores como por ejemplo Antivirus, Windows Server, etc.

En el 2014 se trabajó ya teniendo una estructura organizada de la Red con la implementación del Wireless en todo el Edificio Matriz logrando conseguir y alinearse a la propuesta del Ministerio de Telecomunicaciones el cual indica que el servicio de Internet debe ser gratuito, por este motivo el MCYP creó tres estructuras de la red Wi-Fi las cuales son, Invitados, Wifi-MCYP y Ministro.

La red de Invitados está disponible para todos los Usuarios que se encuentran dentro o fuera del edificio matriz en el rango moderado, cabe indicar que dicha red no proporciona ningún tipo de servicio interno o intranet que tiene el MCYP, ni tampoco a ningún servidor.

También se implementó servidores con el Checkpoint quien cumple con las funciones de estar al frente de toda la red del MCYP brindando el servicio de internet, a finales del 2014 y 2015, adicionalmente el área de Seguridad trabajó en temas de seguridad informática, la instalación de nuevas cuchillas para el chekpoint, puesta de host en impresoras, la implementación de servidores, la posible compra de un servidor de archivos, entre algunos proyectos destinados a mejorar la calidad del servicio y la mejora continua del mismo.

NCI 410-04 Políticas y Procedimientos

Bajo indicaciones de Auditoría se requiere la formalización de políticas y procedimientos para el MCYP, desde el 2011 hasta la actualidad como se indica en documentos formales no se ha dado respuesta a la solicitud expuesta y para lo cual se ha indicado lo siguiente:

"No se han establecido procedimientos tecnológicos apropiados"(Auditoria-MCYP, 2011)

La recomendación de Auditoría Interna ha sido que el Director de Gestión Administrativa dispondrá al responsable de la Unidad de Tecnologías de la Información y Comunicación elabore las políticas y procedimientos que permitan organizar apropiadamente el área de Tecnologías de la Información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

Hasta mediados del 2015 se tenía entre proyectos principales la elaboración de Políticas y procedimientos ya que el MCYP tenía un Oficial de Seguridad que fue designado por la Máxima Autoridad para cumplir con estos

lineamientos, se logró hacer levantamiento de información de los servicios que actualmente tiene y sus falencias, debido al cambio de estructura organizacional por cambio de Ministro y Jerárquicos Superior, algunos de estos proyectos quedaron rezagados hasta nueva orden por lo que actualmente el MCYP no ha procedido con ninguna política requerida por Auditoría Interna.

Aunque no es nuestro caso de estudio para este proyecto se verificarán algunas observaciones que solicita Auditoria.

NCI 410-06 Administración de proyectos tecnológicos

"No existe mecanismos que faciliten la administración de proyectos informáticos" (Auditoria-MCYP, 2011)

Se necesita mecanismos que faciliten el inicio, planeación, ejecución, control, monitoreo y cierre de los proyectos informáticos.

NCI 410-09 Mantenimiento y control de la infraestructura tecnológica.

"No existe inventario de los bienes informáticos" (Auditoria-MCYP, 2011)

La disposición de Contraloría y Auditoria es que la Dirección de Gestión Administrativa disponga al responsable de activos fijos entregue a la Unidad de Tecnologías de la Información y Comunicación el inventario de los equipos informáticos a nivel nacional, este requerimiento en la actualidad lleva un levantamiento de información por parte de la Unidad de bienes del 90 % por lo que aun no se puede tener un información adecuada para proceder con este hito.

NCI 410-10 Seguridad de tecnología de información

"No se ha implementado mecanismos de protección y salvaguardia de tecnología de la información." (Auditoria-MCYP, 2011)

La recomendación es que se designe al Responsable de Tecnologías de la Información y Comunicación, elabore mecanismos que protejan y salvaguarden contra pérdidas y fugas de medios físicos y de la información que se procesa a través de los sistemas informáticos, al igual que respaldos periódicos de dicha información.

Actualmente el MCYP tenía entre sus proyectos la compra de un servidor de archivos el cual se encaminaba a cumplir la función antes expuesta, dicho proyecto aún está en ejecución por lo que no se logra cumplir dicho requerimiento.

NCI 410-11 Plan de contingencias

"La entidad no cuenta con un plan de contingencias." (Auditoria-MCYP, 2011)

La recomendación es que la Unidad de Tecnologías de la Información elabore un plan de contingencias que debe ser de carácter confidencial, considerando la respuesta a los riesgos de tecnología de la información, definición y ejecución de procedimientos de control de cambios, continuidad de las operaciones, recuperación de desastres

Aunque en el 2015 se trabajó en un plan de contingencias o acuerdos de servicios, los documentos no han sido analizados y autorizados para cumplir con este hito, la elaboración de dicho documento lo hizo el Administrador de la Red conjuntamente con el Encargado de TICs y el encargado de la Seguridad Informática.

NCI 410-12 Administración de soporte de tecnología de información.

"La entidad no dispone de soporte de tecnología de información." (Auditoria-MCYP, 2011)

La recomendación es que el Director de Gestión Administrativa disponga al responsable de Tecnologías de la Información elabore procedimientos de prevención, detección y corrección que proteja a los sistemas informáticos de la entidad, facilitando una adecuada administración del soporte tecnológico.

En la actualidad ya existe herramientas para prevención y corrección de errores , para verificación de incidencias y un plan de mantenimiento correctivo y preventivo, el éxito de dicho plan depende de la persona que actualmente está a cargo de la Coordinación General Estratégica quien debería incluir entre sus proyectos esta recomendación.

NCI 410-13 Monitoreo y evaluación de los procesos y servicios

"No existe monitoreo y evaluación de los procesos y servicios." (Auditoria-MCYP, 2011)

La recomendación es que el Director de la Gestión Administrativa dispondrá al responsable de la Unidad de Tecnologías elabore una metodología que permita monitorear el impacto de los servicios tecnológicos recibidos de los clientes internos y externos.

El MCYP tiene el equipo CheckPoint quien realiza estadísticas de todos los servicios tecnológicos de la Institución, cabe indicar que aunque el equipo realiza variedad de funciones no existen documentos o metodologías que permitan regularizar o plasmar este hito.

2.6Verificación de normas EGSI para el MCYP

Es importante conocer que la organización de las instituciones del Estado debe estar regulada por normas de aplicación general para que, en virtud de su cumplimiento, respondan a las exigencias de la sociedad, brindando un servicio público eficaz, eficiente y de calidad; de modo que, como

parte del control interno, los Oficiales de Seguridad de la Información deben observar todas estas normas obligatorias al momento de diseñar los controles de seguridad de la información.

Las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos reconocen como uno de sus objetivos el garantizar la confiabilidad, integridad y oportunidad de la información por lo cual los servidores públicos deben conocer las consecuencias de un manejo inadecuado de la información pública.(Auditoria-MCYP, 2011)

En términos generales, todo el sector público debe cumplir con las mismas normas referentes a vinculación, sanciones, responsabilidades, asuntos disciplinarios, desvinculaciones, inhabilidad para ejercer cargos públicos, administración del talento humano, tipos de contratos que se manejan, evaluaciones de desempeño, etc.

2.7La seguridad de la información y su importancia en el Plan Nacional de Gobierno Electrónico.

Dentro del pilar “Marco Regulatorio” del Plan Nacional de Gobierno Electrónico de Ecuador y como uno de los habilitadores se encuentra el Acuerdo Ministerial 166 - Esquema Gubernamental de Seguridad de la Información. (SNAP, 2013)

Ese acuerdo establece disponer a las entidades de la Administración Pública, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de la familia de Normas Técnicas Ecuatorianas **NTE INEN-ISO/IEC 27000** para la Gestión de Seguridad de la Información.

La importancia de la seguridad de la información para el Plan Nacional de Gobierno Electrónico radica en la protección de la disponibilidad,

confidencialidad e integridad de los servicios e información que se pone a disposición de los ciudadanos.

Además, se relaciona estrechamente con la eficacia y eficiencia de los procesos de la gestión pública, puesto que es un factor que aporta al cumplimiento de las expectativas ciudadanas y uso adecuado de los recursos disponibles. La aplicación de un enfoque de riesgos para la identificación y análisis de riesgos de seguridad de la información y tratamiento de riesgos que corren la información e infraestructura involucrada en la implementación del Plan Nacional de Gobierno Electrónico en cada entidad gubernamental permitirá alcanzar los objetivos y el nivel de madurez deseado.

Hay que hacer referencia a varias actividades que tienen como objetivo común tratar adecuadamente todos los riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos de información de las organizaciones. La seguridad de la información no solo es inherente a la tecnología, sino también a procesos de negocio y de las personas que conforman la organización. En muchas ocasiones se manejan como sinónimos, por tanto, es necesario saber que la seguridad de la información no es igual que la seguridad informática.

La seguridad de la información debe ser considerada como un proceso transversal a todos los demás procesos de la organización debido a que protege todo lo que genera, procesa o almacena información de la institución o lo que se conoce como activo de información.(SNAP, 2013)

Para entender mejor el EGSI hay que tomar en cuenta que se hace también referencia a las Normas Técnicas Ecuatorianas INEN ISO/IEC 27001 y 27002. Con la finalidad de interpretar adecuadamente la nomenclatura de nombramiento de las distintas normas ISO, es necesario conocer que se compone de dos números separados por los dos puntos (:), el primer número indica el código de la norma y el segundo número indica el año de su publicación. Por ejemplo, la ISO/IEC 27001:2005 indica que 27001 es el código

para la norma (en este caso, contiene los requisitos de un Sistema de Gestión de Seguridad de la Información) y 2005 es el año de su publicación.(SNAP, 2013)

Cada una de las normas indicadas hace referencia a lo siguiente:

- NTE INEN ISO/IEC 27001: Norma que contiene los requisitos que debe cumplir un Sistema de Gestión de Seguridad de la Información, por tanto, es auditable y certificable. Además, su Anexo A enumera en forma de resumen los objetivos de control y controles que son detallados en la NTE NEN ISO/IEC 27002.

- NTE INEN ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles de seguridad de la información. En total contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.(SNAP, 2013)

Estas normas serán estudiadas más adelante para detallar los temas de seguridad de la información y tener un objetivo más claro en el tema de las políticas aplicables a este caso de estudio.

La Secretaría Nacional de la Administración Pública, como ente encargado de establecer las políticas, metodologías de gestión e innovación institucional y herramientas necesarias para el mejoramiento de la eficiencia, calidad y transparencia de la gestión en las entidades y organismos de control de la Función Ejecutiva, creó en agosto de 2011 la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría de Inteligencia y la Secretaría de la Administración Pública. Esta Comisión tiene, como una de sus atribuciones, la de establecer lineamientos de seguridad informática, protección de infraestructura y todo lo relacionado.(SNAP, 2013)

La Comisión indicada realizó un análisis de la situación con respecto a la seguridad de la información en las instituciones de la Administración Pública Central, Dependiente e Institucional, llegando a determinar la necesidad de aplicar normas y procedimientos, así como de incorporar una cultura de seguridad de la información.

Con base en lo determinado por la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, en septiembre de 2013 la Secretaría Nacional de la Administración Pública (SNAP) publicó en el Registro Oficial n.º 88 el Acuerdo n.º 166, que dispone que todas las entidades que dependan de la Administración Pública y de la Función Ejecutiva utilicen obligatoriamente las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información en función de los siguientes hitos:

- Designar un Comité de Seguridad de la Información, que debe estar liderado por el Oficial de Seguridad de la Información, esto hasta el 30 de octubre de 2013.

- Implementación de controles prioritarios, hasta el 31 de marzo de 2014.

- Hasta el 31 de marzo de 2015, deberá estar implementado todo el EGSI.(SNAP, 2013)

A manera de control, la Secretaría de la Administración Pública utiliza el sistema de Gobierno por Resultados (GPR), y, debido a que la implementación del EGSI es obligatoria en las entidades públicas, su avance debe ser registrado en este sistema. Por eso, se creó un programa institucional llamado “Gestión de la Seguridad de la Información en las Entidades de la Administración Pública Central Institucional, dependiente de la Función Ejecutiva”.

Cabe señalar que, a pesar de estar basado en la NTE INEN ISO/IEC 27002, el EGSI es un cuerpo de controles independiente que no reemplaza a la norma indicada, sino que marca como prioridad la implementación de los controles que indica en su contenido.

A continuación se presenta la hoja de ruta de la implementación del EGSI en el Ministerio de Cultura:

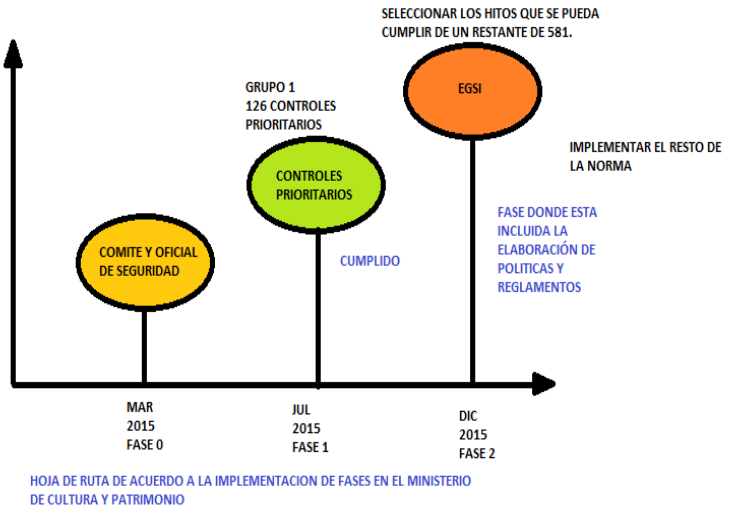

Fig. 20 Hoja de Ruta para implementación de fases MCYP

Según lo revisado en el MCYP el avance es el siguiente: Fase I: 93 % Fase II: 33 % Debido al Oficial de Seguridad en el 2015 se tuvo un alto progreso para el cumplimiento de esta normativa, los avances fueron realizados en conjunto con toda la Unidad de Tecnologías de la Información realizando y buscando documentación requerida para la ejecución del EGSI, cabe mencionar que para el cumplimiento de hitos no solo depende del área técnica si no de documentación de áreas Administrativas o de RRHH ya que por ejemplo se pide documentación como el inventario de bienes que ya fue expuesto anteriormente en la Normativa de Control Interno, las áreas de Infraestructura, Soporte, Desarrollo y Seguridad Informática lograron cumplir la mayoría de hitos de la fase I, la fase dos comenzó a estructurarse para poderla

culminar el 2016, en la actualidad los avances en esta norma se ha retrasado debido a las reformas Publicas de Gobierno(SNAP, 2013)

Lograr gestionar la seguridad de la información en las entidades es una tarea que puede llegar a ser compleja; sin embargo, tanto en el ámbito local como global existen normas que contienen buenas prácticas aplicables para dicha gestión y una de ellas es la familia de normas ISO/IEC 27000.

El EGSI, cuyo contenido se presenta en el Anexo 1 del Acuerdo No. 166 del 19 de Septiembre del 2013, toma como base los controles de la Norma Técnica Ecuatoriana INEN-ISO/IEC 27002; sin embargo, no incluye el conjunto de requisitos para un diseño e implementación del EGSI, los cuales se detallan en la Norma Técnica Ecuatoriana INEN-ISO/IEC 27001.

De forma resumida, el INEN mantiene las siguientes normas relacionadas con seguridad de la información:

Para poder entender Esquema Gubernamental de Seguridad de la Información (EGSI) e implementarlo adecuadamente se debe aclarar que van de la mano la Norma de control interno la ISO 27002 y la norma dispuesta por la SNAP EGSI y los beneficios de implementarlas son los siguientes:

- El principal beneficio es el cambio de cultura organizacional porque para implementar y aplicar controles se realizan campañas de difusión y capacitación permanentes, los involucrados obtienen una visión más amplia de las amenazas, las vulnerabilidades, los riesgos y sobre todo, consecuencias de incidentes de seguridad de la información, es así que, el cambio de cultura se da al existir la necesidad de aplicar la seguridad de la información tanto en sus funciones diarias como en su vida personal (Asociación Española de Normalización, 2013)

- La mejor comprensión de los riesgos en procesos de negocio y la información de la cual dependen ya que el análisis de riesgos que la

entidad ejecuta como parte de los procesos de seguridad, en el cual, se analiza a profundidad los procesos de negocio con el fin de identificar los activos de información, amenazas, vulnerabilidades e impactos en la actividad empresarial. (NORMA ISO, 2011)

- La reducción de costos debido a la existencia de un adecuado tratamiento de los incidentes de seguridad y se mitigará al máximo la probabilidad de que algo similar ocurra en el futuro, además, mediante la implementación de controles, los usuarios utilizarán adecuadamente los activos que la organización les asigne para realizar su trabajo. (SGS, 2013)

- El cumplimiento de requisitos legales y regulatorios ya que debe haber una identificación meticulosa de los mismos y su cumplimiento es exigido y monitoreado como parte de un sistema de gestión de seguridad de la información. (Normalización, 2011)

- Se debe considerar que existe un orden jerárquico para el cumplimiento de requisitos legales y existe el siguiente orden: leyes internacionales, Constitución, leyes nacionales, leyes seccionales, leyes locales y finalmente normativa interna de la Entidad.

- Continuidad de Institucional.

La implementación del EGSI en cualquier institución no es fácil ya que requiere experiencia para lo cual no existe documentos que indiquen como realizarlo efectivamente, el MCYP opto por implementar su EGSI dentro de un alcance delimitado, para luego, habiendo adquirido más experiencia, replicarlo o seguirlo mejorando en el resto de la institución, ya que se encuentra distribuida geográficamente en el ámbito nacional y con el avance de la Ley de Cultura y si esta es aprobada todos los museos, casas culturales, etc., pasarían a ser parte de un solo ente regulatorio por lo que la implementación del EGSI se aplicaría con mayor experiencia luego.

Para elegir un alcance adecuado para el EGSI, el MCYP considero un proceso institucional y su dimensión geográfica y a nivel de recurso humano, es decir, identifico claramente hasta donde se puede llegar en la implementación inicial.

Cuando ya se identificó el proceso, se definió sus interrelaciones existentes con otros procesos de soporte, se diseñó un mapa de procesos, se plasmó en documento para la fase I del EGSI y son los hitos que se solicita para que sean cumplidos se dividen en nueve: Políticas, Organización, Gestión de Activos, Seguridad RRHH, Seguridad Física, Gestión de Comunicaciones, Control de Acceso, Adquisición y desarrollo, Gestión de Incidentes, lo cual en dichas fase ya se comienza hablar de las Políticas para el MCYP y a continuación se detalla los documentos obtenidos:

2.7.1. Política de Seguridad de la Información

Tabla 2. Cumplimiento de Política de Seguridad de la Información

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	**Cumplido**		**Observaciones**
1.1 Documento de la Política de la Seguridad de la Información	SI	NO	
Disponer la implementación del EGSI en la institución por la máxima autoridad.		X	Disposición de la máxima autoridad
Difundir la política de seguridad de la información de referencia o propia de la institución.		X	Elaborar la propuesta de Política de Seguridad de la Información Revisar jurídico. Aprobar por Comité. Difundirla mediante comunicación interna, correo e intranet.
3.3 Uso aceptable de los activos			
3.3.1 Reglamentar el uso de correo electrónico institucional:			Revisión políticas. Actualizar las políticas. Aprobar por parte del CSI. Implementar controles

			TICs.
Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.			
Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.			
Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de las instituciones.			
Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.			
La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo			
Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios.			
Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.			
Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.			
Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.			
3.3.2 Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios:			Revisión política. Actualizar las políticas. Aprobar por parte del CSI. Implementar controles TICs.
Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la			

institución, y no debe utilizarse para ningún otro fin.			
Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.			
El Oficial de Seguridad de la Información debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas.			
Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.			
El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad			
La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.			
Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.			

7. **CONTROL DE ACCESO**			
7.4 **Gestión de contraseñas para usuarios**			
Establecer un proceso formal para la asignación y cambio de contraseñas			Actualmente está en 45 días, se lo hace mediante active directory. En caso de olvido de contraseña, se les pone una contraseña genérica y se cambia al primer inicio de sesión. Validar la configuración actual de los parámetros de las contraseñas. Elaborar un procedimiento para la gestión de contraseñas usuarios y administradores, que incluya mejores prácticas para la creación de contraseñas, política de contraseñas.
Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados		x	Elaborar la política de contraseñas
Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta		x	Elaborar la política de contraseña
Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables		x	Elaborar la política de contraseñas
Controlar el cambio periódico de contraseñas de los usuarios		x	Elaborar la política de contraseñas
7.8 Política de puesto de trabajo despejado y pantalla limpia		x	Elaborar política de buenas prácticas de usuarios.
Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina		x	Enviar comunicaciones internas de tips o boletines de seguridad para toda la Institución, socialización. Ojo no existe seguridad en los

			cajones, cambiar las chapas.
Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave		x	PC no, sistemas servicios (correo, quipux, AD, bpm, esigef, esipren). Campaña de concientización para que los usuarios cierren la sesión. Ver la mejor estrategia, fondo de pantalla, boletines.
Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas			Inventario de impresoras. Revisión interna de la configuración de seguridad de las impresoras, y solicitar soporte de ser el caso, ver más opciones con uso de software especializado.
Retirar información sensible una vez que ha sido impresa			
Retirar información sensible, como las claves, de sus escritorios y pantallas			Normativa.
Retirar información sensible, como las claves, de sus escritorios y pantallas			
Retirar los dispositivos removibles una vez que se hayan dejado de utilizar			Normativa.

Adaptado de :(ISO-EGSI, 2015)

El alcance seleccionado debe ser formalizado en un documento y aprobado por la máxima autoridad de la institución.

2.8.Definición de la Política de Seguridad de la Información

Como segundo paso, debe establecerse la Política del EGSI, considerando que esta no es la Política de Seguridad de la Información.

La Política del EGSI debe ser la intención de la organización hacia la sociedad mientras que la Política de Seguridad de la Información define la intención interna u operativa con respecto al cumplimiento de los controles de

seguridad de la información. La Política del EGSI debe ser una intención institucional y estratégica, que exprese lo que la seguridad de la información desea instaurar en la organización.

Al igual que con el alcance, la Política del EGSI también debe ser formalizada en un documento aprobado por la máxima autoridad; una vez formalizado debe ser difundido para consumo de toda la institución.

Ya que está terminado la Fase I del MCYP, conjuntamente con el oficial de Seguridad se comenzó a obtener información para comenzar el proceso de la Fase II, la cual contiene aproximadamente 1053 hitos referentes a varios temas que influyen en el tema de Seguridad de la Información, entre los cuales se encuentran los temas relacionados a contraseñas, correos, escritorio limpio, internet y serán analizados en el Capítulo III y que son el caso de estudio de este documento.

CAPÍTULO III

3. Verificación y comparación de hitos de las normas y buenas prácticas, aplicables la políticas de internet, contraseña, correo y escritorio limpio

3.1 La información pública como garantía

Debido a que las instituciones públicas deben gestionar adecuadamente su información, y el llamado a liderar esto es el Oficial de Seguridad de la Información, es importante saber que la información pública también es considerada una garantía para el Estado ecuatoriano, ya que la Constitución garantiza la acción de acceso a la información pública cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna; además, considerando que la información podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquier otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por la autoridad competente y de acuerdo con la ley.

Verificación de la Normativa ISO27002 y el EGSI para la implementación de políticas de contraseña, internet, escritorio seguro, correo.(Gobierno Electrónico, 2016)

3.2 Verificación de hitos entre normas ISO VS EGSI

3.2.1Política de contraseñas

Norma ISO 27002 y EGSI (Contraseñas)
ISO: HITO 11.2.3-11.3.1- 11.5.1- 11.5.3
EGSI: HITO 7.4 - 7.17 - 7.18 - 7.5 - 7.6 - 7.8 - 6.26.6 - 7.16.6 - 8.7.1.7

Tabla 3. Contraseñas

Uso de contraseñas para usuarios	
Control: La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.(ISO 27002)	
ISO 27002	ESGI
Se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este; esta declaración firmada se podría incluir en los términos y condiciones laborales.	Establecer un proceso formal para la asignación y cambio de contraseñas. Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);
Cuando se exige a los usuarios mantener sus propios contraseñas, inicialmente se le debería suministrar una contraseña temporal segura que este forzados a cambiar inmediatamente.	Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.
Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal de reemplazo o nueva.	Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.
Las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección.	Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
Las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables.	Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible
Los usuarios deberían confirmar la entrega de contraseñas.	Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo

	electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.
Las contraseñas nunca se deberían almacenar en sistemas de computadora en un formato no protegido.	Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).
Las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.	Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información
Uso de Contraseñas	
Control: Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y uso de las contraseñas.	
Mantener la confidencialidad de las contraseñas	Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).
Evitar conservar registros (Por ejemplo papel, archivos de software o dispositivos manuales, va de la mano con la política de escritorio limpio o seguro) de las contraseñas a menos que estas se puedan almacenar de forma segura y el método de almacenamiento este aprobado.	Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados
Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.	Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables
Seleccionar contraseñas de calidad con longitud mínima suficiente que: • Sean fáciles de recordar. • No se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo nombre, números telefónicos, fechas de cumpleaños, etc.; • No sean vulnerables al ataque de diccionarios(es decir, que no consistan en palabras incluidas en diccionarios)	Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta

• No tengan caracteres idénticos consecutivos que no sean todos numéricos ni todos alfabéticos.	
Cambiar las contraseñas a intervalos regulares o con base en el número de accesos(las contraseñas para cuentas privilegiadas se deberían cambiar con más frecuencia que las contraseñas normales) y evitar reutilización de contraseñas antiguas.	Controlar el cambio periódico de contraseñas de los usuarios
Cambiar las contraseñas temporales en el primer registro de inicio	Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión
No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.	
No compartir las contraseñas de usuario individuales	La identificación de usuario es única e intransferible, por lo que, debe estar registrado y evidenciado en la política de accesos que no se permite el uso de una identificación de usuario de otra persona, y el responsable de toda actividad realizada con este identificador responderá a cualquier acción realizada con éste.
Procedimiento de registro seguro	
Control: El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro.	
No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.	Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente
Mostrar una advertencia de notificación general indicando que solo deberían tener acceso al computador los usuarios autorizados.	Definir alarmas originadas por el sistema de control de acceso
No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.	Evitar que se desplieguen mensajes de ayuda durante el procedimiento de registro de inicio de sesión.
Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar que parte de los datos	Validar la información de registro de inicio únicamente al terminar todos los datos de entrada, y en el caso que se presentara un error o se generara sentencias de error, el sistema no

es correcta o incorrecta.	indique qué parte de los datos es correcta o incorrecta o emita mensajes propios de las características del sistema.
Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos y considerar • Registrar intentos exitosos y fallidos • Forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización especifica • Desconectar las conexiones de enlaces de datos • Enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio • Establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege	Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos
Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación	Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica
Mostrar la siguiente información al terminar un registro de inicio exitoso: • Fecha y hora del registro de inicio exitoso previo • Detalles de los intentos fallidos de registro de inicio desde el último registro exitoso	Registrar la fecha, hora y detalles de los eventos clave, como registro de inicio y registro de cierre.
No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos	Establecer un proceso formal para la asignación y cambio de contraseñas
No transmitir contraseñas en texto claro en la red.	

Sistemas de gestión de contraseñas	
Control: Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían **Asegurar la calidad de las contraseñas**	
Hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad.	
Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos.	• Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados. • Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran. • Controlar el cambio periódico de contraseñas de los usuarios
Imponer una elección de contraseñas de calidad.	Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta
Imponer cambios de contraseña	• Controlar el cambio periódico de contraseñas de los usuarios • Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión
Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio.	Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión. Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad

Conservar un registro de contraseñas de usuario previas y evitar su reutilización;	• Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional. • Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.
No mostrar contraseñas en la pantalla cuando se hace su ingreso.	
Almacenar y transmitir las contraseñas en formatos protegidos(por ejemplo encriptados o codificadas).	Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).

Adaptado de :(ISO-EGSI, 2015)

Información adicional (ISO27002 Y EGSI)

- Las contraseñas son un medio de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información de acuerdo con la autorización del usuario.

- La gestión de los sistemas de ayuda del escritorio auxiliar que tratan con las contraseñas perdidas u olvidadas necesita cuidado especial puesto que también puede ser un medio de ataque al sistema de contraseñas.

- El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado

- Las contraseñas que se transmiten en texto claro durante la sesión de registro de inicio pueden ser capturadas en la red por un programa "husmeador" de red

- Todos los usuarios deberían tener un identificador único (ID de usuario) para su uso personal, y se debería elegir una técnica apropiada de autentificación para comprobar la identidad declarada de un usuario. Este control se debería aplicar a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos).

- Los identificadores de usuarios (ID) se deberían utilizar para rastrear las actividades de la persona responsable. Las actividades de usuarios regulares no se deberían realizar desde cuentas privilegiadas.(NORMA ISO, 2011)

- Cuando se requiere verificación de identidad y autentificación solidas se deberían utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, token o medios biométricos.(NORMA ISO, 2011)

Recomendaciones

Para el caso del Ministerio de Cultura y Patrimonio se consideró trabajar con los dos equipos de seguridad que son Checkpoint y Active Directory(WindowsServer 2012) disponibles para la identificación y autentificación de los usuario, el MCYP bajo normas de seguridad trabaja con una contraseña única para los Usuarios y que sincroniza con todos los servicios internos de la Institución, para los casos de firmas digitales se aplica los Tokens para nivel Jerárquico superior los cuales llevan consigo certificados de verificación y autentificación de firma, para autentificar permisos de ingresos se cuenta con biométricos y para permisos de Administradores a áreas

protegidas se cuentas con tarjetas de ingreso y contraseña de validación que son asignadas por una sola persona que maneja el Servidor de biométricos.

Para la elaboración de políticas de contraseña bajo lo expuesto en el cuadro comparativo se debe tomar en cuenta criterios técnicos y la norma vigente, entre lo más principales se debe considerar lo siguiente:

- Las contraseñas deben ser únicas para cada usuario incluidos personal técnico, administradores, etc.

- No se debe trabajar en los servidores con contraseñas de Administradores ya que viola la norma establecida se debe tener control del usuario y ingreso a los servicios del mismo para tener un registro de cambios.

- Las contraseñas deben ser cambiadas al primer inicio de sesión y deben tener complejidad como son números, letras, longitud(mínimo 8 caracteres) y de lo posible caracteres especiales.

- Las contraseñas deben ser de carácter oculto, bajo ninguna circunstancia se puede mostrar los caracteres de ingreso.

- Debe existir un periodo de cambio de contraseña obligatorio para la Institución el cual el oficial de seguridad lo debe analizar.

- Debe existir el proceso para la creación e identificación del Usuario.

- Debe existir un registro de usuarios y contraseñas

- Por ningún motivo se debe compartir la contraseña individual.

El sistema de Active Directory el cual proporciona control de todas las contraseñas establece lineamientos y parámetros que pueden ajustarse con dichas normas.

Los accesos a servicios tecnológicos están alineados a la política de seguridad y contraseñas del MCYP, y el acceso es con autorizaciones y únicos.

Los Usuarios son los únicos responsables del buen manejo de sus contraseñas y de las buenas prácticas que realizan a diario, por lo que están sujetos a sanciones administrativas del MCYP en caso de incurrir en faltas expuestas en el Capítulo IV en la política de contraseña.

3.2.2. Política de escritorio despejado y pantalla despejada

Norma ISO 27002 y EGSI (Escritorio despejado y pantalla despejada)

ISO: HITO 11.3.3- 11.5.5

EGSI: HITO 7.8 - 7.21

Tabla 4. Escritorio despejado y pantalla despejada

Política de escritorio despejado y de pantalla despejada	
Control: Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	
ISO 27002	ESGI
Cuando no se requiere la información sensible o critica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se deberían asegurar bajo llave(idealmente una caja fuerte, un gabinete u otro mueble de seguridad), especialmente cuando la oficina está vacía;	Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina
Las sesiones de los computadores y	Desconectar de la red, servicio o

los terminales se deberían cerrar o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, un token o un mecanismo similar de autentificación de usuario cuando no están atendidos, y se deberían proteger mediante bloqueos de clave, contraseñas u otros controles cuando no se estén utilizando;	sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave
Se deberían proteger los puntos de entrada y salida de correo y las máquinas de desatendidas	Proteger los puntos de recepción de correo y fax cuando se encuentren desatendidas.
Es conveniente evitar el uso no autorizado de fotocopiadoras y otrastecnologías de reproducción (por ejemplo, escáneres, cámaras digitales, etc.)	Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas
Los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras	• Retirar información sensible una vez que ha sido impresa • Retirar información sensible, como las claves, de sus escritorios y pantallas • Retirar los dispositivos removibles una vez que se hayan dejado de utilizar
Tiempo de inactividad de la sesión	
Control:Las sesiones inactivas se deberían suspender después de un periodo definido de inactividad	
Un tiempo de inactividad debería despejar la pantalla de sesión y más tarde, cerrar tanto la sesión de la aplicación como la red después de un periodo definido de inactividad. La dilación del tiempo de inactividad debería reflejar los riesgos de seguridad del área, la clasificación de la información que maneja y las aplicaciones que se utilizan, así como los riesgos relacionados con los usuarios del equipo. Algunos sistemas pueden suministrar una forma limitada de utilidad de tiempo de inactividad la cual despeja la pantalla y evita el acceso no autorizado, pero no cierra las sesiones	• Suspender las sesiones inactivas después de un periodo definido de inactividad sin consideración de lugar dispositivo de acceso. • Parametrizar el tiempo de inactividad en los sistemas de procesamiento de información para suspender y cerrar sesiones

de aplicación ni de red.	

Adaptado de :(ISO-EGSI, 2015)

Información adicional (ISO Y EGSI)

- EGSI. El Oficial de Seguridad de la Información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.

- Cifrar los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere necesarios, de las máximas autoridades de la institución.

- En la política deescritorio despejado y pantalla despejada se debería considerar las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización.

- Una política sobre escritorio despejado/ pantalla despejada reduce los riesgos de acceso no autorizado, perdida y daño de la información durante y fuera de las horas laborales normales.

- Las cajas fuertes u otras formas de almacenamiento seguro también podrían proteger la información almacenada allí contra desastres como incendio, terremotos, inundación o explosión.

- Se debería pensar en la utilización de impresoras con función de código de pines(pin code) de forma que quien inicia la impresora sea el único que pueda usarla y únicamente cuando este cerca de la impresora.

- El control de inactividad es importante particularmente en lugares de alto riesgo, los cuales incluyen áreas públicas o externas fuera de la gestión de la seguridad de la organización. Las sesiones de deberían cerrar para evitar el acceso de personas no autorizadas y negar ataques al servicio.

Recomendaciones

El MCYP con sus áreas Administrativas y de Tecnologías deben trabajar en un despliegue para asegurar todas las área, aéreos y escritorios de la Institución para asegurar que cada funcionario tenga a su custodio llaves de seguridad.

La política de escritorio despejado y pantalla despejada va de la mano con la Política de contraseñas ya que se debe asegurar que exista un bloqueo de pantalla al existir inactividad lo cual lo realiza en Active Directory, el cual garantizara el tiempo y luego de ello el ingreso de la contraseña única del usuario para poder trabajar con el equipo.

Para la elaboración de políticas de escritorio despejado y pantalla despejada bajo lo expuesto en el cuadro comparativo se debe tomar en cuenta criterios técnicos y la norma vigente, entre los más importantes se debe considerar lo siguiente:

- Debe existir un bloqueo de los equipos tecnológicos al verificar inactividad de los mismos lo cual ayuda a que no exista violación de seguridad en archivos o de red.

- Se debe retirar equipos removibles (usb, teléfonos, discos duros, etc.) una vez que se dejan de utilizar para evitar la pérdida de información.

- No se debe tener sobre nuestro puesto de trabajo información confidencial, se debe guardar bajo llave en los escritorios o aéreos. Únicamente se debe tener información con la que estemos trabajando.

- No se debe contar con claves de seguridad o servicio en nuestras pantallas o escritorios que no estén encriptados o bien resguardadas.

- Se debería mantener claves en impresoras que garanticen los documentos al tener un registro del usuario, se debe retirar inmediatamente los documentos que están en las impresoras que pueden contener información confidencial de la empresa

3.2.3.Política de uso de internet

Norma ISO 27002 y EGSI (USO DE INTERNET)

ISO: HITO 11.4.1 - 11.5 - 11.5.4 - 11.2 - 11.2.2

EGSI: HITO 6.26.8 - 6.26.5- 6.26.10 - 6.26.1

Tabla 5. Internet

Política de uso de internet	
Control:Los usuario solo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados.	
ISO 27002	ESGI
Registrar acceso a las redes y los servicios de red a los cuales se permite el acceso;	Registrar los accesos y tipos de acceso
Los procedimientos de autorización para determinar a quién se le permite el acceso a que redes y que servicios en red	Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.
Los controles y procedimientos de gestión para proteger el acceso a las	Establecer controles especiales para salvaguardar la confidencialidad y la

conexiones de red y los servicios de red	integridad de los datos que pasan por las redes públicas, redes locales e inalámbricas; así como la disponibilidad de las redes.
Los medios utilizados para el acceso a las redes y los servicios de red(por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de internet o a un sistema remoto)	Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de re-direccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.
Control de acceso al sistema operativo	
Objetivo: Evitar el acceso no autorizado a los sistemas operativos. Se recomienda utilizar medios de la seguridad para restringir el acceso de usuarios autorizados a los sistemas operativos.	
Autenticar usuarios autorizados , de acuerdo con una política definida de control acceso	Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada
Registrar intentos exitoso y fallidos de autentificación del sistema;	Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema
Registrar el uso de privilegios especiales del sistema	Llevar un registro de definición para el uso de privilegios especiales del sistema
Emitir alarmas cuando se violan las políticas de la seguridad del sistema	Definir alarmas originadas por el sistema de control de acceso
Suministrar medios adecuados para la autentificación	Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios
Cuando sea apropiado, restringir el tiempo de conexión de los usuarios	Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución
Gestión de privilegios	
Control: Se debería restringir y controlar la asignación y el uso de privilegios.	
Se debería identificar los usuarios y privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y aplicaciones;	Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.

Se deberían asignar los privilegios a los usuarios sobre principios de necesidad de uso y evento por evento, y de manera acorde con la política de control de acceso, es decir, el requisito mínimo para su función, solo cuando sea necesario.	Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la institución y su función.
Se deberían conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización este completo;	Controlar la asignación de privilegios a través de un proceso formal de autorización.
Es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.	Llevar un registro de definición para el uso de privilegios especiales del sistema
Control de accesos	
Control: Se debería establecer , documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	
Perfiles estándar de acceso de usuario para funciones laborales comunes en la organización	Definir perfiles de usuario para las diferentes instancias o ambientes.
Requisitos para la autorización formal de las solicitudes de acceso	Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.
Requisitos para la revisiónperiódica de los controles de acceso	Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información
Retiro de los derechos de acceso	• Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que

	se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente. • Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución.
Gestión de acceso de usuarios	
Control: Debería haber un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información	
Uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debería permitir cuando son necesarios por razones operativas o de negocio, y deberían estar aprobados y documentados	• Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico. • Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables de proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad; • Usar como excepción, y solo por temas de necesidad de la institución, identificadores(ID) de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado
Verificación de que el usuario tenga autorización de responsable del sistema para el usuario del sistema o servicio de información,	• Identificar y documentar los sistemas sensibles y al responsable de la aplicación.

tambiénpueden ser conveniente que la dirección apruebe por separado los derechos de acceso	• Revisar y actualizar periódicamente los derechos de accesos a las áreas restringidas, mismos que serán documentados y firmados por el responsable. • Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables • Definir el administrador de accesos que debe controlar los perfiles y role • Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.
Verificación de que el nivel de acceso otorgado sea adecuado para los propósitos de negocio y sea consistente con la política de la seguridad de la organización, es decir, no pone en peligro la distribución de funciones.	• Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad); • Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden

	y completos. • Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones. • Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la institución y su función.
Dar a los usuarios una declaración escrita de sus derechos de acceso	• Notificar a los usuarios del sistema sobre el cambio a realizar. Se enviará una notificación para informar sobre el tiempo que durará la ejecución del cambio y para informar cuando se haya terminado la ejecución del cambio.
Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso	• Proporcionar accesos a usuarios o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización	Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);

Mantenimiento de un registro formal de todas las personas registradas para usar el servicio	Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.
Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización.	• Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente. • Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución.

Adaptado de :(ISO-EGSI, 2015)

Información adicional (ISO27002 Y EGSI)

- Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deberían controlar la asignación de privilegios a través de un proceso formal autorizado

- El uso no apropiado de los privilegios de administrador del sistema(cualquier característica o servicio de un sistema que permita al usuario anular los controles del sistema o de la aplicación)puede ser un

factor contribuyente importante a las fallas o vulnerabilidades del sistema.

- Se debería formular una política con respecto al uso de las redes y los servicios de red.

- La política sobre el uso de los servicios de red debería ser consistente con la política de control de acceso de la organización

- La mayoría de las instalaciones de computador tiene uno o más programas utilidades del sistema que pueden anular los controles del sistema y de la aplicación.

- Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control de acceso. Los controles de acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

- Se debe diferenciar entre reglas que siempre se deben hacer cumplir y directrices que son opcionales o condicionales.

- Establecimiento de reglas basadas en la premisa "En general todo está prohibido, a menos que este expresamente permitido" y no en la regla más débil de "En general todo está permitido a menos que este expresamente prohibido"

- Se debe tener cuidado con los cambios en los permisos de usuarios que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados por un administrador.

- Reglas que requieren aprobación especifica antes de su promulgación y aquellas que no.

Recomendaciones

El MCYP debe regularizar las conexiones inseguras y no autorizadas a servicios de red pueden afectar a toda la organización. Es importante tener este control para las conexiones de red de aplicaciones sensibles o críticas para el negocio o para usuarios en lugares de alto riesgo, por ejemplo en áreas públicas o externas que se hallan fuera de control y la gestión de la seguridad de la organización.

El equipo Chekpoint es el que regulariza las políticas de internet en el MCYP, dicho equipo se basa en la Norma ISO, las reglas asignadas deben cumplir con todos los lineamientos del Administrador de la Red y del Negocio bajo autorizaciones respectivas.

Entre algunas de las consideraciones que se debe tener en cuenta están:

- Se debe considerar el establecimiento de roles de acceso de usuario basadas en los requerimientos del negocio que incluyan un numero de derechos en perfiles típicos de acceso de usuario. Las solicitudes y revisiones de acceso se gestionan más fácilmente en el ámbito de dichas funciones que en el ámbito de derecho particulares

- Es conveniente considerar la inclusión de cláusulas en los contratos del personal y de los servicios que especifiquen las sanciones si el personal o los agentes del servicio intentan el acceso no autorizado.

- Se debe realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días, con ello se puede garantizar que no exista usuarios con reglas o permisos atendidos.

- Se debe mantener un registro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.

- Se debe garantizar las buenas prácticas de internet en cada usuario.

3.2.4 Política de correo

Norma ISO 27002 y EGSI (USO DE CORREO)

ISO: HITO 7.1.3 - 7.24 - 10.8.4 - 10.8.2

EGSI: HITO 8.14 - 3.3 - 4.9 - 8.10 - 6.19

Tabla 6. Correo

Política de uso correo	
Fuga de información	
Control: La información puede ser vulnerable al acceso no autorizado, al uso inadecuado o a la corrupción durante el transporte físico, es el caso de los envíos de medios a través de servicios postales o de mensajería.	
ISO 27002	ESGI
	Restringir el envío de información a correos externos no institucionales.
Uso aceptable de los activos	
Regla para uso de correo electrónico y de internet	Reglamentar el uso de correo electrónico institucional
Retiro de privilegios de acceso	
	Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.) inmediatamente luego de que se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente.

Políticas y procedimientos para el intercambio de información	
Procedimiento diseñados para proteger la información intercambiada contra interceptación, copiado, modificación enrutamiento inadecuado y destrucción	Establecer procedimientos para proteger la información intercambiada contra la interpretación, copiado, modificación, enrutamiento y destrucción.
Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas	Definir procedimientos para detección y protección contra programas maliciosos, cuando se utilizan comunicaciones electrónicas.
Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y los reglamentos locales y nacionales correspondientes.	Definir directrices de retención y eliminación de la correspondencia incluyendo mensajes, según la normativa legal local.
Responsabilidad de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación, acoso, suplantación de identidad, envío de cadenas, adquisición no autorizada, etc.	Establecer responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la institución con un mal uso de la información.
Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes electrónicos, según la legislación y los reglamentos locales y nacionales correspondientes	Definir directrices de retención y eliminación de la correspondencia incluyendo mensajes, según la normativa legal local.
Controles y restricciones asociadas con él envió de servicios de comunicación, como él envió automático de correo electrónico a direcciones de correo externas	Establecer responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la institución con un mal uso de la información.
	Establecer directrices para el uso de los servicios de comunicación electrónica.
Mensajería electrónica	
Proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios	Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.
Garantizar que la dirección y el transporte de mensaje son correctos	Supervisar que la dirección y el transporte de mensajes sean correctos.
Confiabilidad general y disponibilidad de servicio	
Consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas	• Tomar en cuenta consideraciones legales como la de firmas electrónicas.

	• Encriptar los contenidos y/o información sensibles que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la entidad o el Gobierno Nacional.
Obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir archivos	Monitorear los mensajes de acuerdo al procedimiento que establezca la institución.

Adaptado de :(ISO-EGSI, 2015)

Información adicional (ISO27002 Y EGSI)

- Mantener la seguridad de la información y del software que se intercambian dentro de la organización y entre organizaciones se debería basar en una política formal de intercambio, ejecutar según acuerdos de intercambio y cumplir la legislación correspondiente.

- Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información de tránsito.

- Procedimientos diseñados para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.

- Procedimientos para la detección y protección contra códigos malicioso que se pueden transmitir con el uso de comunicaciones electrónicas.

- Procedimientos para proteger la información electrónica sensible comunicada que está en forma de adjunto.

- El intercambio de información se puede producir a través de la utilización de diferentes tipos de servicios de comunicación, incluyendo correos electrónicos, voz, fax, y video.

- El intercambio de software se puede dar a través de diferentes medios, incluyendo descargas desde internet y adquiridos de vendedores de productos de mostrador.

- El negocio debería considerar las implicaciones legales y de la seguridad asociada con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, así como los requisitos para los controles.

- La información podría verse amenazada debido a la falta de conciencia, de políticas o procedimientos sobre el uso de los servicios de intercambio de información, por ejemplo por la escucha en un teléfono móvil en un lugar público, la dirección incorrecta de un mensaje de correo electrónico, las escucha de los contestadores automáticos, el acceso no autorizado a sistemas de correo de voz de marcación o el envío accidental de facsímiles al equipo errado de fax

Recomendaciones

La mensajería electrónica como, por ejemplo, el correo electrónico, el intercambio de datos electrónicos(EDI) y la mensajería instantánea tienen una función cada vez más creciente en las comunicaciones de los negocios. La mensajería electrónica tiene riesgos diferentes que las comunicaciones en papel.

El MCYP debe regularizar la transmisión y recepción del correo electrónico, en la actualidad tiene un servidor de correo Zimbra como herramienta web y para almacenar o guardar correos maneja una herramienta de software desktop Thunderbirt, se debe garantizar la disponibilidad del servicio y garantizar la confiabilidad del mismo.

Entre las políticas más importantes se debe verificar lo siguiente:

- Que el usuario no haga mal uso del correo electrónico con fines de lucro propio.

- No se debe permitir el envío de correos masivos con fines irregulares

- La violación de contraseñas para el robo de información

- Se debe controlar la eliminación de los correos electrónicos.

3.3Verificación de ITIL

3.3.1. Organización

Cuando una organización está bien estructurada se puede tomar decisiones en poco tiempo y ejecutarla con éxito. Para lograr esto es necesario que los roles y responsabilidades estén bien definidas con claridad. Uno de los modelos que pueden resultar útiles en este sentido es el modelo RACI.RACI es un acrónimo formado por las iníciales de los cuatro roles más importantes:

Responsable de ejecutar(Responsable):La persona que es responsable de realizar la tarea

Alto responsable(Accountable):Aquella única que es responsable final de la tarea

Consultado(Consulted):Personas que asesoran

Informado(Informed):Personas que deben recibir información sobre el progreso del proyecto.

Para crear un sistema RACI son necesarios los siguientes pasos:

- Identificar actividades y procesos

- Identificar y definir roles funcionales
- Llevar a cabo reuniones y delegar los códigos RACI
- Identificar carencias y posibles solapamientos
- Comunicar el esquema y tener en cuenta la retroalimentación
- Comprobar que se siguen las asignaciones

Aptitudes

- A pesar de que cada puesto exige aptitudes y competencias específicas, la persona responsable debe:
- Conocer las prioridades y objetivos del negocio
- Ser consciente del rol que desempeñan las tecnologías de la información.
- Poseer aptitudes de servicio al cliente
- Saber lo que las tecnologías de la información pueden ofrecer al cliente
- Tener las competencias y los conocimientos necesarios para desempeñar bien su función.
- Tener la habilidad de utilizar, entender e interpretar las políticas de buena práctica y los procedimientos para garantizar su cumplimiento. (MOLINA, Gestión de Servicios de TI, 2008)
- El MCYP en el 2013 se creó áreas específicas para el manejo de los recursos de TI estas áreas son Infraestructura, Soporte, Desarrollo,

Seguridad Informática. Los SLA internos para cada área específica se deben alinear a las recomendaciones de ITIL, la capacitación y las responsabilidades que debe manejar cada personal deben tener las prioridades, objetivos del negocio. Esto no solo se alinea a la norma de control interno o al EGSI, ITIL nos aclara que para un buen uso del Internet es necesario manejar lineamientos bases para un buen servicio y una buena práctica.

3.3.2 Implementación de Diseño del Servicio

ITIL recomienda implementar todos los procesos al mismo tiempo, esto se debe a que todos ellos están relacionados unos con otros y con frecuencia también dependen unos de otros.

El objetivo final es lograr conseguir un conjunto integrado de procesos que los servicios de TI puedan gestionar y supervisar durante todo el Ciclo de vida. En la mayor parte de los casos es sumamente raro que las organizaciones puedan implementar todo de una sola vez, por lo que siempre se debe empezar por el proceso que sea más necesario, no se debe olvidar que todos los procesos están relacionados. (MOLINA, 2008)

3.3.3Operación de Servicio

Existen procesos y actividades que se debe tomar en cuenta:

- Gestión de Eventos
- Gestión de Incidentes
- Gestión de Peticiones
- Gestión de Problemas
- Gestión de Accesos

- Monitorización y control
- Operaciones de TI

Hay otros procesos que serán ejecutados y apoyados durante la Operación del Servicio, pero que se dirigen desde otras fases del ciclo de vida de la gestión del servicio

- Gestión de Cambios
- Gestión de la Capacidad
- Gestión de la Disponibilidad
- Gestión Financiera
- Gestión de Conocimiento
- Gestión de la Continuidad del Servicio de TI
- Medición y generación de informes del servicio

Para la implementación de políticas en el MCYP y el cambio en algunos de los servicios para que se cumplan, es necesario tener en cuenta el proceso de implementación, es necesario implementar todos los procesos al mismo tiempo ya que las políticas están relacionadas unas con otras para así poder monitorear el ciclo de vida de los servicios y poder reaccionar de manera óptima en caso de alguna falencia.

3.3.4. Gestión de accesos

El proceso de Gestión de Accesos permite utilizar el servicio a los usuarios autorizados y limita el acceso a los usuarios sin autorizaciones algunas organizaciones, este proceso recibe también el nombre de gestión de derechos o identidades.

La gestión de accesos ayuda a garantizar que el acceso este siempre disponible en los momentos acordados, algo de lo que se encarga la Gestión de la Disponibilidad.

La gestión de accesos se puede iniciar con una petición de servicio presentada a través del centro de atención al usuario. (MOLINA, Gestión de Servicios de TI, 2008)

La gestión de Accesos consiste en:

- Requerimiento de acceso
- Verificación
- Asignación de derechos de acceso
- Monitorización del estado de identidad
- Registro y seguimiento de accesos
- Retirada o limitación de derechos de acceso

La gestión de accesos se alinea con la Políticas de Internet y de contraseñas, bajo la recomendaciones de ITIL s puede verificar que los accesos estén siempre disponibles en los momentos acordados y que únicamente tengan acceso usuarios autorizados, la limitación o retirada de derechos o permisos ayudan a mejorar las buenas prácticas de internet, esto recae inicialmente en la mesa de ayuda lo cual ayudaría si se tiene en cuenta la gestión de accesos.

3.3.5. Gestión de red

La gestión de red es crucial de la provisión del servicio, esto se da a que la gran mayoría de los servicios de TI dependen de la conectividad. Por otra

parte, el personal de Operación del Servicio accede a importantes componentes del servicio a través de la gestión de red.

En todas las organizaciones, la gestión de red es responsable de todas las redes de área local (LAN), las redes de área metropolitana(MAN) y las redes de área amplia(WAN). (MOLINA, 2008)

Para la gestión de red existe en el MCYP el equipo checkpoint, lo cual se alinea a la normativa ISO27001 y 27002.

3.3.6. Almacenamiento y archivo

En la mayoría de los servicios se necesita almacenar datos durante un cierto tiempo. En la mayor parte de los casos se requiere que esos datos estén disponibles siempre así no se tenga servicio de internet. Esto no es solo consecuencia de la legislación y normas externas, sino que además los datos pueden ser muy importantes para una organización por diferentes motivos.

La actividad de almacenamiento y archivo requiere una buena gestión de los componentes de la infraestructura, además de una **política** que defina donde se debe almacenar los dato, durante cuánto tiempo, en que formato y quien puede acceder a ellos. (MOLINA, Gestión de Servicios de TI, 2008)

Se debe tener claro para la política de escritorio limpio las recomendaciones de ITIL acerca de almacenamiento y archivo y que es algo común en nuestra épocatener archivos fundamentales para el trabajo diario.

3.3.7. Soporte al Puesto de Trabajo

En la actualidad todos los usuarios acceden a servicios de TI a través de un ordenador o equipos informáticos. El Soporte al Puesto de Trabajo es responsable de hardware, el software y los equipos periféricos de todos los

ordenadores de sobremesa y portátiles en una organización. Sus responsabilidades incluyen:

- Política y procedimiento para puestos de trabajo: Política de licencias, uso personal de ordenadores y sobremesa y portátiles, etc.

- Mantenimiento de puestos de trabajo: Implementación de versiones, actualizaciones, parches, soluciones inmediatas, etc.

- Soporte a problemas de conectividad (junto con la gestión de red): Para tele-trabajadores y personal desplazado. (MOLINA, 2008)

3.3.8. Gestión de Internet/Web

Todas las organizaciones requieren de internet en la actualidad para sus operaciones de negocio, lo que hace que se dependa de la disponibilidad y rendimiento de sus sitios WEB. En tales casos es preciso contar con un equipo propio para la Gestión de Internet/Web que se ocupe, entre otras, de las siguientes tareas:

- Diseñar la arquitectura de servicios para Internet y Web

- Especificar los estándares de desarrollo y gestión de aplicaciones Web, contenidos, sitios Web y páginas Web(normalmente durante el Diseño del Servicio).

- Mantener todas las aplicaciones de desarrollo y gestión de Web

- Dar soporte a las interfaces con sistemas de respaldo y heredados

- Monitorizar y gestionar el rendimiento en la Web mediante simulaciones de la experiencia de los usuarios, comparativas, virtualización, etc.

Para lograr tener buen uso del internet es necesario que el departamento de TI realicehitos que logren optimizar sus recursos, entre ellos esta tener un diagrama claro de los servicios que tiene la institución al igual que licencias de los servidores o estándares a manejar, registrar y tener un registro de mantenimientos y constar siempre con etapas de producción para luego lanzar a producción.

3.3.9. Gestión de la Seguridad de la Información y Operación del Servicio

La Gestión de la Seguridad de la Información, considera como un proceso en el Diseño del Servicio, es responsable de definir políticas, estándares y procedimientos que garanticen la protección de los activos, datos, información y servicios de TI de la organización. Los equipos de Operación del Servicio participan en la aplicación de dichas políticas, estándares y procedimientos y colaboran con los equipos o departamentos responsables de la Gestión de la Seguridad de la Información. El rol que desempeña un equipo de operación del servicio consiste en:

- **Política e informe:** El personal operativo revisa registros de sistema, alertas de monitorización, eventos, detecciones de hackers e informes de violaciones potenciales o reales de la seguridad. Para ello tienen que colaborar estrechamente con la Gestión de Seguridad de la Información creando así un sistema de "revisión y compensación" que garantiza la detección y el control de problemas de seguridad.

- **Asistencia técnica**: Hay ocasiones que el personal de seguridad de TI necesita colaboración para analizar incidencias de seguridad, para generar informes o para pruebas que se puedan utilizar para iniciar acciones disciplinarias o procesos criminales.

- **Gestión de la seguridad operativa:** Existen razones operativas por las que el personal técnico necesita acceder a áreas técnicas importantes,

como contraseñas de súper usuarios, entradas físicas a centros de procesos de datos o salas que estas actividades sean comprobadas y queden registradas.

- **Formación y concienciación:** La plantilla de Operación del Servicio debe recibir formación sobre la política y procedimientos de seguridad de una organización para que sean más conscientes de su importancia. Esta formación debe incluir detalles sobre acciones disciplinarias. (MOLINA, Gestión de Servicios de TI, 2008)

3.4Centro de Servicio al Usuario

Para la implementación de políticas y servicios, verificación de los mismos es muy importante garantizar la disponibilidad de empleados necesarios para que el Centro de Servicios al Usuarios pueda hacer frente a la demanda del negocio en todo momento. En muchas organizaciones es la parte fundamental para el primer contacto con los usuarios, el número de llamadas puede variar considerablemente según el día y la hora, por lo que una buena planificación debe tener en cuenta cuales son las horas punta y cuando hay menos trabajo.

También son sumamente importantes los niveles y aptitudes de la plantilla del Centro de Servicio al Usuario. Los tiempos estipulados para hallar una solución deben estar adaptados a la complejidad de los sistemas y a lo que la empresa esté dispuesta a pagar para determinar el nivel de conocimientos necesarios. Normalmente, el método más eficaz y rentable consiste en utilizar el Centro de Servicios al Usuario como primera línea de soporte, que recibe las llamadas y las escala rápidamente a los grupos más experimentados de segunda y tercera línea de soporte. Sin embargo, el punto básico de partida puede ser mejorado con el tiempo si se proporciona al personal una base de conocimientos, procedimientos de diagnóstico y herramientas integradas, así como formación y concienciación continuadas de manera que se pueda elevar

los ratios de primer nivel de resolución. (MOLINA, Gestión de Servicios de TI, 2008)

El centro de usuarios en sumamente importante para una buena práctica de internet ya que el único punto de contacto es el de la mesa de ayuda, el MCYP implemento en su central telefónica marca elaxtic dos recursos fundamentales para la atención al usuario.

El primero en la línea de soporte 355 la cual es el único medio telefónico para el contacto con personal de soporte, esta línea está disponible 8 horas laborales, tiene saltos de llamada para cuando el usuario de soporte tenga la línea ocupada, salte automáticamente a otro disponible.

Un correo para atención al usuario soporte@culturaypatrimonio.gob.ec el cual es el único mecanismo de contacto vía mail para el registro y la atención de incidencias, esto se alinea a una herramienta libre OTRS la cual maneja las incidencias por orden de llegada, alerta y saca reportes mensuales del mismo.

3.5Gestión de la Seguridad de la Información

La meta de la Gestión de la Seguridad de la Información es alinear la seguridad de TI con la del negocio y garantizar una gestión eficaz de la seguridad de la información en todos los servicios y actividades de Gestión del Servicio.

Los objetivos son:

- Garantizar que la información esté disponible y se pueda usar cuando se necesite(disponible).

- Garantizar que la información esté disponible exclusivamente para personas autorizadas(confidencialidad).

- Garantizar que la información sea completa, precisa y este protegida contra cambios no autorizados(integridad).(MOLINA, Gestión de Servicios de TI, 2008)

3.5.1.Ámbito

La Gestión de la Seguridad de la Información debe cubrir toda la información de TI y del negocio.

Entre otras cosas esto incluye:

- La política y los planes actuales y futuros de seguridad del negocio
- Los requisitos de seguridad
- Los requisitos legales
- Las obligaciones y las responsabilidades
- Los riesgos para TI y el negocio(y su gestión).

Esto permite al proceso gestionar de manera eficiente los aspectos de seguridad, actuales y futuros del negocio. El proceso de Gestión de la Seguridad de la Información deberían incluir los siguientes elementos:

- Elaboración, mantenimiento distribución y fortalecimiento de una política de seguridad de la información.
- Entendimiento de los requisitos de seguridad, actuales y futuros, del negocio, que se hayan acordado.
- Implementación(y documentación) de controles que faciliten la política de seguridad de la información y gestión de riesgos.

- Gestión de promovedores de servicios de TI y de contratos, en lo referente a acceso al sistema y a los servicios

- Mejora proactiva de los sistemas de control de la seguridad.(MOLINA, Gestión de Servicios de TI, 2008)

Valor para el negocio

La Gestión de la Seguridad de la Información garantiza que la política sobre seguridad de la información cumple la política general de la empresa sobre seguridad y los requisitos de gobierno corporativo.

3.6 Gestión de Incidencias

El proceso de Gestión de Incidencias cubre todo tipo de incidencias, ya sean fallos, preguntas o consultas planteadas por el usuario, cambios de contraseñas, permisos de red(generalmente con una llamada al Centro de Servicio al Usuario)o personal técnico o bien detectadas automáticamente por herramientas de monitorización de eventos.

"Para ITIL una incidencia es una interrupción no planificada o una reducción de calidad de un servicio de TI. El fallo de un elemento de configuración que no haya afectado todavía al servicio también se considera una incidencia" (MOLINA, Gestión de Servicios de TI, 2008)

El principal objetivo es solventar rápidamente del proceso de Gestión de Incidencias y volver a una situación normal y así minimizar el impacto sobre procesos de negocio.

El personal técnico también puede comunicar alguna incidencia, aunque esto no significa que todo sea una incidencia.

Tanto las incidencias como las peticiones de servicios comunican al Centro de Servicio al Usuario, pero no son iguales. Las peticiones de servicio no representan interferencias para servicio, sino solicitudes de soporte, entrega, información, consejo o documentación por parte de los usuarios.

Límites de tiempo: Se deben definir límites de tiempo para todas las fases y emplearlos como objetivos en Acuerdos de Nivel Operativo(OLA) y contratos de soporte.

Modelos de incidencias: Un modelo de incidencia es una manera de determinar los pasos necesarios para ejecutar correctamente un proceso, lo que significa que las incidencias estándar se gestionaran de forma correcta y en el tiempo establecido

Incidencias graves: Las incidencias graves requieren un procedimiento distinto, con plazos más cortos y mayor nivel de urgencia. Hay que definir que es una incidencia grave y describir todo el sistema de prioridades para incidencias.

En ocasiones se confunde incidencias graves con un problema, pero una incidencia siempre será una incidencia; es posible que aumente su impacto o su prioridad, pero nunca llegara a ser un problema. Un problema es la causa que subyace a una o más incidencias y siempre será una entidad diferenciada. (MOLINA, Gestión de Servicios de TI, 2008)

Los pasos de proceso de Gestión de Incidencias es el siguiente:

- Identificación
- Registro
- Clasificación

- Priorización
- Diagnostico
- Escalado
- Investigación y diagnostico
- Resolución y recuperación
- Cierre

3.7Gestión de Peticiones

"Una petición de servicio es una solicitud de información asesoramiento, cambio estándar o acceso a un servicio por parte de un usuario.

Un ejemplo de una petición de servicio es solicitud de cambio de contraseña o de la instalación de una aplicación software en una determinada estación de trabajo. Estas peticiones se plantean con mucha frecuencia y suponen muy poco riesgo, por lo que es recomendable gestionarlas con un proceso independiente

- Poner a disposición de los usuarios un canal a través del cual puedan solicitar y recibir servicios; para ello debe existir un proceso de aprobación y cualificación.
- Proporcionar a usuarios y clientes información sobre la disponibilidad de servicios y el procedimiento para obtener dichos servicios.
- Proporcionar los componentes de servicio estándar (por ejemplo, licencias y software).

- Facilitar información general, quejas y comentarios.

La gestión de peticiones depende de los siguientes Factores Críticos de Éxito

- Existencia de acuerdo sobre qué servicios son estándar y quien está autorizado a solicitarlos, así como sobre el costo de estos servicios.

- Publicación de estos servicios en beneficio de los usuarios como parte del Catálogo de Servicios.

- Definición de un procedimiento de gestión estándar para cada uno de los servicios solicitados

- Uso de un único punto de contacto para solicitar el servicio, normalmente se utilizar el Centro de Servicio al Usuario o Internet, pero también puede ser una petición autorizada en el sistema de gestión de peticiones.

- Uso de herramientas de autoservicio para la interfaz de usuarios; es importante que esta interfaz se pueda comunicar con las herramientas de gestión.(MOLINA, Gestión de Servicios de TI, 2008)

3.8 Identificación de la normativa aplicable a las políticas públicas gubernamentales para la gestión tecnológica y de comunicación que rigen al MCYP.

3.8.1. Plan Nacional De Gobierno Electrónico

La Organización de las Naciones Unidas, se ha referido al uso de Tecnologías de Información y Comunicación (TIC), por parte de las instituciones de Gobierno, para mejorar cualitativamente los servicios de información que se ofrecen a las ciudadanas y ciudadanos; aumentar la eficiencia y eficacia de la gestión pública; incrementar sustantivamente la

transparencia del sector público y la participación ciudadana.

El Gobierno Electrónico no es un fin en sí mismo, sino que tiene un carácter instrumental que requiere la revisión, rediseño y optimización de los procesos como paso previo a la introducción de cualquier cambio en la tecnología o en las funciones de las organizaciones públicas.

Para la implementación del Gobierno Electrónico, el Estado ha previsto la creación, revisión y optimización de procesos tecnológicos, usados en la captura, procesamiento, almacenamiento y transmisión de información, para las soluciones tecnológicas que impulsa este modelo de Gobierno.

Dentro del marco regulatorio, se ha utilizado instrumento legales y jurídicos que permiten la construcción de soluciones, garantizando la operatividad, calidad, sostenibilidad y funcionalidad de las mismas , se destacan: Acuerdo de Constitución y operación del Observatorio de Gobierno Electrónico, Acuerdo de Difusión de Conocimiento público, libre y/o abierto, Acuerdo 166 Esquema de Seguridad de la Información, Decreto Ejecutivo de Firma Electrónica, Ley de Gobierno Electrónico, Ley Orgánica de Transparencia y Acceso a la información Pública, así como las Normas de Calidad, Estandarización de Sitios Web, Normativa de Gobierno de IT, Normativa de Software Público, Normativa de Usabilidad. y Normativa de Utilización de Nube.

3.8.2. Elementos Habilitadores del pilar Marco Regulatorio

- **Ley de Gobierno Electrónico:** Es el marco legal que rige el acceso a la información pública y el diseño, ejecución e implementación de procesos y servicios soportados por tecnologías de la información y comunicaciones, con el fin último de desarrollar el Gobierno Electrónico en el Ecuador.

- **Ley Orgánica de Transparencia y Acceso a la Información Pública:** Esta ley regula el ejercicio del derecho fundamental de las personas a acceder a la información pública, conforme a las garantías consagradas en la Constitución del Ecuador y otros instrumentos internacionales vigentes. La aplicación de lo establecido en esta ley está normado en su reglamento general.(Lexis)

- **Decreto Ejecutivo 1014 Software Libre y estándares abiertos:** Decreto ejecutivo del 10 de abril del 2008 en el cual se establece como política pública la utilización de software libre en los sistemas y equipamientos informáticos de la función ejecutiva.

- **Decreto Ejecutivo 1384 Interoperabilidad:** Decreto ejecutivo del 13 de diciembre de 2012. Establece como política pública el desarrollo de la interoperabilidad gubernamental, que consiste en el esfuerzo mancomunado y permanente de todas las entidades de la Administración Pública central, institucional y dependiente de la función ejecutiva para compartir e intercambiar entre ellas datos e información necesarios para la prestación de servicios públicos.(Lexis)

- **Decreto Ejecutivo de Firma Electrónica:** Este decreto regula la vigencia de la firma electrónica a la vez que fomenta la utilidad de los certificados de firma electrónica de las personas naturales.(Lexis)

- **Acuerdo 166 Esquema de Seguridad de la Información:** Acuerdo emitido el 19 de septiembre del 2013 donde se establece las directrices y lineamientos para la Seguridad de la Información dentro de las entidades de la Administración Pública Central institucional y dependiente de la Función Ejecutiva.(Lexis)

- **Norma de Estandarización de Sitios Web:** Esta norma busca facilitar la usabilidad y accesibilidad de los sitios web de las instituciones de la

Administración Pública central, institucional y dependiente de la Función Ejecutiva.(Lexis)

- **Normativa de Calidad:** Normativa que establecerá los lineamientos y mecanismos para planificar, evaluar y mejorar la calidad de los procesos y servicios que proveen las instituciones de la Administración Pública Central, institucional y dependiente de la Función Ejecutiva.(Lexis)

- **Normativa de Gobierno de TI:** Definen estándares para garantizar que las unidades de TI soporten los objetivos institucionales y tengan, a la vez, un proceso de madurez continuo en TI y Gobierno Electrónico.(Lexis)

- **Normativa de Software Público:** Busca establecer el concepto de software público, que implica el derecho de uso público de los sistemas desarrollados o adquiridos por institución pública en particular.(Lexis)

- **Norma de Utilización de Nube de Gobierno:** Normativa que regula el uso de los distintos servicios que se prestan a través de la nube gubernamental.(Lexis)

- **Normativa de usabilidad:** Normativa que regula la implementación de mecanismos para generar, mantener y desarrollar la facilidad de la interfaz y facilitad uso de las soluciones de Gobierno Electrónico.(Lexis)

La Secretaría Nacional de la Administración Pública a través de la Subsecretaría de Gobierno Electrónico, será la dependencia encargada de efectuar la coordinación, articulación interinstitucional, emisión de las políticas, directrices, normativas y lineamientos, así como, de la generación de programas y proyectos que sean necesarios para la implementación del Plan Nacional (art 4. Ley gobierno electrónico de la función ejecutiva)

3.8.3. Plan Nacional Para el Buen Vivir

Dentro del área de la Tecnología, innovación y conocimiento la estrategia de acumulación, distribución y redistribución, el desarrollo de las fuerzas productivas se centra en la formación de talento humano y en la generación de conocimiento, innovación, nuevas tecnologías, buenas prácticas y nuevas herramientas de producción, con énfasis en el bio-conocimiento y en su aplicación a la producción de bienes y servicios ecológicamente sustentables.

Estos procesos se orientan en función de la satisfacción de las necesidades del país y, por ello, conllevan el fomento de los sectores productivos priorizados para la transformación de la matriz productiva a mediano y largo plazo. (Lexis S.A)

Dentro de las políticas y lineamientos estratégicos, lo que el Estado Ecuatoriano requiere es que se afiance una gestión pública inclusiva, oportuna, eficaz, y de excelencia agilizando y simplificando los procesos procedimientos administrativos, con el uso y el desarrollo de tecnologías de información y comunicación, a fin de prevenir y controlar la delincuencia común organizada, por ello estas políticas de optimización tecnológica lo que conseguirá en el sector público específicamente en el desarrollo de las TICs del Ministerio de Cultura y Patrimonio, para lograr modernizar la infraestructura, el equipamiento y la tecnología, para mejorar el servicio y la capacidad de repuesta.

3.8.4. Ley Orgánica de Telecomunicaciones

Corresponde al órgano rector del sector de las Telecomunicaciones y de la Sociedad de la Información las competencias señaladas en el artículo 141 de la Ley Orgánica de Telecomunicaciones:

"2. Formular, dirigir, orientar y coordinar las políticas, planes y proyectos para la promoción de las tecnologías de la información y la comunicación y el

desarrollo de las telecomunicaciones, así como supervisar y evaluar su cumplimiento."(Lexis)

"4. Promover, en coordinación con instituciones públicas o privadas, la investigación científica y tecnológica en telecomunicaciones, tecnologías de la información y comunicación, así como la ejecución de los proyectos que la apoyen."(Lexis)

"7. Coordinar y liderar el uso efectivo de las tecnologías de la información y comunicación en los organismos públicos." (Lexis)

Puesto que las Tecnologías de la información y comunicación TIC, son un conjunto de servicios, redes y plataformas integradas que permiten el acceso o generación de datos a través del procesamiento, almacenamiento, análisis y presentación de la información.

CAPÍTULO IV

4. Elaboración de Políticas Internas de Internet, correo, contraseñas y escritorio limpio, adaptables para las buenas prácticas tecnológicas y de la información en el Ministerio de Cultura y Patrimonio.

4.1 Política de uso de Internet

Tabla 7:Flujo de Aprobación Internet

Acción	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado:		Especialista TIC		
Revisado y Aprobado:		Directora de Auditoría Interna		
		Directora de Gestión de Talento Humano		
		Director de Gestión Administrativa		
		Responsable de TIC		

4.1.1 Introducción

La política de uso del servicio de Internet en el Ministerio de Cultura y Patrimonio, es un instrumento que apegado a los mandatos institucionales, busca alcanzar la gestión eficaz, eficiente y efectiva para el buen funcionamiento del servicio de Internet; beneficiando a todos los/las

servidores/as, funcionarios/as y trabajadores/as de la Institución que hacen uso del mismo, sin dejar de lado sus obligaciones y derechos con la institución.

4.1.2 Objetivo

El objeto del presente, es normar y optimizar la disponibilidad, uso y control del servicio de Internet que se encuentra a disposición de los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio.

4.1.3 Alcance

La presente política se aplica a todos los funcionarios que labora en el Ministerio de Cultura y Patrimonio, así como para los usuarios externos, como consultores, contratistas y proveedores que trabajen con información de la Institución, quienes tienen la obligación de cumplir lo indicado en la presente política.

4.1.4 Definiciones

Para efectos del presente documento, se entenderá por:

Internet: Es una red de equipos informáticos conectados a nivel mundial, con el propósito de brindar acceso a la información a los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio. Internet permite la conexión, visualización y acceso a páginas web y servicios que se encuentran publicados en la red, incluyendo ciertos servicios propios de la institución.

Máxima Autoridad Ejecutiva: El (la) Ministro(a) de Cultura y Patrimonio.

Servidor Público: Son servidoras o servidor es públicos todas las personas trabajan, prestan servicios o ejercen un cargo, función o dignidad dentro del sector público. (DefinidoenlaLOSEP–Art.4).

Perfil de uso: Es el grado de accesibilidad y restricción al servicio de internet.

Ancho de banda: Es la capacidad del medio físico por donde se transmite la información de la institución. El ancho de banda es limitado, por lo que será distribuido mediante los perfiles de uso, a los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio.

4.1.5 Base legal

El presente tiene como base legal la siguiente disposición:

- Normas de Control Interno de la Contraloría General del Estado para las Entidades, Organismos del Sector Público y de las de las personas jurídicas de derecho privado que dispongan de recursos públicos, N° 410-14.
    - DecretoEjecutivo1384del13deDiciembrede 2013,Articulo1.
    - Esquema Gubernamental de Seguridad de la Información.

4.1.6 Ámbito de aplicación

Las políticas descritas en el presente documento son de aplicación y cumplimiento obligatorio por parte de los/las servidores/as, funcionarios/as y trabajadores/as en todas las unidades organizacionales del Ministerio de Cultura y Patrimonio.

4.1.7 Responsabilidades

Elincumplimientoalodispuestoenelpresentedocumento,generaráresponsabilidades de acuerdo a la LOSEP, Art. 42.- De las faltas disciplinarias, inciso a) y Art. 43.- Sanciones disciplinarias, incisos a) y b), de la misma forma, tendrá incidencia sobre la responsabilidad de la función pública.

Es responsabilidad de los/las servidores/as, funcionarios/as y trabajadores/as de esta Cartera de Estado cumplir con las disposiciones descritas en el presente documento.

Coordinación General de Gestión Estratégica

- Facultara la Unidad de Tecnologías de la Información y Comunicación sobre la gestión de los usuarios respecto al uso del servicio de Internet.
- Difusión de la presente política.

Unidad de Tecnologías de la Información y Comunicación

- Habilitar el servicio de acceso a internet a los/las servidores/as, funcionarios/as y trabajadores/as, de las diferentes unidades organizacionales de la institución.
- Velar por el servicio continuo y adecuado del acceso a internet para todas las unidades organizacionales de la institución.
- RealizarseguimientoycontroldelusoadecuadodelosserviciosdeInternet. Elaborarinformespreviasolicituddelaautoridad,acercadelinapropiadouso del servicio de Internet.

Servidores/as, Funcionarios/as y Trabajadores/ascumpliryhacercumplirlaspolíticasdeusoparaelaccesoalserviciodeInternet.

4.1.8 Aprobación y Difusión de la Política

Es facultad del Sr. (a)Ministro(a) de Cultura y Patrimonio la aprobación y su difusión del presente documento, por medio del Comité de Seguridad de la Información.

4.1.9 Revisión y Actualización de la política

El Comité de Seguridad de la Información, revisará periódicamente las políticas de uso de Internet; de ser necesario actualizará el presente documento con base al análisis de la experiencia de uso del Internet dentro de la Institución con el propósito de mejorar la disponibilidad, eficiencia y eficacia del servicio.

4.1.10 Política

Conocimiento del usuario

La utilización del servicio de Internet proporcionado por el Ministerio de Cultura y Patrimonio, indica que el usuario conoce, entiende y acepta en su totalidad los términos, condiciones y restricciones del servicio en mención.

Alcances y limitaciones del servicio

El Ministerio de Cultura y Patrimonio a través de la Unidad de Tecnologías de Información y Comunicación, proporciona el acceso al servicio de internet únicamente bajo los siguientes términos y condiciones:

El uso del servicio de Internet está limitado a actividades específicamente laborales, relacionadas con las funciones asignadas al cargo de cada servidores/as, funcionarios/as y trabajadores/as.

Los/las servidores/as, funcionarios/as y trabajadores/asde la Institución son responsables de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución asignados.

Se otorgará derechos de acceso a Internet a personas ajenas (visitantes) al Ministerio de Cultura y Patrimonio, a través de una red de datos destinada para el uso del personal ajeno a la Institución.

Para acceder a los servicios de Internet, se lo debe hacer sólo a través del navegador Mozilla Firefox; para lo cual la Unidad de Tecnologías de Información y Comunicación instalará el navegador mencionado y configurará el equipo asignado a los/las servidores/as, funcionarios/as y trabajadores/as, para que éste haga uso responsable del servicio de Internet.

La Unidad de Tecnologías de la Información y Comunicación tiene la facultad de monitorear el uso responsable del servicio de internet, con la plena facultad de excluir y suspender el servicio a cualquier equipo de computación que esté haciendo mal uso de éste. El servidor/a, funcionario/a y trabajador/aresponsable del equipo podrá ser sancionado de acuerdo a la LOSEP, Art. 43.- Sanciones disciplinarias, inciso a) y b) conforme lo establezca los reglamentos internos a través de la Dirección de Gestión del Talento Humano.

Todos los puntos de acceso a la red del Ministerio de Cultura y Patrimonio serán monitoreados por la Unidad de Tecnologías de Información y Comunicación, analizando el consumo del servicio de internet de cada servidor/a, funcionario/a y trabajador/a, con el propósito de optimizar su funcionamiento y evitar la saturación de la infraestructura de comunicaciones para no degradar el servicio de Internet.

Los sistemas como: el correo institucional, sistema de gestión documental y demás sistemas gubernamentales estarán habilitados para todos los/las

servidores/as, funcionarios/as y trabajadores/as, por ser medios de comunicación de carácter oficial.

La Unidad de Tecnologías de la Información y Comunicación está en la facultad de establecer limitaciones respecto al uso del servicio de internet mediante Perfiles de Uso, los cuales permitirán clasificar al funcionario público para el uso adecuado del servicio de internet.

Durante el uso del servicio de internet, cualquier tipo de archivo malicioso descargado o activado involuntariamente, que provoque la degradación del servicio de internet, será entera y total responsabilidad del servidor/a, funcionario/a y trabajador/a asociado a ese equipo. Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que éste provenga de una fuente confiable, en caso de dudas el servidor/a, funcionario/a y trabajador/adeberá consultar con la UTICs.

El servidor/a, funcionario/a y trabajador/aes responsable directo de toda la actividad que sea realizada en la computadora asignada, por tal razón deberá bloquearlo al no estar presente y apagarlo al finalizar la jornada laboral.

Todo servidor/a, funcionario/a y trabajador/adel Ministerio de Cultura y Patrimonio deberá comunicar a la Unidad de Tecnologías de la Información y Comunicación del incumplimiento de la presente política.

El acceso del servicio a internet no deberá ser utilizado para propósitos fraudulentos, comerciales, publicitarios, o propagación de mensajes destructivos u obscenos.

4.1.11 Consideraciones adicionales EGSI

El Oficial de Seguridad de la Información de la institución elaborará y pondrá en marcha el control y la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte del servidor/a, funcionario/a y

trabajador/asin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas.

Todos los accesos podrán ser sujetos de monitoreo y conservación permanente por parte de la institución.

El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.

La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los/las servidores/as, funcionarios/as y trabajadores/aso a terceros que accedan tanto por medio alámbrico como inalámbrico.

Expresamente está prohibido la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso Institucional o del servidor/a, funcionario/a y trabajador/a, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.

4.1.12 Prohibiciones y control

El Ministerio de Cultura y Patrimonio proporciona el acceso al servicio de internet únicamente bajo los términos y condiciones mencionados a continuación:

El acceso por medio de dispositivos fijos y/o móviles a los portales, aplicaciones y servicios de la Internet y la web está limitado y controlado mediante el uso de perfiles de usuario; estos perfiles implementados para el

uso exclusivo del servicio de Internet son: VIP, Avanzado, Básico y Redes Sociales.

Expresamente está prohibido el acceso a Internet, portales, aplicaciones, servicios web en general a contenidos de: pornografía, racismo, violencia, delincuencia, contenidos ofensivos y contrarios a los intereses institucionales, entre otros, y valores de la institución que impacten negativamente en la productividad y trabajo de la Institución por ejemplo: mensajería instantánea-chat, redes sociales, video y otros) y aquellos que particularmente que atenten a la ética y mora.

Perfil VIP

El perfil de uso VIP está constituido por usuarios de carácter jerárquico como: Ministro(a) y Viceministro(a) de Cultura y Patrimonio. El perfil VIP no tiene restricciones de uso de servicio de Internet.

Perfil Avanzado

Este perfil está constituido por: Subsecretarios(as), Asesores Ministeriales y Coordinadores(as) Generales y Directores(as) Técnicos de Área, los mismos que comparten el ancho de banda y poseen ciertas restricciones de navegación.

Perfil Básico

Los usuarios que dispongan de este perfil tendrán acceso al uso del servicio de internet medianamente restringido, es decir, serán habilitadas páginas exclusivas previa solicitud del Jefe(a) inmediato(a) superior de acuerdo a la naturaleza de sus funciones.

Perfil Redes Sociales

Este perfil dispondrá de páginas relacionadas a redes sociales además de lo contemplado en el perfil básico.

Los/las servidores/as, funcionarios/as y trabajadores/as que tienen habilitado el servicio de Internet están prohibidos de:

- Usar el servicio de Internet para fines que no sean los del Ministerio de Cultura y Patrimonio.

- Cambiar la configuración de red de los equipos ya configurados.

- Navegar en páginas o redes sociales. (Blogger, Facebook, skype, youtube, entre otras), excepto cuando la naturaleza de sus funciones laborales lo requiera.

- Acceder y usar a los servicios de correo electrónico gratuito como: gmail, hotmail, yahoo, facebook, Outlook, servicios de mensajería instantánea, entre otros.

- Realizar descargas de programas, videos, música, otros; por medio de software que permita el intercambio directo de la información, P2P. (BitDownload, Bitgrabber, Bitroll,BitLord, BitTorrent, Ares, entre otras).

- Escuchar radios o música On Line, ver videos, TV o películas, partidos de fútbol nacionales e internacionales On Line.

- Usar el Internet para realizar llamadas internacionales.

- Participar en juegos de entretenimiento en línea. Participar en foros o chats de discusión, excepto cuando la naturaleza de sus funciones

laborales lo requiera, para lo cual solicitará el acceso con la debida autorización de su jefe inmediato.

- Navegar en páginas de contenido pornográfico, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos.

- Navegar en páginas de contenido ilícito o que atenten contra la dignidad humana o alienten a la violencia y discriminación, aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista, etc.

- Usar los servicios del acceso a internet para propósitos fraudulentos, comerciales o publicitarios, o para la propagación de mensajes destructivos u obscenos.

- Descargar y transmitir programas de computación dañinos, virus, códigos, expedientes o programas privativos y de software libre (freeware o shareware) que afecten y alterará el correcto funcionamiento de los mismos.

- Descargar programas ilícitos sin licencia obtenida legalmente e instalarlos en los computadores de la institución.

- Hacer o intentar hacer, actividades que afecten desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios.

- Realizar técnicas de hackeo interno o externo (ataques negación de servicios, ataques contra otros sistemas y contra sistemas propios del Ministerio de Cultura y Patrimonio).

- Cualquier otro servicio, página, equipo, que la Unidad de Tecnología de Información y Comunicación determine, como ilegal, abusiva o dañina.

- Liberar, publicar y difundir a través del internet, información confidencial, sensible o de uso exclusivo del Ministerio de Cultura y Patrimonio.
- Burlar y evadir las restricciones de uso de internet, por medio de equipos y/o software informático.
- Vulnerar los controles de seguridad para los servicios de Internet.
- Utilizar programas que burlen los controles de seguridad informáticos que les permita acceder a contenido prohibido descrito en la presente política. (ej. Proxys anónimos, Red Thor, freproxys, etc.).

El incumplimiento a las prohibiciones establecidas en el presente numeral, y dependiendo de la naturaleza de la acción realizada, se analizará caso por caso y se adoptarán las medidas pertinentes mismas que podrían dar lugar a las siguientes sanciones.

- Primera vez: Llamada de atención verbal.
- Segunda vez: Llamada de atención escrita y cancelación temporal del servicio de internet.
- Tercera vez: Severa llamada de atención escrita y la suspensión definitiva de la misma, así como sanciones contempladas en la ley y reglamentos internos.

Los usuarios utilizarán únicamente los equipos asignados bajo su responsabilidad para acceder a los servicios de internet para los cuales están autorizados. No deberán usar los equipos de otras personas, ni intentar apoderarse de claves de acceso de otros equipos, para acceder a los servicios de internet sin restricción.

La infracción de cualquiera de los aspectos anteriormente mencionados causa la suspensión del servicio, y puede suponerle sanciones institucionales, así como otro tipo de consecuencias legales. El Ministerio de Cultura y Patrimonio se reserva el derecho, de investigar el mal uso del servicio de

internet para determinar si se infringe los aspectos mencionados en este documento.

Indemnización

- El usuario acepta indemnizar al Ministerio de Cultura y Patrimonio, frente a reclamos de terceros relacionados con el uso del servicio, incluyendo la responsabilidad o gasto ocasionado por los reclamos, pérdidas, daños de todo tipo, litigios, resoluciones, costos procesales y honorarios de abogados.

- El Ministerio de Cultura y Patrimonio le hará llegar la notificación escrita de dicho reclamo, litigio o acción, a fin de que el usuario ejerza su derecho a la defensa

- El Ministerio de Cultura y Patrimonio no se hará responsable por el mal uso de la información que se encuentre registrada como propiedad intelectual.

4.1.13 Modificaciones a las políticas

- El Comité de Seguridad de la Información y el Oficial de Seguridad de la Información están en pleno derecho de hacer las modificaciones/actualizaciones que sean necesarias a este documento "Política de uso de internet" y los procedimientos a los cuales hace referencia, con la obligación de hacer públicos los cambios realizados.

- La Unidad de Tecnologías de Información y Comunicación a través del Responsable de Seguridad de TIC, elaborará los respectivos procedimientos de seguridad informática para la ejecución y aplicación de los controles descritos en la presente política.

- Es responsabilidad del usuario revisar regularmente los términos, condiciones y restricciones de uso adicionales, expuestas en el presente documento.

- El uso continuo del servicio de internet supone la aceptación de todos los términos, condiciones y avisos aquí expuestos. Así mismo, el desconocimiento de las normas no exime a los usuarios de las sanciones a que hubiere lugar en caso de incumplimiento de las mismas.

4.1.14 Exclusión de Responsabilidades

- El Ministerio de Cultura y Patrimonio no realiza ninguna manifestación sobre la idoneidad, fiabilidad, disponibilidad, oportunidad, ausencia de virus u otros componentes dañinos así como de la exactitud de la información, software, productos y servicios relacionados con el servicio de internet para cualquier fin.

- El usuario acepta específicamente que el Ministerio de Cultura y Patrimonio no será responsable por el acceso y/o la alteración no autorizada de las transmisiones o datos enviados/recibidos, a través del servicio de internet.

- El usuario acepta específicamente que el Ministerio de Cultura y Patrimonio no es responsable de ningún contenido o conducta amenazadora, difamatoria, obscena, ofensiva o ilícita de cualquier otra parte ni de cualquier infracción de los derechos de terceros, incluidos los derechos de propiedad intelectual e industrial.

- El Ministerio de Cultura y Patrimonio se excluye, en la máxima medida permitida por las leyes, de cualquier responsabilidad por los daños y perjuicios que se deriven de la pérdida de datos o de beneficios, que se deriven o estén relacionados con el uso del servicio de acceso a internet; con la demora o la imposibilidad de poder usar el servicio de acceso a internet o los servicios relacionados con el mismo, o con cualquier información, software, productos y servicios relacionados que se obtengan a través del servicio de acceso a internet.

- Cuando ello sea razonablemente posible, la Unidad de Tecnologías de la Información y Comunicación del Ministerio de Cultura y Patrimonio, advertirá previamente las interrupciones en la prestación del servicio de internet.

- Si el usuario no está satisfecho parcial o totalmente con el servicio de acceso a internet o con alguna las condiciones impuestas en este documento, su único y exclusivo recurso será dejar de utilizar el servicio de acceso a internet proporcionado por el Ministerio de Cultura y Patrimonio.

4.1.15 Sanciones

El incumplimiento de la presente política, en referencia a las disposiciones indicadas en la misma así como el Esquema Gubernamental de Seguridad de la Información, tendrá como resultado la aplicación de las sanciones de acuerdo a la normativa legal vigente.

El incumplimiento de la presente Política puede provocar un incidente de seguridad comprometiendo la Confidencialidad, Integridad o Disponibilidad de la Información, afectar las operaciones, procesos y actividades en la Institución.

Incidente de Seguridad de la información: Es un evento adverso en un sistema de información, red, computador, que pueda comprometer la Confidencialidad, Integridad o Disponibilidad de la información, puede ser causado mediante el aprovechamiento de alguna vulnerabilidad del sistema, un intento de amenaza o violentar los mecanismos de seguridad.

Se consideran como incidentes de seguridad, los siguientes eventos:

- Violentar y vulnerar la seguridad física para acceder a la información no autorizada;

- Violentar los accesos y la información no autorizada;

- Compartir contraseñas de cualquier sistema;

- Acceder a los recursos o sistemas por medios o mecanismos no autorizados;
- Acceder a los recursos, información o sistemas no autorizados;
- Publicar, difundir o divulgar información a nombre de la Institución sin la debida autorización y el procedimiento legalmente establecido para el efecto;
- Otros que comprometan la Confidencialidad, Integridad o Disponibilidad de la Información.

4.1.16 Punto de contacto

Cualquier inquietud en materia de seguridad de la información podrá ser notificado al funcionario/servidor que actúe como Oficial de Seguridad de la Información o a la dirección de correo electrónico seguridad@culturaypatrimonio.gob.ec.

4.1.17 Referencias

- Acuerdo N° 166 25 de Septiembre de 2013, Secretaría Nacional de la Administración Pública (SNAP), Anexo 1 - Esquema Gubernamental de Seguridad de la Información v1.0.
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001, ISO/IEC 27002
- Esquema Gubernamental de Seguridad de la Información (EGSI)

4.2. Política de puesto de trabajo despejado y pantalla limpia

Tabla 8.Flujo de Aprobación Puesto despejado

Acción	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado:		Especialista TI		
Revisado y Aprobado:		Directora de Auditoría Interna		
		Directora de Gestión de Talento Humano		
		Director de Gestión Administrativa		
		Responsable de TI		

4.2.1 Introducción

En el trabajo del día a día en el Ministerio de Cultura y Patrimonio, se maneja variada información en formato electrónico y físico, dicha información tiene valor ya que constituye un insumo para desarrollar las principales actividades que se realizan en la Institución.

Por tal motivo es necesario gestionar los riesgos que se puedan presentar por la mala manipulación y control que se realice.

La información física que se maneja reposa en los escritores de trabajo, archivadores; la información digital se almacena en los sistemas de información, computadores, dispositivos móviles, entre otros; la presente política se enfoca en disponer ciertas directrices necesarias para proteger la información física que el/la servidor/a, funcionario/a y trabajador/a manipula en su entorno diario.

4.2.2 Objetivo

Definir las pautas generales para brindar protección adecuada a la información que se maneja en el entorno del área de trabajo de los funcionarios es decir de información física.

4.2.3 Alcance

La presente política se aplica a todos los/las servidores/as, funcionarios/as y trabajadores/as que laboran en el Ministerio de Cultura y Patrimonio, quienes tienen la obligación de cumplir lo indicado en la presente política.

4.2.4 Definiciones

La Seguridad de la Información se garantiza mediante la preservación de las siguientes características:

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Se garantiza la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y recursos relacionados con la misma, toda vez que lo requieran.

4.2.5 Política

- Los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio deberán guardar en sus respectivos archivadores asignados la documentación, archivos e información bajo su custodia que se encuentra en su escritorio de trabajo, al finalizar su jornada laboral como en el horario de almuerzo. La única documentación e información que se puede dejar desatendida sobre los escritorios de trabajo es aquella que no genere impacto cuantitativo o cualitativo para

la Institución por su pérdida, copia, alteración o divulgación.

- La falta de espacio o de las facilidades para guardar la documentación e información en los archivadores o cajones, no será considerada como excepción a la presente política, en tal circunstancia el/la servidor/a, funcionario/a y trabajador/a deberá solicitar a la Dirección de Gestión Administrativa las facilidades del caso.

- Cuando se maneje información de carácter confidencial, reservada y sensible el/la servidor/a, funcionario/a y trabajador/a deberá guardarla en una caja fuerte, bóveda, archivador con llave, tanto al finalizar la jornada laboral como en el horario de almuerzo, inclusive en los períodos cortos de tiempo en los que el/la servidor/a, funcionario/a y trabajador/ase ausente de su puesto de trabajo.

- Todos los/las servidores/as, funcionarios/as y trabajadores/as deberán cerrar con llave los cajones de escritorios, archivadores tras haber culminado la jornada laboral, en las horas de almuerzo y en los períodos de tiempo prolongado en los que el empleado se encuentre ausente de la Institución.

- Todos los/las servidor/a, funcionario/a y trabajador/a deberán retirar información sensible una vez que esta haya sido impresa.

Respecto al uso del Computador:

- Será responsabilidad de todos los/las servidores/as, funcionarios/as y trabajadores/as de la Institución:

    - Bloquear el computador asignado (haciendo uso de las teclas ***ctrl*** mas ***alt*** mas ***supr)***cada vez que se aleje de su computador, inclusive si es por periodos cortos de tiempo.
    - Bloquear el computador asignado cada vez que se ausente en horas

de almuerzo.

- Apagar el computador asignado al finalizar la jornada laboral. El personal de la Unidad de TIC debido a sus actividades de soporte podrá mantener prendido su computador.

- Desconectar de los puertos USB respectivos, los dispositivos de Firma Electrónica asignados, cada vez que se los deje desatendidos.

- Cuando la computadora de el/la servidor/a, funcionario/a y trabajador/a se encuentre en estado de inactividad por más de 5 minutos, éste automáticamente se desconectará de la red activando el protector de pantallas con clave; para ello la Unidad de TIC aplicará las configuraciones correspondientes.

- Los/las servidores/as, funcionarios/as y trabajadores/as deberán retirar toda información sensible una vez que esta haya sido impresa.

- La Unidad de TIC implementará un fondo de pantalla común para todos los computadores y portátiles asignados a los/las servidores/as, funcionarios/as y trabajadores/as que se encuentren conectados a red Institucional.

4.2.6 Responsabilidades

Las siguientes responsabilidades se aplican a todos los/las servidores/as, funcionarios/as y trabajadores/as de la Institución:

- Cumplir con la presente Política de Puesto de trabajo despejado y pantalla limpia.

- El/la servidor/a, funcionario/a y trabajador/a al que se le ha hecho custodia de documentación e información sensible, confidencial y reservada es el

único responsable por todas las acciones u omisiones que se realicen sobre la misma.

4.2.7 Sanciones

El incumplimiento de la presente Política, en referencia a las disposiciones indicadas en la misma así como el EGSI, tendrá como resultado la aplicación de las sanciones de acuerdo a la normativa legal vigente.

El incumplimiento de la presente Política puede provocar un incidente de seguridad comprometiendo la Confidencialidad, Integridad o Disponibilidad de la Información, afectar las operaciones, procesos y actividades en la Institución.

Incidente de Seguridad de la información: Es un evento adverso en un sistema de información, red, computador, que pueda comprometer la Confidencialidad, Integridad o Disponibilidad de la información, puede ser causado mediante el aprovechamiento de alguna vulnerabilidad del sistema, un intento de amenaza o violentar los mecanismos de seguridad.

Se consideran como incidentes de seguridad, los siguientes eventos:

- Violentar y vulnerar la seguridad física para acceder a la información no autorizada;
- Violentar los accesos y la información no autorizada;
- Compartir contraseñas de cualquier sistema;
- Acceder a los recursos o sistemas por medios o mecanismos no autorizados;
- Acceder a los recursos, información o sistemas no autorizados;

- Publicar, difundir o divulgar información a nombre de la Institución sin la debida autorización y el procedimiento legalmente establecido para el efecto;
- Otros que comprometan la Confidencialidad, Integridad o Disponibilidad de la Información.

4.2.8 Punto de contacto

Cualquier inquietud en materia de seguridad de la información podrá ser notificado al Oficial de Seguridad de la Información o a la dirección de correo electrónico seguridad@culturaypatrimonio.gob.ec.

4.2.9 Referencias

- Acuerdo N° 166 25 de Septiembre de 2013, Secretaría Nacional de la Administración Pública (SNAP), Anexo 1 - Esquema Gubernamental de Seguridad de la Información v1.0.
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001, ISO/IEC 27002
- Esquema Gubernamental de Seguridad de la Información (EGSI)

4.3. Política de Contraseñas

Tabla 9.Flujo de Aprobación Contraseñas

Acción	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado:		Especialista TI		
Revisado y Aprobado:		Directora de Auditoría Interna		
		Directora de Gestión de		

		Talento Humano		
		Directora de Gestión Administrativa		
		Responsable de TI		

Introducción

Con el fin de mantener la confidencialidad de la información como objetivo principal de la seguridad de la información, se emplean mecanismos de protección mediante la utilización de contraseñas.

Las contraseñas son códigos o claves asignados a los/las servidores/as, funcionarios/as y trabajadores/as que interactúan con los sistemas de información para acceder a información confidencial, pública o institucional que se encuentra almacenada en dichos sistemas, correo electrónico, cuentas bancarias, Quipux o cualquier otra fuente de información.

El principal problema de la seguridad en las contraseñas es el uso de contraseñas inseguras o débiles para proteger el acceso a la información de los sistemas, al utilizar estas contraseñas inseguras existe el riesgo que personas no autorizadas o mal intencionadas traten de “descifrarlas” comprometiendo de esa manera la confidencialidad de información.

Una solución ante ello es la utilización de contraseñas fuertes que brinden un grado o nivel de seguridad adecuado a fin de proteger la información, sin embargo contar con una contraseña fuerte no es suficiente, por ello es necesario definir reglas o normas para que el servidor/a, funcionario/a y trabajador/a de la protección necesaria y haga un buen uso de la misma.

Cabe indicar que los sistemas de información deberán permitir controlar la utilización de contraseñas para acceder a los mismos con lo cual se podrá incrementar la protección de la información.

4.3.1 Objetivo

Definir las pautas para el uso y protección de las contraseñas de los/las servidores/as, funcionarios/as y trabajadores/as y en los sistemas de información en el Ministerio de Cultura y Patrimonio.

4.3.2 Alcance

La presente política se aplica a todos los/las servidores/as, funcionarios/as y trabajadores/a que labora en el Ministerio de Cultura y Patrimonio, así como para los usuarios externos, como consultores, contratistas y proveedores que trabajen con información de la Institución, quienes tienen la obligación de cumplir lo indicado en la presente política.

4.3.3 Definiciones

La Seguridad de la Información se garantiza mediante la preservación de las siguientes características:

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Se garantiza la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y recursos relacionados con la misma, toda vez que lo requieran.

4.3.4 Política

Es política del Ministerio de Cultura y Patrimonio:

Consideraciones Generales de las contraseñas asignadas a los funcionarios:

- Las contraseñas serán consideradas como información confidencial.
- Las contraseñas independientemente del sistema, serán de carácter secreto, personal e intransferible.
- Las contraseñas entregadas serán definidas por el/la servidor/a, funcionario/a y trabajador/a y este será el único responsable de la misma.
- Se prohíbe compartir contraseñas asignadas, cualquiera que sea su tipo, su inobservancia a esta definición será sancionada de acuerdo a lo indicado en la Política de Seguridad de la Información y la normativa legal vigente que se aplique para el efecto.

4.3.5 Sistema de Gestión de Contraseñas

Para el acceso al computador asignado a los/las servidores/as, funcionarios/as y trabajadores/as, y por ende a la red institucional, el sistema de gestión de contraseñas del sistema de autenticación o Directorio Activo, deberá brindar las facilidades para la utilización de contraseñas seguras, controlar el cambio de la misma para todo tipo de usuarios incluyendo al personal de la UTICs así como los administradores, en rangos de tiempo y complejidad.

El sistema de gestión de contraseñas forzará el cambio de contraseñas en el primer acceso o inicio de sesión, para lo cual el/la servidor/a, funcionario/a y trabajador/a deberá establecer su contraseña de acuerdo a los lineamientos indicados en la presente política.

El sistema de gestión de contraseñas implementará el cambio de las mismas cada 3 meses (90 días) para todos los/las servidores/as, funcionarios/as y trabajadores/as sin excepción.

Se implementará el uso de contraseñas avanzadas o seguras con las siguientes características:

Longitud o tamaño mínima de las contraseñas, 8 caracteres alfanuméricos como mínimo.

Utilizar como mínimo 2 de las 3 siguientes características:

- Una mayúscula (A-Z)
- Un número (0-9)
- Un carácter especial (ej. %*+#)

El sistema de gestión de contraseñas deberá notificar con 15 días de anticipación al servidor/a, funcionario/a y trabajador/a los días restantes para la expiración de la contraseña.

El sistema de gestión de contraseñas podrá mantener un histórico de contraseñas de hasta 5 (cinco) contraseñas, para lo cual el/la servidor/a, funcionario/a y trabajador/a no podrá utilizar las últimas contraseñas utilizadas.

4.3.6 Responsabilidades

Las siguientes responsabilidades se aplican a los/las servidores/as, funcionarios/as y trabajadores/a del Ministerio de Cultura y Patrimonio:

- Cumplir con la presente Política de Contraseñas.
- No compartir las contraseñas o claves de acceso a los sistemas: correo electrónico, computador, Quipux, GPR, Zimbra, BPM, Bases de Datos, servidores, etc.
- El/la servidor/a, funcionario/a y trabajador/a al que se le ha asignado una contraseña es el único responsable por todas las acciones u omisiones que se realicen en dichos sistemas con el uso de su contraseña.

- El/la servidor/a, funcionario/a y trabajador/a es responsable de proteger y cuidar su contraseña, a fin de evitar su conocimiento, deducción y robo de la misma.

- Los/las servidores/as, funcionarios/as y trabajadores/as deberán memorizar las contraseñas, no serán anotadas en medios físicos o electrónicos que se encuentre al alcance de cualquier persona. Por ejemplo no se deberá anotar las contraseñas en papeles o en archivos electrónicos de email, notas de teléfonos celulares o en su computador.

- Los/las servidores/as, funcionarios/as y trabajadores/as procurarán estar atentos ante ataques de ingeniería social, los cuales intenten sorprenderlo solicitándole su contraseña por vía telefónica, mail, páginas web, de manera presencial u otro, incluso aunque le hablen en nombre de la Unidad de TICs o de su jefe superior en la Institución; en todo caso nunca compartirán su contraseña con terceros.

- No se entregará la contraseña inclusive cuando el usuario se encuentre en vacaciones, en caso que el/la servidor/a, funcionario/a y trabajador/a se quede a cargo de las funciones, deberá solicitar con anticipación a la unidad respectiva la creación de un nuevo usuario y contraseña respectiva. La solicitud de acceso por reemplazo deberá realizarse por escrito con la aprobación del jefe inmediato y tendrá validez únicamente durante el período de reemplazo.

- Cambiar la contraseña dentro del período de tiempo establecido; en caso que el servidor/a, funcionario/a y trabajador/a haya permitido que su contraseña caduque o expire, su cuenta asignada se bloqueará temporalmente, misma que deberá ser solicitada el reseteo de la contraseña mediante correo electrónico a soporte de la UTICs para el desbloqueo de la cuenta o solicitada vía telefónica.

- Utilizar contraseñas seguras de acuerdo al control establecido en el sistema de gestión de contraseñas. Los/las servidores/as, funcionarios/as y trabajadores/as podrán crear sus contraseñas seguras de acuerdo a lo indicado en el Anexo “Como crear contraseñas seguras”.

4.3.7 Sanciones

El incumplimiento de la presente Política de Contraseñas, en referencia a las disposiciones indicadas en la misma así como el EGSI, tendrá como resultado la aplicación de las sanciones de acuerdo a la normativa legal vigente.

El incumplimiento de la presente Política puede provocar un incidente de seguridad comprometiendo la Confidencialidad, Integridad o Disponibilidad de la Información, afectar las operaciones, procesos y actividades en la Institución.

Incidente de Seguridad de la información: Es un evento adverso en un sistema de información, red, computador, que pueda comprometer la Confidencialidad, Integridad o Disponibilidad de la información, puede ser causado mediante el aprovechamiento de alguna vulnerabilidad del sistema, un intento de amenaza o violentar los mecanismos de seguridad.

Se consideran como incidentes de seguridad, los siguientes eventos:

- Violentar y vulnerar la seguridad física para acceder a la información no autorizada;
- Violentar los accesos y la información no autorizada;
- Compartir contraseñas de cualquier sistema;
- Acceder a los recursos o sistemas por medios o mecanismos no autorizados;
- Acceder a los recursos, información o sistemas no autorizados;

- Publicar, difundir o divulgar información a nombre de la Institución sin la debida autorización y el procedimiento legalmente establecido para el efecto;
- Otros que comprometan la Confidencialidad, Integridad o Disponibilidad de la Información.

4.3.8 Punto de contacto

Cualquier inquietud en materia de seguridad de la información podrá ser notificado al Oficial de Seguridad de la Información o a la dirección de correo electrónico seguridad@culturaypatrimonio.gob.ec.

4.3.9 Creación de contraseñas robustas

Cuando se cree una contraseña segura, es una buena idea seguir las siguientes pautas:

No haga lo siguiente:

- *No utilice solamente palabras o números* — Nunca debería utilizar únicamente letras o sólo números en una contraseña.

  Algunos ejemplos inseguros incluyen:

  - 8675309
  - juan
  - atrápame
- *No utilice palabras reconocibles* — Palabras tales como nombres propios, palabras del diccionario o hasta términos de shows de televisión o novelas deberían ser evitados, aún si estos son terminados con números.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

Algunos ejemplos inseguros incluyen:

- bettylafea1
- enchufetv-9
- antonioValencia21

- *No utilice palabras en idiomas extranjeros* — Los programas de descifrado de contraseñas a menudo verifican contra listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña.(DELGADO, FERRÍN, & GUTIÉRREZ, 2012)

  Algunos ejemplos inseguros incluyen:

  - Giveme5
  - Cheguevara
  - bienvenue1
  - 1dumbKopf

- *No utilice terminología de hackers* — Si piensa que usted pertenece a una élite porque utiliza terminología hacker — también llamado hablar l337 (LEET) — en su contraseña, piense otra vez. Muchas listas de palabras incluyen lenguaje LEET.

  Algunos ejemplos inseguros incluyen:

  - H4X0R
  - 1337

- *No utilice información personal* — Manténgase alejado de la información personal. Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil. La lista siguiente muestra los tipos de información que debería evitar cuando esté creando una contraseña:(Ministerio del Interior-Chile, 2016)

Algunos ejemplos inseguros incluyen:

- Su nombre
- El nombre de sus mascotas
- El nombre de los miembros de su familia
- Fechas de cumpleaños
- Su número telefónico o código postal

- *No invierta palabras reconocibles* — Los buenos verificadores de contraseñas siempre invierten las palabras comunes, por tanto invertir una mala contraseña no la hace para nada más segura.

  Algunos ejemplos inseguros incluyen:

  - R0X4H
  - nauj
  - 21-antonioValencia

- *No escriba su contraseña* — Nunca guarde su contraseña en un papel. Es mucho más seguro memorizarla.
- *No utilice la misma contraseña para todas las máquinas* — Es importante que tenga contraseñas separadas para cada máquina. De esta forma, si un sistema es comprometido, no todas sus máquinas estarán en peligro inmediato.

Haga lo siguiente:

- *Cree contraseñas de al menos ocho caracteres* — Mientras más larga sea la contraseña, mejor.
- *Mezcle letras mayúsculas y minúsculas* —Mezcle las letras para reforzar su contraseña.
- *Mezcle letras y números* — Agregando números a las contraseñas, especialmente cuando se añaden en el medio (no

solamente al comienzo o al final), puede mejorar la fortaleza de su contraseña.

- *Incluya caracteres no alfanuméricos* — Los caracteres especiales tales como &, $, y > pueden mejorar considerablemente su contraseña.
- *Seleccione una contraseña que pueda recordar* — La mejor contraseña en el mundo será de poca utilidad si usted no puede recordarla. Por lo tanto utilice acrónimos u otros dispositivos nemónicos que lo ayuden a memorizar las contraseñas.

Con todas estas reglas, puede parecer difícil crear una contraseña que reúna todos estos requisitos para las buenas contraseñas a la vez que se evitan los rasgos de las malas. Afortunadamente, hay algunos pasos que uno puede tomar para generar una contraseña segura y fácil de recordar.

4.3.10 Metodología para la creación de contraseñas seguras

Hay muchos métodos que la gente utiliza para crear contraseñas seguras. Uno de los métodos más populares incluye acrónimos. Por ejemplo:

- Piense en una frase memorable, tal como:

  "Es más fácil creer que pensar con espíritu crítico."

- Luego, cámbielo a un acrónimo (incluyendo la puntuación).

  emfcqpcec.

- Añada un poco de complejidad sustituyendo números y símbolos por letras en el acrónimo. Por ejemplo, sustituya **7** por **e** y el símbolo arroba (@) por **c**:

  7mf@qp@7@.

- Añada un poco más de complejidad colocando mayúscula al menos una letra, tal como **M**.

  7Mf@qp@7@.

- Por último, no utilice esta contraseña de ejemplo en ninguno de sus sistemas.

Mientras que la creación de contraseñas seguras es imperativa, manejarlas adecuadamente es también importante, especialmente para los administradores de sistemas dentro de grandes organizaciones.

4.3.11 Referencias

- Acuerdo N° 166 25 de Septiembre de 2013, Secretaría Nacional de la Administración Pública (SNAP), Anexo 1 - Esquema Gubernamental de Seguridad de la Información v1.0.
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001, ISO/IEC 27002
- Esquema Gubernamental de Seguridad de la Información (EGSI)
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-pass.html.

4.4. Política de uso de Correo Electrónico

Tabla 10.Flujo de Aprobación uso correo

Acción	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado:		Especialista TIC		
Revisado y Aprobado:		Directora de Auditoría Interna		
		Directora de Gestión de Talento Humano		
		Director de Gestión Administrativa		
		Responsable de TIC		

4.4.1 Introducción

Las políticas de uso para el sistema de correo electrónico institucional del Ministerio de Cultura y Patrimonio, es un instrumento que apegado a los mandatos institucionales, busca alcanzar la gestión y utilización eficaz, eficiente y adecuada del servicio de correo electrónico que dispone cada uno de los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio.

4.4.2 Objetivo

Normar y optimizar la disponibilidad, uso y control del sistema de correo electrónico institucional que se encuentra a disposición de los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio.

4.4.3 Alcance

La presente política se aplica a todos los/las servidores/as, funcionarios/as y trabajadores/as que labora en el Ministerio de Cultura y Patrimonio, así como para los usuarios externos, como consultores, contratistas y proveedores que trabajen con información de la Institución, quienes tienen la obligación de cumplir lo indicado en la presente política.

4.4.4 Definiciones

Correo Electrónico: El correo electrónico (también conocido como e-mail, un término inglés derivado de electronic mail), es un servicio que permite el intercambio de mensajes a través de dispositivos electrónicos conectados por una red de datos (Internet). Los mensajes de correo electrónico permiten el envío de cualquier tipo de documento digital (imágenes, videos, audios, texto, entre otros).

Cuota: Capacidad de almacenamiento asignado a los/las servidores/as, funcionarios/as y trabajadores/as, para el uso del servicio de correo electrónico.

Máxima Autoridad Ejecutiva: El Ministro(a) de Cultura y Patrimonio.

Servidor Público: Serán servidoras o servidores públicos todas las personas que presten servicios o ejerzan un cargo, función o dignidad dentro del sector público. (Definido en la LOSEP – Art. 4).

Usuario Normal: Es todo los/las servidores/as, funcionarios/as y trabajadores/as que pertenece al Ministerio de Cultura y Patrimonio y dispone de una capacidad de almacenamiento estándar, para la recepción de correos electrónicos.

Usuario Directivo: Es toda autoridad de nivel Jerárquico Superior, que pertenece al Ministerio de Cultura y Patrimonio y dispone de mayor capacidad de almacenamiento para la recepción de correos electrónicos

Usuario VIP: Son los dos funcionarios más altos a nivel jerárquico. Ministro/a y Viceministros.

4.4.5 Base legal

El presente tiene como base legal la siguiente disposición:

- Normas de Control Interno de la Contraloría General del Estado para las Entidades, Organismos del Sector Público y de las de las personas jurídicas de derecho privado que dispongan de recursos públicos,N°410-14.
- DecretoEjecutivo1384del13deDiciembrede 2013,Artículo1.
- Esquema Gubernamental de Seguridad de la Información.

4.4.6 Ámbito de aplicación

Aplicación y cumplimiento obligatorio por parte de las y los servidores públicos en todas las unidades organizacionales del Ministerio de Cultura y Patrimonio.

4.4.7 Responsabilidades

La Dirección de Gestión Administrativa del Talento Humano será la encargada de verificar el cumplimiento de las presentes políticas, en todas las unidades organizacionales del Ministerio de Cultura y Patrimonio.

El incumplimiento a lo dispuesto en el presente documento, generará responsabilidad de acuerdo a la LOSEP, Art. 42.- De las faltas disciplinarias, inciso a) y Art. 43.- Sanciones disciplinarias, incisos a) y b). De la misma forma, incidirá sobre la Responsabilidad por la Función Pública.

Coordinación General de Gestión Estratégica.

Gestionar a través de la Unidad de TICs, la coordinación con las Direcciones de Talento Humano y Comunicación Social, para que se socialicen las políticas de uso del correo institucional a todos los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio, recalcando la responsabilidad única del funcionario público, para dar cumplimiento con las políticas expresadas en este documento.

Dirección de Gestión Administrativa del Talento Humano.

Notificar a los/las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio del cumplimiento de las políticas de uso del correo institucional.

Solicitar a la Unidad de Tecnologías de Información y Comunicación la habilitación y deshabilitación de los/las servidores/as, funcionarios/as y trabajadores/as, en el sistema de correo electrónico institucional.

Unidad de Tecnologías de la Información y Comunicación

Realizar la gestión de creación y eliminación de las cuentas de correo institucional, para los /las servidores/as, funcionarios/as y trabajadores/as del Ministerio de Cultura y Patrimonio, previo pedido de la Dirección de Gestión del Talento Humano.

Monitorear el servicio de correo electrónico para mantenerlo en continua operatividad para todas las unidades organizacionales de la institución.

Controlar el uso inadecuado del correo institucional en sitios externos a la institución. El registro del mismo en páginas no autorizadas provocará la auditoria y sanción correspondiente (de ser el caso) de los /las servidores/as, funcionarios/as y trabajadores/as asociado a su cuenta de correo electrónico.

Controlar la recepción de correos masivos conocidos como SPAM.

Controlar el envío y conservación de la información implementando mecanismos de cifrado (criptografía) de datos, de acuerdo a la criticidad y sensibilidad de la información. Utilizar programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos antes de la recepción en los buzones de los usuarios.

Implementar mecanismos para que la información y correos sea gestionada en forma centralizada en los servidores y no en las estaciones de trabajo de los usuarios.

Servidor Público

Es el responsable de cumplir y hacer cumplir las políticas de uso del correo electrónico institucional.

Es responsable por la eliminación de los correos con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no se debe contestar dichos correos ni tampoco acceder a los links o descargar archivos adjuntos, se deberá solicitar al Oficial de Seguridad de la Información para que analice dichos correos en Coordinación con el Responsable de Seguridad de la Unidad de TICs.

Es responsable de la cantidad y tamaño de mensaje que envíe, controlar el envío de correos masivos y cadenas de mensajes.

4.4.8 Aprobación y Difusión de la Política

Es facultad del Sr. (a)Ministro(a) de Cultura y Patrimonio la aprobación y difusión del presente documento, por medio del Comité de Seguridad de la Información.

Revisión y Actualización de la política

EL Comité de Seguridad de la Información revisará y actualizará periódicamente la presente política, sobre la base del análisis de la experiencia de su aplicación y la dinámica administrativa, buscando una mayor eficacia y uso adecuado del servicio.

4.4.9 Política

Conocimiento de usuario

El sistema de correo electrónico proporcionado por el Ministerio de Cultura y Patrimonio, posee una interface gráfica amigable e intuitiva, la cual brinda al servidor/a, funcionario/a y trabajador/a las facilidades para enviar, recibir,

buscar, entre otras; correos y datos adjuntos que se intercambian a nivel institucional por la red del Ministerio de Cultura y Patrimonio.

El correo electrónico institucional es una herramienta de trabajo colaborativa comunicacional dentro de la institución, por lo que el usuario final debe conocer, entender y aceptar en su totalidad los términos y condiciones de uso de este medio, así como también las restricciones que a nivel institucional se dispongan.

Acceso al correo electrónico desde la institución

En el computador de cadaservidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio se instalará la aplicación Thunderbird que gestionará el correo electrónico institucional, funcionará a nivel interno para el envío y recepción de los mensajes, deberá ser usada de forma predeterminada para el acceso a la cuenta de correo electrónico institucional. Thunderbird es una herramienta basada en software libre equivalente a la aplicación Outlook de Microsoft.

Acceso al correo electrónico fuera de la institución

Para acceder al servicio de correo electrónico institucional desde cualquier lugar externo a las instalaciones del Ministerio de Cultura y Patrimonio, el servidor/a, funcionario/a y trabajador/a podrá ingresar a través de internet digitando en el navegador web la dirección https://mail.culturaypatrimonio.gob.ec; una vez desplegada la página de registro de usuario, el servidor/a, funcionario/a y trabajador/a deberá ingresar su usuario y contraseña asignada por la Unidad de Tics.

Acceso al correo electrónico mediante dispositivos móviles

El servidor/a, funcionario/a y trabajador/a que disponga de dispositivos móviles (tablet, smartphone, PDA, otros.) podrá configurar su cuenta de correo electrónico institucional, para enviar y recibir correos de la institución, en su

dispositivo móvil. Los pasos a seguir para la configuración del correo institucional se encuentra en el documento, “Manual de configuración de correo electrónico institucional en dispositivos móviles “. Si es necesario, el servidor/a, funcionario/a y trabajador/a podrá recibir asesoría de la Unidad de Tecnologías de la Información y Comunicación, para lo cual solicitará mediante correo a soporte@culturaypatrimonio.gob.ec.

4.4.10 Esquema Gubernamental de Seguridad de la Información

Todos los mensajes de correo serán monitoreados y conservados permanentemente por parte de la institución.

Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario. La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.

El servicio de correo electrónico deberá contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.

Alcances y limitaciones del servicio

El Ministerio de Cultura y Patrimonio proporciona el servicio de correo electrónico únicamente bajo los términos mencionados a continuación:

El correo electrónico es para uso netamente laboral y no puede ser usado en actividades que no tiene relación laboral directa con el Ministerio de Cultura y Patrimonio. Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que realiza esta Cartera de Estado.

Todo usuario es responsable del contenido del mensaje enviado así como de todo documento adjunto.

El/la servidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio dispondrá de un espacio (Cuota) temporal de almacenamiento para sus correos y archivos recibidos.

El usuario entiende y acepta que es de su total responsabilidad guardar copias personales de los datos transmitidos a través del servicio de correo electrónico y que el Ministerio de Cultura y Patrimonio, no es responsable por la pérdida o la falta de disponibilidad de los mensajes recibidos anteriormente, así como tampoco se responsabilizará por daños o perjuicios causados a usuarios o terceros por la pérdida o la falta de disponibilidad de los datos.

Cuando un mensaje que contenga datos personales es enviado a través del servicio de correo electrónico, aquella persona de quien proceda el mensaje será la única responsable del tratamiento de los datos contenidos en el correo enviado. El Ministerio de Cultura y Patrimonio no se responsabiliza por el tratamiento que se dé a los datos enviados.

Los mecanismos para verificar la autenticidad e integridad de los datos enviados a través del correo electrónico son establecidos de común acuerdo por las partes (emisor, receptor) y, en caso de no haberse establecido ningún mecanismo, se tomará por auténtico el mensaje tal cual lo recibió el destinatario. El Ministerio de Cultura y Patrimonio no se responsabiliza por daños o perjuicios causados por la alteración maliciosa de los datos.

El Ministerio de Cultura y Patrimonio no se responsabilizará por daños o perjuicios causados a usuarios o terceros por la no recepción de mensajes como consecuencia de exceder la cuota de almacenamiento establecida para cada servidor/a, funcionario/a y trabajador/a.

Capacidad de Almacenamiento

Las cuotas de almacenamiento para los servidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio que fueron analizadas y autorizadas por la autoridad competente, están distribuidas de la siguiente manera:

- 500 MB para usuarios Normales
- 3000 MB para usuarios Directivos
- 5000 MB para usuarios VIP.

El Ministerio de Cultura y Patrimonio tiene completa autonomía para modificar esta cuota de almacenamiento en cualquier momento y cuantas veces sea necesario para ajustarse a las necesidades del personal del Ministerio de Cultura y Patrimonio y los recursos computacionales que se disponen para brindar el servicio de almacenamiento de correo.

Si el usuario sobrepasa la cuota de almacenamiento asignada, no podrá enviar y recibir correos electrónicos. Para solventar este inconveniente, el aplicativo THUNDERBIRD permite migrar los correos de su cuenta (servidor de correo) a una carpeta local (computador personal); liberando el espacio de cuota proporcionada y archivando sin perder su información.

Nombres de cuentas de correo

Características

El nombre de la cuenta de correo electrónico debe cumplir las siguientes características:

- Máximo 15 caracteres
- Puede contener los caracteres, de la (a) a la (z)
- No puede contener caracteres especiales (Letra ñ)
-

4.4.11 Estándar para creación de cuentas

El estándar para la creación del nombre de la cuenta de correo institucional, para todo servidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio es:

- Inicial del primer nombre + primer apellido + @ + culturaypatrimonio.gob.ec
- (ej. Funcionario: Pedro Javier Estévez Brito, Cuenta de correo electrónico:
- pestevez@culturaypatrimonio.gob.ec)

En el caso de existir nombres de funcionarios homónimos, el estándar para la creación del nombre de la cuenta de correo será:

- Inicial del primer nombre + inicial del segundo nombre + primer apellido + @ + culturaypatrimonio.gob.ec (ej. Funcionario: Pedro Javier Estévez Brito, Cuenta de correo electrónico: pjestevez@culturaypatrimonio.gob.ec)

4.4.12 Creación de cuentas temporales

La creación de cuentas temporales destinadas a cumplir el propósito de enviar información a un grupo de destinatarios, sobre un determinado evento deben cumplir los siguientes requisitos:

Enviar un correo a soporte@culturaypatrimonio.gob.ec con la siguiente información:

- Nombre Completo del servidor/a, funcionario/a y trabajador/a responsable de la creación de la cuenta (Apellidos y Nombres)
- Nombre de la cuenta a crear; que no exceda el número de caracteres permitidos.

- Siglas de la Dirección a la que pertenece
- Tiempo de vigencia de la cuenta

Listas de distribución por unidad

La lista de distribución es una cuenta que agrupa a los/las servidores/as, funcionarios/as y trabajadores/as de una misma unidad/área. El objeto de la lista de distribución es enviar información (correos), a todo el grupo de trabajo dentro de la misma unidad/área. La lista de distribución será identificada por las Siglas de la unidad. (ej. UTIC@culturaypatrimonio.gob.ec)

Pie de firma

El pie de firma para el correo electrónico institucional, se encuentra estandarizado a través de la página web http://firmacorreo.culturaypatrimonio.gob.ec/, por medio de la cual, se personalizará los datos del servidor/a, funcionario/a y trabajador/a ingresando los siguientes campos:

- Nombre y Apellido
- Cargo
- Dirección o Unidad a la que pertenece
- Secretaría o Coordinación a la que pertenece
- Extensión telefónica.

Creación y Eliminación de cuentas de correo

Creación

Las cuentas de correo electrónico son creadas conforme va ingresando nuevo personal al Ministerio de Cultura y Patrimonio, bajo las normas establecidas en el presente documento.

Todo servidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio dispondrá de una sola cuenta de correo electrónico institucional.

La Unidad de Tecnologías de Información y Comunicación será la responsable de entregar a el/la nuevo/a servidor/a, funcionario/a y trabajador/a, el usuario y contraseña de acceso para el uso del sistema de correo electrónico. La Unidad de Tecnologías de Información y Comunicación brindará el soporte necesario para la configuración del correo electrónico en dispositivos móviles.

La contraseña entregada será inicialmente el número de cédula de/la servidor/a, funcionario/a y trabajador/a, misma que deberá ser cambiada en el primer ingreso al sistema de correo.

Eliminación

Cuando un servidor/a, funcionario/a y trabajador/a, presente su renuncia o deje de formar parte del Ministerio de Cultura y Patrimonio, la Unidad de Tecnologías de Información y Comunicación, procederá a la baja o desactivación de la cuenta de correo electrónico tras la solicitud de la Dirección de Gestión de Talento Humano, quien enviará una copia al Oficial de Seguridad de la Información.

Al detectar inactividad de una cuenta de correo electrónico por el período de 30 días, la Unidad de Tecnologías de Información y Comunicación enviará un informe a la Dirección de Gestión del Talento Humano, recomendando la eliminación permanente de dicha cuenta.

4.4.13 Seguridad

El Ministerio de Cultura y Patrimonio dispone de un sistema Anti Spam, el cual previene y filtra los correos basura que tienen como destinatarios a usuarios de la institución.

Los correos basura no podrán ser recibidos por el destinatario, sin embargo, el/la servidor/a, funcionario/a y trabajador/a será notificado vía correo electrónico que dispone de un correo retenido por el sistema Anti Spam. Para

recibir el correo retenido deberá notificar a la Unidad de Tecnologías de la Información y Comunicación mediante la cuenta de soporte@culturaypatrimonio.gob.ec, la confiable y segura procedencia del remitente del correo en cuestión.

Existen correos que por ningún motivo podrán ser recibidos, como correos de anuncios, propagandas, publicidad, promociones, entre otros.

Al detectar inactividad de una cuenta de correo electrónico por el período de 30 días, la Unidad de Tecnologías de Información y Comunicación enviará un informe a la Dirección de Talento Humano, recomendando la eliminación permanente de dicha cuenta.

Acerca del uso

El correo electrónico institucional deberá ser utilizado solo para actividades inherentes al

Ministerio de Cultura y Patrimonio.

Restricciones

El/la servidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio no podrá utilizar su cuenta de correo electrónico para los siguientes fines:

- Anunciar o enviar por correo electrónico contenido ilegal, peligroso, vulgar, obsceno, es decir, contenido impropio de las actividades normales de trabajo.

- Hacerse pasar por alguna persona, entidad o cargo del Ministerio de Cultura y Patrimonio.

- Anunciar o enviar por correo electrónico algún contenido que no tiene derecho a transmitir por ley o por relación contractual o fiduciaria (tal como información interna, de propiedad y confidencial adquirida o entregada como parte de las relaciones de empleo o bajo Reglamentos de confidencialidad).

- Anunciar o reenviar correos de anuncios o materiales promocionales, cartas en cadena, esquemas de pirámides, entre otros.

- Anunciar o reenviar correos electrónicos que contengan virus de software, o cualquier otro código de computadora que destruya o limite el funcionamiento de los servicios brindados por la red del Ministerio de Cultura y Patrimonio.

- Acechar u hostigar a otro usuario de la institución.

- Usar el servicio con fines fraudulentos o inapropiados.

La infracción de cualquiera de los aspectos anteriormente mencionados podría causar la suspensión del servicio y sanciones institucionales, así como otro tipo de consecuencias legales.

El Ministerio de Cultura y Patrimonio se reserva el derecho, de investigar el uso del servicio para determinar, si se ha infringido las políticas del presente documento.

4.4.14 Contenido del servicio

El Ministerio de Cultura y Patrimonio se reserva el derecho, para suprimir o rechazar la distribución de correos electrónicos que tengan contenidos que infrinjan las condiciones detalladas en la presente política.

El Ministerio de Cultura y Patrimonio también se reserva el derecho de acceder, leer, preservar y mostrar cualquier tipo de información que razonablemente se considere necesaria para:

- Cumplir con leyes, regulaciones, procesos legales o solicitudes gubernamentales.

- Aplicar o ejecutar las políticas de uso de correo electrónico, incluyendo investigación de posibles infracciones.

- Detectar, prevenir, o abordar de situaciones de fraude, seguridad, o temas técnicos.

- Responder a solicitudes de soporte de los usuarios.

- Proteger los derechos, propiedad y seguridad de la institución.

Todas estas acciones se realizarán previa autorización legal de la autoridad judicial o extrajudicial, de tal forma, que no contraponga los principios concebidos en la Constitución de la República del Ecuador.

4.4.15 Derechos de propiedad intelectual del usuario

El Ministerio de Cultura y Patrimonio no reclama la titularidad de ninguno de los contenidos, incluyendo textos, datos, información, imágenes, fotografías, música, sonido, vídeo u otro tipo de material, que el usuario cargue, transmita o archive en su cuenta de correo electrónico.

El Ministerio de Cultura y Patrimonio no utilizará ninguno de sus contenidos para otro propósito que no sea el de proporcionar el servicio.

Indemnización

El usuario acepta indemnizar al Ministerio de Cultura y Patrimonio, frente a reclamos de terceros relacionados con el uso del servicio de correo institucional; incluyendo la responsabilidad o gasto ocasionado por pérdidas, daños, litigios, resoluciones, costos procesales y honorarios de abogados.

De ser el caso, el Ministerio de Cultura y Patrimonio le hará llegar al funcionario, la notificación escrita de dicho reclamo, litigio o acción.

4.4.16 Normas de seguridad

El/la servidor/a, funcionario/a y trabajador/a del Ministerio de Cultura y Patrimonio deberá cumplir con las siguientes normas de seguridad:

- Mantener la confidencialidad de su contraseña de acceso al sistema de correo institucional, ya que es de uso personal e intransferible.

- Notificar de forma inmediata a la Unidad del Tecnologías de Información y Comunicación, de cualquier uso no autorizado de su cuenta de correo electrónico o de cualquier otra falla de seguridad.

- Asegurarse de que su cuenta sea cerrada al final de cada sesión.

- Cambiar periódicamente su contraseña de acceso al sistema de correo electrónico.

El Ministerio de Cultura y Patrimonio no será responsable por pérdida o daño que resulte como consecuencia del incumplimiento a las disposiciones antes mencionadas.

El Ministerio de Cultura y Patrimonio no podrá entregar o dar a conocer la contraseña de ninguna cuenta de correo bajo ninguna circunstancia.

Modificaciones a las políticas

El Comité de Seguridad de la Información está en pleno derecho de hacer las modificaciones que crea necesarias a este documento y los procedimientos a los cuales hace referencia, con la obligación de hacer públicos los cambios.

El uso continuo del servicio de correo electrónico supone la aceptación de todos los términos, condiciones y políticas expuestos en el presente documento. Así mismo, el desconocimiento de las normas no exime a los usuarios de las sanciones a que hubiere lugar en caso de incumplimiento de las mismas.

Es responsabilidad del usuario revisar regularmente los términos y condiciones de uso expuestos en este documento.

Exclusión de responsabilidades

El usuario de correo electrónico, acepta específicamente que el Ministerio de Cultura y Patrimonio no será responsable por el acceso y/o la alteración no autorizada de las transmisiones o datos proporcionados por el servicio de correo electrónico, cualquier material o dato enviado/recibido, o no enviado/recibido, ni por cualquier transacción en la que haya participado a través del servicio de correo electrónico.

El usuario de correo electrónico, acepta específicamente que el Ministerio de Cultura y Patrimonio no es responsable de ningún contenido de conducta amenazadora, difamatoria, obscena, ofensiva o ilícita, ni de cualquier infracción de los derechos de terceros, incluidos los derechos de propiedad intelectual e industrial.

La Unidad de Tecnologías de la Información y Comunicación del Ministerio de Cultura y Patrimonio, de ser posible, advertirá con anterioridad las interrupciones en la prestación del servicio de correo electrónico.

4.4.17 Sanciones

El incumplimiento de la presente política, en referencia a las disposiciones indicadas en la misma así como el Esquema Gubernamental de Seguridad de la Información, tendrá como resultado la aplicación de las sanciones de acuerdo a la normativa legal vigente.

El incumplimiento de la presente Política puede provocar un incidente de seguridad comprometiendo la Confidencialidad, Integridad o Disponibilidad de la Información, afectar las operaciones, procesos y actividades en la Institución.

Incidente de Seguridad de la información: Es un evento adverso en un sistema de información, red, computador, que pueda comprometer la Confidencialidad, Integridad o Disponibilidad de la información, puede ser causado mediante el aprovechamiento de alguna vulnerabilidad del sistema, un intento de amenaza o violentar los mecanismos de seguridad.

Se consideran como incidentes de seguridad, los siguientes eventos:

- Violentar y vulnerar la seguridad física para acceder a la información no autorizada;
- Violentar los accesos y la información no autorizada;
- Compartir contraseñas de cualquier sistema;
- Acceder a los recursos o sistemas por medios o mecanismos no autorizados;
- Acceder a los recursos, información o sistemas no autorizados;
- Publicar, difundir o divulgar información a nombre de la Institución sin la debida autorización y el procedimiento legalmente establecido para el efecto;
- Otros que comprometan la Confidencialidad, Integridad o Disponibilidad de la Información.

Punto de contacto

Cualquier inquietud en materia de seguridad de la información podrá ser notificado al Oficial de Seguridad de la Información o a la dirección de correo electrónico seguridad@culturaypatrimonio.gob.ec.

4.4.18 Referencias

- Acuerdo N° 166 25 de Septiembre de 2013, Secretaría Nacional de la Administración Pública (SNAP), Anexo 1 - Esquema Gubernamental de Seguridad de la Información v1.0.
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001, ISO/IEC 27002
- Esquema Gubernamental de Seguridad de la Información (EGSI)

CONCLUSIONES

- Al integrar las diferentes normas relacionadas a la Tecnología de la Información y Comunicación se logra realizar y cumplir los objetivos de estudio que ayudan a mejorar la calidad del servicio para el usuario, esto se alinea a las buenas prácticas, ITIL y la Norma de Control Interno.

- Al realizar el análisis entre la Norma de Control Interno, bajo la implementación del EGSI en comparación con la norma ISO y la verificación de ITIL se puede determinar lo necesario para implementar las políticas con el estudio de hitos y que estas buenas prácticas son semejantes entre sí.

- Existen varias normas que nos ayudan al mejoramiento de nuestro servicios, cada una de ellas representa un pilar fundamental en la organización y buenas prácticas en los trabajos. Se debería realizar un estudio en cada empresa o institución pública y su correspondiente capacitación para realizar una implementación adecuada y óptima de Políticas del buen del internet y sus derivados.

- Así como el Oficial de Seguridad de las Entidades Públicas, es el encargado de verificar el cumplimiento de las políticas aplicables, a las buenas prácticas tecnológicas para los servicios de internet y otros, y de velar por la seguridad de la información y comunicación, de igual forma se concluye que toda institución de orden público o privado debe contar con una persona que maneje de una manera responsable los servicios tecnológicos, que dé cumplimiento y reglamente todos los servicios institucionales.

- Como se pudo verificar en las normas de ITIL, la mesa de ayuda es un pilar fundamental en las organizaciones, son el eje motor para el soporte de primer nivel a los usuarios y todas las incidencias son registradas

primeramente con los propios usuarios, así también bajo SLA se escala los problemas en servicios a las diferentes áreas, en este contexto se puede concluir que la mesa de ayuda debe ser capacitada y aplicada con las normativas como por ejemplo ITIL y ser informada de todos los servicios o implementaciones que se realicen dentro de las organizaciones, con ello se consigue una mejora en los tiempos de reacción a los problemas y buenas prácticas de internet, la implementación de políticas en las organizaciones son dirigidas por la mesa de ayuda.

- Con el estudio y la aplicación de las Políticas de Internet, correo, contraseñas y escritorio limpio, se puede determinar que el nivel de madurez alcanzado que tiene el Ministerio de Cultura y Patrimonio en cuanto a las aplicación de las buenas prácticas tecnológicas es óptimo, puesto que se ha observado las norma de control interno y el EGSI, para determinar los problemas actuales que deben ser atacados para la efectiva implementación de dichas políticas, una vez realizada la implementación se lograra tener un servicio más eficiente y unas buenas prácticas de los mismos.

- Si se requiere una organización más eficiente, se debe tomar en cuenta los distintos marcos de referencia y buenas prácticas, pero no solo depende de ello, debe existir un compromiso de toda la organización comenzando con el ejemplo de los niveles de Jerárquico Superior ,quienes son las autoridades que toman decisiones para la gestión desarrollada dentro del Ministerio de Cultura y Patrimonio o cualquier entidad en el país. Se deben tener claros los objetivos, la misión y visión de la organización, manejar un liderazgo óptimo, contar con funcionarios comprometidos a los cambios institucionales y sus políticas, y tecnología apropiada que contemple y vaya enfocada a los principios deconfidencialidad, integridad, disponibilidad de los servicios.

RECOMENDACIONES

- Se recomienda crear un Comité de Seguridad el cual se encargue de la verificación e implementación de todas las normativas y políticas de las organizaciones, este comité será el responsable de las buenas prácticas y la disponibilidad de los servicios.

- Con el presente trabajo de investigación se recomienda que se procure fomentar la capacitación continua en las herramientas que contempla la mesa de ayuda, para de esta manera garantizar que el personal conozca sobre la normativa, objetivos, misión, visión de la organización, evitando que esta sea violentada por usuarios con diferentes compromisos de trabajo, y por ende lograr alcanzar los resultados y beneficios para la Institución en el área tecnológica y de la comunicaciones.

- Se recomienda también se ponga énfasis en la capacitación y actualización del personal del área de Tecnologías de la Información y Comunicación TICs, tanto de las herramientas informáticas que ayuda a mejorar el servicio de internet como de las mencionadas políticas, puesto que dicho personal es el pionero en el cambio, en la optimización de recursos e implementación de las políticas que se han efectuado para lograr las buenas prácticas tecnológicas en el Ministerio de Cultura y Patrimonio. Ellos serán los encargados a su vez de impartir y direccionar al usuario en general, siendo su perfil recomendado el estar comprometidos con la misión institucional siendo proactivos y eficientes en la búsqueda de mejores normas, practicas, políticas y recursos que ayudan a mejorar la calidad del servicio institucional.

REFERENCIAS

Asociación Española de Normalización. (2013). *Asociación Española de Normalización.*

ARIZA, S. (2012). PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN DE UNA MESA DE SERVICIOS. *PROYECTO DE GRADO*. BOGOTÁ, CUNDINAMARCA, COLOMBIA: NA.

Auditoría-MCYP. (2011). *Normas de Control Interno.* Quito.

ÁVILA, K. (2016). *CAVSI*. Recuperado el enero de 2016, de http://www.cavsi.com

BLOG, E. (21 de Noviembre de 2010). *ELIANA BLOG*. Recuperado el 01 de Junio de 2013, de http://eliana-ha.blogspot.com/2010/11/gestion-del-problema-itil.html

CÁRDENAS, X. (2012). *libor 1.* Quito: kjdhdg.

Cloud-ITIL. (8 de Junio de 2013). *Cloud-itil*. Obtenido de http://www.cloud-itil.com/acerca-de/

COBIT. (2007). COBIT 4.1. EEUU.

CONTRALORÍA GENERAL DEL ESTADO. (16 de NOV de 2009). *CONTRALORÍA GENERAL DEL ESTADO*. Recuperado el 10 de 12 de 2016, de http://www.contraloria.gob.ec/normatividad_vigente.asp

CONTRALORÍA GENERAL DEL ESTADO. (01 de 12 de 2009). *CONTRALORÍA GENERAL DEL ESTADO*. Recuperado el 12 de 02 de 2013, de http://www.contraloria.gob.ec/

CONTRALORÍA GENERAL DEL ESTADO. (02 de Mayo de 2013). *CONTRALORÍA GENERAL DEL ESTADO*. Obtenido de www.contraloria.gob.ec

CSI. (2013). *CSI*. Recuperado el febrero de 2016, de http://www.csimx.net/

DELGADO, E., FERRÍN, G. M., & GUTIÉRREZ, M. (8 de Agosto de 2012). *Universidad Técnica de Manabí*. Recuperado el enero de 2016, de Manual del uso del Internet y Herramientas Tecnológicas: http://www.utm.edu.ec/seguimosavanzando/wp-content/uploads/carrusel/manuales/fcae/uso.int.her.tec.pdf

DIAGO, D. M. (agosto de 2010). *Scribd*. Recuperado el enero de 2016, de https://es.scribd.com/doc/36868375/Ventajas-y-Desventajas-Del-Correo-Electronico#scribd%29

EXACTA-COBIT. (12 de 03 de 2013). *EXACTA*. Recuperado el 23 de Mayo de 2013, de http://www.isaca.org/COBIT

EXACTA-COBIT. (2013). *EXACTA-APMGROUP.* Quito: AMPGROUP.

GESTIOPOLIS. (01 de 07 de 2008). *METODOS Y TÉCNICAS DE INVESTIGACIÓN*. Recuperado el 28 de 02 de 2013, de METODOS Y TÉCNICAS DE INVESTIGACIÓN: http://www.gestiopolis.com/economia/metodos-y-tecnicas-de-investigacion.htm

GLOBEDIA. (28 de Junio de 2011). *Métricas Proceso de Gestión de Cambios*. Recuperado el 16 de Junio de 2013, de http://ec.globedia.com/metricas-proceso-gestion-cambios

Gobierno Electrónico. (2016). *Gobierno Electrónico*. Recuperado el 2016, de https://www.gobiernoelectronico.gob.ec/

Grupo Context - BMC. (2012). ITIL v3 Service Desing. Quito, Ecuador.

Grupo Context - BMC. (2012). ITIL v3 Service Operation. Quito, Ecuador.

Grupo Context - BMC. (2012). Itil v3 Service Transition. Quito.

GRUPO CONTEXT - BMC. (19 de Julio de 2013). Service Operation . Quito, Ecuador.

GUAPAS, M. A. (2008). *Manual del Estudiante ITIL Foundations.* Quito: New Horizons.

GUAPAS, M. A. (2008). *Manual del Estudiante ITIL Foundations v3.* Quito: New Horizons.

ISACA. (2012). Cobit 5 Enabling Process Spanish. Madrid.

ISACA. (2012). *COBIT 5 Enabling Process Spanish.*Madrid: ISACA.

ISACA. (2012). COBIT 5 Process Assessment Model. USA.

ISACA. (30 de Julio de 2013). *COBIT 5.* Obtenido de www.isaca.org

ISACA INFOSEC. (13 de Marzo de 2012). *ISACA AND INFOSEC.* Recuperado el 01 de 03 de 2013, de http://www.google.com.ec/url?sa=t&rct=j&q=beneficios%20de%20utilizar%20cobit5&source=web&cd=1&cad=rja&ved=0CC8QFjAA&url=http%3A%2F%2Fwww.isaca.org%2FKnowledge-Center%2Fcobit%2FDocuments%2FCOBIT5-and-InfoSec-Spanish.ppt&ei=xJIyUcmHM4220QHi-oHYDw&v6u=http%3

ISACA Self-Assesment Guide. (s.f.). *Self-Assesment Guide*. Recuperado el 30 de Septiembre de 2013, de www.isaca.org/cobit

ISACA-COBIT. (2013). *Isaca*. Recuperado el 23 de Mayo de 2013, de http://www.isaca.org/COBIT

ISO-EGSI. (2015). *FORMAX*. Recuperado el marzo de 2016, de www.formax.edu.ec

ITIL. (2009). *INFORMATION TECHNOLOGY INFRAESTRUCTURE LIBRARY*. Recuperado el 02 de 03 de 2013, de http://www.grupojanus.com/GJ1514/index.php?option=com_content&view=article&id=56&Itemid=57

ITIL V3, OSIATIS. (03 de Mayo de 2013). *ITIL V3*. Obtenido de www.itilv3.osiatis.es

ITIL-Glosario. (2011). Glosario y Abreviaturas de ITIL español. México.

ITNews. (2011). *IT News*. Recuperado el 14 de 02 de 2013, de IT News: http://www.itnews.ec

ITpreneurs. (2012). *Curso ITIL Foundation Version 3.2.1.*

ITPRENEURS. (2012). *Curso ITIL Foundation Version 3.2.1.* ITPRENEURS.

ITpreneurs Nederland B.V. (2011). *Curso ITIL Foundation.* EEUU.

itSMF. (2011). *Gestión del Conocimiento*. Recuperado el 7 de Junio de 2013, de http://gestionconocimientoti.blogspot.com/2011_04_01_archive.html

Lexis. (s.f.). Recuperado el Abril de 2016, de http://www.lexis.com.ec/

Lexis S.A. (s.f.). Obtenido de http://www.lexis.com.ec/

MAGAZCITUM. (12 de 2010). *MAGAZCITUM*. Recuperado el 11 de 02 de 2013, de MAGAZCITUM: www.magazcitum.com.mx

MENDOZA, J. (27 de 4 de 2010). *slideshare.net*. Recuperado el 12 de 2 de 2013, de slideshare.net: http://www.slideshare.net

Ministerio del Interior- Chile. (2016). *Ministerio del Interior y Seguridad Publica*. Recuperado el 2016, de http://www.intendenciaatacama.gov.cl/

MOLINA, M. (2006). *Introducción a la Gestión de Servicios de TI.* Madrid: New Horizons.

New Horizon. (2010). *Manual de estudiante ITIL FOUNDATIONS V3 Formación Oficial de Fundamentos de ITIL.* Quito.

NORMA ISO. (2011). *ISO/IEC.*

Normalización, I. E. (2011).

OCG. (2011). Gestión de Servicios de IT Introducción a ITIL. En OCG. OCG.

OCG. (s.f.). Service Operation Book. Gran Bretaña.

OGC - Gestión de Servicios TI. (2007). The Official Introduction to the ITIL Service Lifecycle. Reino Unido.

OGC. (2009). ITIL v3 Service Desing Book. Gran Bretaña.

OGC. (2009). ITIL V3 Service Transition Book. Gran Bretaña.

OGC. (2009). Service Operation Book. Gran Bretaña.

OGC. (2012). ITIL Operational Support and Analysis.

OSIATIS. (21 de 07 de 2013). *ITIL v3*. Obtenido de http://itilv3.osiatis.es/transicion_servicios_TI/gestion_configuracion_activos_servicio/proceso.php

OSIATIS. (15 de Julio de 2013). *ITIL v3*. Obtenido de http://itilv3.osiatis.es/diseno_servicios_TI/gestion_catalogo_servicios/control_proceso.php

OSIATIS. (03 de Mayo de 2013). *ITIL V3*. Obtenido de www.itilv3.osiatis.es

OSIATIS. (15 de Abril de 2013). *itilv3.osiatis.es*. Obtenido de http://itilv3.osiatis.es/operacion_servicios_TI/funciones.php

OSIATIS ITIL v3. (2011). *OSIATIS*. Recuperado el 11 de 02 de 2013, de http://itilv3.osiatis.es/itil.php

OverTI. (2011). *OVERTI*. Recuperado el 11 de Mayo de 2013, de http://www.overti.es/procesos-itsm/gestion-catalogo-servicios-itsm.aspx

RAMÍREZ, V. (06 de 2011). *monografias.com*. Recuperado el DIC de 2016, de http://www.monografias.com/trabajos81/que-es-internet/que-es-internet2.shtml

RAÚLl, E. (2009 de 06 de 2009). *Técnicas de Investigación*. Recuperado el 07 de 02 de 2013, de Técnicas de Investigación: http://niveldostic.blogspot.com/2009/06/metodo-analitico-sintetico.html

SNAP. (2013). *SNAP*. Recuperado el 2016

UNFV. (2009). *ITIL*. Recuperado el 16 de Junio de 2013, de http://itilunfv.net16.net/Areas%20cubiertas.php

UNIVERSIDAD ECOTEC. (s.f.). *UNIVERSIDAD ECOTEC.* Recuperado el 28 de 02 de 2013, de http://www.ecotec.edu.ec/documentacion%5Cinvestigaciones%5Cdocentes_y_directivos%5Carticulos/5066_Fcevallos_00024.pdf

UTE. (2013). *PLAN DE TESIS.* Recuperado el 07 de 02 de 2013, de REPOSITORIO: http://repositorio.ute.edu.ec/bitstream/123456789/5588/3/18350_3.pdf

WIKIPEDIA. (13 de 07 de 2013). *WIKIPEDIA - Gestión Catálogo de Servicios*. Obtenido de http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_del_Catalogo_de_Servicios#Cat.C3.A1logo_de_Servicios