UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"ANÁLISIS Y PLANTEAMIENTO DE POLÍTICAS DE ACUERDO AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA EMPRESA PÚBLICA YACHAY"

AUTOR: ALEJANDRA MABEL PINTO ERAZO

DIRECTOR: MSC. FABIÁN GEOVANNY CUZME RODRÍGUEZ

IBARRA - ECUADOR

2016

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos de formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
Cédula de identidad:	040129976-3
Apellidos y Nombres:	Alejandra Mabel Pinto Erazo
Dirección:	Ibarra, Ciudadela del Chofer. Calle Honduras 3-49
Email:	almapinto92@gmail.com
Teléfono fijo:	06 2602210
Teléfono móvil:	0996392999
DATOS DE LA OBRA	
Título:	Análisis y planteamiento de Políticas de acuerdo al Esquema Gubernamental de Seguridad de la Información (EGSI) para la Empresa Pública Yachay
Autor/a:	Alejandra Mabel Pinto Erazo
Fecha:	20 de diciembre de 2016
Programa:	Pregrado
Título por el que opta:	Ingeniera en Electrónica y Redes de Comunicación
Director:	Msc. Fabián Geovanny Cuzme Rodríguez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Alejandra Mabel Pinto Erazo, con cédula de identidad Nro. 040129976-3, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior Artículo 144.

3.- CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, a los 20 días del mes de diciembre del 2016

EL AUTOR:

……

Alejandra Mabel Pinto Erazo

Cédula: 040129976-3

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Alejandra Mabel Pinto Erazo**, con cédula de identidad Nro. 040129976-3, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, artículo 4, 5 y 6, en calidad de autor del trabajo de grado denominado: **"ANÁLISIS Y PLANTEAMIENTO DE POLÍTICAS DE ACUERDO AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA EMPRESA PÚBLICA YACHAY"**, que ha sido desarrollado para optar por el título de **Ingeniera en Electrónica y Redes de Comunicación**, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, 20 de diciembre del 2016

……..

Alejandra Mabel Pinto Erazo

Cédula: 040129976-3

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DE DIRECTOR

Certifico que el presente trabajo de Titulación **"ANÁLISIS Y PLANTEAMIENTO DE POLÍTICAS DE ACUERDO AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA EMPRESA PÚBLICA YACHAY",** ha sido realizado con interés profesional y responsabilidad por la señorita: **Alejandra Mabel Pinto Erazo**, portadora de la cédula de identidad N° 040129976-3; previo a la obtención del Título de **Ingeniera en Electrónica y Redes de Comunicación**, bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

Msc. Fabián Cuzme Rodríguez

Cédula: 131152701-2

DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Dedicatoria

Con todo mi amor a quienes que me han apoyado en el camino para lograr esta meta y han dejado una huella importante.

A **DIOS** que me ha dado la vida y me permite llegar a este punto con salud, amor, perseverancia y paciencia; pero lo más importante, me ha dado una familia hermosa que ha estado siempre a mi lado apoyándome.

A mis padres **GUADALUPE** y **WILSON** por ser el pilar fundamental en mi vida y formar a una persona de bien. Por apoyarme incondicionalmente en mi educación, académica y de la vida.

A mi hermana **CAROLINA** que siempre está pendiente de mí y le pone la chispa de alegría a mi diario vivir.

A una persona importante en mi vida, **CARLOS;** por su comprensión y cariño en todo momento, por darme fortaleza para culminar esta etapa de la vida con éxito.

Alejandra Mabel

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Agradecimiento

A mi familia, mi padre **Wilson**, mi madre **Guadalupe**, mi hermana **Carolina**, por brindarme su apoyo incondicional. Por los valores y principios siempre inculcados.

Al personal docente de la Carrera por impartir sus conocimientos con responsabilidad y dedicación, y en especial al Ing. Fabián Cuzme, director de este proyecto de titulación, por su buena predisposición y paciencia, por haberme guiado con su experiencia profesional demostrando sobre cualquier cosa su calidad humana.

A la Gerencia de Tecnologías de la Empresa Pública Yachay, por todo su apoyo, facilidades brindadas al realizar este proyecto, sus consejos e indicaciones que me permitieron cumplir este objetivo.

Alejandra Mabel

Resumen

Se considera la información como un recurso altamente utilizado en hogares, instituciones educativas, empresas, otras organizaciones. Por esta razón es importante determinar las acciones a seguir para protegerla.

La Empresa Pública Yachay es una organización creada para apoyar al proyecto "Ciudad del Conocimiento Yachay", el cual tiene como objetivo principal efectuar investigaciones tecnológicas que mejoren la Matriz Productiva en el país. La Dirección de Tecnologías de la Institución tiene toda la predisposición de respaldar la información que conlleva el proyecto YACHAY.

Se considera importante evaluar los riesgos a los que se enfrentan las tecnologías de la información; es así que existen varias metodologías que permiten realizar este proceso. Algunas son: MARGERIT, OCTAVE, ISO/IEC 27005, MSAT. Cada una de ellas propone una serie de actividades para determinar los peligros tecnológicos a lo que se enfrenta la empresa y se orientan al tipo de organización que se desea aplicar; de tal manera que al seleccionar cuál herramienta es la más adecuada para el proyecto, la decisión es Microsoft Security Assessment Tool que trabaja en 4 áreas esenciales como: infraestructura, aplicaciones, operaciones y personal y sus recomendaciones van enfocadas a la Norma Internacional ISO/IEC 27002.

A partir de la evaluación de riesgos, todos los procesos que se ejecutan deben regirse a Estándares Internacionales. En el caso de la seguridad de la información, el regimiento es en base a la ISO/IEC 27000 propuesta por la Organización Internacional de

Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), que se enfoca en 4 aspectos fundamentales; entre ellos la tecnología de la información.

En el Ecuador, el Instituto Ecuatoriano de Normalización (INEN) acoge la Norma Internacional y la expone para su uso como Norma Técnica Ecuatoriana ISO/IEC 27000. La Norma se clasifica de la siguiente forma: en la ISO/IEC 27000 se encuentran términos y definiciones; así también, en la ISO/IEC 27001 se presentan los requisitos para trabajar con los sistemas de gestión de seguridad de la información (SGSI); además la ISO/IEC 27002 que recoge la guía de buenas prácticas, es decir las medidas a tomar para asegurar los sistemas de información, contenidos en 11 dominios, 39 objetivos de control y 133 controles.

Además, la Secretaría Nacional de Administración Pública presenta en el Esquema Gubernamental de Seguridad de la Información los dominios de la Norma ISO/IEC 27002; que las empresas y entidades públicas deben cumplir los hitos en un 100% al finalizar el año 2016.

De esta manera surgió la necesidad de cumplir con Políticas de Seguridad que sean evidencia del desarrollo de los hitos requeridos por la SNAP. La entidad pública ha venido presentando algunos ítems que conformen la Política de Seguridad y la presente investigación se enfoca a colaborar con el documento en la parte de Gestión de Comunicaciones y Operaciones; aclarando que es una propuesta de Políticas de Seguridad para que la empresa realice su análisis, aceptación y puesta en marcha de los controles según lo crea conveniente.

Abstract

Information is considered as a widely-used resource in homes, educational institutions, companies, other organizations. This is the reason why is important to determinate the appropriate activities to follow in order to protect it.

The Yachay Public Company is an organization created to support the "Yachay City of Knowledge" project, whose main objective is to carry out technological research to improve the Productive Matrix in the country. The Institutional Technologies Department is fully prepared to support the information provided by the YACHAY project.

It is considered important to assess the risks faced by information technologies; So there are several methodologies that can perform this analysis. Some are: MARGERIT, OCTAVE, ISO / IEC 27005, MSAT. Each one of them proposes a series of activities to determine the technological dangers to which the company is faced and they are oriented to the type of organization that is wanted to apply; In order to choose the most appropriate tool for the project, the decision is the Microsoft security assessment tool that works in four essential areas: infrastructure, applications, operations and personnel and its recommendations focused on International Standard ISO / IEC 27002.

Therefore, all executed processes in the entity must be governed by International Standards. About information security, the regulation is proposed by the International Standardization Organization (ISO) and the International Electrotechnical Commission

(IEC) in ISO / IEC 27000, which focuses on four fundamental aspects; one of them is Information technologies.

In Ecuador, the Ecuadorian Institute for Standardization (INEN) takes in the International Standard and exposes it for use as an ISO / IEC 27000 Ecuadorian Technical Standard. The Standard is classified as follows: in ISO / IEC 27000 terms and definitions are found; Also in the ISO / IEC 27001 presents the requirements for working with the information security management systems (ISMS); In addition to the ISO / IEC 27002 standard, which recognizes the good practices guide, ie the measures taken to guarantee information systems, it contains 11 domains, 39 control objectives and 133 controls.

In addition, the Public Administration National Secretariat presents in the Government Information Security Scheme of the Domains of ISO / IEC 27002; That companies and public entities must complete the milestones to 100% at the end of 2016.

In this way, the need to comply with the Security Policies that are evidence of the development of the requirements required by the SNAP arose. The public entity has presented some elements that make up the Security Policy and the present research focuses on collaborating with the Management of Communications and Operations part of the document; Clarifying that it is a proposal of Security Policies for the company to carry out its analysis, acceptance and implementation of the controls.

Presentación

El proyecto descrito a continuación tiene como finalidad realizar un planteamiento de Políticas de Seguridad de acuerdo al Esquema Gubernamental de Seguridad de la Información en la Empresa Pública Yachay.

Inicialmente, se describen los antecedentes, la problemática, los objetivos (general y específicos), el alcance y justificación que explican la ejecución del proyecto.

A continuación, se detalla el fundamento teórico que es el soporte teórico de esta investigación. Específicamente se mencionan los conceptos sobre la Normativa de Seguridad de la Información en base a la ISO/IEC 27002 y el Esquema Gubernamental de Seguridad de la Información propuesto por la Secretaria Nacional de Administración Pública; además se respalda la evaluación de riesgos en base a la herramienta MSAT y la propuesta de Políticas de Seguridad siguiendo la metodología de la Universidad Nacional de Colombia (Guía de Políticas de Seguridad de la Información), enmarcadas en los controles de la seguridad de la información.

Así mismo, se hace un estudio de los procesos de seguridad de la información actuales en la Gerencia de Tecnologías de Yachay E.P y se plasma la documentación que respalda los mismos. Se realiza una evaluación de riesgos para identificar los activos críticos, establecer la magnitud de riesgos y plantear las medidas a corde a los requerimientos de la empresa. De esta manera, se identifica los controles de seguridad necesarios para la propuesta de las Políticas de Seguridad con fundamento en la Norma ISO/IEC 27002 y el EGSI.

Posteriormente, se realiza la propuesta de Políticas de Seguridad de la Información con enfoque en la gestión de comunicaciones y operaciones, así como la documentación de desarrollo de la misma. Se presenta un bosquejo de políticas y se genera un escenario para el desarrollo que contiene la creación y revisión del proyecto.

Finalmente se exponen los respectivos resultados obtenidos luego de los procesos de desarrollo, así como las recomendaciones de la presente investigación en la Empresa Pública Yachay.

Tabla de contenido

Índice de ilustraciones

Índice de tablas

Capítulo I.

Antecedentes

En este capítulo se recopila la información acerca del problema de investigación, los objetivos planteados para este proyecto, la delimitación del problema y la justificación de la importancia para disponer un Planteamiento de Políticas de Seguridad de la Información en la Empresa.

1.1 Problema.

La Empresa Pública Yachay EP. del Ecuador fue creada el 13 de marzo de 2013, la cual es la encargada de la administración del proyecto Ciudad del Conocimiento Yachay. Su sede se encuentra en la ciudad de Quito; no obstante, en la Hacienda San Eloy, cantón San Miguel de Urcuquí, provincia de Imbabura, se localizan otras oficinas administrativas.

Uno de los procesos que maneja la empresa es la Gestión de Tecnologías a través de su Gerencia, ofreciendo disponibilidad, seguridad y continuidad de los recursos y servicios Tics; de esta forma alcanzar un nivel de estándares acorde a los requerimientos corporativos. Para lograr la gestión mencionada existen Departamentos que conforman la Gerencia, y son:

a) Departamento de Soporte y Operaciones Tecnológicas.
b) Departamento de Telecomunicaciones, Energía y Automatización.
c) Departamento de Sistemas Informáticos.

Según las disposiciones de la Secretaría Nacional de la Administración Pública (SNAP) se exige a todas las empresas públicas del Ecuador implementar un sistema que gestione la seguridad de la información, basado en los dominios del Esquema Gubernamental de Seguridad de la Información (EGSI), el cual permita proteger la infraestructura gubernamental de un proyecto emblemático del Gobierno como es Yachay E.P.

La Empresa cuenta con documentación que sustenta el desarrollo de los proyectos actualmente implementados, sin embargo, el entorno de tecnologías de información vigente y el incremento de normas y estándares inducen al uso de las mejores prácticas de tecnologías de la información en base a controles y objetivos ajustándose al EGSI.

Entonces, para garantizar disponibilidad, integridad y confiabilidad de la información se propone analizar los factores de inseguridad que aún no han sido controlados. Así mismo, contar con una estructura de políticas correspondiente a seguridad de la información, en este caso el EGSI que no es más que un documento resumen de la INEN/ISO/IEC 27002:2005.

1.2 Objetivos.

1.2.1 Objetivo General.

- ✓ Plantear políticas en base al Esquema Gubernamental de Seguridad de la Información (EGSI) para la Empresa Pública Yachay con el fin de permitir ejecutar eficientemente los requisitos de seguridad.

1.2.2 Objetivos Específicos.

- ✓ Analizar el Esquema Gubernamental de Seguridad de la Información (EGSI) dispuesto por la SNAP y los documentos que respaldan los procedimientos de Yachay E.P. para establecer los requerimientos de seguridad de información.

- ✓ Describir el estado actual de la seguridad de información de Yachay E.P., normativa y prácticas de seguridad actuales.

- ✓ Promover las mejores prácticas de seguridad al desarrollo de los sistemas de información, elaborando la propuesta de seguridad de información según los dominios, objetivos y controles.

- ✓ Evaluar los procesos estableciendo un ambiente de pruebas, permitiendo obtener resultados para su posterior análisis y mejora continua.

1.3 Alcance

La investigación debe fundamentarse con terminología sobre seguridad de la información, Normativa nacional e internacional.

El desarrollo de la investigación se enfoca a la Gerencia de Tecnologías de Yachay E. P. y sus procesos internos, donde se realizará el levantamiento de información, considerando las siguientes categorías:

- ✓ Infraestructura
- ✓ Aplicaciones
- ✓ Operaciones
- ✓ Personal

El EGSI basado en la Norma INEN/ISO/IEC 27002:2005 cubre todos los aspectos de la Seguridad de la Información, incluido el factor humano; sin embargo, el presente proyecto se enfoca en utilizar los controles que se relacionen directamente con la gestión de comunicaciones y operaciones. El planteamiento comprende los dominios:

a) 1. Políticas de Seguridad
b) 6. Gestión de comunicaciones y operaciones

Se llevará a cabo a través del estudio de los controles expuestos en el dominio de Gestión de comunicaciones y operaciones del EGSI, específicamente se estudiará los objetivos:

a) 6.13. Controles de las redes
b) 6.14. Seguridad de los servicios de la red.
c) 6.26. Registro de auditorías.

La versión más reciente de la Norma ISO/IEC 27002 es la realizada en 2013, por lo que se realiza una validación de articulación entre ambas para aclarar conceptos según la necesidad de la propuesta.

Se planificará un ambiente de pruebas, donde se pueda crear y revisar la Política, y finalmente realizar la socialización de la propuesta a la gerencia para sugerir mejoras en los procesos ya implementados.

1.4 Justificación

La presente investigación se realiza con la finalidad de presentar una propuesta de seguridad de información para la Empresa Pública Yachay, pues al considerarse como uno de los proyectos emblemáticos de Gobierno, la infraestructura gubernamental debe protegerse de ataques informáticos o incidentes de seguridad bajo políticas que regulen su desempeño. La institución cuenta con equipamiento de seguridad y documentos que han respaldado los procesos ya implementados.

El cumplimiento del EGSI exige a las empresas públicas que cumplan con Políticas de la Seguridad de la Información, lo que conlleva a las empresas a tomar la decisión a adquirir nuevas soluciones de seguridad u optimizar la existente. La puesta en producción de nuevos recursos tecnológicos implica un costo económico adicional a la planificación inicial. Por el contrario, el planteamiento de políticas en base a una normativa internacional optimizaría las funcionalidades del equipamiento existente y revela los riesgos que no son cubiertos; lo que significaría una menor inversión.

La Secretaria Nacional de Administración Pública monitorea constantemente el cumplimiento de los Hitos en la plataforma de GPR, y sugiere culminar el proceso al 100% al finalizar el año 2016. Se ejecuta un reporte en el que se manifiesta los resultados para posterior auditorias. Este es un justificativo importante para el proyecto puesto que el tiempo es fundamental para su culminación.

Capítulo II

Fundamento Teórico

En el presente capítulo se efectúa una breve descripción de contenidos de Seguridad de la Información, como fundamentos necesarios para el desarrollo de la propuesta. Se analiza la norma técnica ISO/IEC 27002 y su relación con el Esquema Gubernamental de Seguridad de la Información.

2.1 Información

Las instituciones que manejan grandes volúmenes de información deben tener en cuenta que esta debe ser lo más clara posible ya que permiten a los usuarios de los sistemas la correcta toma de decisiones; entonces se tiene claro que:

> La tecnología de la información es la ciencia que estudia las técnicas y procesos que actúan sobre los datos y la información. La palabra "informática" proviene de la fusión de los términos "información" y "automática", lo que originalmente significaba la realización de tareas por medio de máquinas. (Suárez & Alonso, 2007)

La información que se maneja en la Empresa Pública YACHAY está enfocada a un mega proyecto que es la Ciudad del Conocimiento, por lo que es necesario tratar sobre la seguridad de la información.

2.1.1 Clasificación de la Información

La Norma (ISO/IEC 27000:2012, 2012) plantea la clasificación de la información siguiendo los siguientes criterios:

Se especifica 4 niveles de clasificación (0 – 3) siendo 3 el nivel más sensible y 0 el menos sensible. Según lo que cumpla el activo de información el propietario definirá su criticidad (baja, media o alta).

a) Confidencialidad:
   - ✓ Público
   - ✓ reservado (uso interno)
   - ✓ reservado (confidencial)
   - ✓ reservado (secreto)

b) Integridad: Debido a modificaciones no autorizadas en la información
   - ✓ Se puede reparar fácilmente.
   - ✓ Se puede reparar, aunque puede dejar algunas pérdidas.
   - ✓ Es difícil su reparación y puede dejar pérdidas significativas.
   - ✓ No puede repararse ocasionando pérdidas grandes.

c) Disponibilidad: La inaccesibilidad a la información
   - ✓ No afecta.
   - ✓ Durante un periodo de tiempo no menor a una semana podría causar pérdidas significativas.

- ✓ Durante un periodo de tiempo no menor a un día podría causar pérdidas significativas.
- ✓ Durante un periodo de tiempo no menor a una hora podría causar pérdidas significativas.

2.2 Seguridad de la Información

Se considera a la Seguridad de la Información mucho más que un antivirus, cortafuego o cifrado de datos, estos términos son el resultado de operaciones realizadas por personas y que son soportadas por la tecnología. (Álvarez Marañon & Pérez García, Seguridad Informática para Empresas y Particulares, 2004).

2.2.1 Definición

La seguridad de la información corresponde al proceso para salvaguardar la continuidad de las operaciones y proteger de amenazas, que se encuentran en un computador o una red de más dispositivos, además de la defensa del acceso a todos los recursos del sistema. (CYBSEC S.A, 2011)

Es posible desarrollar la seguridad de la información con la colaboración de controles como políticas, buenas prácticas, manuales de funciones, procedimientos, planes de contingencia y funciones de hardware y software; controles que además de diseñarse e implementarse deberá ser necesario el monitoreo y mejora continua para cumplir con las actividades y objetivos que desarrolla la empresa.

Los sistemas de información son activos sometidos a vulnerabilidades y amenazas, implicando desde el personal interno o hasta agentes externos ajenos a la organización. De esta manera los sistemas se encuentran en riesgo, sea físico o lógico. Para la investigación se considera importante al riesgo lógico, que es aquel que se relaciona con

el ámbito tecnológico y que está aumentando cada día, afectando directamente con los principios de la seguridad que se ofrece a los usuarios. Algunos riesgos son robos de identidad, accesos no autorizados, virus, espionaje digital.

2.2.2 Seguridad Informática vs Seguridad de la Información

Mientras la seguridad informática implica la protección de la infraestructura que soporta el negocio; la seguridad de la información es la protección de la información de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar las oportunidades. (Norma ISO/IEC, 2005)

2.2.3 Pilares de la seguridad de la información

La seguridad de la información se sustenta a través de 3 pilares fundamentales según lo manifiesta (BLIGOO, 2010): son principios importantes que garantizan el desenvolvimiento del trabajo mediante políticas y mecanismos. En la ilustración 1 se puede observar los principios:

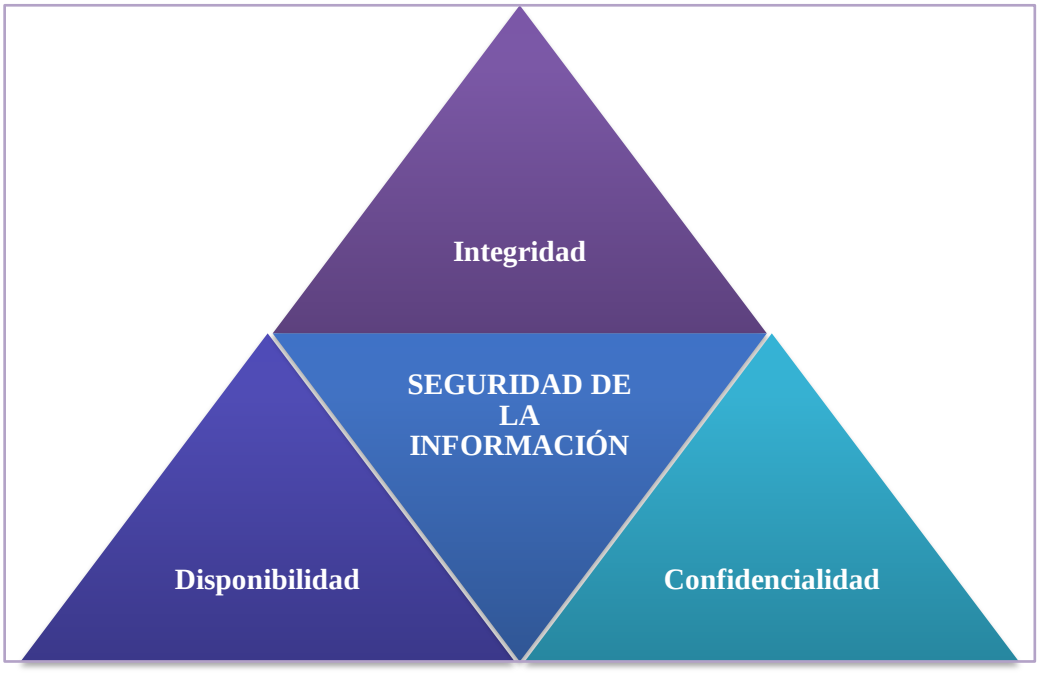

Ilustración 1. Pilares de la Seguridad de la Información
Fuente: (ISO27000.ES, 2013)

La norma (ISO/IEC 27000:2012, 2012) define a los principios de la siguiente manera:

2.2.3.1 *Disponibilidad*

Garantiza a los usuarios que han sido autorizados con anterioridad el acceso a la información en el momento que lo requieran. Implica que se puede disponer libremente de los recursos informáticos y a la vez previene interrupciones no autorizadas.

2.2.3.2 *Integridad*

Es la propiedad de proteger la precisión y complejidad de los activos. Asegura que los datos no sufran modificaciones no autorizadas durante su tránsito. Para avalar el proceso puede usar la solución de autenticación para verificar que el tráfico de origen sea igual al enviado.

Las entidades públicas constantemente reciben ataques para obtener información, modificar y evidenciar los niveles de seguridad implementados.

2.2.3.3 *Confidencialidad*

Es la cualidad de prevenir divulgación de los datos a personas o sistemas no autorizados. Implica restringir el acceso a datos sensibles. Para sustentar este principio se utilizaría mecanismos de seguridad, credenciales de acceso, cifrado de tráfico.

Es fundamental realizar la valoración de riesgos, identificar su magnitud y proponer medidas para eliminar, transferir, asumir o mitigar el riesgo.

2.3 Definición de riesgo

En la Norma (ISO/IEC TR 13335-1, 2009), se define: riesgo es el potencial de que una amenaza dada explote las vulnerabilidades causando perdida o daño a un activo o grupo de activos, afectando directamente a la organización. El análisis de riesgos en sistemas de información permite tomar decisiones para proteger al sistema, de tal manera que se efectivice las operaciones y se cumplan los reglamentos.

Los componentes expuestos al análisis de riesgos son procesos y/o activos, sean físicos o de información.

- ✓ Activos físicos: edificios, infraestructura, maquinaria, equipos de oficina.
- ✓ Activos de información: bases de datos, aplicaciones, sistemas de gestión, sistemas de monitoreo, archivos de datos.

Se precisa los riesgos aplicados en tecnologías de la información adquiridos de (ISO/IEC TR 13335-1, 2009).

- ✓ Asociados a catástrofes o eventos producto de la fuerza natural.
- ✓ Por variaciones o perdida de energía eléctrica a través del servicio público.
- ✓ Por mal uso o configuración de equipos, por descuido o con intención.
- ✓ De pérdida de información, asociados a daños en fuentes de almacenamiento o ingreso no permitido.
- ✓ De pérdida de confidencialidad de la información, vinculados al robo o filtración de funcionarios internos o externos a la empresa.

2.3.1 Evaluación de riesgo

"Determina los componentes de un sistema que requiere protección, las vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su

grado de riesgo" (Ulloa, 2015), "tomando como objetivo establecer una valoración y priorización de los riesgos en base a la información obtenida y de esta manera establecer el nivel de riesgo y las acciones que se deben implementar el proceso" (UTE, 2013) .

Es una herramienta que ayuda a los dirigentes de la organización a mantenerse informados de los riesgos asociados a la información. A partir del análisis es posible plantear estrategias que reduzcan el nivel de riesgo.

2.3.2 Gestión de riesgo

En la Norma (ISO/IEC 27001, 2013) se explica la gestión de riesgo que son las actividades para aminorarlo. Así mismo es importante tratar el conflicto, esto implica tomar medidas e implementarlas. Para dicha gestión se puede tomar alternativas como: aceptar, transferir, mitigar, evitar el riesgo.

Entonces, existen varias metodologías para analizar el riesgo. Se fundamenta algunas de ellas y posteriormente se tomará la decisión según sea la más adecuada a las exigencias de la empresa.

2.3.3 Metodologías para evaluación de riesgo en las TI

Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los temas organizacionales como los técnicos, examina como los usuarios emplean la infraestructura en su entorno. Implica una práctica fundamental porque genera una visión para la empresa acerca de los riesgos proporcionando una base para futuras mejoras. En consecuencia, se debe contar con una metodología para la evaluación, análisis y gestión de riesgos. Actualmente, existen varias guías, estándares y herramientas de sustento que buscan encargarse y mitigar los riesgos.

En la tabla 1, se realiza un análisis de algunas herramientas que gestionan el riesgo:

Tabla 1. Metodologías de evaluación de riesgos

METODOLOGÍA	DESCRIPCIÓN	PAÍS
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation	Estados Unidos
MARGERIT	Metodología de Análisis y Gestión de Riesgos de Sistemas de Información.	España
MSAT	Herramienta de evaluación de seguridad de Microsoft.	Estados Unidos
ISO/IEC 27005	Tecnología de la información, técnicas de seguridad, información de gestión de riesgos de seguridad.	Estados Unidos

Fuente: Autor

Las principales metodologías de evaluación, análisis y gestión en el ámbito de la seguridad de información investigados de (Duque & Gómez, 2010) son:

- ✓ OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation.
- ✓ MARGERIT (Metodología de Análisis y Gestión de Riesgos de Sistemas de Información).
- ✓ MSAT (Microsoft Security Assessment Tool).
- ✓ ISO/IEC 27005.

Para determinar cuál es la herramienta aplicable al proceso, en la tabla 2 se muestra algunas características con las que cumplen.

Tabla 2. Comparativa de Metodologías de evaluación, análisis y gestión de riesgos.

EVALUACIÓN		OCTAVE	ISO7IEC 27005	MARGERIT	MSAT
Alcance considerado	Evaluación de riesgo	✓	✓	✓	✓
	Gestión de riesgo	✓	✓	✓	✓
Tipo de análisis	Cuantitativo	X	X	✓	X
	Cualitativo	✓	✓	✓	✓
Elementos del modelo	Procesos	✓	✓	X	✓
	Activos	✓	✓	✓	✓
	Recursos	✓	✓	✓	✓
	Dependencias	✓	✓	X	✓
	Vulnerabilidades	✓	✓	✓	✓
	Amenazas	✓	✓	✓	✓
Objetivos de seguridad	Confidencialidad	✓	✓	✓	✓
	Integridad	✓	✓	✓	✓
	Disponibilidad	✓	✓	✓	✓
Implementación	Herramienta	X	X	PILAR ($250-$2000)	✓
Fases de cumplimiento	Etapas	3	6	3	Encuesta 4 categorías
Costo		Uso libre	Uso libre	Licencia comercial	Uso libre

Fuente: Autor

La tabla comparativa define los ítems decisivos para la evaluación que son: etapas y costo; porque las metodologías cumplen con la mayoría de los parametros para evaluación de riesgos y estos aspectos son los que diferencian entre ellas. Según la tabla son OCTAVE y MSAT, que serán detalladas a continuación.

2.3.3.1 *Metodología OCTAVE*

La metodología OCTAVE se enfoca a la organización que tiene una estructura de trabajo jerárquica y defiende sobre bases tecnológicas propias que ejecuta las herramientas para la valoración de la vulnerabilidad e interpretación de los resultados. Es una metodología que consiste en encontrar seguridad de información, en base al adecuado análisis del riesgo y la planeación de una estrategia de seguridad.

EL método en el documento (Duque & Gómez, 2010) plantea fases para examinar aspectos organizacionales y de tecnología, aprovechando el conocimiento de múltiples niveles de la organización, centrándose en:

- ✓ Identificar los elementos críticos y las amenazas a los activos.
- ✓ Identificar vulnerabilidades, tanto organizativas como tecnológicas.
- ✓ Desarrollar la estrategia de protección basada en la práctica y los planes de riesgo.

2.3.3.1.1 Objetivo de OCTAVE

El autor (Palma, 2011) precisa que la organización estará en la capacidad de:

- ✓ Tomar decisiones adecuadas, basadas en el análisis de riesgos.
- ✓ Evaluar y controlar los riesgos en la seguridad de la información.
- ✓ Enfocarse en el aseguramiento de sus activos tecnológicos.

2.3.3.1.2 Guía de implementación de OCTAVE

Incluye procesos paso a paso, constan instrucciones para su implementación y material de apoyo para la adaptación. En su libro, (Palma, 2011) analiza la metodología OCTAVE a través de las siguientes fases:

a. Fase Startup

Constituye la obtención del apoyo de las autoridades en todas las áreas de trabajo para el análisis y evaluación. Implica la selección del equipo de trabajo, la definición de los alcances del análisis y determinación de un equipo de apoyo.

b. Fase 1

La fase uno es una evaluación con visión organizativa. Determina los activos críticos para la operación empresarial e identifica las actividades de protección actuales. Los procesos enfocados en esta fase se consolidan en la visión de área gerencial, operativa y personal de apoyo; como se muestra en la tabla 3.

Tabla 3. Procesos y actividades de la fase 1. Metodología OCTAVE

FASE 1	PROCESO	ACTIVIDAD	PASOS
Construir perfiles de amenaza basados en activos	**Proceso S1:** Identificar la información organizacional	**S1.1** Establecer los criterios de evaluación de impacto	1
		S1.2 Identificar activos organizacionales	2
		S1.3 Evaluar las prácticas de seguridad organizacionales	3, 4
	Proceso S2: Crear perfiles de amenaza	**S2.1** Seleccionar activos críticos	5, 6, 7, 8, 9
		S2.2 Identificar los requerimientos de seguridad para los activos críticos	10, 11
		S2.3 Identificar amenazas a los activos críticos.	12, 13, 14, 15, 16

Fuente: OCTAVE Implementation Guide.

c. Fase 2

Es una evaluación con visión tecnológica, en la cual se identifica las vulnerabilidades de la infraestructura como: red, aplicaciones; así como las vías de acceso y los responsables de configuraciones; como se muestra en la tabla 4.

Tabla 4. Procesos y actividades de la fase 2. Metodología OCTAVE

FASE 2	PROCESO	ACTIVIDAD	PASOS
Identificar vulnerabilidades de la infraestructura.	**Proceso S3:** Examinar la infraestructura computacional en relación con los activos críticos.	**S3.1** Examinar rutas de acceso.	17, 18
		S3.2 Analizar procesos relacionados con la tecnología.	19, 20, 21

Fuente: OCTAVE Implementation Guide

d. Fase 3

Desarrolla la estrategia de seguridad que consiste en el análisis específico de los riesgos, la decisión de protección y la implementación del plan con sus respectivas evidencias; como se muestra en la tabla 5.

Tabla 5. Procesos y actividades de la fase 3. Metodología OCTAVE

FASE 3	PROCESO	ACTIVIDAD	PASOS
Desarrollo de estrategias y planes de seguridad.	**Proceso S4:** Desarrollar estrategias de protección y planes de mitigación	S4.1 Describir las estrategias de protección actuales.	22
		S4.2 Seleccionar aproximaciones de mitigación.	23, 24
		S4.3 Desarrollar planes de mitigación de riesgos.	25
		S4.4 Identificar cambios en las estrategias de protección.	26
		S4.5 Identificar los pasos siguientes.	27

Fuente: OCTAVE Implementation Guide

2.3.3.2 *Herramienta de evaluación de seguridad de Microsoft (MSAT)*

MSAT es una herramienta gratuita diseñada para ayudar a las organizaciones de menos de 1.000 empleados a evaluar los puntos débiles de su entorno de seguridad de TI. Presenta un listado de cuestiones ordenadas por prioridad, así como orientación específica para minimizar esos riesgos. Además, permite fortalecer la seguridad de su negocio de manera fácil y efectiva.

La evaluación permite obtener un perfil de la situación de la seguridad de su entorno tecnológico y proporciona un mapa bien definido sobre las actuaciones prioritarias, soluciones y recomendaciones prescriptivas a seguir.

Una vez terminada la evaluación, MSAT ofrece un informe complementario que recoge recomendaciones específicas sobre cuestiones de negocio identificadas durante la evaluación. La finalidad de este informe es ayudarle a entender la situación inicial de la seguridad y priorizar los pasos a seguir para mitigar los riesgos identificados.

2.3.3.2.1 Conocer los riesgos

MSAT está diseñado para ayudarle a identificar y abordar los riesgos de seguridad en su entorno de TI. La herramienta utiliza un enfoque integral para medir el nivel de seguridad y cubre aspectos tales como usuarios, procesos y tecnología.

MSAT proporciona:

- ✓ Un conocimiento constante, completo y fácil de utilizar del nivel de seguridad,
- ✓ Informes detallados y actuales comparando su plan inicial con los progresos obtenidos.

- ✓ Recomendaciones comprobadas y actividades prioritarias para mejorar la seguridad.

2.3.3.2.2 El proceso de MSAT

MSAT consta de más de 200 preguntas que abarcan infraestructura, aplicaciones, operaciones y usuarios. Las preguntas, respuestas asociadas y recomendaciones se obtienen a partir de las mejores prácticas comúnmente aceptadas, estándares tales como las normas ISO 27002 y NIST (National Institute of Standards and Technology)-800 series.

La evaluación está diseñada para identificar los posibles riesgos de negocio de su organización y las medidas de seguridad implementadas para mitigarlos. Centrándose en problemas comunes, las preguntas han sido desarrolladas para proporcionar una evaluación de seguridad de alto nivel de la tecnología, procesos y usuarios que participan en el negocio.

A partir de una serie de preguntas acerca del modelo de negocio de su compañía, la herramienta crea un Perfil de Riesgos de Negocio (Business Risk Profile) (BRP), calculando el riesgo de su empresa al hacer negocios según el modelo empresarial y de negocio definido por BRP. Una segunda serie de preguntas tienen como fin elaborar un listado con las medidas de seguridad que su empresa ha implementado a lo largo del tiempo. Juntas, estas medidas de seguridad forman capas de defensa, proporcionando una mayor protección contra los riesgos de seguridad y vulnerabilidades específicas. Cada capa contribuye a una estrategia combinada para una protección a fondo. La suma de ellas se conoce como defensa en profundidad (Defense-in-Depth Index) (DiDI). El BRP

y DiDI se comparan entonces para medir la distribución del riesgo a través de las áreas de análisis: infraestructura, aplicaciones, operaciones y usuarios.

2.4 Requisitos de la Seguridad de información

En el proyecto Metodología para la Gestión de la Seguridad de la Información expuesto por (Oficina de Seguridad para las redes informáticas, 2013) se puede encontrar los principios para establecer los requisitos de la seguridad de información según una valoración de riesgos lo expuesto en la ilustración 2:

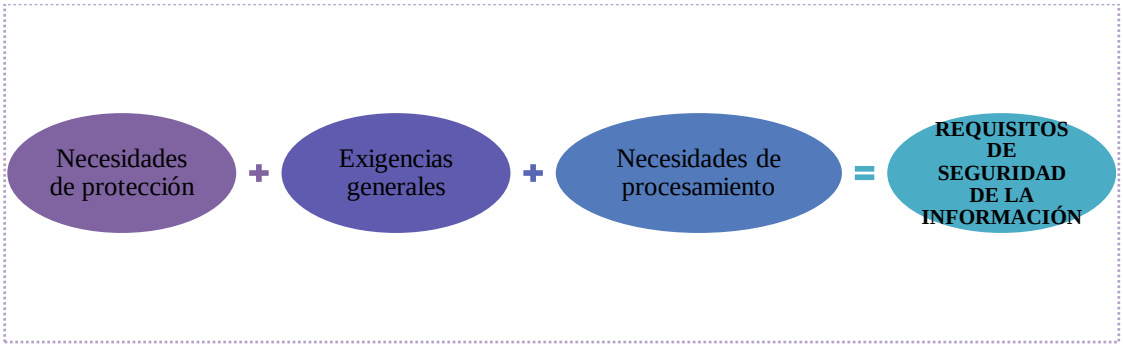

Ilustración 2. Requisitos Seguridad de Información
Fuente: Autor

Debido a la importancia y la necesidad de asegurar la información en los tiempos actuales se debe buscar las maneras de lograr esta seguridad que puede ser a través de la implementación de políticas. De esta manera se considera el establecimiento de los controles y objetivos para equilibrar y culminar con los inconvenientes de seguridad.

(Oficina de Seguridad para las redes informáticas, 2013). Los requisitos de protección están determinados por estudio de activos informáticos, historial de amenazas, evaluación de debilidades. Por su parte, las exigencias generales involucran a las normas legales, estatutos y técnicas de procedimientos. Además, las necesidades de procesamiento de información son las que la empresa concreta para apoyar sus operaciones.

2.4.1 Enfoques de Seguridad de la Información

En relación a la aplicación de un procedimiento de seguridad de información, se toma en cuenta que:

Varios autores concuerdan que entre las mejores prácticas se incluye documentación de la política de seguridad de información, asignación de responsabilidades, formación y capacitación, procedimientos correctos de aplicaciones, registro de incidencias de seguridad y mejoras.

Es importante definir los términos relacionados. Qué se entiende por: ¿POLÍTICA?, ¿NORMA?, ¿ESTÁNDAR?, ¿GUÍA?, se lo presenta en la Guía para elaboración de políticas de seguridad. (Universidad Nacional de Colombia, 2003).

- ✓ **Política:** es una declaración de principios para presentar la posición de la administración para un área específica. Se elaboran con el fin de que sean aplicadas a largo plazo, que cumplan con el desarrollo de reglas y criterios según situaciones presentes.
- ✓ **Norma:** Establece los instrumentos de los lineamientos definidos y las directrices de seguridad de información. Contribuye al cumplimiento de la Política.
- ✓ **Estándar:** En el Manual planteado por (Departamento de Seguridad en cómputo UNAM, 2010) define al término Estándar como "las reglas que describen las acciones ante las situaciones suscitadas. Son diseñados para promover el cumplimiento de las Políticas"
- ✓ **Guía:** Es un documento que sirve para recomendar acciones que sustenten a la Política y al Estándar.

Además, (ISO/IEC 27001, 2013) define la pirámide de evaluación en que se debe documentar la seguridad de la información, como se muestra en la ilustración 3.

Ilustración 3. Pirámide de documentación.
Fuente: Autor

2.5 Política de Seguridad

El autor (Mifsud E. , 2012) en su texto "Políticas de Seguridad. Cómo podemos proteger el sistema", manifiesta que:

> "El objetivo de la Política de Seguridad de Información de una organización es servir de base para desarrollar los procedimientos concretos de seguridad. Las políticas deben contener las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente".

En el Manual de Normas y Políticas propuesto por (Universidad de Oriente UNIVO) se manifiesta una definición precisa sobre Políticas de Seguridad, así: "Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización."

Para generar una Política, el departamento de tecnologías de la Universidad Nacional de Colombia en su "Guía de elaboración de Políticas" (2003) indica la existencia de etapas que se van cumpliendo conforme los requerimientos de la empresa. En la ilustración 4 se desglosa la clasificación en base a 11 etapas agrupadas en 4 fases, de esta manera:

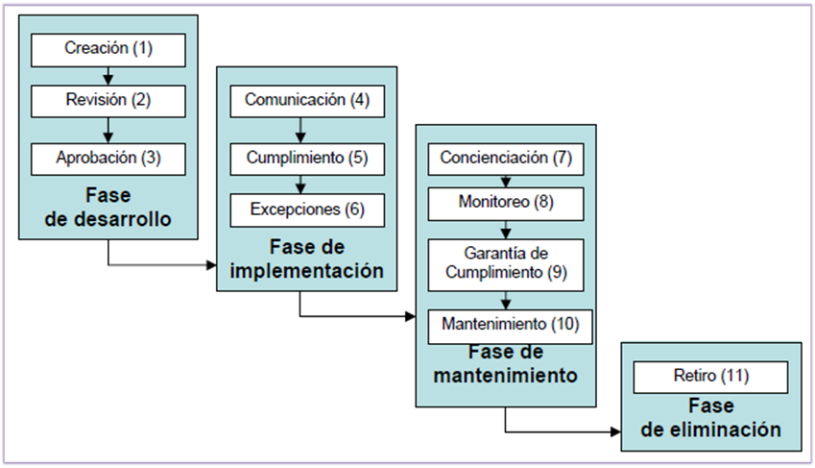

Ilustración 4. Etapas Política de Seguridad
Fuente: (Universidad Nacional de Colombia, 2003)

2.5.1 Ciclo de vida de la Política de Seguridad.

En El Ciclo de Vida de la Política de Seguridad de (Howard, 2003) se explica paso a paso el ciclo de la Política de Seguridad:

2.5.1.1 *Fase de desarrollo.*

Durante esta fase la Política es creada, revisada y aprobada. La *creación* es la fase donde se debe planear, indagar, fundamentar y coordinar continuamente con los departamentos de la entidad y agentes externos pertinentes en el desarrollo del formato de redacción. Se precisa:

- ✓ Necesidad de la política
- ✓ Alcance
- ✓ Aplicabilidad

- ✓ Roles
- ✓ Responsabilidades

Posteriormente, se encuentra la *revisión*, que consiste en remitir la documentación a un equipo de revisores para que evalúen independientemente. Es interesante la revisión a razón de que se recibirá recomendaciones y comentarios para realizar los cambios correspondientes y con la seguridad de que habrá una aprobación satisfactoria por parte de la autoridad adecuada. La *aprobación* implica el compromiso institucional y hace posible la implementación.

2.5.1.2 *Fase de implementación.*

En esta fase la política es comunicada y cuestionada. La primera etapa de esta fase significa *difundir* la política a los miembros de los departamentos correspondientes en la empresa, efectuar significa atender los procesos en base al documento que los sustenta, continuamente el realizar seguimientos y *agenciar el cumplimiento* progresivo; todo esto a través de informes. Asimismo, existirán *excepciones* en que no puedan ejecutarse los procesos, también se deben documentar debido a que será una no aplicación temporal según las circunstancias justificadas.

2.5.1.3 *Fase de mantenimiento.*

Los usuarios deben ser conscientes de la importancia de la Política, su cumplimiento, monitoreo y el mantenimiento o actualización.

Comprende el esfuerzo por garantizar el cumplimiento de la Política. Significa *comunicar* a jefes, usuarios a través de reuniones, cursos, correos electrónicos como forma de difusión. Este proceso viene relacionado con el *monitoreo* puesto que implica el seguimiento y reportes del cumplimiento de la Política; esto es a través de

evaluaciones, inspecciones y análisis de reportes. Así mismo, se debe asegurar que la Política este actualizada, que se garantice su vigencia y desarrollo continuo de la misma.

2.5.1.4 *Fase de eliminación.*

La política se retira cuando no se requiera más. Al cumplir con las directrices sugeridas en la Política de Seguridad se considera que deba ser *retirada*. Este paso dentro de la fase debe realizarse con atención porque se requiere archivar información para referencias futuras.

2.5.2 Lineamientos de creación

Los lineamientos de la etapa de creación de la política que la guía precisa se resume en:

- Definiciones de seguridad
    - Necesidad de la Política
    - Objetivos
    - Alcance
    - Aplicabilidad
- Declaración de la Dirección apoyando la propuesta.
- Explicación de Políticas
- Definición de roles y responsabilidades
- Referencias que sustenten la Política
- Anexos

Las políticas de seguridad de la información tienen su guía o complemento en los estándares o normas de seguridad.

2.6 Estándares o normas de seguridad

Las empresas comúnmente mencionan el trabajo bajo estándares y normas de seguridad, entonces se toma en cuenta que:

Un estándar es un documento con un contenido de tipo técnico-legal que establece lineamientos para cumplir una actividad o procedimientos. Su uso en la actualidad es común debido a que se busca que los procesos y actividades de organizaciones y sus personas sean organizados, y estructurados. (Borbón, J., 2011, pp. 14-16).

Es por lo citado que instituciones públicas con YACHAY E.P., pueden aplicar este tipo de normas de seguridad, con el propósito de precautelar la información que se procesa y que se pone a disposición de la sociedad.

2.6.1 Norma ISO

> ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización. Esta entidad es una organización no gubernamental constituida por más de 160 países y otras organizaciones, así como es la mayor en el desarrollo y publicación de estándares internacionales con más de 18.500 estándares publicados en la actualidad. (FUNIVSCYL, 2012, p. 85).

La organización ISO además se encuentra en Ecuador, por lo que los estándares que desarrollan se aplican en YACHAY E.P. como medida para precautelar la información.

2.6.2 Serie ISO/IEC 27000

ISO/IEC 27000 es un conjunto estándares desarrollados por ISO e IEC que proporcionan un marco gestión de la segundad de la información utilizable por cualquier organización o institución bajo verificables de aplicación.

- ✓ ISO es un organismo que promueve el desarrollo de las normas voluntarias internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción del campo de eléctrica y electrónica. Su objetivo principal es estandarizar normas, productos y seguridad para las organizaciones y empresas de todo el mundo. (ISO, s.f.)
- ✓ IEC es una organización que se encarga de la normalización en el campo eléctrico, electrónico y de tecnologías relacionadas. La organización prepara y publica normas internacionales para todas las tecnologías relacionadas con el fin de trabajar con seguridad en todo nivel.

En el país, existe el servicio ecuatoriano de normalización INEN que se encarga de planificar, organizar, dirigir, controlar y evaluar los parámetros de la calidad, inocuidad y seguridad de los productos, servicios, tecnologías que se comercializan en el país, a través del desarrollo de documentos normativos necesarios acorde con el avance tecnológico, de tal forma que estos documentos se constituyan en el punto de referencia técnico-legal que garantice orden en las actividades a desarrollarse.

Pertenecen a la serie ISO/IEC 27000 lo que se muestran en la tabla 6:

Tabla 6. Resumen de la Serie ISO 27000

RESUMEN DE LA SERIE ISO 27000		
ISO/IEC 27000	✓	Presenta los términos y definiciones de seguridad de la información.
ISO/IEC 27001	✓	Certificación que deben obtener las organizaciones.
	✓	Requisitos del SGSI.
	✓	Enfoque de gestión de riesgos y mejora continua de procesos.
ISO/IEC 27002	✓	Guía de buenas prácticas para el SGSI.
	✓	Describe 11 dominios, 33 objetos de control y 133 controles para la seguridad de la información.
ISO/IEC 27003	✓	Son directrices para la implementación del SGSI.
	✓	Soporte de ISO/IEC 27001.
ISO/IEC 27004	✓	Métricas y técnicas de medida para determinar eficacia del SGSI.
	✓	Recomendaciones de quien, cuando y como realizar las mediciones.
ISO/IEC 27005	✓	Directrices para la gestión de riesgos en la seguridad de la información.
	✓	Recomendaciones y lineamientos de evaluación de riesgos.
ISO/IEC 27006	✓	Especifica los requisitos para acreditarse como entidad certificadora de ISO 27001 (2007)
ISO/IEC 27007	✓	Guía para auditar al SGSI
ISO/IEC 27011	✓	Guía de implementación de un SGSI para el sector de Telecomunicaciones (2008).
ISO/IEC 27799	✓	Es una guía para implementar ISO/IEC 27002 en la industria de la salud y sanitaria.

Fuente: (ISO, s.f.)

2.6.3 Norma ISO/IEC 27002

Es una norma no certificable y sin embargo sugiere varias recomendaciones para la seguridad de la información, publicado por primera vez como ISO/IEC 17799:2000 con el título Tecnologías de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. Posteriormente, luego de un periodo de revisión y actualización de contenidos, se denomina 27002:2005 y cuenta con los controles que se muestran en el anexo. **(Ver Anexo 1)**. Actualmente, al 2016 es posible encontrar una actualización del estándar con el nombre de ISO/IEC 27002:2013 como se observa en el anexo. **(Ver Anexo 2)**.

La Norma ISO/IEC 27002:2005 se conforma de 11 dominios, 39 objetivos de control y 133 controles; mientras que la actualización del 2013 contempla 14 dominios, 35 objetivos de control y 144 controles. Se ha realizado una validación entre ambas actualizaciones para identificar sus diferencias, puesto que son aspectos fundamentales para definir posteriormente los controles de estudio.

Inicialmente la Norma presenta los numerales del 0 al 4 de la siguiente manera:

0. Introducción.
1. Objeto y campo de aplicación.
2. Términos y definiciones
3. Estructura de la Norma.
4. Evaluación y tratamiento de riesgo.

Posteriormente, desde el numeral 5 se presenta la equivalencia de contenido entre ambas actualizaciones como se muestra en la tabla 7:

Tabla 7. Dominios ISO/IEC 27002

DOMINIOS DE ISO/IEC 27002:2013	DOMINIOS DE ISO/IEC 27002:2005
5. Política de Seguridad.	5. Política de Seguridad.
6. Aspectos organizativos de la seguridad de la información.	6. Aspectos organizativos de la seguridad de la información.
7. Seguridad ligada a recursos humanos.	8. Seguridad ligada a recursos humanos.
8. Gestión de activos	7. Gestión de activos.
9. Control de acceso.	11. Control de acceso.
10. Cifrado*[1]	-
11. Seguridad física y ambiental	9. Seguridad física y del entorno.
12.Seguridad en la operativa* 13. Seguridad en las telecomunicaciones*	10. Gestión de comunicaciones y operaciones.
14. Adquisición, desarrollo y mantenimiento de sistemas de información.	12. Adquisición, desarrollo y mantenimiento de sistemas de información.
15. Relaciones con suministradores. *	-
16. Gestión de incidentes en la seguridad de la información.	13. Gestión de incidentes en la seguridad de la información.
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	14. Gestión de la continuidad del negocio.
18. Cumplimiento	15. Cumplimiento

Fuente: (ISO27000.ES, 2013)

Son muy claros los cambios a nivel de dominios en las actualizaciones de la Norma ISO/IEC 27002 entre 2005 y 2013. En la actualización reciente se encuentran dominios nuevos como 10. Cifrado, 15. Relaciones con suministradores. Además, se observa la separación en el estudio de objetivos de control y controles para el campo de

[1] (*) Muestra los dominios nuevos en ISO/IEC 27002:2013

comunicaciones y operaciones; por lo que a continuación se analiza los cambios entre sus objetivos de control. En la tabla 8 se evidencia que en la actualización del 2005 no existían los nuevos controles.

Tabla 8. Objetivos de control de nuevos dominios ISO/IEC 27002

ISO/IEC 27002:2013	ISO/IEC 27002:2005
10.1 Controles criptográficos.	No existe objetivo de control
15.1 Seguridad de la información en las relaciones con suministradores. 15.2 Gestión de la prestación del servicio por suministradores.	No existe objetivo de control

Fuente: (ISO27000.ES, 2013)

El estándar proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información. Cada organización debe considerar cuantos serán realmente los que se apliquen según las necesidades.

(ISO, s.f.) El proceso a seguir para la implementación del estándar es:

- ✓ Realizar análisis y gestión de riesgos.
- ✓ Seleccionar los objetivos de control
- ✓ Definir Políticas de seguridad de la información relacionadas con el negocio.
- ✓ Implementar y evidenciar el cumplimiento.

2.7 Esquema Gubernamental de Seguridad de la Información (EGSI)

Para el desarrollo del proyecto es importante enfocarse en el documento base que es el EGSI, conociendo los siguientes antecedentes:

El Esquema Gubernamental de Seguridad de la Información (EGSI) se basa en la Norma INEN ISO/IEC 27002 donde se disponen de controles prioritarios.

El Esquema Gubernamental de Seguridad de la Información surgió como respuesta a los avances en las tecnologías de la información y comunicaciones; así como de la necesidad del Gobierno por salvaguardar sus activos de información manejados en las instituciones públicas.

2.7.1 Secretaria Nacional de la Administración Pública (SNAP)

La Secretaría Nacional de la Administración Pública (SNAP) tiene como misión "Mejorar la eficiencia de los establecimientos del Estado Central a través de políticas y procesos que optimicen la calidad, la transparencia y la calidez del servicio público." (Secretaría Nacional de la Administración Pública, s.f.)

La SNAP creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, quien desarrolló el EGSI en base a la Norma NTE INEN-ISO/IEC 27002.

2.7.2 Acuerdo Ministerial 166

Con fecha 25 de septiembre del 2013, la Secretaria Nacional de Administración Pública mediante este Acuerdo N° 166 (SNAP, 2013) dispone:

Artículo 1.- Las entidades que dependen de la Función Ejecutiva el uso necesario de las Normas NTE INEN-ISO/IEC 27000 para la Gestión de seguridad de la información.

Artículo 2.- Las entidades de la Administración Pública implementará en un plazo de dieciocho (18) meses el Esquema Gubernamental de la Seguridad de la Información (EGSI) a excepción de las disposiciones marcadas como prioritarias, las cuales se implementarán en un plazo de seis (6) meses desde la emisión del presente Acuerdo.

El desarrollo del EGSI se aplicará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de conocimiento en gestión de Seguridad de la Información.

Artículo 3.- Las entidades conformarán un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI.

En base a lo expuesto, el documento presenta algunas disposiciones de manera general para el debido cumplimiento del EGSI.

- Revisar habitualmente el EGSI en base a las sugerencias de la SNAP.
- Cualquier propuesta para incluir controles o directrices adicionales, se debe comunicar a la Secretaría antes de aplicar los cambios.
- Justificar las excepciones de manera técnica y comunicarlas a la misma Secretaría.

2.7.3 Contenido del EGSI

El EGSI está basado en la Norma INEN ISO/IEC 27002:2005 y enmarca prioridades en algunos objetivos de acuerdo a la gestión de la Seguridad de la Información.

El resumen contiene: (SNAP, 2013)

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de los activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de Sistemas de Información

- Gestión de los Incidentes de la Seguridad de la Información
- Gestión de la continuidad del negocio
- Cumplimiento

El Esquema presentan 715 controles distribuidos en 11 dominios, 115 son considerados prioritarios, identificados a través de un asterisco en el documento oficial. El resumen por dominios se muestra en la tabla 9:

Tabla 9. Capítulos y sus controles en el EGSI

CAPÍTULOS	N° DIRECTRICES	N° DIRECTRICES PRIORITARIAS
Política de Seguridad de la Información	3	2
Organización de la Seguridad de la Información	50	10
Gestión de los activos	47	20
Seguridad de los recursos humanos	25	3
Seguridad física y del entorno	61	12
Gestión de comunicaciones y operaciones	173	27
Control de acceso	106	37
Adquisición, desarrollo y mantenimiento de Sistemas de Información	138	2
Gestión de los Incidentes de la Seguridad de la Información	20	2
Gestión de la continuidad del negocio	30	0
Cumplimiento	62	0
TOTAL	**715**	**115**

Fuente: (SNAP, 2013)

Para identificar las secciones a ser estudiadas en la investigación, el EGSI desglosa los capítulos y sus ítems prioritarios a los que se enfoca cada una, según el objetivo de aplicación, y se detalla a continuación:

2.7.3.1 Política de seguridad de la información.

2.7.3.1.1 Documento de la Política de Seguridad de la Información.

El documento de la Política se Seguridad de la Información debería enunciar el compromiso de la Gerencia de la siguiente manera:

a) Definición de la seguridad de información, objetivos, alcances e importancia.

b) Intención de la Gerencia, objetivos y principios de seguridad de información.

c) Marco referencial del EGSI para establecer objetivos de control y controles.

d) Explicación de las políticas, estándares y requerimientos acorde a la seguridad.

e) Definición de responsabilidades para la gestión de la seguridad incluyendo reportes de incidentes.

2.7.3.1.2 Revisión de la Política de seguridad de la Información.

La Norma propone que La Política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar el uso continuo

2.7.3.2 Organización de la seguridad de la información.

2.7.3.2.1 Compromiso de la máxima autoridad de la institución con la Seguridad de la Información.

La Gerencia debería apoyar activamente dentro de la organización con compromiso y conocimiento de responsabilidades de la Seguridad de la Información. Los aspectos fundamentales son:

a) Realizar el seguimiento de la puesta en marcha de las normas de este documento.

b) Disponer la difusión, capacitación y sensibilización del contenido de este documento.

c) Conformar oficialmente el Comité de Gestión de la Seguridad de la información de la institución (CGSI) y designar a los integrantes, donde se involucrará la

participación y cooperación de los cargos directivos de la institución. Se deberán llevar registros y actas de las reuniones.

2.7.3.2.2 Coordinación de la Gestión, de la Seguridad de la Información

Las actividades deberían ser coordinadas por los representantes de las áreas, designar un oficial de la Seguridad y un responsable de la seguridad quien identificará el incumplimiento, efectividad de los controles y hará las recomendaciones para responder a incidentes identificados.

2.7.3.2.3 Acuerdos de confidencialidad

Los acuerdos de confidencialidad implican los requisitos para proteger la información confidencial. Se debe considerar los siguientes:

a) Definir la información a proteger

b) Acciones cuando el acuerdo se termina

c) Responsabilidades y acciones para evitar divulgación.

d) Precisar la propiedad de la información.

e) Derecho de monitoreo de actividades.

f) Acciones en caso de incumplimiento.

2.7.3.3 Gestión de activos de información

2.7.3.3.1 Responsabilidad por los activos

Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos; para el caso del EGSI se considera como prioritarios: Inventariar los activos de hardware, de soporte Software, de soporte de redes.

2.7.3.3.2 Uso aceptable de activos

Las reglas para el uso adecuado de la información y de los activos asociados deben ser identificados, documentados e implementados, prioritariamente de:

- ✓ Reglamentación del uso de correo electrónico institucional.
- ✓ Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios.
- ✓ Reglamentar el uso de los sistemas de video-Conferencia**.**

2.7.3.3.3 Directrices de clasificación de la información

Implica clasificar la información como en función de su valor, requisitos legales, sensibilidad y criticidad para la organización.

2.7.3.4 Seguridad de los recursos humanos

2.7.3.4.1 Funciones y responsabilidades

Las funciones y responsabilidades de empleados deben ser definidas y documentadas según lo establecerá la Política, así:

a) Verificar el certificado de antecedentes penales y revisar la información entregada del candidato para el empleo

b) Actuar acorde con las Políticas de la Seguridad de la Información de la organización.

c) Ejecutar actividades con responsabilidad.

d) Entregar formalmente informes de eventos de seguridad o riesgos de seguridad.

2.7.3.4.2 Responsabilidades de la dirección a cargo del funcionario

Las responsabilidades de la dirección incluyen el garantizar que los empleados y usuarios sigan el proceso de:

a) Estar adecuadamente informados sobre las funciones y responsabilidades de la Seguridad de la Información antes de otorgar accesos.

b) Lograr un grado de concientización sobre la seguridad de la información correspondiente a las funciones y responsabilidades.

2.7.3.5 Seguridad física y del entorno

La información importante para la institución debe ser ubicada en áreas seguras, protegidas con controles adecuados.

2.7.3.5.1 Perímetro de la seguridad física

Para definir la seguridad física se deberían considerar:

a) Definición de perímetros de seguridad.

b) La estructura física debería ser robusta; con paredes sólidas y puertas externas con protección adecuada.

c) Se debe establecer un área de recepción con personal para controlar acceso al lugar.

2.7.3.5.2 Controles de acceso físico

Se debe tomar en cuenta que:

a) Registrar la fecha y hora de entrada y salida de visitantes a áreas restringidas.

b) Exigir a los empleados, contratistas y usuarios el uso de identificación y notificar en caso de no tenerla.

c) Los derechos de acceso a áreas seguras se deben revisar y actualizar con regularidad.

2.7.3.5.3 Seguridad de oficinas, recintos e instalaciones

Es necesario recomendar algunas directrices:

a) Conocer los reglamentos y normas pertinentes a seguridad de la información.

b) Se debe proteger las instalaciones claves de tal manera que se evite el acceso al público.

c) Ubicar impresoras, copiadoras en áreas protegidas.

2.7.3.5.4 Protección contra amenazas externas y ambientales

Las recomendaciones para evitar daños como incendios, explosión, o desastres naturales o artificiales son:

a) Realizar mantenimiento de las instalaciones eléctricas y UPS.

b) Realizar mantenimientos en los sistemas de climatización y ductos de ventilación.

c) Los materiales inflamables se deben almacenar a una distancia prudente del área de seguridad.

2.7.3.5.5 Trabajo en áreas seguras

Se debe considerar que:

No permitir equipos de grabación, cámaras, equipos de video y audio, dispositivos móviles, etc., a menos de que estén autorizados.

2.7.3.5.6 Áreas de carga, despacho y acceso público

Se recomienda:

a) Permitir el acceso al área de despacho y carga, únicamente al personal identificado y autorizado.

b) El material que llega se debe registrar de acuerdo con los procedimientos de gestión de activos.

2.7.3.5.7 Ubicación y protección de los equipos

Se recomienda considerar las directrices siguientes:

a) Establecer normas para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información.

b) Es conveniente monitorear las condiciones ambientales que podrían afectar al procesamiento de información.

2.7.3.5.8 Seguridad del cableado

Se recomienda tener en cuenta las siguientes directrices:

a) Se debe utilizar rótulos de equipo y cables identificables para minimizar errores en las conexiones.

b) Disponer de documentación, planos y la distribución de conexiones de: datos locales/remotas, voz, eléctricas polarizadas; para reducir la posibilidad de errores.

2.7.3.5.9 Mantenimiento de equipos

Se recomienda considerar:

a) Solo personal autorizado debe realizar las reparaciones y mantenimiento de equipos.

b) Lleva registros de las fallas y el mantenimiento preventivo y correctivo.

2.7.3.5.10 Retiro de los equipos

Es importante considerar que:

a) Los equipos, la información y software no se debería retirar sin autorización previa.
b) Se establezca límites de tiempo para el retiro de equipos y verificar el cumplimiento del proceso.
c) Registrar que el equipo es retirado

2.7.3.6 Gestión de las comunicaciones y operaciones

Se establece las responsabilidades y procedimientos para la gestión y operación de todos los servicios de procesamiento de información.

2.7.3.6.1 Documentación de los procedimientos de Operación

Los procedimientos de operación deberían especificarse detalladamente incluyendo:

a) Procesamiento y manejo de información
b) Copias de respaldo
c) Instrucciones para el manejo de errores incluyendo restricciones al uso de los sistemas.
d) Contactos de soporte en caso de dificultades técnicas u operativas.
e) Procedimientos para el reinicio y recuperación de los sistemas en caso de fallas.
f) Gestión de registros de auditoria.

2.7.3.6.2 Prestación de servicios

La prestación de servicios debería incluir acuerdos sobre disposiciones de seguridad del servicio y aspectos de gestión. Es importante planificar las transiciones necesarias y garantizar que la seguridad se mantiene durante todo el periodo.

2.7.3.6.3 Monitoreo y revisión de los servicios por terceros.

El monitoreo y la revisión de los servicios por terceros deberían garantizar el cumplimiento de los términos y condiciones de la seguridad de la información. La organización debe garantizar que el tercero asigne responsabilidades para verificar el cumplimiento de los acuerdos. Es fundamental que se presenten reportes y registros con regularidad, así como que las auditorias se lleven a cabo con intervalos determinados.

2.7.3.6.4 Gestión de la capacidad

Se recomienda monitorear y adaptar el sistema para garantizar y mejorar la capacidad y la eficacia de los sistemas. En las proyecciones de los requisitos de capacidad futura se deberían considerar los requisitos del sistema, así como las tendencias actuales y proyectarlas en la capacidad de procesamiento de información de la organización.

2.7.3.6.5 Controles contra código malicioso

La protección contra códigos maliciosos se debería basar en software de detección y reparación de códigos maliciosos, acceso apropiado al sistema y controles en la gestión de cambios. Se recomienda considerar las siguientes directrices:

a) Establecer una política formal que prohíba el uso de software no autorizado.
b) Establecer una política formal para la protección contra los riesgos ligados con la obtención de archivos y software, indicando las medidas de protección que se deberían tomar.
c) Llevar a cabo revisiones regulares del software y del contenido de los sistemas que dan soporte a los procesos; se debería investigar la presencia de archivos no aprobados o modificaciones no autorizadas.
d) Instalación y actualización del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios.

e) Definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos en los sistemas.

2.7.3.6.6 Respaldo de la Información

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios, se recomienda considerar los siguientes elementos:

a) Identificar a los responsables del área de Tecnologías de la información, Oficial de Seguridad de la Información, quienes determinarán los procedimientos para el resguardo y contención de la información.
b) Definir el nivel necesario para la información de respaldo.
c) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.
d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.
e) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias.

2.7.3.6.7 Control de las redes

Se debería implementar controles que garanticen la Seguridad de la Información en las redes y la protección de los servicios conectados contra el acceso no autorizado. Es conveniente tener en cuenta los siguientes elementos:

a) La responsabilidad operativa de las redes debería estar separada de las operaciones de computador, según sea el caso.

b) Establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.

c) Especificar controles especiales para mantener la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas.

d) Se deberían aplicar el registro y el monitoreo adecuados para permitir y registrar las acciones de seguridad pertinentes.

e) Coordinar las actividades de gestión para optimizar el servicio para la organización y para garantizar que los controles se aplican en toda la infraestructura del procesamiento de información.

2.7.3.6.8 Seguridad de los Servicios de la Red

Se debería determinar y monitorear periódicamente la capacidad del proveedor del servicio de red para gestionar los servicios de forma segura. La organización debería garantizar que los proveedores de servicios de red implementan estas medidas.

2.7.3.6.9 Políticas y Procedimientos para el Intercambio de Información

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

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

b) Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas.

c) Procedimientos para proteger la información electrónica sensible comunicada en forma de adjunto.

d) No dejar información sensible en los dispositivos de impresión como copiadoras, impresoras y máquinas de facsímil.

e) Controles y restricciones asociados con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas.

f) Recordar al personal que deberían tomar precauciones adecuadas como no revelar información sensible.

2.7.3.6.10 Registro de Auditorías

Los registros para auditoría deberían incluir, cuando corresponda.

a) Identificación de usuario.

b) Fecha, hora y detalles de los eventos clave (registro de inicio y registro de cierre).

c) Identidad o ubicación de la terminal.

d) Registros de los intentos aceptados y rechazados de acceso al sistema.

e) Registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos.

f) Cambios en la configuración del sistema.

g) Uso de las utilidades y aplicaciones del sistema.

h) Archivos a los que se ha tenido acceso y tipo de acceso.

i) Direcciones y protocolo de red.

j) Alarmas originadas por el sistema de control de acceso.

k) Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión.

2.7.3.6.11 Monitoreo del Uso del Sistema

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado.

b) Todas las operaciones privilegiadas.

c) Intentos de acceso no autorizado.

d) Alertas o fallas del sistema.

e) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

2.7.3.6.12 Registros del Administrador y del Operador

Se deberían registrar las actividades tanto del operador como del administrador del sistema. Los registros deberían incluir:

a) La hora en que ocurrió el evento.

b) Información sobre el evento o la falla.

c) Qué administrador estuvo involucrado.

d) Cuáles procesos estuvieron implicados.

2.7.3.6.13 Registro de Fallas

Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación. Deberían existir reglas claras para el manejo de las fallas reportadas, incluyendo:

a) Revisión de los registros de fallas para garantizar que éstas se han resuelto satisfactoriamente.

b) Revisión de las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.

2.7.3.7 Control de accesos

Se deberían establecer procedimientos para controlar el acceso a los sistemas y servicios de información, éstos deberían comprender desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debería poner atención especial con los usuarios con capacidad para modificar estos controles.

2.7.3.7.1 Gestión de Contraseñas para Usuarios

La asignación de contraseñas se debería controlar a través de un proceso formal de gestión. El proceso debería incluir los siguientes requisitos:

a) Se debe 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 éste.

b) Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.

c) Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, nueva.

d) 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.

e) Las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables.

f) Las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.

2.7.3.7.2 Uso de Contraseñas

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

a) Mantener la confidencialidad de las contraseñas.

b) Evitar conservar registros de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

c) Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.

d) Seleccionar contraseñas de calidad (fáciles de recordar, con caracteres especiales, difíciles de adivinar, no tengan caracteres idénticos consecutivos).

e) Cambiar las contraseñas temporales en el primer registro de inicio.

f) No compartir las contraseñas de usuarios individuales.

2.7.3.7.3 Equipo de Usuario Desatendido

Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

a) Terminar las sesiones cuando finalice el trabajo.

b) Realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión.

c) Cuando no están en uso, asegurar los terminales contra el uso no autorizado mediante una clave de bloqueo o una contraseña.

2.7.3.7.4 Política de Escritorio Despejado y de Pantalla Despejada

En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información, los riesgos correspondientes de la organización. Es recomendable tener presentes las siguientes directrices:

a) Las sesiones de los terminales se deberían proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, para que se activen automáticamente después de un lapso de inactividad.

b) Se deberían proteger los puntos de entrada y salida de correo.

c) Es conveniente evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción.

d) Los documentos que contengan información sensible se deberían retirar inmediatamente de las impresoras.

2.7.3.7.5 Identificación de los Equipos en las Redes

En la identificación automática de los equipos se debería considerar un medio para autenticar conexiones de equipos y ubicaciones específicas. Un identificador en el equipo se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores deberían indicar con claridad a qué red está permitido conectar el equipo, si existe más de una red y si estas tienen sensibilidad diferente.

2.7.3.7.6 Protección de los Puertos de Configuración y Diagnóstico Remoto

Los controles para el acceso a los puertos de diagnóstico y configuración, incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/software que requiere el acceso.

2.7.3.7.7 Separación en las Redes

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemas de información. Un método para el control en las redes grandes es dividirlas en dominios lógicos de red separados, cada uno protegido por un perímetro de seguridad. Se puede implementar un perímetro de red instalando una puerta de enlace (Gateway) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace (Gateway) se debería configurar para filtrar el tráfico entre estos dominios y para bloquear el acceso no autorizado, este tipo de puerta de enlace es lo que se conoce comúnmente como barrera de fuego (firewall).

2.7.3.7.8 Procedimiento de Registro de Inicio Seguro

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por ello, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.

b) Mostrar una advertencia de notificación general indicando que solo deberían tener acceso al computador los usuarios autorizados.

c) No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.

d) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada.

e) Limitar la cantidad de intentos permitidos de registro de inicio.

f) Limitar el tiempo máximo permitido para el procedimiento de registro de inicio.

g) Mostrar información de fecha y hora de registro exitoso y el detalle de intentos fallidos.

h) No mostrar la contraseña que se introduce o esconder los caracteres mediante símbolos.

2.7.3.7.9 Identificación y Autenticación de Usuarios

Todos los usuarios deberían tener un identificador único (ID del usuario) para su uso personal, y se debería elegir una técnica de autenticación para comprobar la identidad de un usuario. Los identificadores de usuario (ID) se deberían utilizar para rastrear las actividades de la persona responsable.

2.7.3.8 Adquisición, desarrollo y mantenimiento de SI

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, servicios y aplicaciones desarrolladas para usuarios. Se deberían identificar

los requisitos de seguridad antes del desarrollo y/o la implementación de los sistemas de información.

2.7.3.8.1 Análisis y Especificación de los Requisitos de Seguridad

Implica la definición de:

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

2.7.3.9 Gestión de incidentes en la seguridad de la información

Es conveniente establecer el reporte formal del evento y los procedimientos. Se les debería exigir a todos los miembros de una empresa que reporten todos los eventos de Seguridad de la Información y las debilidades tan pronto sea posible al punto de contacto designado.

2.7.3.9.1 Reporte sobre los Eventos de Seguridad de la Información

Todos los empleados, contratistas y usuarios deberían tener conciencia de su responsabilidad para reportar todos los eventos de Seguridad de la Información lo más pronto posible a través de los canales de gestión apropiados y con el procedimiento definido. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de Seguridad de la Información reciben notificación de los resultados después que se ha tratado y solucionado el problema.

b) Formatos para el reporte de los eventos de Seguridad de la Información para soportar la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de Seguridad de la Información.

c) Referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de seguridad.

2.7.3.10 Gestión de continuidad del negocio

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la pérdida de activos de información en la organización. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la Seguridad de la Información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, materiales, transporte e instalaciones. Este dominio no contiene ítems prioritarios.

2.7.3.11 Cumplimiento

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad estatutarios, reglamentarios y contractuales. Se debería buscar asesoría sobre estos requisitos. Este dominio no contiene ítems prioritarios.

Capítulo III

Situación actual

El presente capítulo explica el diagnóstico inicial de la Institución e identificación de controles para contribuir a la Política de Seguridad en el campo de Gestión de comunicaciones y operaciones.

Inicialmente, se recopila información básica de la Institución a través de la fuente web que está abierta al público. Continuamente, se realizó una encuesta al personal encargado de la Seguridad de la Información en la Gerencia de Tecnologías para identificar el cumplimiento de los controles del ESGI, y finalmente se realizó una evaluación de riesgos de la empresa aplicada al Responsable de Seguridad del área de tecnologías de la información, para determinar la necesidad de políticas de seguridad correspondiente al capítulo de la propuesta.

3.1 Antecedentes

Según el Acuerdo 166 de la Secretaría de Administración Pública, es responsabilidad de empresas como la Empresa Pública YACHAY aplicar las políticas ligadas a la seguridad de los sistemas de información, el ambiente tecnológico, seguridad física de los equipos y recurso humano, aplicando el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la norma NTE INEN-ISO/IEC 27002 para la Gestión de Seguridad de la Información.

3.2 Empresa Pública Yachay

Las propuestas generadas en el país referente a la Matriz productiva, impulsaron a la creación de la empresa pública YACHAY, que viene ejerciendo una gestión eficiente con el manejo de la edificación de la Ciudad del Conocimiento Yachay, siendo la primera urbe planificada del país. Para llevar a cabo el proyecto de la Ciudad del Conocimiento Yachay, la dirección de la oficina matriz de la Empresa es N26-146 y La Niña, Av. Amazonas, Quito, Pichincha; y las oficinas de las áreas de Infraestructura, Fiscalización y Tecnológica están ubicadas en la Hacienda San Eloy y Sector Los bloques, Urcuquí, Imbabura. Una de las funciones de Yachay E. P. es la de generar instrumentos de apoyo a emprendedores, innovadores y científicos a través de pre incubadoras de empresas, incubadoras de empresas, hábitats tecnológicos (parque tecnológico), centro de transferencia de tecnología, centro de prototipos industriales y diversidad de áreas de negocios.

3.2.1 Misión

Desarrollar y gestionar la ciudad del conocimiento YACHAY bajo estándares internacionales integrando la actividad científica, académica y económica, impulsando la investigación, transferencia y desagregación de tecnología e innovación para contribuir al cambio de matriz productiva del país.

3.2.2 Visión

Ser una empresa referente en la región en el desarrollo y gestión de una ciudad del conocimiento con prioridad en la investigación, innovación y producción de conocimiento contribuyendo de esta manera a la riqueza del país y teniendo como base la economía del conocimiento.

3.2.3 Principios

En la Resolución N°. YACHAY-GG-2014-0022 se resuelve expedir el Código de Ética para la Empresa Pública Yachay. Los servidores de la Empresa desempeñarán sus competencias, funciones, atribuciones y actividades con los siguientes principios:

- ✓ Integridad
- ✓ Transparencia
- ✓ Responsabilidad
- ✓ Eficiencia y eficacia
- ✓ Superación Personal
- ✓ Liderazgo
- ✓ Calidad
- ✓ Vocación de servicio

3.2.4 Actividades que realiza la Empresa Pública Yachay.

La Entidad, dentro de sus funciones tiene la responsabilidad de generar instrumentos de apoyo a emprendedores, innovadores y científicos a través de pre incubadoras de empresas, incubadoras de empresas, hábitats tecnológicos (parque tecnológico), centro de transferencia de tecnología, centro de prototipos industriales y diversidad de áreas de negocios.

Para hacer posible el desarrollo de estas actividades, existen Gerencias encargadas de varios campos. Una de ellas es la Gerencia de Tecnologías, la misma que cuenta con las siguientes Direcciones: Telecomunicaciones, Energía y Automatización, Sistemas Informáticos, Soporte y Operaciones Tecnológicas.

En la ilustración 5 se expande el árbol institucional, como referencia para el ámbito de aplicación en tecnologías:

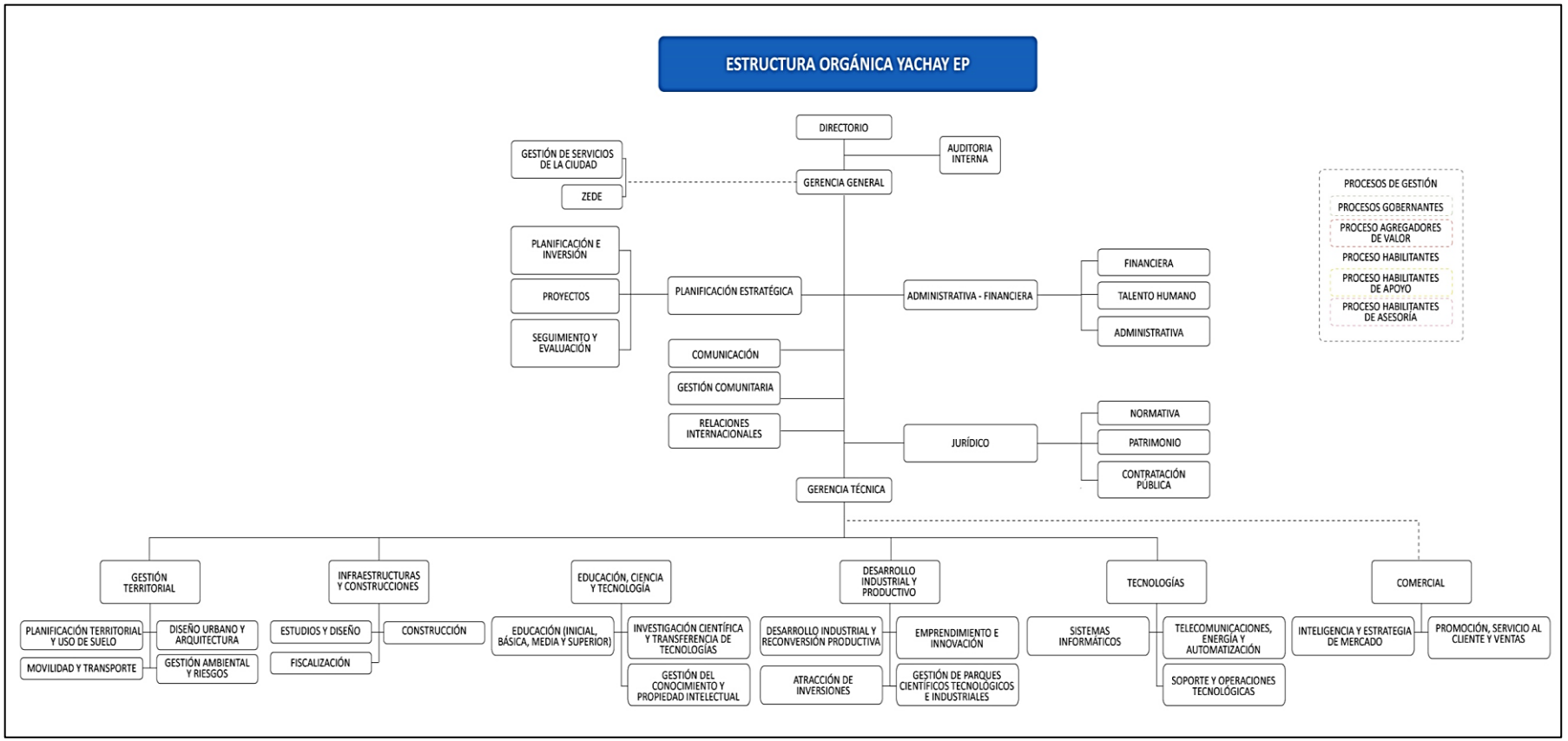

Ilustración 5. Estructura orgánica YACHAY E.P.
Fuente: yachay.gob.ec

3.2.5 Gerencia de Tecnologías

La Institución ha estado trabajando desde su creación con 3 direcciones a cargo de la Gerencia de Tecnologías como se muestra en la ilustración 6:

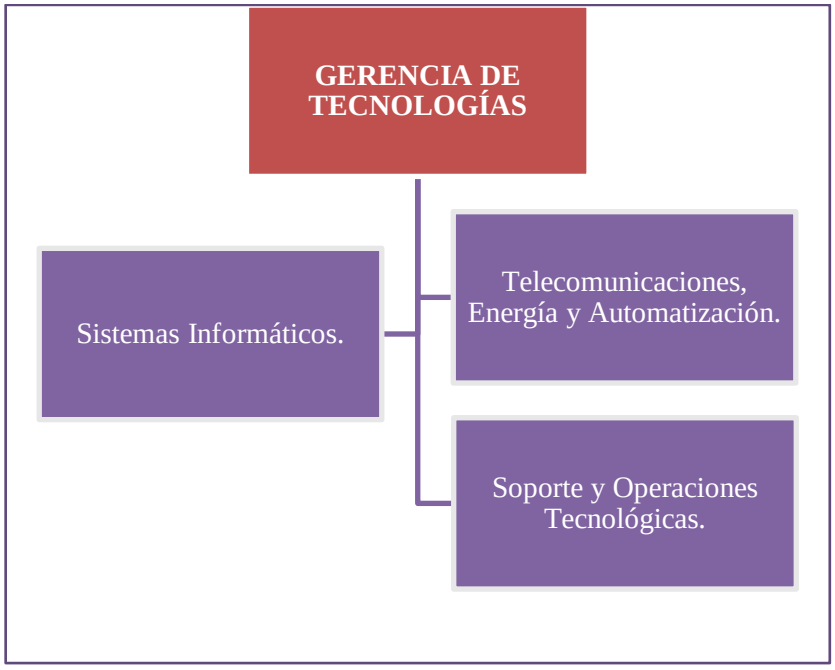

Ilustración 6. Direcciones de Gerencia de Tecnologías Yachay E. P.
Fuente: Organigrama Yachay E. P.

3.3 Población

La recolección de los datos se realizó en la Empresa Pública Yachay ubicada en la ciudad de Urcuquí. El presente proyecto se desarrolla en el ámbito de las tecnologías de la información, en consecuencia, la población está conformada por el equipo de Tecnologías de la entidad.

3.4 Muestra

Se aplica el muestreo no probabilístico, que es aquel para el que no se puede calcular la probabilidad de extracción de una determinada muestra. Este método busca seleccionar a individuos que tienen un conocimiento profundo del tema bajo estudio y se considera que la información aportada por esas personas es vital para la toma de decisiones.

Se consideró la aplicación de una encuesta al personal que trabajan en la Gerencia, quienes evidencian el progreso en el cumplimiento de los ítems del Esquema Gubernamental de Seguridad de la Información en la Gerencia de la Empresa Pública Yachay. Son 11 personas, por este motivo no se aplica técnica de muestreo y se aplica al total de la población.

3.4.1 Aplicación de cuestionario

Con la finalidad de obtener información, se elaboró un cuestionario (**Ver Anexo 3**) que hace referencia a los dominios del Esquema Gubernamental de Seguridad de la Información (EGSI) y fue aplicado al personal antes mencionado de las Direcciones de: soporte y operaciones tecnológicas; telecomunicaciones, energía y automatización; sistemas informáticos.

Se evalúan los 11 dominios que contiene el EGSI y son:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de los activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de los Incidentes de la Seguridad de la Información
- Gestión de la continuidad del negocio
- Cumplimiento

3.4.2 Análisis de resultados

DOMINIO 1: Políticas de seguridad

1. De los encuestados, el 45% de profesionales manifiesta desconocimiento de una Política de Seguridad de la Información aprobada, publicada y comunicada. El 55% hace referencia a un Manual de Políticas y Planes de Seguridad; como se presenta en la ilustración 7.

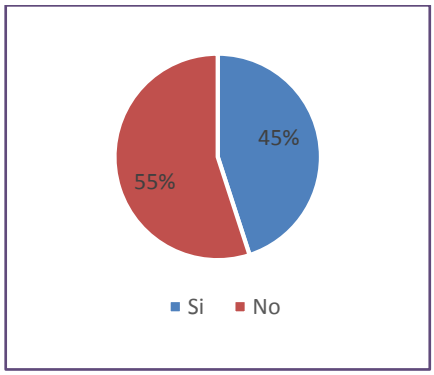

Ilustración 7. Pregunta 1 - Políticas de Seguridad
Fuente: Autor

DOMINIO 2: Organización de la Seguridad de la Información

2. El 97% de las respuestas afirma que existe la asignación y reconocimiento de responsabilidades por parte de los funcionarios de la Gerencia. Mientras, el 3% precisa que no existe una documentación detallada de los procesos de este ítem. El resultado de esta pregunta se muestra en la ilustración 8.

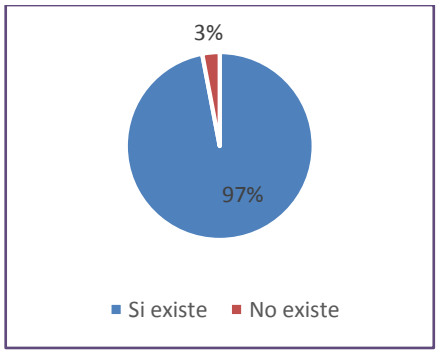

Ilustración 8. Pregunta 2 - Organización de la Seguridad de la Información
Fuente: Autor

DOMINIO 3: Gestión de activos.

3. Un 87% de los consultados indica que existe correcto funcionamiento de los activos y servicios. Un 13% manifiesta que no está a cargo de esas responsabilidades. El resultado se muestra en la ilustración 9.

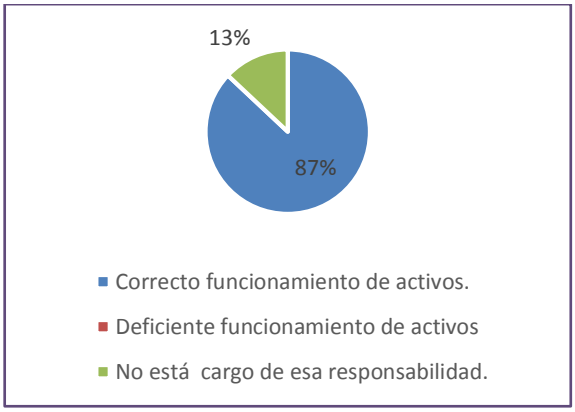

Ilustración 9. Pregunta 3 - Gestión de Activos
Fuente: Autor

DOMINIO 4: Seguridad ligada a los recursos humanos

4. Cuando una persona o proveedor finaliza su contrato, cambia sus funciones o responsabilidades; siempre se toma medidas de los accesos o privilegios asignados sean éstos, la eliminación de privilegios o el deshabilitar las cuentas de usuario. El resultado al 100% se presenta en la ilustración 10.

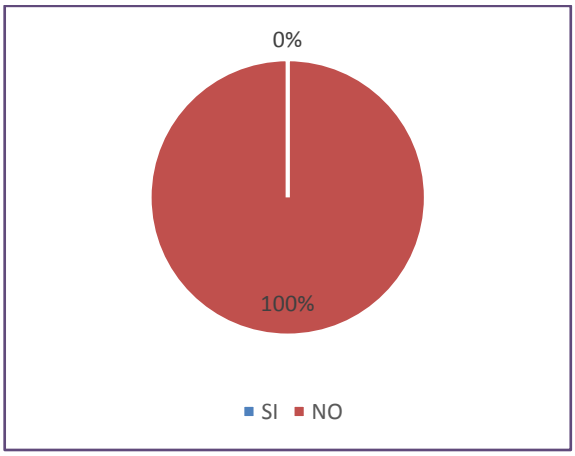

Ilustración 10. Pregunta 4 - Seguridad ligada a los recursos humanos
Fuente: Autor

DOMINIO 5: Seguridad física y del entorno

5. Existe el 40% que afirma que se documenta los procedimientos de operación, así mismo, otro 40% manifiesta que se documenta reportes, reuniones, incidentes de los proveedores, pruebas. Un 20% manifiesta el desconocimiento del tema. Todo el resultado se muestra en la ilustración 11.

Ilustración 11. Pregunta 5 - Seguridad física y del entorno
Fuente: Autor

DOMINIO 6: Gestión de comunicaciones y operaciones

6. El 92% de los encuestados afirmó que se realizan regularmente respaldos de seguridad de toda la información del negocio. El 8% indica que no conoce. El resultado se muestra en la ilustración 12.

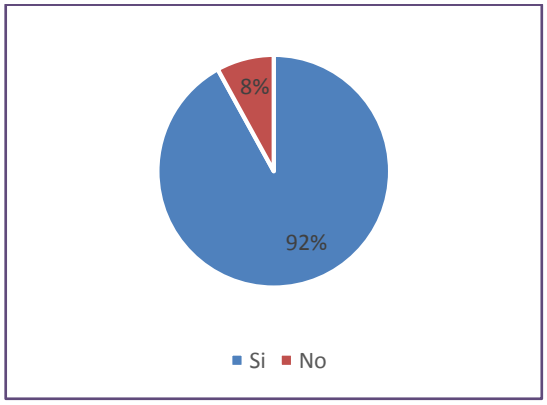

Ilustración 12. Pregunta 7 - Gestión de comunicaciones y operaciones
Fuente: Autor

DOMINIO 6: Gestión de comunicaciones y operaciones

7. Un 48% de profesionales manifiesta que existen acuerdos establecidos para el intercambio de información entre la organización y los proveedores. Un 52% enuncia que no existen políticas formales para proteger la información. El resultado se muestra en la ilustración 13.

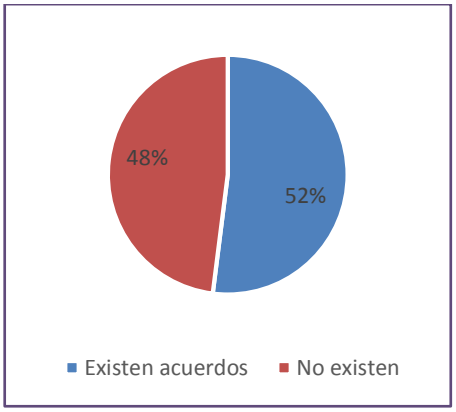

Ilustración 13. Pregunta 8 - Gestión de comunicaciones y operaciones
Fuente: Autor

DOMINIO 7: Control de accesos

8. El 85% de los encuestados afirma que se otorga el acceso a la información y a las funciones de red y sistema de aplicaciones solo al usuario determinado. El 13% indica que no conoce del tema, pues no es una de sus responsabilidades. EL 2% indica que se otorga privilegios a todos los usuarios. El resultado se muestra en la ilustración 14.

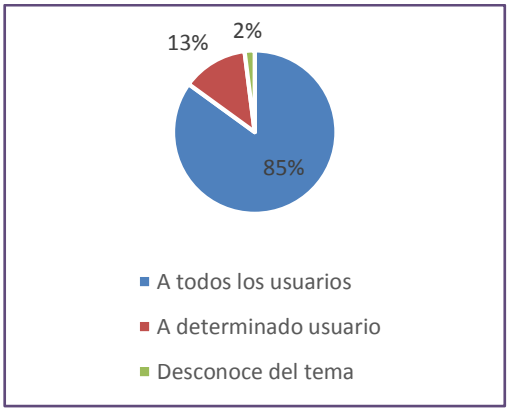

Ilustración 14. Pregunta 9 - Control de accesos
Fuente: Autor

DOMINIO 8: Adquisición, desarrollo y mantenimiento de sistemas

9. Los encuestados indican que en la institución se evidencian diferentes controles para garantizar la seguridad de los archivos del sistema, un 46% considera que existen procedimientos para controlar la instalación de software en sistemas operacionales; de la misma manera un 46% manifiesta que el administrador capacitado realiza las actualizaciones de librerías o aplicación de parches en el software determinado. Un 8% indica que se restringe el acceso al código fuente de los programas. Se muestra el resultado en la ilustración 15.

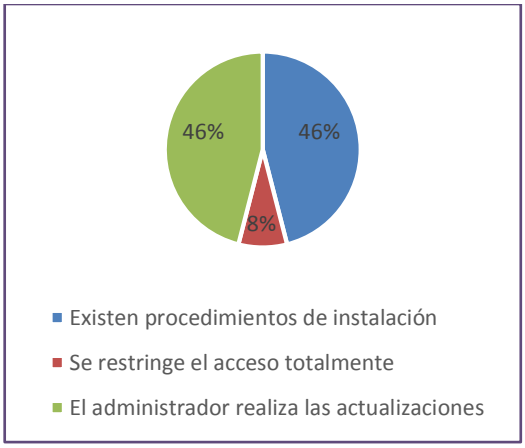

Ilustración 15. Pregunta 10 - Adquisición, desarrollo y mantenimiento de sistemas
Fuente: Autor

DOMINIO 9: Gestión de vulnerabilidades técnicas

10. El 86% indica que los eventos son reportados en el menor tiempo posible, el 14% indica que no hay reportes. Se muestra el resultado en la ilustración 16.

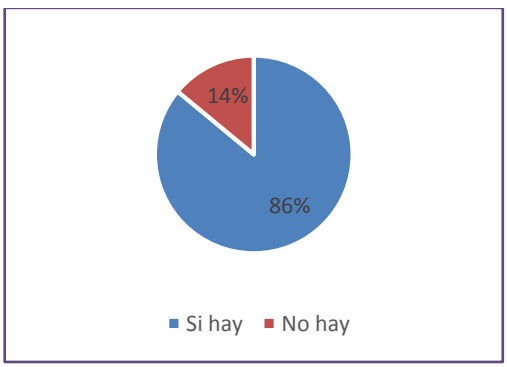

Ilustración 16. Pregunta 11 - Gestión de vulnerabilidades técnicas
Fuente: Autor

DOMINIO 11: Cumplimiento

11. El 38% de respuestas comprueba regularmente el cumplimiento de Normas de implementación de seguridad. El 62% manifiesta no conocer detalladamente el contenido de estándares implementados en la Gerencia. Se muestra el resultado en la ilustración 17.

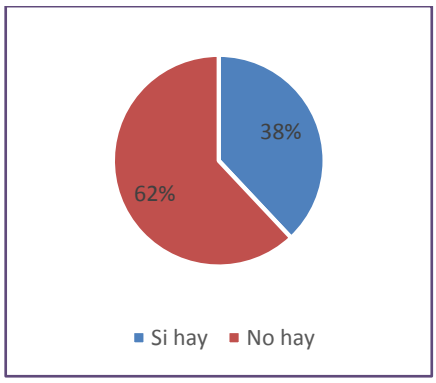

Ilustración 17. Pregunta 12 – Cumplimiento
Fuente: Autor

3.4.3 Resultados de tabulación.

Luego de realizar la tabulación de la encuesta aplicada, se identificó que los controles a considerar deben ser el de gestión de comunicaciones y operaciones puesto que evidencia mayor riesgo en los porcentajes obtenidos de esa sección. De esta manera, la Norma ISO/IEC 27002 y el EGSI proveen parámetros para plantear Políticas que se enfoquen en:

1. 1.Políticas de Seguridad de la Información.
2. 6. Gestión de las comunicaciones y operaciones

A continuación, una metodología de análisis de riesgos permitirá verificar los controles a desarrollar.

3.5 Análisis de Riesgos

Se provee las herramientas de las metodologías OCTAVE y MSAT. Inicialmente, se socializó con la gerencia de tecnologías de la empresa el proceso para ejecutar OCTAVE, sin embargo, las actividades que desarrollan los funcionarios no permitieron que se conforme un equipo de trabajo estable para desarrollarlo. Además, algunas políticas de privacidad de la información que tiene la institución, impidieron obtener varios datos.

La siguiente opción es la herramienta MSAT que al ser socializada con la empresa aceptó colaborar en su aplicación. La metodología sugiere ser trabajada con personal a cargo de la seguridad de la información; para el caso, el responsable de la seguridad en el área de tecnologías de la información es a su vez un funcionario de la Gerencia de Tecnologías, quien tiene amplio conocimiento de la infraestructura, aplicaciones, operaciones y personal. El cuestionario completo se encuentra en el anexo. **(Ver anexo 8).**

3.5.1 Evaluación de riesgos con MSAT

Mediante la evaluación con MSAT se puede determinar los riesgos a los que se enfrenta en entorno de TI de YACHAY E. P. y las medidas que se sugieren para combatirlos. El proceso detalla y analiza los resultados con el fin de proporcionar una guía para minimizar los riesgos encontrados.

MSAT considera las áreas de infraestructura, aplicaciones, operaciones, personal como se muestra en la ilustración 18:

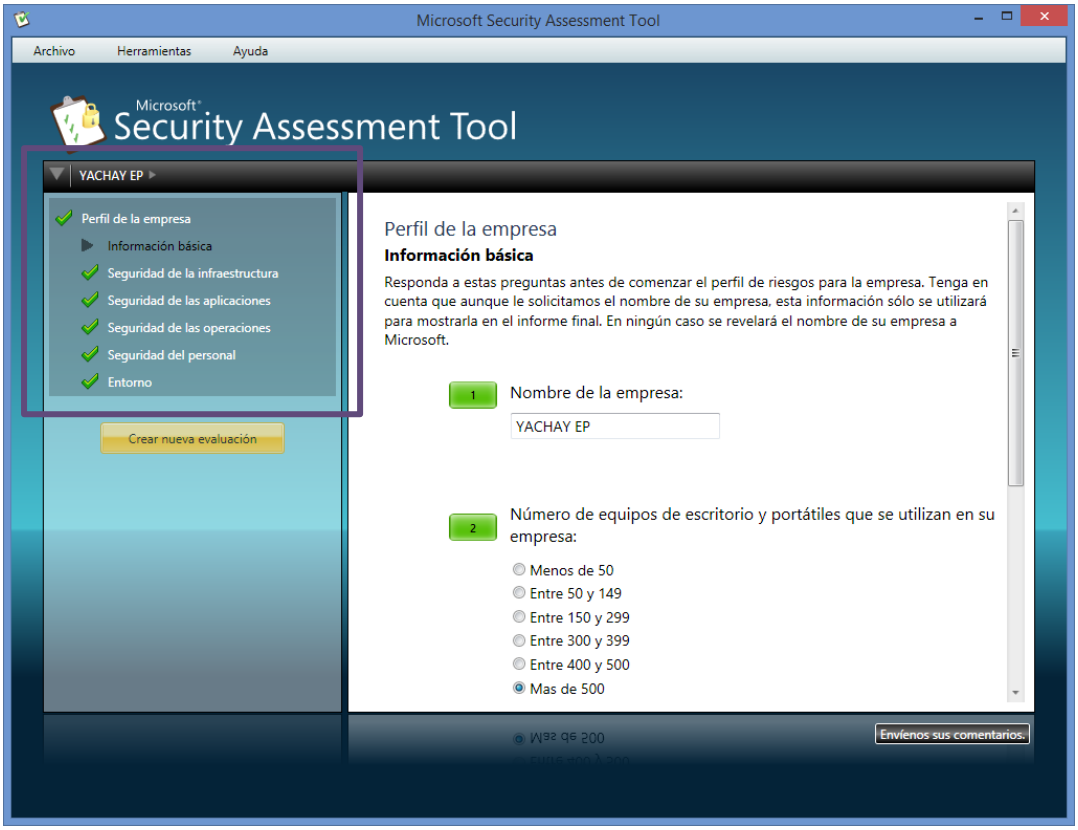

Ilustración 18. Interfaz de herramienta MSAT
Fuente: Herramienta MSAT

Se presenta una definición de los términos que se encuentran a lo largo del proceso:

- ✓ BRP (Business Risk Profile) es una medición del riesgo relacionado al modelo empresarial y al sector de la empresa.

- ✓ DiDI (Defense in Depth Index) es una medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una empresa. Se considera adecuado tener un BRP y un DiDI en el mismo nivel.

En la ilustración 19, el gráfico dividido en áreas de análisis, muestra las diferencias en el resultado de la defensa en profundidad.

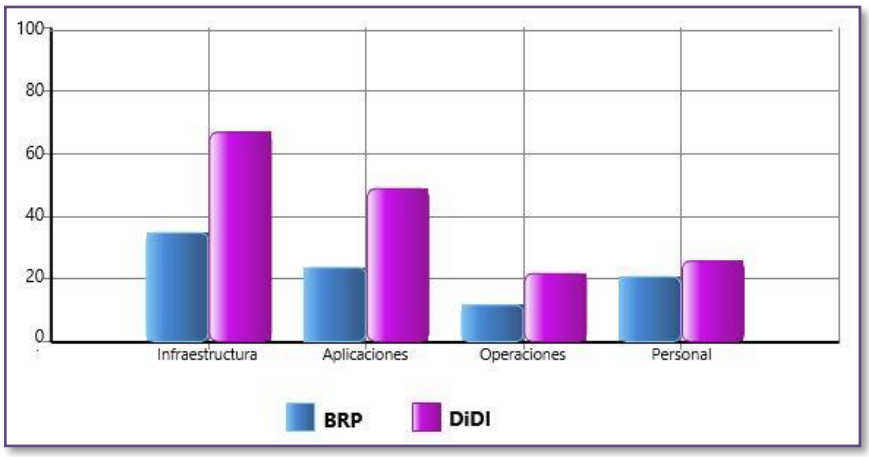

Ilustración 19. Evaluación de riesgos con MSAT
Fuente: Herramienta MSAT

Interpretación de gráfico

La puntuación del BRP va de 0 a 100. Una puntuación más alta significa un riesgo posible aumentado al que está expuesta la empresa en esta área de análisis. Es importante tener saber que una puntuación de 0 no es posible; dedicarse a una actividad comercial siempre implica un nivel de riesgo. También es importante comprender que hay riesgos comerciales que no se pueden mitigar directamente.

DiDI también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno donde han tomado más medidas para implementar estrategias de DiDI en el área de análisis específica. La puntuación DiDI no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno.

En principio, una puntuación baja del BRP y alta del DiDI parecería un buen resultado, pero no siempre es así. Está fuera del ámbito de la presente autoevaluación tener en cuenta todos los factores. Una disparidad significativa entre la puntuación del BRP y la del DiDI para un área de análisis específica significa que se recomienda una revisión del área. Cuando analiza los resultados, es importante tener en cuenta las puntuaciones individuales, tanto de BRP como de DiDI, y cómo se relacionan entre sí. Un entorno estable probablemente tendría como resultado puntuaciones iguales en todas las áreas. Disparidades entre las puntuaciones DiDI son un indicio de una estrategia general de seguridad concentrada en una sola técnica de mitigación. Si la estrategia de Seguridad no abarca el personal, los procesos ni la tecnología, el entorno estará expuesto a un mayor riesgo de ataque.

3.5.1.1 *Resultados de la evaluación con MSAT*

Una vez implementado la herramienta MSAT en el área de Tecnologías de la Información de Yachay E. P. se obtuvo los siguientes resultados respecto a la distribución de defensa de riesgos y la madurez de la seguridad de la empresa., como se muestra en la ilustración 20:

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Personal	🟢	🟡
Operaciones	🟢	🔴
Aplicaciones	🔴	🟢
Infraestructura	🔴	🟢

Ilustración 20. Evaluación de riesgos MSAT
Fuente: Herramienta MSAT

Leyenda		
	☒ Distribución pareja	☒ Optimizada
	☒ Disparidad leve	☒ Estándar
	☒ Disparidad significativa	☒ Básica

Todas las empresas deben esforzarse en alinear su nivel de madurez y estrategia de seguridad, en relación a los riesgos que conlleva su actividad comercial:

- ✓ **Básica:** Algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva.

- ✓ **Estándar:** Capas múltiples de defensa utilizadas para respaldar una estrategia definida.

- ✓ **Optimizada:** Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas.

3.5.1.2 *Medidas de defensa*

En base a las respuestas sobre la evaluación de riesgos la herramienta califica las medidas de defensa de la siguiente manera:

Leyenda

☒ Cumple las mejores prácticas recomendadas ☒ Necesita mejorar ☒ Carencias severas

A continuación, se muestran los resultados para cada área de análisis.

- ✓ Infraestructura
- ✓ Aplicaciones
- ✓ Operaciones
- ✓ Personal

3.5.1.2.1 Infraestructura

La seguridad de la infraestructura se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que se deben implantar, cómo se crean y utilizan los hosts y la gestión y el mantenimiento de la red. Un estudio de éste parámetro puede ayudar a mejorar significativamente la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos.

La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudar a mitigar el riesgo para la infraestructura enfocándose en las áreas de seguridad de infraestructura que pertenecen a esta sección; a su vez éstas tienen sub-secciones que son analizadas de acuerdo a los resultados.

Las secciones y subsecciones de esta área son:

- ✓ **Defensa del perímetro**
  - Cortafuegos
  - antivirus
  - acceso remoto
  - segmentación
- ✓ **Autentificación**
  - directivas de contraseñas
- ✓ **Gestión y control**
  - hosts de gestión
  - archivos de registro
- ✓ **Estación de trabajo**
  - Configuración de creación

Defensa de perímetro

Trata la seguridad del perímetro de la red, donde la red interna se conecta al exterior. Se encontraron riesgos en las subsecciones como se muestra en la tabla 10.

Tabla 10. Defensa del perímetro.

Subsecciones	
Reglas y filtros de cortafuegos	☒
Antivirus	☒
Antivirus – Equipos de escritorio	☒
Antivirus – Servidores	☒
Acceso remoto	☒
Segmentación	☒
Sistema de detección de intrusos (IDS)	☒
Inalámbrico	☒

Fuente: Herramienta MSAT

Resultados:

En la tabla 11 se indica los resultados de las respuestas en la herramienta MSAT para esta sección, con enfoque en las que muestran riesgos y están de color rojo en la tabla anterior.

Tabla 11. Resultados de la evaluación de la defensa del perímetro.

Acceso remoto	✓ Existen empleados y/o socios que se conectan remotamente a la red interna y ha dado el paso importante de utilizar tecnología VPN para permitir el acceso. ✓ Sin embargo, no ha utilizado autenticación multifactor como un segundo escudo protector.
Segmentación	✓ Los servicios ofrecidos en Internet se alojan en la red de su empresa.

	✓ La red presenta más de un segmento; actualmente se considera importante mantener los servicios extranet de clientes y socios en sus segmentos de red propios.
Sistema de detección de intrusos (IDS)	✓ No se utiliza ningún hardware ni software de detección de intrusiones.
Inalámbrico	✓ Existe la opción de conexión inalámbrica a la red. Además, se ha modificado el SSID predeterminado del punto de acceso. ✓ No se ha desactivado la difusión del SSID en el punto de acceso, no se utiliza el cifrado WEP en el entorno inalámbrico; únicamente el cifrado WPA en el entorno inalámbrico. No se utiliza la restricción por MAC en el entorno inalámbrico.

Fuente: Herramienta MSAT

Autenticación

Los procedimientos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no acceden sin autorización a la red mediante ataques locales o remotos; contribuye al acceso a los recursos en base a una autorización.

Las subsecciones donde se encontraron riesgos se muestran en la tabla 12.

Tabla 12. Riesgos de autenticación.

Subsecciones	
Usuarios administrativos	☒
Usuarios internos	☒
Usuarios de acceso remoto	☒
Directivas de contraseñas	☒
Directivas de contraseñas – cuenta administrador	☒
Directivas de contraseñas – cuenta usuario	☒
Directivas de contraseñas – cuenta de acceso remoto	☒
Cuentas inactivas	☒

Fuente: Herramienta MSAT

Resultados:

En la tabla 13 se indica los resultados de las respuestas en la herramienta MSAT para esta sección, con enfoque en las que muestran riesgos y se encuentran de color rojo en la tabla anterior.

Tabla 13. Resultado de los riesgos de autenticación encontrados.

Usuarios administrativos	✓ Los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo.

	✓ No se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas ni de los dispositivos del entorno. ✓ Actualmente, sólo se requiere autenticación de contraseñas complejas para el acceso administrativo a dispositivos y hosts.
Usuarios de acceso remoto	✓ Los empleados y terceros usuarios pueden conectarse a la red de forma remota, no los contratistas. ✓ Actualmente se requiere sólo autenticación de contraseñas complejas para el acceso remoto a la red interna y a los hosts.

Fuente: Herramienta MSAT

En la tabla 13 se presentan los análisis a las respuestas que representan riesgo para la entidad. Los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo, lo que puede provocar que usuarios inexpertos configuren las máquinas de forma errónea, dando paso a huecos de seguridad. Actualmente utiliza sólo autenticación de contraseñas complejas para el acceso remoto a la red interna y a los hosts. Una contraseña se considera compleja si cumple los siguientes criterios:

- ✓ Alfanumérica
- ✓ Incluye mayúsculas y minúsculas
- ✓ Al menos un carácter especial
- ✓ Longitud mínima de 8 caracteres

Gestión y control

La gestión adecuada es vital para mantener y analizar los entornos de información. Se considera aún más importante después de un ataque cuando es necesario un análisis de incidentes. En esta sección, las sub-secciones que contienen riesgos se muestran en la tabla 14.

Tabla 14. Riesgos de gestión y control.

Subsecciones	
Informes sobre incidentes y respuesta	☒
Creación segura	☒
Seguridad física	☒

Fuente: Herramienta MSAT

Resultados:

La tabla 15 presenta la sub-sección crítica con sus respectivos resultados.

Tabla 15. Resultados de la evaluación de riesgos de gestión y control.

Creación segura	✓ No se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno. ✓ Todos los procesos de creación de los dispositivos de infraestructura, de servidores y estaciones de trabajo están documentados. ✓ El software de acceso remoto del cliente está instalado en las estaciones de trabajo que se conectan remotamente a la red interna.

Fuente: Herramienta MSAT

Los resultados indican que la empresa no utiliza ningún software de cifrado de discos en el entorno. Por otro lado, si utiliza tarjetas de identificación para empleados y visitantes, además de controles de entrada. Una manera de proteger los portátiles es utilizando un protector de pantalla protegido por contraseña en el entorno.

3.5.1.2.2 Aplicaciones

El área de aplicaciones cuenta con las secciones y subsecciones siguientes:

- ✓ **Implementación y uso**
  - equilibrio de carga
  - clústeres
  - aplicación y recuperación
  - vulnerabilidades
- ✓ **Diseño de aplicaciones**
  - Autenticación
  - directivas de contraseñas
  - registro
  - validación
  - metodología de desarrollo de seguridad de software
- ✓ **Almacenamiento y comunicación de datos**
  - cifrado

Implementación y uso

Al implementar aplicaciones críticas para la empresa, hay que asegurar la seguridad y la disponibilidad de esas aplicaciones y de los servidores. El mantenimiento continuo es imprescindible para ayudarle a asegurarse de que los errores de seguridad se corrigen y minimizar las vulnerabilidades. (MSAT, 2016).

En la tabla 16 se presenta las sub-secciones con riesgos de esta sección.

Tabla 16. Subsección de implementación y uso.

Subsecciones	
Equilibrio de carga	☒
Clústeres	☒
Aplicación y recuperación de datos	☒
Fabricante de software independiente (ISV)	☒
Desarrollado internamente	☒
Vulnerabilidades	☒

Fuente: Herramienta MSAT

Resultados:

La tabla 17 presenta la sub-sección crítica con sus respectivos resultados.

Tabla 17. Resultados de la evaluación de implementación y uso.

Aplicación y recuperación de datos	En la empresa no se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.
Fabricante de software independiente (ISV)	En la empresa, otros fabricantes no han desarrollado ninguna de las aplicaciones principales del entorno.

Desarrollado internamente	La empresa utiliza macros personalizadas en las aplicaciones ofimáticas. El equipo interno de desarrollo de software suele ofrecer revisiones y actualizaciones de seguridad.
Vulnerabilidades	Actualmente no se conocen vulnerabilidades para la seguridad en ninguna aplicación del entorno.

Fuente: Herramienta MSAT

La empresa cuenta con equilibradores de carga y clústeres en su entorno; de esta manera la empresa considera que se garantiza la disponibilidad de los servicios para mantener activos los procesos de negocios.

No se realiza pruebas periódicas de recuperación de aplicaciones y datos, esto puede afectar al tiempo de respuesta ante incidentes que necesiten actividades y procedimientos de recuperación.

Se utiliza macros personalizadas en las aplicaciones ofimáticas y debido a ello las configuraciones se seguridad de office se reclasifican en un nivel inferior, las aplicaciones ofimáticas quedan expuestas a documentos peligrosos.

Diseño de aplicaciones

Un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, la autorización, y la validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad para acceder a información confidencial. (MSAT, 2016)

La tabla 18 muestra las subsecciones donde se encontraron riesgos.

Tabla 18. Diseño de aplicaciones.

Subsecciones	
Autenticación	☒
Directivas de contraseñas	☒
Autorización y control de acceso	☒
Registro	☒
Validación de datos de entrada	☒
Metodología de desarrollo de seguridad de software	☒

Fuente: Herramienta MSAT

Resultados:

La tabla 19 presenta la sub-sección crítica con sus respectivos resultados.

Tabla 19. Resultado de evaluación de riesgos en el diseño de aplicaciones

Registro	Se registran los intentos fallidos de autenticación; sin embargo, no se registran los intentos de autenticación correctos, los errores de las aplicaciones, los accesos denegados a los recursos, los accesos correctos a los recursos, los cambios en los datos, cuentas de usuario.
Metodología de desarrollo de seguridad de software	La empresa utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad. Sin embargo, no proporciona formación sobre metodologías de seguridad para software para su personal.

Fuente: Herramienta MSAT

Almacenamiento y comunicación de datos

Se trata de la integridad y confidencialidad de los datos, puesto que la pérdida o el robo de datos puede afectar negativamente tanto a los ingresos de una entidad como a su reputación. Es importante comprender como las aplicaciones controlan y protegen los datos críticos. (MSAT, 2016).

A continuación, en la tabla 20 se analiza las subsecciones donde se encontró riesgos.

Tabla 20. Almacenamiento y comunicación de datos.

Subsecciones	
Cifrado	☒
Cifrado - algoritmo	☒

Fuente: Herramienta MSAT

Resultados:

La tabla 21 presenta la sub-sección crítica con sus respectivos resultados.

Tabla 21. Resultado de la evaluación de riesgos en almacenamiento y comunicaciones de datos.

Cifrado	Las aplicaciones no cifran los datos confidenciales antes de transmitirlos. Las aplicaciones principales del entorno no cifran los datos confidenciales cuando están almacenados.
Cifrado - algoritmo	Se utiliza el algoritmo de hash MD5 y SHA-1

Fuente: Herramienta MSAT

3.5.1.2.3 Operaciones

El área de operaciones comprende las siguientes secciones y subsecciones:

- ✓ **Entorno.**
  - Host de gestión
  - Host de gestión – servidores
  - Host de gestión – dispositivos de red
- ✓ **Directiva de seguridad.**
  - Clasificación de datos
  - Eliminación de datos
  - Protocolos y servicios
  - Uso aceptable
  - Gestión de cuentas de usuarios
  - Regulación
  - Directiva de seguridad
- ✓ **Gestión de actualizaciones y revisión.**
  - Documentación de la red
  - Flujo de datos de la aplicación
  - Gestión de actualizaciones
  - Gestión de cambios y configuración
- ✓ **Copias de seguridad y recuperación.**
  - Archivos de registro
  - Planificación de recuperación ante desastres y reanudación del negocio
  - Copias de seguridad
  - Dispositivos de copia de seguridad
  - Copias de seguridad y restauración

Entorno

Yachay E.P. depende de los procedimientos operativos, los procesos y pautas que se aplican; entonces es necesaria una documentación clara y exacta.

La tabla 22 indica las subsecciones donde se detectó riesgos:

Tabla 22. Entorno de operaciones.

Subsecciones	
Host de gestión	☒
Host de gestión – servidores	☒
Host de gestión – dispositivos de red	☒

Fuente: Herramienta MSAT

Resultados:

En Yachay E. P. no existe ningún equipo de gestión dedicado a los dispositivos de red, lo que representa una vulnerabilidad ya que es necesario contar con una estación de gestión de estos dispositivos para comprobar que las conexiones estén disponibles y seguras.

Directiva de seguridad

La directiva de seguridad corporativa hace referencia a las directivas y pautas individuales para regular el uso adecuado y seguro de las tecnologías y los procesos. Incluye seguridad de usuarios, sistemas y datos. Se muestra en la tabla 23 las subsecciones con riesgos encontrados.

Tabla 23. Directivas de seguridad.

Subsecciones	
Clasificación de datos	☒
Eliminación de datos	☒
Protocolo y servicios	☒
Uso aceptable	☒
Gestión de cuentas de usuarios	☒
Regulación	☒
Directiva de seguridad	☒

Fuente: Herramienta MSAT

Resultados:

Yachay E. P. no cuenta con procedimientos para la gestión y eliminación de información en formato impreso y electrónico, a esto la confidencialidad de la información se ve afectada.

Gestión de actuaciones y revisiones.

La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y otras a punto de ataque. Se muestra en la tabla 24 las subsecciones que identificaron riesgos.

Tabla 24. Gestión de actualizaciones y revisiones.

Subsecciones	
Documentación de la red	☒
Flujo de datos de la aplicación	☒
Gestión de actualizaciones	☒
Gestión de cambios y configuración	☒

Fuente: Herramienta MSAT

Resultados:

La empresa no cuenta con directivas que controlen la gestión de actualizaciones, esto representa un riesgo ya que si no se aplican actualizaciones se seguridad pueden surgir problemas que afectan los procesos.

Yachay E. P. No cuenta con procedimientos formales para la correcta gestión de cambios y configuraciones de hardware y software, lo que supone una vulnerabilidad.

Copias de seguridad y recuperación

Las copias de seguridad y la recuperación de datos son imprescindibles para el mantenimiento de la continuidad de los servicios comerciales en caso de un accidente o fallo de hardware o de software. La falta de procedimientos adecuados para realizar copias de seguridad y recuperación podría producir una pérdida significativa de datos y de productividad. (MSAT, 2016).

La tabla 25 presenta las subsecciones que mostraron riesgos.

Tabla 25. Copias de seguridad y recuperación.

Subsecciones	
Archivos de registro	☒
Recuperación ante desastres y reanudación de negocio	☒
Copias de seguridad	☒
Dispositivos de copia de seguridad	☒
Copias de seguridad y restauración	☒

Fuente: Herramienta MSAT

Resultados:

Yachay E.P. no cuenta con procedimientos definidos para la recuperación ante desastres y reanudación de negocio., tampoco se realizan pruebas periódicas para asegurar la recuperación en un periodo aceptable.

3.5.1.2.4 Personal

El área de personal cuenta con las siguientes secciones y subsecciones:

- ✓ **Requisitos y evaluaciones**
  - Requisitos de seguridad
  - Evaluaciones de seguridad

- ✓ **Directiva y procedimientos**
  - Comprobaciones del historial personal
  - Directiva de recursos humanos
  - Relaciones con terceros

- ✓ **Formación y conocimiento**
  - Conocimiento de seguridad
  - Formación sobre seguridad

Requisitos y evaluaciones

Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí. (MSAT, 2016)

La tabla 26 muestra los riesgos presentados en el aspecto de requisitos y evaluaciones.

Tabla 26. Requisitos y evaluaciones.

Subsecciones	
Requisitos de seguridad	☒
Evaluaciones de seguridad	☒

Fuente: Herramienta MSAT

Resultados

La tabla 27 presenta la sub-sección crítica con sus respectivos resultados.

Tabla 27. Resultados de evaluación en la sección de personal.

Requisitos de seguridad	✓ Existen equipos comerciales y de seguridad que trabajan definiendo requisitos de seguridad. ✓ El equipo de seguridad no participa en la fase de planificación, comprobación, utilización, ni diseño del ciclo de vida de la tecnología. ✓ La empresa no tiene ningún modelo para la asignación de ✓ niveles de gravedad a cada componente del entorno informático. ✓ No hay responsabilidades ni roles definidos para los individuos involucrados en la seguridad de la información.
Evaluaciones de seguridad	No encarga a empresas independientes la evaluación de los medios de seguridad, pero tampoco las realiza el personal interno.

Fuente: Herramienta MSAT

Directiva y procedimientos

Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa. Los procedimientos para contratar aspirantes y finalizar sus contratos pueden proteger a la empresa contra empleados sin escrúpulos o descontentos. Las evidencias de los riesgos encontrados en la sección se muestran en la tabla 28.

Tabla 28. Directivas y procedimientos.

Comprobaciones del historial personal	☒
Directiva de recursos humanos	☒
Relaciones con terceros	☒

Fuente: Herramienta MSAT

Resultados:

Se muestra en la tabla 29 el resultado de la evaluación de riesgo en estas secciones.

Tabla 29. Resultado de evaluación de riesgo en directivas y procedimientos.

Relaciones con terceros	Los sistemas se configuran por parte de personal interno. No existe ninguna directiva para las relaciones con terceros.

Fuente: Herramienta MSAT

Formación y conocimiento

Este apartado trata sobre como los empleados deben recibir formación para que sean conscientes de cómo las medidas de seguridad afectan a sus actividades diarias, para que no expongan a la empresa a mayores riesgos de forma inadvertida. Las subsecciones donde se encontró riesgos se muestra en la tabla 30.

Tabla 30. Formación y conocimiento.

Subsecciones	
Conocimiento de seguridad	☒
Formación sobre seguridad	☒

Fuente: Herramienta MSAT

Resultados:

Se muestra en la tabla 31 el resultado de la evaluación de riesgo en estas secciones.

Tabla 31. Resultados de la evaluación de la formación y conocimiento.

Conocimiento de seguridad	✓ Se asigna a un individuo o grupo la seguridad de la empresa. ✓ El equipo de seguridad participa en la definición de los requisitos para las nuevas tecnologías o para las ya existentes.
Formación sobre seguridad	La empresa no ofrece actualmente a los empleados formación específica por temas.

Fuente: Herramienta MSAT

No existe programa de divulgación de las medidas de seguridad en la empresa. La capacitación permitirá al personal de TI mejorar los conocimientos, habilidades y estar al día con las nuevas tecnologías, para responder a los incidentes que se presenten.

3.5.1.3 *Análisis de la evaluación realizada con MSAT*

Al finalizar el análisis, la herramienta presenta la tabla 32 los aspectos que no cumplen con las mejores prácticas recomendadas y deben enfocarse en aumentar la seguridad dentro de Yachay E. P.

Tabla 32. Niveles de prioridad.

PRIORIDAD ALTA	PRIORIDAD INTERMEDIA	PRIORIDAD BAJA
✓ Acceso remoto ✓ Desarrollado internamente ✓ Requisitos de seguridad ✓ Segmentación ✓ Usuarios de acceso remoto	✓ Creación segura ✓ Conocimiento de seguridad ✓ Inalámbrico ✓ Registro	✓ Host de gestión – servidores. ✓ Antivirus – equipos de escritorio ✓ Antivirus – servidores ✓ Directivas de contraseñas – cuentas de administrador ✓ Directivas de contraseñas – cuentas de usuario

Fuente: Herramienta MSAT

Las 4 áreas presentan disparidades en su evaluación, lo que indica que es necesario plantear una estrategia para afrontar estos riesgos. MSAT presenta carencias severas en cuanto a aplicaciones e infraestructura mientras que en madurez de la seguridad el ítem de operaciones necesita mejorar.

El área de operaciones presenta varias subsecciones críticas que tienen que mejorar sus prácticas de seguridad. Por consiguiente, este resultado ha verificado lo expuesto en la herramienta aplicada a los funcionarios de la Gerencia donde se afirma la propuesta de Políticas aplicado al ámbito de la gestión de comunicaciones y operaciones según el Esquema Gubernamental de la Información.

3.6 Resoluciones de la Empresa Pública Yachay sobre el EGSI

Yachay EP expide sus resoluciones y es posible encontrar contenido sobre el desarrollo del Esquema Gubernamental de Seguridad de la Información en su resolución Nro. YACHAY EP-GG-2014-0021.

En el acuerdo se define la organización de la Comisión para la seguridad de la Información y de las Tecnologías de la Información y Comunicación y el establecimiento de lineamientos de seguridad informática, protección de infraestructura computacional, así como la creación del Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

El seguimiento y control a la implementación del EGSI se realizará mediante herramientas que para el efecto implemente la Secretaría Nacional de la Administración Pública. Yachay E.P. se acoge a las entidades que no tienen desplegado Gobierno por Resultados, para lo cual se elabora una matriz en hoja de cálculo basada en la plantilla usada en GPR, para presentar los avances de forma manual, a través de correo electrónico o documento Quipux dirigido a la Dirección de Arquitectura Tecnológica y Seguridad de la Información de la SNAP, adjuntando dicha matriz con los hitos cumplidos, así como el formato emitido por la Secretaría con las firmas de responsabilidad.

La resolución Nro. YACHAY EP-GG-2014-0021 presenta la conformación del Comité de Gestión de la Seguridad de la Información (CSI) de la Empresa Pública YACHAY integrado de la siguiente forma:

- ✓ El Gerente Técnico, en su calidad de delegado del Gerente General, quien a su vez actuará como Oficial de Seguridad de la Información.
- ✓ El Gerente de Planificación o su delegado.
- ✓ El Director de Tecnologías de la Información y Comunicación.
- ✓ El Director Administrativo o su delegado, quien a la vez actuará como Secretario del Comité.
- ✓ El Director de Talento Humano.
- ✓ El Director de Sistemas Informáticos.

Además, la resolución Nro. YACHAY EP-GG-2014-0021 contiene las responsabilidades del Comité de Gestión de la Seguridad de la Información así:

- ✓ Definir y mantener la política y normas particulares de la empresa en materia de seguridad de la información y gestionar su aprobación y puesta en vigencia por parte de la Máxima Autoridad.
- ✓ Acordar y aprobar metodologías y procesos específicos, en base al EGSI relativos a la seguridad de la información.
- ✓ Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
- ✓ Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la empresa frente a incidentes de seguridad imprevistos.

- ✓ Designar a los custodios o responsables de la información de las diferentes áreas de la entidad.
- ✓ Velar por la aplicación de la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000 en la empresa según el ámbito de cada norma.
- ✓ Presentar al Gerente General de la Empresa Pública "YACHAY E.P." informes mensuales sobre el seguimiento de la puesta en marcha de las normas del EGSI;
- ✓ Preparar y poner en consideración del Gerente General de "YACHAY E.P." las disposiciones relacionadas a la Seguridad de la Información para que sean oficializadas en la institución.
- ✓ Coordinar con la Secretaría Nacional de la Administración Pública y proveer la información que se requiera.

El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

- ✓ Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- ✓ Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.
- ✓ Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- ✓ Verificar el cumplimiento de las normas, procedimientos y controles de seguridad establecidos en la empresa.

La resolución mencionada indica que existe un responsable de Seguridad del área de Tecnologías de la Información designado por el Comité y tendrá las siguientes responsabilidades:

- ✓ Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- ✓ Evaluar el posible impacto operativo a nivel de seguridad de los cambios previsto a sistemas y equipamiento asignando responsabilidades para verificar su implementación.
- ✓ Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad para soportar posibles amenazas a la seguridad de la información.
- ✓ Desarrollar y verificar el cumplimiento de los procedimientos para comunicar las fallas en el procesamiento de la información, que permita medidas correctivas.
- ✓ Implementar los controles de seguridad definidos.
- ✓ Gestionar los incidentes de seguridad de la información de acuerdo a procedimientos establecidos.

Una vez establecidos los roles y responsabilidades, se tiene una pauta para la elaboración de las Políticas de Seguridad de la Información; aclarando que la empresa pública ha venido desarrollando algunos ítems de acuerdo a sus actividades diarias como:

- ✓ Activación, desactivación o modificación de servicios
- ✓ Control
- ✓ Gestión y uso de contraseñas

- ✓ Servicio de Internet
- ✓ Correo electrónico
- ✓ Telefonía fija y móvil
- ✓ Equipamiento
- ✓ Almacenamiento y respaldo de información institucional.
- ✓ Desarrollo de aplicativos internos
- ✓ Publicación de contenido institucional
- ✓ Actuaciones por incumplimiento

Así mismo, se recibe frecuentemente la información de la SNAP, manifestando se continúe trabajando en los hitos del EGSI. La Empresa Pública Yachay ha desarrollado en base a lo requerido por la SNAP, las matrices que corresponden a los hitos prioritarios y no prioritarios. El último reporte enviado por la Empresa Pública Yachay fue realizado con fecha diciembre del 2016 y manifiesta el 100% de hitos cumplidos según se planteó la empresa.

Además, es posible observar el Ranking de entidades públicas que han cumplido la implementación del EGSI en fases en el anexo. **(Ver Anexo 4)**

Capítulo IV

Políticas de Seguridad de la Información

La propuesta inicialmente presenta los datos informativos necesarios que a continuación se detallan en la tabla 33:

Tabla 33. Datos informativos propuesta.

✓ **Título**	Análisis y planteamiento de Políticas de acuerdo al Esquema Gubernamental de Seguridad de la Información (EGSI) Para La Empresa Pública Yachay.
✓ **Persona que desarrolla la propuesta**	Srta. Alejandra Pinto Erazo
✓ **Director de trabajo**	Msc. Fabián Cuzme Rodríguez
✓ **Beneficiario**	Empresa Pública Yachay
✓ **Ubicación**	Hacienda San Eloy, Urcuquí.
✓ **Tiempo estimado para desarrollo de propuesta**	*Fecha de Inicio:* junio 2016. *Fecha de finalización:* diciembre 2016.
✓ **Equipo colaborador**	Funcionarios: Ing. Nataly Culqui e Ing. Giovanni Moreno.

Fuente: Autor

4.1 Definición de Requisitos para la propuesta

La metodología de la Universidad Nacional de Colombia indica que, en la fase de desarrollo, las etapas correspondientes a la ilustración 21 contienen requisitos para dar cumplimiento correcto a la propuesta.

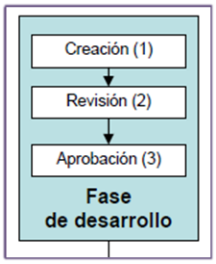

Ilustración 21. Etapas de la fase de desarrollo.

Fuente: (Universidad Nacional de Colombia, 2003)

El tema planteado para este proyecto de grado tiene como alcance el desarrollo de las etapas de creación y revisión; la etapa de aprobación implica estudios a nivel organizacional que la empresa pública Yachay realizará en los plazos que sus directivos determinen, más no es un alcance planteado.

Los requisitos para cada etapa son:

- ✓ **Creación**
  - Objetivo
  - Alcance
  - Aplicabilidad
  - Responsabilidades
- ✓ **Revisión**
  - Versiones
  - Certificación de revisión

A continuación, se explicará cada uno de los requisitos de la Política de Seguridad.

Objetivo

La política tiene como objetivo establecer los lineamientos respecto a la Seguridad de la Información dentro de Yachay EP, con enfoque a la Gestión de comunicaciones y operaciones, con la finalidad de garantizar la seguridad, confidencialidad y disponibilidad de la misma con el uso de Sistemas de Información de las que posee la institución.

Alcance

Se presenta a la entidad, las Políticas desarrolladas siguiendo el ítem "Gestión de Operaciones y Comunicaciones que plantea el EGSI en sus literales:

- ✓ 6.13. Controles de las redes
- ✓ 6.14. Seguridad de los servicios de la red
- ✓ 6.26. Registro de auditorías.

El alcance no determina la realización de los procedimientos o manuales técnicos, sin embargo, se proporciona el informe aplicado a la empresa a través de la herramienta MSAT donde es posible encontrar varias recomendaciones y posibles soluciones de seguridad de la información.

Además, las Política planteada debe ser socializada inicialmente con la Gerencia de Tecnologías de la Institución para revisión y posibles correcciones.

Aplicabilidad

El documento contiene una casilla que indica el beneficiario de determinada política. Entre los que se puede indicar:

- ✓ Dirección de soporte y operaciones tecnológicas.
- ✓ Dirección de telecomunicaciones, energía y automatización.
- ✓ Dirección de sistemas informáticos.
- ✓ Gerencia de Tecnologías de la Información y Comunicación.
- ✓ Usuarios finales.

Responsabilidad y Autoridad

La responsabilidad de elaborar el documento es del Oficial de Seguridad de la Información; es por eso que se ha trabajado conjuntamente con el personal encargado del comité. La revisión de las Políticas es responsabilidad del Comité de Gestión de la Seguridad de la Información.

4.2 Desarrollo del documento "Políticas de Seguridad de la Información"

El manual de políticas de seguridad describe de manera más detallada los objetivos de control enfocados a la gestión de comunicaciones y operaciones, este a su vez contiene: firma de autor, firmas de la revisión del encargado de la seguridad de la información, la fecha de elaboración, revisión y la versión actual. Además, contiene el objetivo, destinatario y definiciones referentes seguridad de la información.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

POLÍTICAS DE SEGURIDAD

Elaborado por	Fecha de elaboración	Firma
Alejandra Pinto Erazo	Junio 2016	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Revisado por	Fecha de revisión	Firmas
Ing. Nataly Culqui **DIRECCIÓN DE TELECOMUNICACIONES, ENERGÍA Y AUTOMATIZACIÓN**	Diciembre 2016	_ _ _ _ _ _ _ _ _ _ _ _ _ _
Ing. Giovanni Moreno **RESPONSIBLE DE SEGURIDAD DEL ÁREA DE TECNOLOGÍAS DE LA INFROMACIÓN**		_ _ _ _ _ _ _ _ _ _ _ _ _ _

Versión	1.0

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Política de Seguridad
Destinatario:	Gerencia de Tecnologías
Objetivo:	Identificar los términos y definiciones de seguridad de la información.

Definiciones

Activo de información. - Es cualquier información generada que sustenta uno o varios procesos de una unidad o área de la institución, es clasificada como importante y de gran valor para la institución y el estado. Esta información generada puede ser documentación (contratos, informes, consultarías, entre otros), usuarios, contraseñas, audio, video, bases de datos, configuraciones de equipos y servidores, etc.

Confidencialidad. - Garantía de que acceden a la información, sólo aquellas personas autorizadas a hacerlo.

Disponibilidad. - Garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Incidente de la seguridad de la información. - Acción o evento que ha generado algún efecto negativo e inesperado en la seguridad de la información. Tienen una probabilidad significativa de comprometer las operaciones de la institución y de amenazar a la seguridad de la información atentando en contra de las políticas, normativas, confidencialidad, integridad y disponibilidad de la información.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Política de Seguridad
Destinatario:	Gerencia de Tecnologías
Objetivo:	Identificar los términos y definiciones de seguridad de la información.

Definiciones

Integridad. - Mantenimiento de la exactitud y totalidad de la información y de los métodos de procesamiento.

Información Confidencial. - Es aquella información que es accesible sólo para aquellos autorizados a tener acceso.

Normativa. - Conjunto de normas aplicables a una determinada materia o actividad.

Política de seguridad de la información. - Es un documento de alto nivel que denota el compromiso de las autoridades con la seguridad de la información.

Procedimiento. - Conjunto de actividades detalladas y alineadas a un objetivo que genera un resultado específico.

Respaldo. - Copia de información importante de un dispositivo primario a uno o varios dispositivos secundarios.

Seguridad de la Información. - Son medidas preventivas y reactivas de las personas, de las instituciones y de los sistemas de información que permitan resguardar y proteger la información buscando mantener su confidencialidad, la disponibilidad y la integridad.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Política de Seguridad
Destinatario:	Gerencia de Tecnologías
Objetivo:	Identificar los términos y definiciones de seguridad de la información.

Definiciones

Sistema de información. - Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Usuario: Toda persona que bajo cualquier relación de dependencia con la Institución hace uso de los sistemas de información para el desarrollo de las actividades que relacionan la generación, procesamiento y resguardo de la información.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Política de Seguridad
Destinatario:	Gerencia de Tecnologías
Objetivo:	Plantear Políticas de seguridad generales

Art 1.- Este documento, "Políticas de Seguridad en base al EGSI", establece el enfoque para manejar la seguridad de la información acorde a la gestión de comunicaciones y operaciones.

Art 2.- Otorgar una guía a los empleados sobre políticas que deben cumplir para conservar los activos más importantes de la institución.

Art 3.- La Gerencia es la responsable de las políticas, además que se debe hacer cumplir los procedimientos a todos usuarios y de comunicar a todos los implicados si hubo cambios en el sistema de seguridad.

Art 4.- La Política de seguridad debe ser revisada a intervalos concretos y periódicos de tiempo o cuando se produzcan cambios significativos.

Art 5.- La política de seguridad debe ser recibida por la gerencia para socialización con los funcionarios que la integran.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Informar políticas generales a los usuarios de la gerencia.

Art 6.- Se debe utilizar de forma responsable y solamente para actividades laborales, las comunicaciones en forma electrónica. Toda información que se genera mediante de sistemas de comunicación institucionales; así como las copias de respaldo de los mismos, se consideran propiedad de la institución.

Art 7.- El uso personal de los sistemas de comunicación en forma ocasional es permisible, siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del funcionario ni con las actividades de la Institución.

Art 8.- De existir personal temporal (por ejemplo, pasantes), no se les otorgará cuentas o perfiles donde se comprometa la seguridad de la información de la institución.

Art 9.- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento o diversión.

Art 10.- Los funcionarios no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben colaborar con otros para que lo hagan.

Art 11.- Queda prohibido el uso de software no autorizado por la institución. Para esto, se realizarán revisiones periódicas del contenido de software en los equipos informáticos y de telecomunicaciones.

Art 12.- Todo equipo informático que sea asignado a un usuario se lo debe entregar sin dejar información del anterior usuario de este equipo.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Informar políticas generales a los usuarios de la gerencia.

Art 13.- Los respaldos de información se manejarán de la siguiente manera:

- Personal que sale de la Institución. Se debe hacer un respaldo del equipo para proceder a formatearlo. La información se mantiene un número de días definido en el procedimiento para tal efecto.
- Personal que se cambia de área: La información se mantiene un número de días definido en el procedimiento para tal efecto.
- Personal que se cambia el computador: La información se mantiene se mantiene un número de días definido en el procedimiento para tal efecto.
- La Unidad de Tecnologías de la Información respaldará todos los sistemas con sus respectivos archivos de configuración y base de datos, de manera que se asegure la continuidad del negocio.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Gestionar las comunicaciones y operaciones

Art 14.- Solo el personal de la gerencia puede realizar la gestión para la adquisición de equipos tecnológicos para la institución, como, por ejemplo: computadoras de escritorio, portátiles, impresoras, servidores, firewall. En las características y marcas que ellos crean necesarios.

Art 15.- El personal encargado de generar los requerimientos técnicos para la adquisición de nuevo hardware/software lo realizará según sea el área requirente de acuerdo al tipo de componente que se solicite. Así mismo serán los encargados de recibir, probar, configurar e implementar dentro de la infraestructura de la organización los nuevos componentes tecnológicos adquiridos.

Art 16.- Solo el personal de soporte y operaciones tecnológicas está autorizado para instalar o desinstalar el software en los computadores de los usuarios.

Art 17.- El jefe de la dirección de telecomunicaciones establecerá los privilegios que tiene cada dirección en cuanto a su acceso a internet y recursos de la red interna, en base a base a lo que estipula el manual de funciones de los servidores públicas del área.

Art 18.- Solo en casos excepcionales mediante escrito a la máxima autoridad de la gerencia se podrán habilitar accesos a servicios previa aprobación del pedido.

Art 19.- La administración del contenido de la página web de la institución, solo será gestionada por la dirección de sistemas informáticos.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Respaldar y asegurar la información

Art 20.- Mantener el servidor de respaldos disponible y con el espacio suficiente para que los usuarios realicen sus respaldos respectivos de la información sensible de la organización.

Art 21.- Si un usuario reporta actividad inusual en su computador, deberá ser entregado inmediatamente a la dirección de soporte y operaciones tecnológicas para su revisión y corrección de cualquier tipo.

Art 22.- La información que encuentra en los servidores, infraestructura de telecomunicaciones y usuarios finales solo puede ser respaldada por el jefe de la dirección de soporte y operaciones tecnológicas, dependiendo del servicio esta información se puede almacenar semanalmente.

Art 23.- El jefe de la dirección de soporte y operaciones tecnológicas tiene bajo su poder las herramientas necesarias para el respaldo de la información de todos los equipos computacionales o de servicios, solo él puede tener estas herramientas a menos que la gerencia autorice entregar a otra persona.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Gestión de la seguridad en las redes

Art 24.- Se identificará y realizarán acuerdos de servicios de red en el que consten los métodos de seguridad, niveles de servicio y requisitos de gestión de los servicios que presta la empresa.

Art 25.- Se deberá potenciar al máximo el sistema de cortafuegos para proteger a la red y sus servicios de daños externos.

Art 26.- Se debe determinar y monitorizar regularmente la capacidad del proveedor de servicio de red para manejar los servicios contratados de una manera segura, y se debe acordar el derecho de auditoría.

Art 27.- Se deben identificar los acuerdos de seguridad necesarios para servicios particulares, como las características de seguridad, niveles de servicio y requerimientos de gestión.

Art 28.- Se deben implantar controles de autenticación, codificación y conexión de red.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Operaciones

Art 29.- Definir e implementar procedimientos para la gestión y eliminación de información en formato impreso y electrónico. Proporcionar a los usuarios permitidos dichos procedimientos para que los lean y los apliquen. Las instrucciones deben ser concisas para destruir de forma segura la información.

Art 30.- Actualizar el diagrama de red de la empresa conforme se produzcan cambios en el mismo.

Art 31.- Desarrollar una directiva para actualizar periódicamente los sistemas operativos y las aplicaciones utilizando procesos adecuados.

Art 32. – Poner en práctica un proceso formal de gestión para las configuraciones y los cambios para verificar y documentar todas las actualizaciones antes de su puesta en práctica. Guardar una documentación completa acerca de las configuraciones de todos los sistemas que se encuentran a cargo de la gerencia de tecnologías.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Revisión y supervisión

Art 33.- Para cada activo, y dependiendo de su tipo, se definirán los mecanismos de registro y localización adecuados. Estos mecanismos deberán de incorporar la capacidad de seleccionar el nivel de detalle del registro generado.

Art 34.- Las aplicaciones deberán generar registros de actividad que permitan de manera sencilla realizar seguimiento de operaciones y eventos. Los registros deberán ser almacenados de forma transparente.

Art 35.- Los mecanismos de registro de eventos deberán generar una alerta si por cualquier motivo, no es posible generar el registro.

Art 36.- Debido a la información que aportan los registros de eventos sobre los sistemas, redes, aplicaciones y usuarios, el acceso a estos registros deberá quedar limitado a las personas autorizadas para su análisis.

Art 37.- Los registros se guardarán durante periodos predefinidos, que cómo mínimo serán los establecidos por la legislación vigente en cada momento.

Art 38.- Los registros de eventos serán utilizados como pistas de auditoría en la función de revisión y control. En consecuencia, los relojes de los sistemas deben estar sincronizados para generar registros adecuados.

EMPRESA PÚBLICA YACHAY

SAN ELOY, CASA HACIENDA, INGENIO SAN JOSE, EL ROSARIO, CHALET

Gerencia de Tecnologías

Control:	Gestión de comunicaciones y operaciones
Destinatario:	Gerencia de Tecnologías
Objetivo:	Revisión y supervisión

Art 39.- Los registros de información (administrativos, contables, documentación legal) que recojan la actividad de la Empresa Pública Yachay deben ser almacenados y protegidos frente a pérdida, destrucción, alteración y falsificación.

Art 40.- Desarrollar, documentar, implementar y someter los planes de recuperación ante desastres a revisiones, pruebas y actualizaciones periódicas. Debe incluirse al personal, sistemas y cuestiones de tecnología.

4.3 Revisión de la Política Institucional de Seguridad de la Información.

La Política Institucional de Seguridad de la Información propuesta fue revisada por Dirección de telecomunicaciones y la Dirección de soporte y operaciones tecnológicas como se muestra la certificación en el anexo **(Ver Anexo 6)**, considerando que el Comité de Seguridad de la Información realizará el análisis correspondiente y tomará la decisión de aplicar la propuesta de "Políticas de Seguridad de la Información de la Empresa Pública YACHAY E.P" desarrollada en el presente trabajo de grado.

Conclusiones

- ✓ La ejecución de proyectos enfocados a empresas públicas requiere de conocimientos de leyes, normas y reglamentos para estructurarlos de tal manera que se tenga un complemento entre el área técnica y las definiciones del Estado.

- ✓ La empresa pública facilitó los datos legales sobre la conformación del comité de seguridad de la información, para solicitar colaboración en el desarrollo del presente proyecto de grado.

- ✓ Se cumplió con el objetivo de realizar un diagnóstico de vulnerabilidades; fue posible aplicar la herramienta de Microsoft al responsable de seguridad del área de Tecnologías de la Información de Yachay E. P. obteniendo carencias severas en el área de operaciones, sin dejar de lado a las áreas de infraestructura, aplicaciones y personal que también evidenciaron puntos críticos en su seguridad en menor porcentaje.

- ✓ El resultado de la evaluación Microsoft Security Assessment Tool propuso la elaboración de mejores prácticas de seguridad para la entidad, siendo este, un respaldo para desarrollar las Políticas de Seguridad necesarias.

- ✓ Además, la Gerencia de Tecnologías conformada por 11 funcionarios aportó en la encuesta realizada, cuyos resultados también evidencian que existen falencias en el desarrollo de los controles que presenta el Esquema Gubernamental de Seguridad de la Información y corresponden al dominio de gestión de comunicaciones y operaciones.

- ✓ La Gerencia de Tecnologías de Yachay E. P. designó al responsable de seguridad del área para trabajar en la elaboración y revisión del presente documento, que consta de artículos propuestos para la gestión de comunicaciones y operaciones y contribuirán a una mejora continua.

- ✓ La guía que propuso la Universidad de Colombia para la elaboración de las Políticas de Seguridad de la Información permitió el desarrollo paso a paso y de la manera más clara y concisa.

- ✓ Yachay E.P se encuentra en la segunda fase de la implementación del EGSI, que corresponde al cumplimiento de ítems no prioritarios; se presentó el último reporte con fecha diciembre 2016, cumpliendo en un 100% y de esta manera permitiendo culminar a la vez el desarrollo del presente documento como respaldo a determinado hito del Esquema.

- ✓ El documento de Políticas de seguridad acorde al dominio de comunicaciones y operaciones fue entregado a la Empresa Pública Yachay y fue revisado por la Dirección de Soporte y Operaciones.

Recomendaciones

- ✓ Se recomienda utilizar siempre una metodología de análisis de riesgos de acuerdo a las actividades a las que se dedica la empresa; en algunos casos será necesario aplicar una metodología con análisis cualitativo y en otros casos de forma cuantitativa.

- ✓ Es fundamental documentar los eventos a través de registros; en este caso las políticas contribuyen a determinar bajo procesos formales determinadas decisiones.

- ✓ La implementación de las Políticas planteadas debe ser trabajo continuo entre todos los involucrados de la empresa.

- ✓ Se recomienda que las políticas de seguridad sean socializadas por medios digitales al personal de la gerencia para posibles sugerencias y aprobación.

Glosario

ISO. - Se conoce por ISO tanto a la Organización como a las normas establecidas por la misma para estandarizar los procesos de producción y control en empresas y organizaciones internacionales.

IEC. - más conocida por sus siglas en inglés: IEC (International Electrotechnical Commission), es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.

EGSI. - establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública.

GPR. - Es una herramienta que permite orientar las acciones del Gobierno y sus instituciones, al cumplimiento de objetivos nacionales y resultados concretos que mejoran la ejecución del presupuesto gubernamental.

TI.- (TI, o más conocida como IT por su significado en inglés: Information technology). Con frecuencia utilizado en el contexto de los negocios u otras empresas. El término es comúnmente utilizado como sinónimo para los computadores, y las redes de computadoras, pero también abarca otras tecnologías de distribución de información, tales como la televisión y los teléfonos.

LOTAIP. - Ley Orgánica de Transparencia y Acceso a la Información Pública, busca garantizar los derechos a acceder a las fuentes de información, como mecanismo para ejercer la participación democrática respecto al manejo del ámbito público y la rendición de cuentas que están sujetos los funcionarios públicos y entidades del estado.

Riesgo. - término hace referencia a la proximidad o contingencia de un posible daño, además la noción de riesgo suele utilizarse como sinónimo de peligro. El riesgo, sin embargo, está vinculado a la vulnerabilidad, mientras que el peligro aparece asociado a la factibilidad del perjuicio o daño.

Riesgo informático. - comprende la identificación de vulnerabilidades y amenazas a los que se encuentran expuestos los activos informáticos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Amenaza. - El término amenaza es una palabra que se utiliza para hacer referencia al riesgo o posible peligro que una situación, un objeto o una circunstancia específica puede conllevar para la vida, de uno mismo o de terceros.

Vulnerabilidad. - El concepto puede aplicarse a una persona o a un grupo social según su capacidad para prevenir, resistir y sobreponerse de un impacto.

Salvaguardas. - se definen como medidas “de urgencia” que se aplican en casos de eventualidades como amenazas, riesgos o vulnerabilidades de la información.

Activo de información. - Es cualquier información generada que sustenta uno o varios procesos de una unidad o área de la institución, es clasificada como importante y de gran valor para la institución y el estado. Esta información generada puede ser documentación (contratos, informes, consultarías, entre otros), usuarios, contraseñas, audio, video, bases de datos, configuraciones de equipos y servidores, etc.;

Confidencialidad. - Garantía de que acceden a la información, sólo aquellas personas autorizadas a hacerlo;

Disponibilidad. - Garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran;

Incidente de la seguridad de la información. - Acción o evento que ha generado algún efecto negativo e inesperado en la seguridad de la información. Tienen una probabilidad significativa de comprometer las operaciones de la institución y de amenazar a la seguridad de la información atentando en contra de las políticas, normativas, confidencialidad, integridad y disponibilidad de la información;

Integridad. - Mantenimiento de la exactitud y totalidad de la información y de los métodos de procesamiento;

Normativa. - Conjunto de normas aplicables a una determinada materia o actividad;

Política de seguridad de la información. - Es un documento de alto nivel que denota el compromiso de las autoridades con la seguridad de la información;

Procedimiento. - Conjunto de actividades detalladas y alineadas a un objetivo que genera un resultado específico;

Respaldo. - Copia de información importante de un dispositivo primario a uno o varios dispositivos secundarios;

Seguridad de la información. - Son todas aquellas medidas preventivas y reactivas de las personas, de las instituciones y de los sistemas de información que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma;

Sistema de información. - Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo;

Usuario. - Toda persona que bajo cualquier relación de dependencia con la Institución hace uso de los sistemas de información para el desarrollo de las actividades que relacionan la generación, procesamiento y resguardo de la información.

Bibliografía

Álvarez Marañon, G., & Pérez García, P. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid: McGraw-Hill.

Álvarez Marañon, G., & Pérez García, P. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid: McGraw-Hill. Recuperado el 23 de Mayo de 2016

BLIGOO. (2010). *Los pilares de la seguridad informática*. Obtenido de www.bligoo.com: http://seguridaddeinformacion.bligoo.com/los-pilares-de-la-seguridad-informatica

BLIGOO. (2010). *Los pilares de la seguridad informática*. Recuperado el 23 de Mayo de 2016, de www.bligoo.com: http://seguridaddeinformacion.bligoo.com/los-pilares-de-la-seguridad-informatica

Cano, J. L. (2007). *Businness Intelligence:Competir con información.* Madrid: Fundación Cultural Banesto.

CYBSEC S.A. (2011). *Fundamento de Seguridad Informática.* Buenos Aires, Argentina.

CYBSEC S.A. (2011). *Fundamento de Seguridad Informática.* Buenos Aires, Argentina. Recuperado el 23 de Mayo de 2016

Dario, I. B. (2009 de abril de 21). DATA WAREHOUSING:Invesigación y sistematización de conceptos. Córdoba, Argentina.

Davenport, T. H., & Prusak, L. (1999). *Working Knowledge: How Organizations Manage What They Know.* USA. Obtenido de http://www.gestiondelconocimiento.com/conceptos_diferenciaentredato.htm

Departamento de Seguridad en cómputo UNAM. (2010). *Gran libro de la seguridad informática.* Mexico. Recuperado el 23 de Mayo de 2016

Duque, B., & Gómez, C. (febrero de 2010). *Auditoria Universidad de Caldas.* Recuperado el 20 de julio de 2016, de www.wikispaces.com: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

Howard, P. (2003). The Security Policy Life Cycle: Funtions and Responsabilities. (T. &. Krause, Ed.) *Information Security Management Handbook*. Recuperado el 20 de julio de 2016

ISO. (s.f.). *ISO STORE*. Recuperado el 20 de julio de 2016, de ISO STORE: http://www.iso.org/iso/store.htm

ISO. (s.f.). *iso.org*. Obtenido de iso.org: http://www.iso.org/home/html

ISO/IEC 27000:2012. (2012). *Tecnologías de la Información - Descripción general y vocabulario ISO/IEC 27000.* INEN. Recuperado el 23 de Mayo de 2016

ISO/IEC 27001. (2013). Norma: Requisitos del Sistema de Gestión de Seguridad de la Información. *ISO/IEC 27001*. Recuperado el Junio de 2016, de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISO/IEC TR 13335-1. (2009). ISO/IEC TR 13335-1. Recuperado el 08 de 07 de 2016

ISO27000.ES. (Octubre de 2013). *Norma ISO/IEC 27002:2013*. Obtenido de ISO : iso27000.ez

IT Gobernance Institute. (2006). *Information Security Gobernance: Guidande for board of DIrectors and Executive Management.* EEUU: 2da.

Mifsud , F. (2015). *Introducción a la seguridad de la información - vulnerabilidades de un sistema informático.* Recuperado el 22 de Mayo de 2016, de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

Mifsud, E. (2012). *Políticas de Seguridad. ¿Cómo podemos proteger el sistema?* Recuperado el 25 de Septiembre de 2016, de Observatorio tecnológico. Gobierno de España: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040- i

MSAT. (2016). *Informe Completo Microsft Security Assessment Tool.* Recuperado el 08 de diciembre de 2016

(2005). *Norma ISO/IEC.* Recuperado el 1 de diciembre de 2016

Oficina de Seguridad para las redes informáticas. (Agosto de 2013). *Metodología para la gestión de la seguridad informática.* Recuperado el 23 de Mayo de 2016, de instituciones.sld.cu: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Palma, L. A. (2011). *Introducción Seguridad informática.* México: ITESM.

Secretaría Nacional de la Administración Pública. (s.f.). *La secretaría*. Recuperado el 23 de Mayo de 2016, de http://www.administracionpublica.gob/la-secretaria/

SNAP. (2013). *Esquema Gubernamental de Seguridad de la Información.* Quito. Recuperado el 29 de Abril de 2016

SNAP. (s.f.). *Administración Publica*. Obtenido de http://gpr.administracionpublica.gob.ec/gpr_ecuador/n4

Students, B. I. (23 de enero de 2011). *www.blogspot.com*. Obtenido de http://businessintelligencemustudents.blogspot.com/2011/01/retos-y-desventajas-de-bussines.html

Suárez, & Alonso. (2007). *Tecnologías de la Información y la Comunicación.* Vigo, España: Ideaspropias Editorial. Recuperado el 25 de Septiembre de 2016

Ulloa, S. G. (2015). *SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS EN COOPERATIVAS.* Ambato. Recuperado el 01 de diciembre de 2016, de http://repositorio.uta.edu.ec/bitstream/123456789/8654/1/Tesis_t975si.pdf

Universidad de Oriente UNIVO. (s.f.). *Manual de Normas y Políticas de Seguridad Informática.*

Universidad Nacional de Colombia. (2003). Guía para elaboración de políticas de seguridad. Recuperado el 24 de Mayo de 2016

UTE. (2013). *ENFÓCATE Revista Científica.* Recuperado el 01 de diciembre de 2016

Anexos

Anexo 1.- Norma ISO/IEC 27002:2005

Anexo 2.- Norma ISO/IEC 27002:2013

Anexo 3.- Cuestionario: Políticas en relación al Esquema Gubernamental de Seguridad de la Información (EGSI)

Anexo 4.- Ranking Entidades Públicas – cumplimiento EGSI

Anexo 5.- Aceptación de desarrollo de Trabajo de grado en Gerencia de Tecnologías Yachay E. P.

Anexo 6.- Certificado de cumplimiento del proyecto de grado en la Gerencia de Tecnologías Yachay E. P.

Anexo 7.- Certificado de aplicación de la encuesta con MSAT

Anexo 8.- Encuesta para la evaluación de riesgos con herramienta MSAT

Anexo 1.- Norma ISO/IEC 27002:2005

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
- 5.1 Política de seguridad de la información.
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- 6.2 Terceros.
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- 7.1 Responsabilidad sobre los activos.
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- 7.2 Clasificación de la información.
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 8.1 Antes del empleo.
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- 8.2 Durante el empleo.
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- 8.3 Cese del empleo o cambio de puesto de trabajo.
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- 9.1 Áreas seguras.
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- 9.2 Seguridad de los equipos.
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- 10.1 Responsabilidades y procedimientos de operación.
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- 10.2 Gestión de la provisión de servicios por terceros.
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- 10.3 Planificación y aceptación del sistema.
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- 10.4 Protección contra el código malicioso y descargable.
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- 10.5 Copias de seguridad.
  - 10.5.1 Copias de seguridad de la información.
- 10.6 Gestión de la seguridad de las redes.
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- 10.7 Manipulación de los soportes.
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- 10.8 Intercambio de información.
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- 10.9 Servicios de comercio electrónico.
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- 10.10 Supervisión.
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- 11.1 Requisitos de negocio para el control de acceso.
  - 11.1.1 Política de control de acceso.
- 11.2 Gestión de acceso de usuario.
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- 11.3 Responsabilidades de usuario.
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- 11.4 Control de acceso a la red.
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- 11.5 Control de acceso al sistema operativo.
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- 11.6 Control de acceso a las aplicaciones y a la información.
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- 11.7 Ordenadores portátiles y teletrabajo.
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- 12.1 Requisitos de seguridad de los sistemas de información.
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- 12.2 Tratamiento correcto de las aplicaciones.
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- 12.3 Controles criptográficos.
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- 12.4 Seguridad de los archivos de sistema.
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- 12.5 Seguridad en los procesos de desarrollo y soporte.
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 13.1 Notificación de eventos y puntos débiles de seguridad de la información.
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- 13.2 Gestión de incidentes y mejoras de seguridad de la información.
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
- 15.1 Cumplimiento de los requisitos legales.
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- 15.3 Consideraciones sobre las auditorías de los sistem. de información.
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Documento sólo para uso didáctico. La norma oficial debe adquirirse en entidades autorizadas para su venta

Ver. 4.0, 16-1-2011

Anexo 2.- Norma ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

 Octubre-2013

Anexo 3.- Cuestionario: Políticas en relación al Esquema Gubernamental de Seguridad de la Información (EGSI)

Cuestionario aplicado a funcionarios de
Gerencia de Tecnologías de Yachay E. P.
ESQUEMA GUBERNAMENTAL DE
SEGURIDAD DE LA INFORMACIÓN (EGSI)"

Encuesta por: Alejandra Pinto Erazo

Encuestado: …… **Fecha de aplicación:** ……

DOMINIO 1: Políticas de seguridad

1. *¿Conoce Usted el establecimiento de Políticas de Seguridad de la información o algún otro procedimiento que se apliquen en la Institución?*

a. Si, ¿Cuáles?

……

b. No

DOMINIO 2: Organización de la Seguridad de la Información

2. *¿Existe la asignación y reconocimiento de responsabilidades en materia de Seguridad de Información?*

a. Si
b. No

Argumente: ……

DOMINIO 3: Gestión de activos

3. *¿Cómo se desarrolla el funcionamiento de los activos de la Institución?*

a. Correcto funcionamiento de activos
b. Deficiente funcionamiento de activos
c. No es su función saber

DOMINIO 4: Seguridad ligada a los recursos humanos

4. *¿Se toma alguna medida sobre los privilegios o accesos a algún usuario al finalizar su actividad dentro de la Institución?*

a. Si
b. No

Argumente: ……

DOMINIO 5: Seguridad física y del entorno

5. *¿Qué acción se toma para establecer seguridad física?*

a. Desconozco del tema
b. Se documenta y actualiza los procedimientos de operación y se pone a disposición del usuario que lo requiera.
c. Se documenta y actualiza los servicios, reportes, reuniones, incidentes de los proveedores

DOMINIO 6: **Gestión de comunicaciones y operaciones**

6. *¿Existen procesos de respaldo y recuperación de la información?*

a. Si
b. No

7. *¿Cuál es el procedimiento para el intercambio de información?*

a. Desconoce del tema
b. Existen políticas o procedimientos formales para proteger la información a través de cualquier medio de comunicaciones.
c. Existen acuerdos establecidos para el intercambio de información entre la organización y los proveedores

DOMINIO 7: Control de accesos

8. *¿A quién se otorga acceso a la información?*

a. A todos los usuarios.
b. A determinado usuario
c. Desconoce del tema

DOMINIO 8: Adquisición, desarrollo y mantenimiento de sistemas

9. *¿Qué procedimiento se realiza en cuanto a desarrollo y mantenimiento de sistemas?*

a. Existen procedimientos para controlar la instalación de software.
b. El administrador actualiza librerías
c. Se restringe el acceso a totalmente

DOMINIO 9: Gestión de vulnerabilidades técnicas

10. *¿Se reporta eventos o vulnerabilidades?*

a. Si
b. No

DOMINIO 11: Cumplimiento

11. *¿Se da cumplimiento a los procesos de seguridad de la información?*

a. Si
b. No

Anexo 4.- Ranking Entidades Públicas – cumplimiento EGSI

Secretaría Nacional de la Administración Pública

RANKING DE ENTIDADES PÚBLICAS DEL CUMPLIMIENTO DE LA IMPLEMENTACION DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Implementación de los hitos no prioritarios (EGSI FASE II)

Periodo: 25 de Julio del 2016 al 25 de Septiembre del 2016

Fecha de corte: **25 de Septiembre del 2016**

RANKING	SIGLAS	NOMBRE DE LA INSTITUCION	EGSI: # DE HITOS PROPUESTOS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
31	PETROAMAZONAS	Petroamazonas EP (*).	134	134	100,00%	100,00%
32	IEE	Instituto Espacial Ecuatoriano	133	133	100,00%	100,00%
33	SETEDIS	Secretaría Técnica de Discapacidades	124	124	100,00%	100,00%
34	BDE	Banco del Estado	119	119	100,00%	100,00%
35	INEVAL	Instituto Nacional de Evaluación Educativa	117	117	100,00%	100,00%
36	DINARDAP	Dirección Nacional de Registro de Datos Públicos	116	116	100,00%	100,00%
37	MICS	Ministerio de Coordinación de Seguridad	114	114	100,00%	100,00%
38	ECORAE	Instituto para el Ecodesarrollo de la Región Amazónica	110	110	100,00%	100,00%
39	INP	Instituto Nacional de Pesca	100	100	100,00%	100,00%
40	INER	Instituto Nacional de Eficiencia Energética y Energías Renovables	97	97	100,00%	100,00%
41	INMOBILIAR	Servicio de Gestión Inmobiliaria del Sector Público	97	97	100,00%	100,00%
42	SENAGUA	Secretaría del Agua	91	91	100,00%	100,00%
43	ARCOM	Agencia de Regulación y Control Minero	82	82	100,00%	100,00%
44	DGRCIC	Dirección General de Registro Civil Identificación y Cedulación	80	80	100,00%	100,00%
45	MCPE	Ministerio de Coordinación de la Política Económica	79	79	100,00%	100,00%
46	IPEEP	Infraestructuras Pesqueras del Ecuador EP	75	75	100,00%	100,00%
47	MECN	Museo Ecuatoriano de Ciencias Naturales (*).	72	72	100,00%	100,00%
48	DGAC	Dirección General de Aviación Civil	68	68	100,00%	100,00%
49	SENESCYT	Secretaría Nacional De Educación Superior, Ciencia, Tecnología E Innovación	67	67	100,00%	100,00%
50	MINTUR	Ministerio de Turismo	60	60	100,00%	100,00%
51	EEQ	Empresa Electrica Quito	54	54	100,00%	100,00%
52	SNAP	Secretaría Nacional de Administración Pública	54	54	100,00%	100,00%
53	MINEDUC	Ministerio de Educación	52	52	100,00%	100,00%
54	ENAMI	Empresa Nacional Minera	51	51	100,00%	100,00%
55	STM	Secretaría Técnica del Mar	48	48	100,00%	100,00%
56	SHE	Secretaría de Hidrocarburos	47	47	100,00%	100,00%
57	FONSAT	Fondo de Seguro Obligatorio de Accidentes de Tránsito	47	47	100,00%	100,00%
58	CDE	Correos del Ecuador	46	46	100,00%	100,00%
59	MICSE	Ministerio de Coordinación de los Sectores Estratégicos	46	46	100,00%	100,00%
60	MIES	Ministerio de Inclusión Económica y Social	43	43	100,00%	100,00%
61	MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información	42	42	100,00%	100,00%
62	MIPRO	Ministerio de Industrias y Productividad	42	42	100,00%	100,00%
63	INIGEMM	Instituto Nacional de Investigación Geológico Minero Metalúrgico	40	40	100,00%	100,00%
64	CONELEC	Consejo Nacional de Electricidad	40	40	100,00%	100,00%
65	MCyP	Ministerio de Cultura y Patrimonio	39	39	100,00%	100,00%
66	CTE	Comisión de Tránsito del Ecuador	35	35	100,00%	100,00%
67	MCDS	Ministerio de Coordinación de Desarrollo Social	33	33	100,00%	100,00%
68	CONAFIPS	Corporación Nacional de Finanzas Populares	32	32	100,00%	100,00%
69	YACHAY	YACHAY EP (*)	32	32	100,00%	100,00%
70	SERCOP	Servicio Nacional de Contratación Pública	31	31	100,00%	100,00%

Anexo 5.- Aceptación de desarrollo de Trabajo de grado en Gerencia de Tecnologías Yachay E. P.

San Miguel de Urcuquí, 16 de diciembre de 2016.

Ingeniero.
Daniel Jaramillo.
COORDINADOR DE LA CARRERA DE CIERCOM
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
UNIVERSIDAD TÉCNICA DEL NORTE
Ibarra. -

De mi consideración:

En nombre y representación de la Gerencia de Tecnologías de la Empresa Pública Yachay, reciba un fraterno saludo.

En respuesta a la solicitud de autorización para que la Srta. Alejandra Mabel Pinto Erazo, portadora de la cédula de ciudadanía 040129976-3 pueda tener acceso a información necesaria para que realice su trabajo de titulación "Análisis y planteamiento de Políticas de acuerdo al Esquema Gubernamental de Seguridad de la Información (EGSI) para la Empresa Pública Yachay", pongo en su conocimiento que la solicitud es aceptada favorablemente desde el mes de Junio del 2016, y la coordinación estará a cargo de la Ing. Nataly Culqui e Ing. Giovanni Moreno, como funcionarios de las áreas de Telecomunicaciones y de Soporte y Operaciones, respectivamente.

Particular que comunico, para los fines legales consiguientes.

DIRECCIÓN DE TELECOMUNICACIONES ENERGÍA Y AUTOMATIZACIÓN
Empresa Pública
YACHAY
INVESTIGA-INNOVA-PRODUCE

Atentamente,

Ing. Edwin Ordóñez
DIRECTOR DE TELECOMUNICACIONES, ENERGÍA Y AUTOMATIZACIÓN
GERENCIA DE TECNOLOGÍAS - YACHAY E. P.

Anexo 6.- Certificado de cumplimiento del proyecto de grado en la Gerencia de Tecnologías Yachay E. P.

San Miguel de Urcuquí, 16 de Diciembre de 2016.

En calidad de **DIRECTOR DE TELECOMUNICACIONES, ENERGÍA Y AUTOMATIZACIÓN DE YACHAY E. P.**

CERTIFICO:

QUE: la señorita **ALEJANDRA MABEL PINTO ERAZO,** con cédula de ciudadanía 040129976-3 de la carrera de Ingeniería en Electrónica y Redes de Comunicación, de la Universidad Técnica del Norte, desarrolló en la Gerencia de Tecnologías, el proyecto de grado titulado: **"ANÁLISIS Y PLANTEAMIENTO DE POLÍTICAS DE ACUERDO AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA EMPRESA PÚBLICA YACHAY".**

QUE: El proyecto fue revisado por los Ingenieros: Nataly Culqui y Giovanni Moreno en el mes de diciembre del 2016. La información fue entregada en documento electrónico para la revisión en la Gerencia de Tecnologías.

Es todo cuanto puedo certificar, facultando a la interesada hacer uso de este documento como estime conveniente, excepto para trámites judiciales.

Atentamente,

DIRECCIÓN DE TELECOMUNICACIONES ENERGÍA Y AUTOMATIZACIÓN

Empresa Pública YACHAY INVESTIGA-INNOVA-PRODUCE

Ing. Edwin Ordóñez

DIRECTOR DE TELECOMUNICACIONES, ENERGÍA Y AUTOMATIZACIÓN

GERENCIA DE TECNOLOGÍAS - YACHAY E. P.

Anexo 7.- Certificado de aplicación de la encuesta con MSAT

Urcuquí, 16 de diciembre de 2016.

En calidad de **RESPONSABLE DE SEGURIDAD DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE YACHAY E. P.**

CERTIFICO

QUE: la señorita **ALEJANDRA MABEL PINTO ERAZO,** con cédula de ciudadanía 040129976-3 de la carrera de Ingeniería en Electrónica y Redes de Comunicación, de la Universidad Técnica del Norte, aplicó la encuesta sobre: **EVALUACIÓN DE RIESGOS DE LA EMPRESA PÚBLICA YACHAY**, a través de Microsoft Security Assessment Tool (MSAT), el día 08 de diciembre del presente; como uno de los requerimientos que presenta su proyecto de grado titulado: **"ANÁLISIS Y PLANTEAMIENTO DE POLÍTICAS DE ACUERDO AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA EMPRESA PÚBLICA YACHAY".**

Además, se debe informar que la señorita Alejandra Pinto compartió con mi persona, una copia digital del Informe completo que provee la Herramienta MSAT y el análisis realizado en base a dicho informe.

Es todo cuanto puedo certificar, facultando a la interesada hacer uso de este documento como estime conveniente, excepto para trámites judiciales.

Atentamente,

Giovanni Moreno Aguilar, Ing.
Responsable De Seguridad Del ÁreaDe Tecnologías De La Información
DIRECCIÓN DE SOPORTE Y OPERACIONES TECNOLÓGICAS
YACHAY E.P.

Anexo 8.- Encuesta para la evaluación de riesgos con herramienta MSAT

De acuerdo con sus respuestas acerca de la evaluación de riesgos, sus medidas de defensa se han calificado de la siguiente forma. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Leyenda: ● Cumple las mejores prácticas recomendadas ● Necesita mejorar ● Carencias severas

Infraestructura	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
Antivirus	●
Antivirus - Equipos de escritorio	●
Antivirus - Servidores	●
Acceso remoto	●
Segmentación	●
Sistema de detección de intrusiones (IDS)	●
Inalámbrico	●
Autenticación	●
Usuarios administrativos	●
Usuarios internos	●
Usuarios de acceso remoto	●
Directivas de contraseñas	●
Directivas de contraseñas-Cuenta de administrador	●
Directivas de contraseñas-Cuenta de usuario	●
Directivas de contraseñas-Cuenta de acceso remoto	●
Cuentas inactivas	●
Gestión y control	●
Informes sobre incidentes y respuesta	●
Creación segura	●
Seguridad física	●

Aplicaciones	●
Implementación y uso	●
Equilibrio de carga	●
Clústeres	●
Aplicación y recuperación de datos	●
Fabricante de software independiente (ISV)	●
Desarrollado internamente	●

Operaciones	●
Entorno	●
Host de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●
Directiva de seguridad	●
Clasificación de datos	●
Eliminación de datos	●
Protocolos y servicios	●
Uso aceptable	●
Gestión de cuentas de usuarios	●
Regulación	●
Directiva de seguridad	●
Gestión de actualizaciones y revisiones	●
Documentación de la red	●
Flujo de datos de la aplicación	●
Gestión de actualizaciones	●
Gestión de cambios y configuración	●
Copias de seguridad y recuperación	●
Archivos de registro	●
Planificación de recuperación ante desastres y reanudación de negocio	●
Copias de seguridad	●
Dispositivos de copia de seguridad	●
Copias de seguridad y restauración	●

Personal	●
Requisitos y evaluaciones	●
Requisitos de seguridad	●
Evaluaciones de seguridad	●
Directiva y procedimientos	●

Vulnerabilidades	🔴
Diseño de aplicaciones	🟡
Autenticación	🟢
Directivas de contraseñas	🟢
Autorización y control de acceso	🟢
Registro	🟡
Validación de datos de entrada	🟢
Metodologías de desarrollo de seguridad de software	🔴
Almacenamiento y comunicaciones de datos	🔴
Cifrado	🔴
Cifrado - Algoritmo	🔴

Comprobaciones del historial personal	🟢
Directiva de recursos humanos	🟢
Relaciones con terceros	🔴
Formación y conocimiento	🔴
Conocimiento de seguridad	🟡
Formación sobre seguridad	🔴

Iniciativas de seguridad

Las siguientes áreas no cumplen las mejores prácticas recomendadas y deben dirigirse a aumentar la seguridad de su entorno. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Prioridad alta	Prioridad intermedia	Prioridad baja
• Acceso remoto • Desarrollado internamente • Requisitos de seguridad • Segmentación • Usuarios de acceso remoto	• Creación segura • Conocimiento de seguridad • Inalámbrico • Registro	• Host de gestión-Servidores • Antivirus - Equipos de escritorio • Antivirus - Servidores • Directivas de contraseñas-Cuenta de administrador • Directivas de contraseñas-Cuenta de usuario