ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE TIC'S DEL DISTRITO ZONAL NO.6 "ELOY ALFARO", UTILIZANDO LA NORMA ISO 27001

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

AGUILAR QUEVEDO VIVIANA DE LAS MERCEDES
vdmaguilar@gmail.com
VALVERDE PAREDES LUIS GUSTAVO
lvalverde@eopensolutions.com

DIRECTOR: MSC. ING. SUNTAXI GABRIELA LORENA
gabriela.suntaxi@epn.edu.ec

QUITO, JULIO 2015

DECLARACIÓN

Nosotros, Aguilar Quevedo Viviana de las Mercedes, Valverde Paredes Luis Gustavo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

_____ _____

Aguilar Quevedo Viviana Valverde Paredes Luis

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Aguilar Quevedo Viviana de las Mercedes y Valverde Paredes Luis Gustavo, bajo mi supervisión.

_____

Msc. Ing. Suntaxi Gabriela Lorena

AGRADECIMIENTO

Agradezco a mi madre por todo el apoyo, a toda mi familia por permanecer conmigo, y las personas que desde el cielo siempre han cuidado de mí.

Aguilar Quevedo Viviana

AGRADECIMIENTO

Agradezco a mis padres por el esfuerzo realizado para brindarme la oportunidad de culminar mis estudios, a mi hermano por estar en los momentos difícil y por motivarme cada día a ser mejor.

Valverde Paredes Luis Gustavo

DEDICATORIA

Dedico este trabajo a mi padre, que día a día me enseño que por más duro que parezca el camino siempre hay que seguir y luchar.

Aguilar Quevedo Viviana

DEDICATORIA

Dedico este trabajo a mis padres que siempre creyeron en mí y me apoyaron en todas las dificultades que se me presentaron.

Valverde Paredes Luis Gustavo

ÍNDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Debido al creciente avance tecnológico de los últimos años, y a la cantidad de amenazas que asechan a las organizaciones en temas referentes al robo de información, surge la propuesta de los autores del presente proyecto; realizar una Planificación de un Sistema de Gestión de la Seguridad de la Información para salvaguardar los activos del Distrito Zonal N° 6 “Eloy Alfaro”, teniendo claro que nos referimos a activos como todo aquello que tenga valor, no únicamente monetario, para la organización.

Para el desarrollo del presente proyecto, se ha implementado la norma enfocada a la seguridad de la información adaptada al Ecuador, NTE INEN ISO/IEC 27001:2011; la misma que permite definir los Requisitos necesarios para poder desarrollar un Sistema de Gestión de la Seguridad de la Información, adaptable a cualquier tipo de empresas sin importar su tamaño, y la misma que ayudará a garantizar la seguridad de los activos.

Es necesario emplear una metodología de análisis de riesgos que permita identificar los pasos que se deben seguir, para realizar un adecuando Análisis de los riegos que se hayan identificado luego de un correcto proceso de identificación de activos; una adecuada identificación de amenazas que podrían afectar los activos, y una correcta identificación de las vulnerabilidades, que permitan realizar una muy acertada descripción de la situación actual de la organización.

Es por esto que el presente proyecto, pretende brindar un apoyo en el proceso de identificar, evaluar y tratar los riegos que puedan afectar la integridad, disponibilidad y confidencialidad de los activos que conforman la organización, mediante la implementación de controles propuestos por la misma norma implementada para realizar la descripción de la situación actual de la organización.

Finalmente se entrega una Planificación de un Sistema de Gestión de la Seguridad de la Información, susceptible a ser revisado, modificado y mejorado por parte de los responsables de la implementación.

RESUMEN

El presente proyecto de titulación se encuentra estructurado por cuatro capítulos, los cuales abarcan los siguientes puntos:

El Capítulo 1 cuenta con la identificación de la Organización, la cual abarca aspectos fundamentales como el detalle de la Misión, Visión y la estructura Organizacional, así como las funciones del Departamento de Tecnologías de la Información y Comunicación; también se identifican los activos que forman parte de la Organización y se describe la situación Actual de la misma.

En el Capítulo 2 a partir de los datos identificados en el capítulo anterior se procede a realizar el Análisis de Riegos para la organización, el cual inicia con la selección de una metodología para dicho Análisis, este proceso abarca diferentes etapas como son: Identificación de Vulnerabilidades, Identificación del Amenazas, Identificación de Salvaguardas, para luego proceder con la Valoración y Determinación de las escalas para la probabilidad y el impacto. Una vez identificado el Riesgo, se procede a realizar el Plan de Tratamiento de Riegos, el cual abarca y agrupa los controles propuestos por la ISO 27001:2011 (Anexo A), que van ser aplicados en la organización para luego crear políticas que nos ayuden a mitigar el impacto de los riesgos identificados.

Para finalizar, se entrega un estudio de la factibilidad de la Aplicación del Plan del SGSI, en donde se describen diferentes aspectos que influyen en la implementación del SGSI, tales como requisitos técnicos, operativos y económicos.

Capítulo 3, en esta sección se desarrolla la Evaluación del Plan, mediante la implementación de una de las políticas propuestas por los autores del proyecto, para luego realizar la debida validación, la misma que permitirá verificar los cambios operacionales dentro de la Organización y ayudar a cumplir con los objetivos establecidos.

Capítulo 4 en esta sección se presenta una serie de Conclusiones y Recomendaciones, que la Organización debe tener en cuenta al momento de la implementación del SGSI para verificar que los objetivos planteados al momento de iniciar el proyecto se hayan alcanzado.

CAPÍTULO 1: IDENTIFICACIÓN DE LA ORGANIZACIÓN

1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN

El Ministerio de Educación (MINEDUC) garantiza y asegura el cumplimiento del derecho a la educación; es decir, busca influir de manera directa sobre el acceso universal y con equidad a una educación de calidad y calidez, lo que implica ejecutar procesos de desconcentración desde la Planta Central hacia las zonas, distritos y circuitos, para fortalecer los servicios educativos y aproximarlos hacia la ciudadanía, atendiendo las realidades locales y culturales. En este contexto, las Coordinaciones Zonales, como parte del MINEDUC, tiene la misión de administrar el sistema educativo, diseñar las estrategias y mecanismos necesarios para asegurar la calidad de los servicios educativos, así también proyectos y programas educativos zonales, aprobados por la Autoridad Educativa Nacional y coordina a los niveles desconcentrados de su territorio. [1]

La implementación del Nuevo Modelo de Gestión Educativa está en desarrollo progresivo en todo el territorio ecuatoriano, incluye 9 Zonas Educativas, 140 distritos educativos y todas las áreas, secciones y direcciones del Ministerio de Educación. [2]

1.1.1 ZONAS EDUCATIVAS:

Son las encargadas de gestionar las estrategias y mecanismos necesarios para asegurar la calidad de los servicios educativos del distrito, en todos sus niveles y modalidades, gestionar proyectos y programas educativos, planificar la oferta educativa del distrito y ofertar servicios a la ciudadanía, con el objeto de fortalecer la gestión de la educación de forma equitativa e inclusiva, con pertenencia cultural que responda a necesidades educativas especiales. En la Tabla 1-1 se muestra las nueve Zonas Educativas.

ZONA ADMINISTRATIVA	PROVINCIA
ZONA 1	Esmeraldas
	Carchi
	Imbabura
	Sucumbios
ZONA 2	Pichincha (excepto el cantón de Quito)
	Napo
	Orellana
ZONA 3	Cotopaxi
	Chimborazo
	Pastaza
	Tungurahua
ZONA 4	Manabí
	Santo Domingo de los Tsáchilas
ZONA 5	Bolívar
	Los Ríos
	Guayas
	Galápagos
	Santa Elena
ZONA 6	Azuay
	Morona Santiago
	Cañar
ZONA 7	El Oro
	Loja
	Zamora Chinchipe
ZONA 8	Distrito de Guayaquil
ZONA 9	Pichincha (distrito metropolitano de quito)

Tabla 1-1 Zonas Educativas.

Fuente: Manual de calidad. Gestión Administrativa Distrital.

1.1.2. DISTRITOS ZONALES.

El distrito zonal es un nivel desconcentrado, que generalmente coincide con el área geográfica de un cantón o unión de cantones. En este nivel se brindan los servicios educativos de manera cercana a la ciudadanía, siguiendo los lineamientos definidos por el Nivel Central, así como la planificación que se desprende del Nivel Zonal.

Todos los distritos poseen una Unidad Administrativa Distrital ubicada en el ámbito cantonal. Mientras que, en el caso de los cantones grandes como Guayaquil, Quito,

Cuenca, Santo Domingo y Ambato las direcciones distritales se organizan en diversas parroquias.

Este Proyecto se centra en la Zona 9, que pertenece al Distrito Metropolitano de Quito, en esta Zona se encuentran nueve distritos Zonales, los cuales están distribuidos y agrupando diferentes Instituciones Educativas. En la Figura 1-1 se muestran los diferentes Distritos Zonales del Distrito Metropolitano de Quito. [2]

1 NOROCCIDENTE Pacto, Guale, Nanegalito, Nanegal
2 CALDERÓN Guayllabamba, Calderón, Llano Chico.
3 LA DELICIA San José de Minas, Atahualpa, Perucho, Puéllaro, San Antonio, Calacalí, Pomasqui, El Condado, Cotocollao, Ponceano, Comité del Pueblo, Carcelén, Chavezpamba, Nono.
4 CENTRO San Juan, La Libertad, Centro Histórico, Chilibulo, Itchimbía, Puengasí.
5 NORTE Cochapamba, Concepción, Belisario Quevedo, Mariscal Sucre, Rumipamba, Jipijapa, Nayón, Kennedy, San Isidro del Inca, Zámbiza, Iñaquito.
6 ELOY ALFARO Lloa, La Mena, Chilibulo, La Magdalena, Solanda, La Argelia, Chimbacalle, La Ferroviaría, San Bartolo.
7 QUITUMBE Guamaní, Chillogallo, Turubamba, Quitumbre, Amaguaña, La Ecuatoriana.
8 LOS CHILLOS La Merced, Alangasí, Amaguaña, Pintag, Guangopolo, Conocoto.
9 TUMBACO Cumbayá, Tumbaco, El Quinche, Puembo, Pifo, Yaruquí, Checa, Tababela.

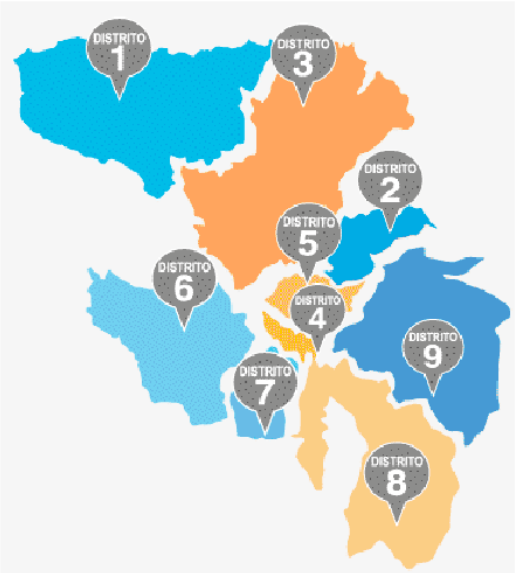


Figura 1-1 Distritos Zonales- Zona Educativa 9

Fuente. Ministerio de Educación.

1.1.2.1 Misión

Garantizar el acceso y calidad de la educación inicial, básica y bachillerato a los y las habitantes del territorio nacional, mediante la formación integral, holística e inclusiva de niños, niñas, jóvenes y adultos, tomando en cuenta la interculturalidad, la plurinacionalidad, las lenguas ancestrales y género desde un enfoque de derechos y deberes para fortalecer el desarrollo social, económico y cultural, el ejercicio de la ciudadanía y la unidad en la diversidad de la sociedad ecuatoriana. [1]

1.1.2.2 Visión

El Sistema Nacional de Educación brindará una educación centrada en el ser humano, con calidad, calidez, integral, holística, crítica, participativa, democrática, inclusiva e interactiva, con equidad de género, basado en la sabiduría ancestral, plurinacionalidad, con identidad y pertinencia cultural que satisface las necesidades de aprendizaje individual y social, que contribuye a fortalecer la identidad cultural, la construcción de ciudadanía, y que articule los diferentes niveles y modalidades de los sistemas de educación. [1]

1.1.2.3 Departamentos

El Ministerio de Educación Distrito Zonal No. 6 “Eloy Alfaro”, cuenta con varios Departamentos en los cuales se apoya para su funcionamiento, los mismos que serán enunciados a continuación:

- Denuncias
- Apoyo, Seguimiento y Regulación
- Atención Ciudadana
- Planificación
- Asesoría Jurídica
- Desarrollo Profesional
- Talento Humano
- Administración Escolar
- Financiero
- Coordinación Educativa.

De estos Departamentos que conforman el Distrito Zonal No. 6 “Eloy Alfaro”, se describirá cual es el objetivo y los servicios que brinda cada uno de ellos. [1]

1.1.2.3.1 Denuncias. [1]

El objetivo del presente departamento es solucionar conflictos del Sistema Educativo. Los servicios que presta este departamento son:

- Cobros indebidos, lesiones, maltrato psicológico, delitos sexuales, instituciones particulares, abusos de autoridad, recursos interpuestos.

1.1.2.3.2 Apoyo, seguimiento y regulación [1]

El objetivo del presente departamentos es asesorar, dar seguimiento, controlar y regular la gestión de las Instituciones Educativas.

Los servicios que presta este departamento son:

- Reconocimiento de estudios en el exterior
- Matrícula excepcional
- Traspaso de tercera matrícula
- Registro del cronograma de los 200 días laborales
- Recalificación de exámenes (Apelaciones Última Instancia)
- Exámenes de Ubicación
- Registro del proyecto Educativo Interinstitucional (PEI)
- Registro del Código de Convivencia
- Traslado de Estudiantes
- Aplicación de Gestión de Excepciones de Sistema SIGEE

1.1.2.3.3 Atención ciudadana [1]

El objetivo del presente departamento es atender a la Comunidad Educativa, proporcionando soluciones efectivas.

Los servicios que presta este departamento son:

- Certificado de Terminación de Educación Básica
- Refrendación de actas de grado
- Duplicado y refrendación de títulos
- Certificación de matrículas y promociones de instituciones educativas desaparecidas
- Registro y legalización de actas de grado y títulos de bachiller de colegios desaparecidos
- Rectificación de nombres y/o apellidos de documentos oficiales
- Legalización de títulos y documentación para el exterior

- Legalización de cuadros de calificaciones y promociones de instituciones educativas
- Legalización de documentos de gremios y asociaciones de formación artesanal
- Reconocimiento de estudios artesanales
- Duplicado de título artesanal
- Reconocimiento de estudios de centros ocupacionales
- Educación especial e inclusiva
- Manejo básico de SIGEE, SIME, tickets y AMIE

1.1.2.3.4 Planificación [1]

El objetivo del presente departamento es coordinar y ejecutar los procesos para Organizar la oferta educativa.

Los servicios que presta este departamento son:

- Permisos de creación, renovación y cambio de domicilio de instituciones educativas
- Cierre de funcionamiento de instituciones educativas
- Autorización de reposición/incremento y reubicación de docentes
- Archivo maestro de instituciones educativas
- Creación de jornadas/niveles educativos y paralelos
- Cierre de jornadas/niveles educativos y paralelos
- Cambio de denominación

1.1.2.3.5 Asesoría jurídica [1]

El objetivo del presente departamento es el de garantizar el cumplimiento de la ley en todos los actos del Distrito e Instituciones educativas.

Los Servicios que presta este departamento son:

- Ratificación de vocales del consejo ejecutivo
- Ratificación de gobierno escolar
- Personas sin fines de lucro (fundaciones y organizaciones)

1.1.2.3.6 Desarrollo profesional [1]

El objetivo del presente departamento es ayudar a la selección y capacitación del personal de cada una de las Instituciones a cargo del Distrito Zonal.

Los servicios que prestan este departamento son:

- Elegibilidad de aspirantes a docentes
- Retorno de becarios del GO-TEACHER
- Concursos de méritos y oposición
- Certificado de SIPROFE

1.1.2.3.7 Talento humano [1]

El objetivo del presente departamento es administrar y gestionar el Talento Humano de manera efectiva.

Los servicios que presta este departamento son:

- Certificación de tiempo de servicio
- Certificado de no haber sido sancionado
- Certificado de no estar inmerso en sumario administrativo
- Comisión de servicios
- Solicitud de vacaciones
- Solicitud de permisos y licencias
- Renuncias
- Jubilaciones
- Ternas

1.1.2.3.8 Administración escolar [1]

El objetivo del presente departamento es gestionar la distribución adecuada de recursos educativos para las Instituciones Educativas.

Los servicios que presta este departamento son:

- Asignación de textos, alimentos y uniformes
- Asignación de mobiliario
- Mantenimiento y construcción de infraestructura

- Plan de riesgos
- Gestión de planillas de proveedores

1.1.2.3.9 Financiero [1]

El objetivo del presente departamento es administrar y gestionar la ejecución de los recursos financieros para cumplir los objetivos del Distrito.

Los servicios que presta este departamento son:

- Asignación de recursos
- Certificado de remuneraciones

1.1.2.3.10 Coordinación educativa [1]

El objetivo del presente departamento es apoyar en la coordinación de cada una de las Instituciones.

Los servicios que presta este departamento son:

- Registro de participación estudiantil
- Aprobación mallas curriculares
- Aprobación de bilingüismo
- Aprobación de proyectos de innovación curricular
- Selección de instituciones educativas postulantes al bachillerato internacional (colegios particulares)
- Aprobación de bachillerato técnico
- Concursos, presentaciones, participaciones y desfiles
- Inscripción de educación inicial, básica y bachillerato
- Aprobación de educación para jóvenes con escolaridad inconclusa
- Aprobación de educación especial e inclusiva
- Aprobación de educación básica para jóvenes y adultos

1.1.2.4 Orgánico Funcional

El Organigrama Funcional es la representación gráfica de la estructura del Ministerio de Educación para todos los Distritos Zonales existentes, todos siguen la misma

estructura. En la Figura 1-2 se puede visualizar la estructura que tiene el Ministerio de Educación y se podrá visualizar la posición de los Distritos. [1]

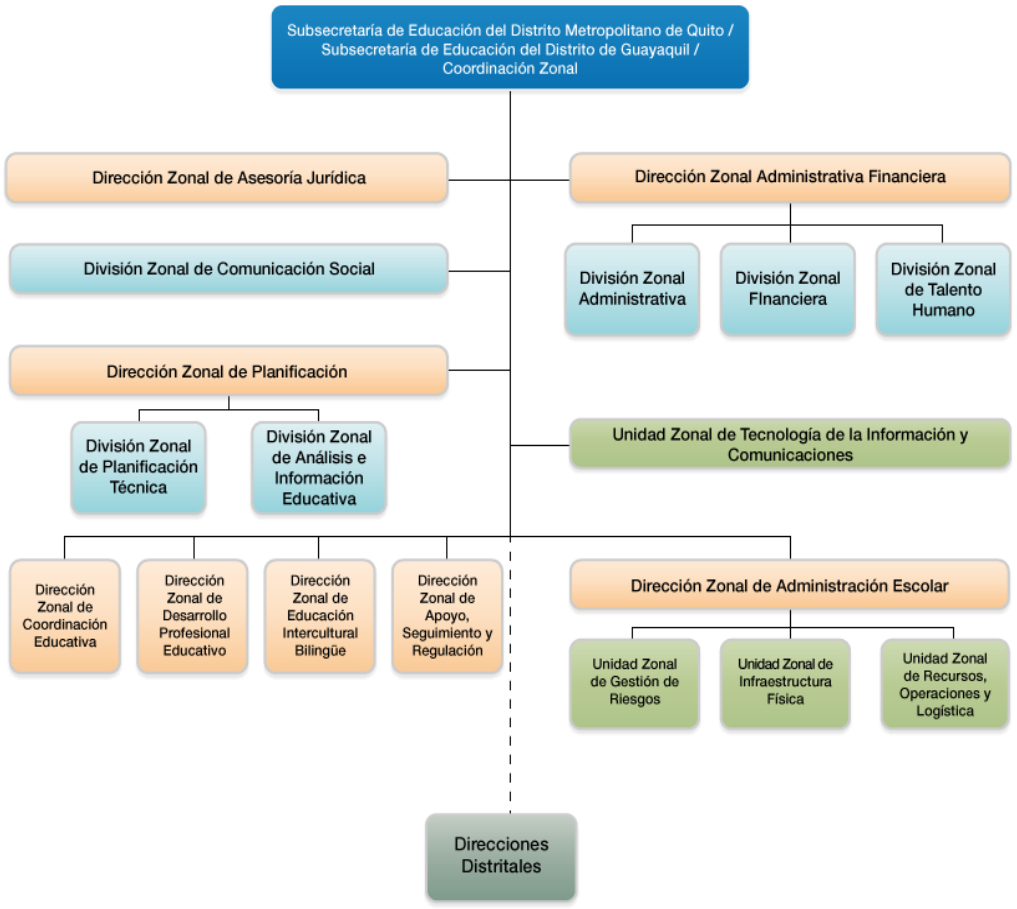


Figura 1-2 Orgánico Funcional del Ministerio de Educación

Fuente: Ministerio de Educación.

El Organigrama Funcional del Distrito Zonal N°6 “Eloy Alfaro”, muestra de forma esquemática y jerárquica todas las áreas que lo integran; dentro del Orgánico se puede observar las principales funciones que tiene asignada cada área. En el Ministerio de Educación este esquema es de mucha utilidad puesto que ayuda en las capacitaciones del personal y presenta la Organización en forma general. La Figura 1-3 muestra la estructura Organizacional del Distrito Zonal N°6 “Eloy Alfaro”. Donde se muestra la estructura interna y los diferentes Departamentos que tiene esta entidad.

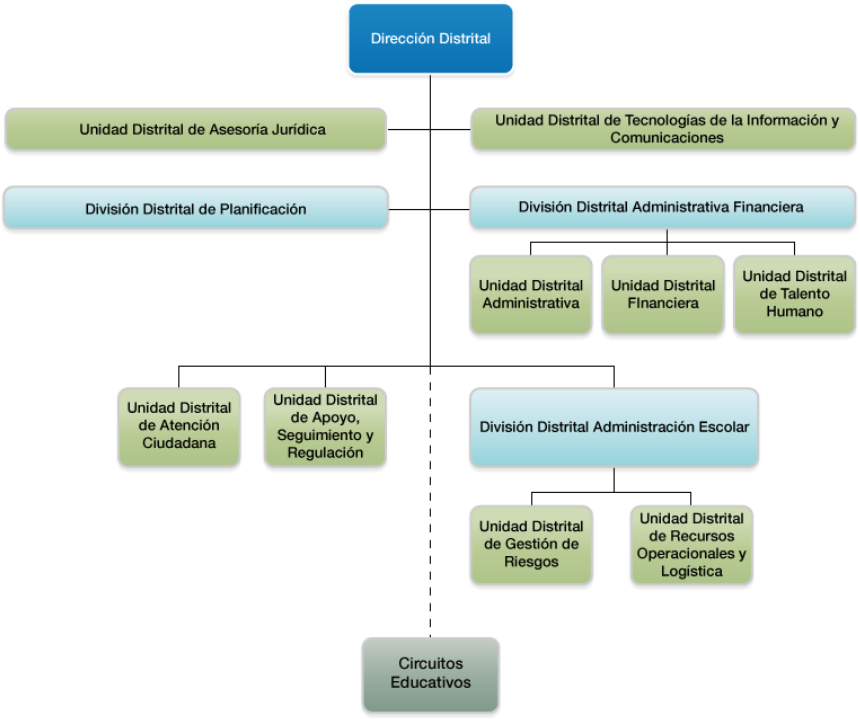


Figura 1-3 Orgánico Funcional del Distrito Zonal No.6 "Eloy Alfaro"

Fuente: Ministerio de Educación.

1.1.2.5 Descripción de la Unidad Informática.

El departamento de Tecnología y Comunicación, es el responsable de brindar soporte a los demás departamentos, para que estos puedan desempeñar sus actividades de forma óptima, mediante la implementación de herramientas tecnológicas de manera eficiente.

El objetivo del departamento es brindar soporte tecnológico al Distrito Zonal y a la ciudadanía siendo estos sus principales clientes.

1.1.2.5.1 Misión [1]

Aplicar e implementar las políticas, normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicación orientados a la optimización de recursos, sistematización y automatización de los procesos en el ámbito de su gestión.

1.1.2.5.2 Funciones [1]

Las principales funciones del área de Informática del Distrito Zonal N 6 “Eloy Alfaro” son las siguientes:

- Aplicar políticas y normativas alineadas a los estándares para la ejecución de proyectos de sistematización, automatización, adquisición y/o contratación de bienes y/o servicios tecnológicos informáticos del distrito.
- Proporcionar soporte en los procesos tecnológicos del Distrito.
- Monitorear de forma permanente los servicios tecnológicos del Distrito.
- Administrar la infraestructura tecnológica en el nivel Distrital.
- Supervisar el buen uso de las herramientas e infraestructura tecnológica del Distrito.
- Apoyar en la coordinación de los proyectos realizados por la Dirección Nacional de Tecnología Educativas y el SITEC.
- Aplicar las políticas para la administración, gestión y control de los bienes y servicios.
- Controlar los bienes del Distrito con sus correspondientes ingresos y egresos.
- Coordinar y consolidar la planificación de las diferentes áreas de la Dirección Distrital a fin de elaborar el Plan Anual de Contrataciones (PAC) para su aprobación.
- Informes de equipo informático en buen funcionamiento.
- Informe mensual de soporte técnico efectuado.
- Reporte de disponibilidad de servicios tecnológicos.
- Informes de disponibilidad de la infraestructura tecnológica.
- Solicitudes de requerimiento de infraestructura tecnológica.

1.1.2.5.3 Roles y responsabilidades. [1]

El Departamento de TIC’s del Distrito Zonal No. 6 “Eloy Alfaro”, cuenta con personal capacitado para el desarrollo de todas la funciones, se manejan cuatro roles en

específico dentro de este Departamento organizado en forma jerárquica, estos roles se puede visualizar en la Figura 1-4.

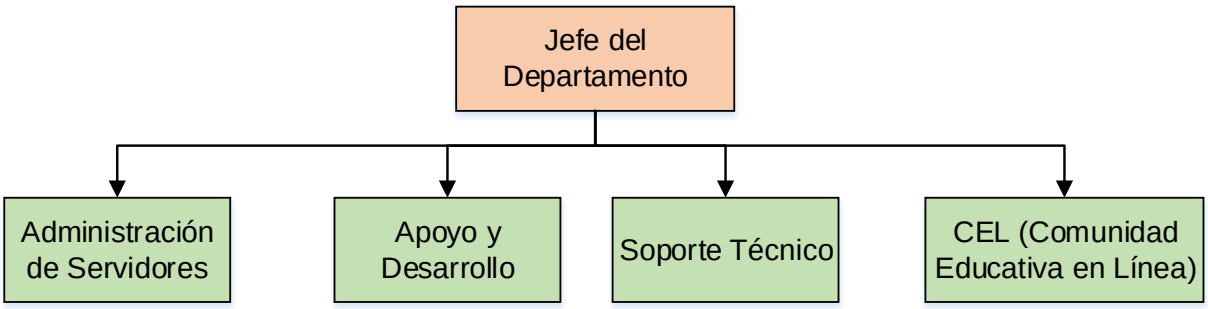


Figura 1-4 Estructura Organizacional del Departamento de TIC's.

Fuente: Los Autores

Jefe del Departamento: es el encargado de supervisar las actividades a realizar por cada persona dentro del Departamento. Así como de asesorar a la ciudadanía, e Instituciones en la adquisición de tecnología y manejo de la misma.

Administración de Servidores: es la persona encargada del adecuado funcionamiento de los Servidores, tomando en cuenta el buen funcionamiento y el cumplimiento de las políticas vigentes sobre las carpetas compartidas que maneja la Institución.

Apoyo y Desarrollo: es la persona encargada de brindar apoyo en el desarrollo de los procesos que la Organización este ejecutando, así como también es la persona encarga de comunicar a las Instituciones de dichos procesos.

El rol del desarrollador es el de realizar el análisis, diseño y desarrollo de aplicaciones requeridas para un mejor funcionamiento del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro".

Soporte Técnico: es la persona encarga del soporte y mantenimiento de todas las máquinas del Distrito, así como del soporte en incidentes que se puedan presentar relacionados con la tecnología.

CEL. (Comunidad Educativa en Línea): son las personas encargadas de brindar la capacitación necesaria a las diferentes Instituciones, estas capacitaciones están orientada al adecuado manejo de la tecnología.

1.2 INFORMACIÓN QUE MANEJA LA ORGANIZACIÓN.

El Distrito Zonal No. 6 “Eloy Alfaro”, maneja Información de las Instituciones a su cargo, de los docentes, trabajadores, estudiantes y ciudadanía en general. Para lo cual cuenta con una Infraestructura Física, una Red y Aplicaciones que ayudan al Departamento de TIC’s a brindar los servicios necesarios para la satisfacción de los usuarios.

1.2.1 INFORMACIÓN FÍSICA.

En la Tabla 1-2 se muestran los activos del Departamento de TIC’s, los cuales son utilizados para su adecuado funcionamiento, esta información fue tomada del inventario realizado a los activos físicos de la Organización Anexo 1.

ACTIVO	CANTIDAD	DESCRIPCIÓN	MARCA	ESTADO
Laptop	2	• INTEL CORE I5 3210 2,50 GHZ • 4GB RAM • DISCO 500 GB	HP	Regular
		• Acer Aspire CI7 3,40 GHZ • 4GB RAM	HACER	Bueno
Monitor	3	Monitor HP L710	HP	Regular
		Monitor Lenovo	Lenovo	Bueno
		Monitor de 18.5” BenQ G910	Ultratech	Bueno

ACTIVO	CANTIDAD	DESCRIPCIÓN	MARCA	ESTADO
CPU	3	• INTEL PENTIUM DUAL E2180 2GHZ • 1GB RAM • DISCO 150 GB	HP	Bueno
		• INTEL CORE 2 QUAD 2.33 GHZ • 2GB RAM • DISCO 250 GB	HP	Bueno
		• INTEL CORE I3 4130 3,0 GHZ • 2GB RAM • DISCO 500 GB	Ultratech	Bueno
Servidor	1	Servidore HP	HP	Regular
Switch	2	Switch Triplite	No Especifica	Regular
		Switch 48 puertos	HP	Regular
Patch Panel	3	Path Panel 24 puertos	No Especifica	Regular
Impresora	3	Impresoras Data Card SD 360	DUAL SIDE	Bueno
		Xerox Phaser 3160 N 24PPM Mono Laser	Xerox	Bueno
		Máquina impresora de tarjetas PVC Data Card 5D 360	Data Card	Bueno
Teléfono IP	1	GXP 2100	GrandStream	Bueno

Tabla 1-2 Activos tecnológicos del Departamento de TIC's

Fuente: Los Autores.

El Departamento de TIC's del Distrito Zonal No. 6 "Eloy Alfaro", cuenta también con bienes muebles los cuales se encuentran inventariados, ver Anexo 1 "Activos Fijos del de Departamento de TIC's del Distrito No.6 Eloy Alfaro".

Para el funcionamiento del Departamento de TIC's del Distrito Zonal 6 "Eloy Alfaro" se usan dos Servidores mediante los cuales se desempeñan las tareas diarias en la Institución, los mismos que serán detallados a continuación:

1.2.1.1 Servidor de documentación

En este servidor se almacena toda la información recolectada en el Departamento de Atención Ciudadana, en la cual se receptan todas las quejas o denuncias

provenientes de las Instituciones bajo su cargo o de personas particulares que requieran realizar algún trámite en la misma.

Características del Servidor:

- Se encuentra administrado por el mismo Distrito Zonal.
- El servidor funciona sobre una máquina virtual con Sistema Operativo Windows 2008 Server R2.
- El sistema operativo donde se encuentra el servidor no cuenta con la licencia respectiva.
- La máquina virtual empleada para administrar el Servidor es VMWare Sphere.

Detalle de la Máquina Virtual:

- Sistema Operativo: Windows Server 2008 R2 Enterprise de 64 bits.
- Memoria (RAM): 4 GB.
- Disco duro: 500 GB.

Detalle de la Máquina Física:

- Sistema Operativo: Windows 8 de 64 bits.
- Memoria (RAM): 6GB.
- Disco duro: 1 TB.
- Procesador: Intel Xeon 2.30 GHz.

1.2.1.2 Servidor de telefonía.

Este servidor ayuda a controlar y gestionar la comunicación dentro del Distrito Zonal No.6 “Eloy Alfaro”

Características del Servidor:

- El servidor se encuentra levantado sobre un sistema operativo Centos 7.
- El servidor se encuentra administrado por la Subsecretaría de Educación específicamente por la Sra. Cecibel Chamba, por esta razón no es posible detallar las características físicas del mismo.

- La aplicación que utiliza este servidor es Asterisk. Asterisk es un framework de código abierto para la creación de aplicaciones de comunicaciones, Asterisk convierte una computadora normal en un servidor de comunicaciones.

1.2.2 RED – TOPOLOGÍA.

El Ministerio de Educación es la entidad responsable del diseño de la Topología de la Red para los diferentes Distritos Zonales, el cual se puede visualizar en la Figura 1-5. Es decir la topología de Red de Todos los Distritos Zonales son los mismos, esto se debe a que los distritos deben cumplir con estándares establecidos por la Norma ISO 9000:2005.

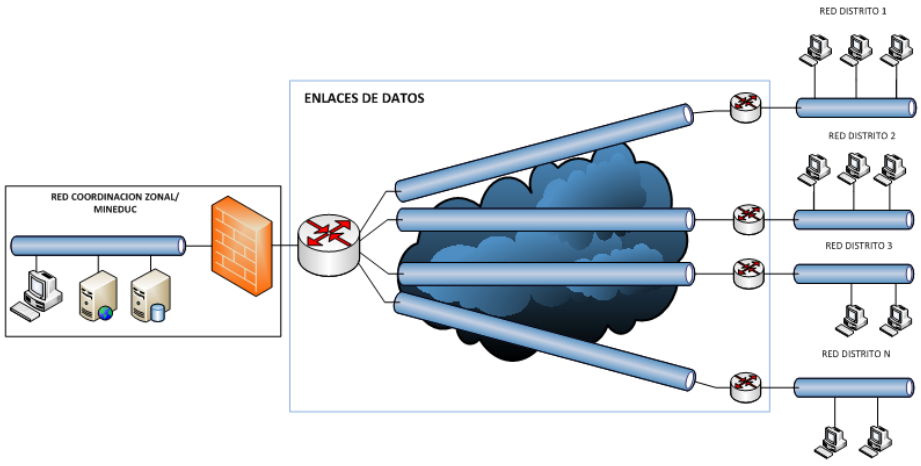


Figura 1-5 Diagrama de Red de los Distritos

Fuente: Subsecretaría de Educación.

El Ministerio de Educación establece el diseño de Red que los Distritos deben tener, el cual se puede visualizar en la Figura 1-6.

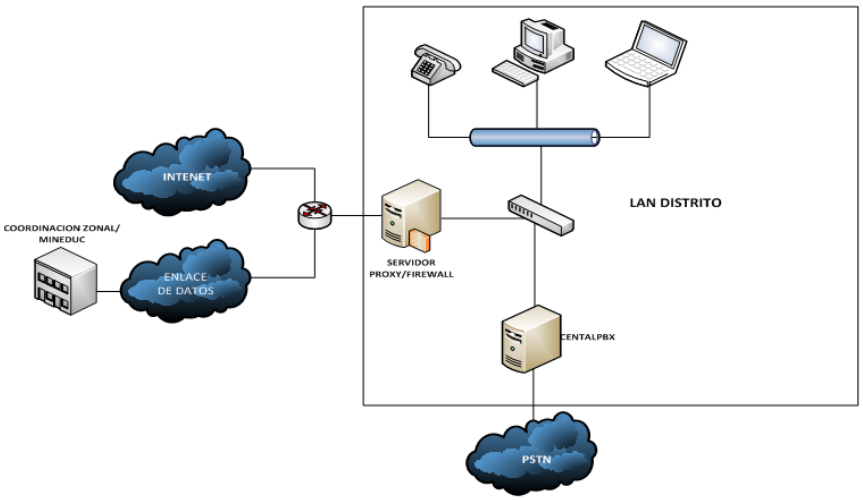


Figura 1-6 Diagrama de Red del Distrito Zonal

Fuente: Subsecretaría de Educación.

1.2.3 APLICACIONES.

Las aplicaciones administradas por el personal del Distrito Zonal N° 6 “Eloy Alfaro” se detallan en Tabla 1-3:

DEPARTAMENTO	SISTEMA
Tecnologías de la Información y la Comunicación	Alfresco
	OSTicket
	MOGAC
	Quipux
	Zentyal
	SIME
	UniFi
	Elastix

Tabla 1-3 Aplicaciones Administradas por el Departamento de TIC’s

Fuente: Los Autores

A continuación se detalla todas las aplicaciones que son utilizadas por el Departamento de TIC’s del Distrito Zonal No.6 “Eloy Alfaro”.

1.2.3.1 ALFRESCO

"Es la plataforma de código abierto para la colaboración y gestión de documentos críticos para la empresa. Al automatizar los procesos empresariales que utilizan muchos documentos y permitir la colaboración a gran escala, Alfresco ayuda a las empresas a mejorar la prestación de servicios a los clientes, y a adaptarse con mayor rapidez a los cambios del mercado."[1]

El sistema es implementado por la Subsecretaría de Educación, con el objetivo de almacenar documentos importantes para la Organización. Siendo los Departamentos que conforman el Distrito los únicos autorizados con el permiso para la lectura de los archivos allí publicados, inclusive el departamento de TIC's.

1.2.3.2 OSTICKET

Este sistema funciona, únicamente en períodos de matrículas en las instituciones bajo la administración Zonal, el sistema se encuentra alojado en el Ministerio de Educación y es utilizado para administrar turnos de matriculación, para los estudiantes en las instituciones.

1.2.3.3 MOGAC

Es un sistema desarrollado por el Ministerio de Educación conjuntamente con personal de la ciudad de Cuenca, cuenta con una plataforma amigable y contiene un mayor número de funcionalidades; por ejemplo: administra la seguridad interna, interacción con la aplicación Quipux y cuantifica el tiempo que un usuario es atendido en los diferentes Departamentos.

En este sistema se manejan todos los procesos solicitados por los usuarios, los mismos que son administrados por el departamento de TIC's, aunque el sistema como tal se encuentra alojado en el Ministerio de Educación, en él se puede verificar los avances de los procesos y administrar nuevos usuarios del sistema.

---

[1] Fuente: http://www.alfresco.com/es/products

1.2.3.4 QUIPUX

"Es un servicio web que la Subsecretaría de Tecnologías de Información de la Secretaría Nacional de la Administración Pública, pone a disposición de entidades o instituciones públicas. Permite el registro, control, circulación y organización de los documentos digitales y/o físicos que se envían y reciben en una Institución.

Quipux, gestiona la documentación digital y/o impresa, dicha documentación puede ser:

Interna: aquella que se remite y se recibe en los departamentos de la misma organización.

Externa: la que es emitida por entidades y la enviada por la ciudadanía a su organización."[2]

El sistema está bajo la custodia directa de la Presidencia de la República del Ecuador, con un delegado en el Distrito Zonal No. 6 "Eloy Alfaro", el cual recibe las notificaciones a realizar y puede administrar usuarios. Estas actividades no se encuentran dentro de las funciones del Departamento de TIC's, por lo que estas actividades deben realizarse fuera de las Instalaciones Distritales, estos procesos son monitoreados por la persona a cargo con la finalidad de cumplir los plazos establecidos.

1.2.3.5 ZENTYAL

"Servidor Zentyal es un servidor Linux para pymes, que puede actuar como una puerta de enlace, Administrador de Infraestructura, Unifica la administración de las Amenazas, servidor de comunicaciones unificadas o una combinación de ellos. Estas funcionalidades están estrechamente integradas, automatizando la mayoría de las tareas, evitando errores y ahorrando tiempo para los administradores del sistema."[3]

Este sistema permite administrar la red de la organización, administrar el ancho de banda y es empleado como Proxy.

---

[2] Fuente: http://www.gestiondocumental.espol.edu.ec/

[3] Fuente: https://wiki.zentyal.org/wiki/Zentyal_Wiki Traducido por: Los Autores

Este sistema es administrado por el responsable del Departamento de TIC's del Distrito.

1.2.3.6 SIME

"Sistema de Información del Ministerio de Educación", este sistema permite administrar los perfiles de las personas que trabajan en las instituciones bajo su cargo, este sistema se encuentra alojado en el Ministerio de Educación.

1.2.3.7 UNIFI

Esta herramienta es utilizada por la organización, únicamente como un Access Point (AP).

1.2.3.8 ELASTIX.

Esta herramienta es utilizada por la organización para administrar la telefonía IP, realiza la asignación de extensiones a cada departamento y la información general es almacenada en el Departamento de TIC's.

1.3 DIAGNÓSTICO DE ACTIVOS DE TI

1.3.1 DESCRIPCIÓN DE LA NORMA NTE INEN[4]-ISO/IEC 27000:2012 [2]

La Norma NTE INEN-ISO/IEC 27000:2012, es un marco de trabajo adaptable a cualquier tipo de organizaciones sea pública o privada, grande o pequeña; teniendo como objetivo principal establecer una descripción global de la familia de normas necesarias para un SGSI. Nos brinda una breve introducción a todos los aspectos relacionados al Sistema de Gestión de la Seguridad de la Información SGSI; así como también detalla el proceso PDCA (plan – do – check- act), términos y definiciones necesarios para el uso de la familia de normas.

1.3.1.1 Familia de normas SGSI.

[4] INE: Instituto Ecuatoriano de Normalización.

La NTE INE-ISO/IEC 27000:2012 está compuesta de una serie de normas, las cuales tienen como objetivo ayudar a la creación, implementación y operación de un SGSI. En la siguiente tabla 1-4 se detalla la Familia de normas SGSI con una descripción de las mismas.

NORMA ISO.	DETALLE
NTE INE-ISO/IEC 27000	Descripción general y vocabulario para un Sistema de gestión de la seguridad de la Información.
NTE INE-ISO/IEC 27001	Requisitos para un Sistema de gestión de la seguridad de la Información.
NTE INE-ISO/IEC 27002	Código de práctica para la gestión de la seguridad de la información.
NTE INE-ISO/IEC 27003	Guía de implementación del sistema de gestión de la seguridad de la información.
NTE INE-ISO/IEC 27004	Medición para la gestión de la seguridad de la información.
NTE INE-ISO/IEC 27005	Gestión del riesgo de la seguridad de la información.
NTE INE-ISO/IEC 27006	Requisitos para las organizaciones que realizan auditorias y proveen certificaciones a los sistemas de gestión de la seguridad de la información.
NTE INE-ISO/IEC 27007	Directrices para realizar auditorías a los sistemas de gestión de la seguridad de la información.
NTE INE-ISO/IEC 27011	Directrices para la gestión de la seguridad de la información para organizaciones de telecomunicaciones, basadas en la NTE INEN ISO/IEC 27002.
NTE INE-ISO/IEC 27799	Gestión de la seguridad de la información para la salud.

Tabla 1-4 Familia de Normas SGSI.

Fuente: Norma INEN-ISO/IEC 27000:2012

1.3.2 DESCRIPCIÓN DE LA NORMA NTE INEN-ISO/IEC 27001:2011 [3]

La NTE INEN – ISO/IEC 27001:2011, se implementó en el 2011, siendo idéntica a la norma ISO/IEC 27001:2005; es considerada la principal norma de la familia SGSI, puesto que es la única certificable.

Tomando en cuenta los riegos a los cuales se encuentra expuesta la organización, la norma específica un modelo para la creación, implementación, ejecución, revisión, mantenimiento y mejora de un Sistema de la Seguridad de la Información; siempre basándose en la implantación de los controles adecuados para satisfacer las necesidades de la organización. La norma siempre tiene como objetivo la mejora continua en la seguridad de la información.

Una de las características más relevantes que brinda la norma ISO/IEC 27001:2011, es que se adapta al modelo PDCA para todos los procesos de la organización, en la Figura 1-7 se puede visualizar el ciclo del modelo PDCA, incluyendo una referencia actual de la situación de la Organización, y una situación futura a la que espera que la Organización pueda llegar luego de implementar el SGSI.

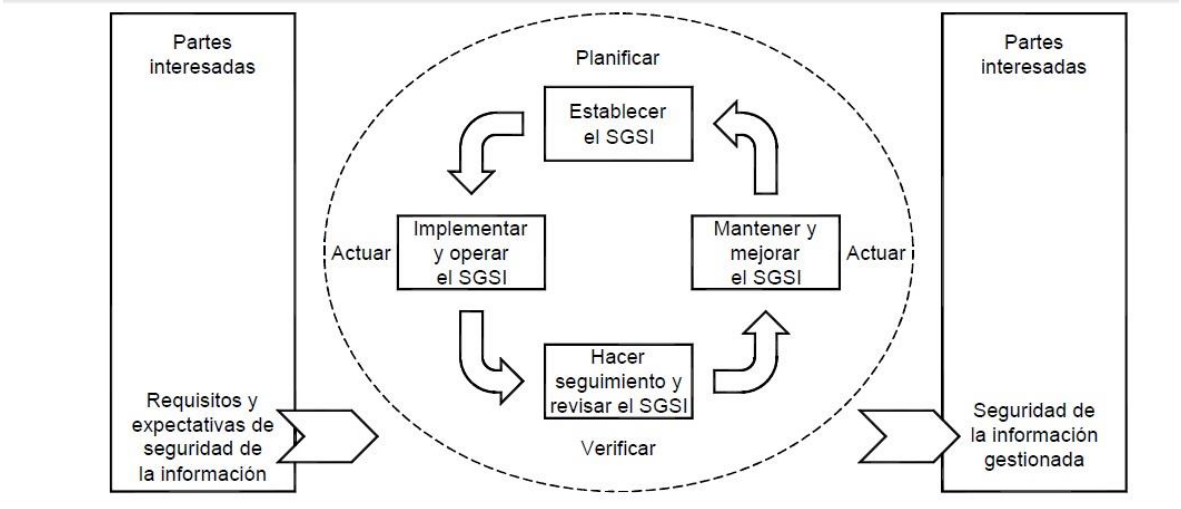


Figura 1-7 Modelo PDCA aplicado a los procesos del SGSI

Fuente: NTE INE-ISO/IEC 27001:2011

Para poder identificar la relación que existe entre en modelo PDCA y el Sistema de Gestión de Seguridad de la Información se utilizará la Tabla 1-5, en donde especifica las actividades a realizar en cada fase.

PDCA		DESCRIPCIÓN.
PLAN	Establecer el SGSI	• Definir el objetivo del SGSI • Definir las políticas del SGSI • Definir procesos y procedimientos del SGSI • Identificar riegos • Análisis y evaluación de riesgos • Tratamiento de riesgos • Selección de controles que faciliten el tratamiento de los mismos.
DO	Implementar y gestionar el SGSI	• Preparara un Plan de Tratamiento de riesgos • Implantar los controles seleccionados. • Implantar las políticas creadas. • Implantar los procesos y procedimientos. • Medir la eficacia de los controles seleccionados • Crear programas de concienciación.
CHECK	Monitorizar y revisar el SGSI	• Revisar internamente el SGSI • Realizar auditorías internas del SGSI. • Informar de los resultados a la Dirección para su revisión.
ACT	Mantener y mejorar el SGSI.	• Adoptar las acciones correctivas • Adoptar las acciones preventivas • Revisión del SGSI por parte de la Dirección para lograr la mejora continua.

Tabla 1-5 Modelo PDCA y su relación con el SGSI

Fuente: NTE INE-ISO/IEC 27001

Dentro de la Planificación de un Sistema de Gestión de la Seguridad de la Información para el departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro", se centra en la primera fase del modelo PDCA, es decir su punto de ejecución es Planificar (creación del SGSI).

1.3.3 SITUACIÓN ACTUAL DEL DEPARTAMENTO DE TI

Para realizar la descripción de la Situación Actual del departamento de TI, se ha utilizado el Anexo A de la Norma ISO/IEC 27001:2011, el mismo que proporciona varios controles recomendados, los mismos que son necesarios para el desarrollo de un Sistema de Gestión de la Seguridad de la Información.

Dicho análisis fue realizado mediante entrevistas con el Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro", en cual se evaluó el cumplimiento o no cumplimiento de cada uno de los controles propuesto por la Norma ISO/IEC 27001:2011, según se muestra en la Tabla 1-6.

ESTADO	VALOR
Cumple	1
No Cumple	0

Tabla 1-6 Valoración de Cumplimiento para los Controles

Fuente: Los Autores

Para realizar el cálculo del porcentaje de cumplimiento actual, se suma el número de controles aplicados (los que tengan valor 1) por dominio, para luego aplicar la siguiente expresión:

$$Porcentaje\ de\ cumplimiento\ actual = \frac{\sum Controles\ Usados\ actualmente * 100\%}{\sum\ Controles\ por\ Dominio}$$

Donde:

- **Porcentaje de cumplimiento actual:** es el valor que se busca calcular.
- **Controles Usados Actualmente:** es la sumatoria de todos los controles que se están utilizando en la actualidad por dominio.

- **Controles por Dominio:** sumatoria de todos los controles propuestos por la Norma ISO/IEC 27001:2011, por dominio.

En la Tabla 1-7 se puede visualizar el porcentaje de cumplimiento de los controles por dominio, antes de implementar los controles, luego de haber realizado el cálculo antes mencionado.

DOMINIO		PORCENTAJE DE CUMPLIMIENTO ACTUAL.
A.5	Política de Seguridad	100.00%
A.6	Aspectos Organizativos de la Seguridad de la Información	18.18%
A.7	Gestión de Activos	40.00%
A.8	Seguridad Ligada a los Recursos Humanos	44.44%
A.9	Seguridad Física y Ambiental	61.54%
A.10	Gestión de Comunicaciones y Operaciones	21.88%
A.11	Control de Acceso	8.00%
A.12	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	12.50%
A.13	Gestión de Incidentes de Seguridad de la Información	20.00%
A.14	Gestión de la Continuidad del Negocio	60.00%
A.15	Cumplimiento	0%

Tabla 1-7 Porcentaje de cumplimiento previo a la implementación de controles

Fuente: Los Autores

Para poder revisar los controles que actualmente se encuentran aplicados en la Organización se puede revisar el Anexo 2.

Una vez definido el porcentaje de los controles utilizados, se presenta un resumen de la situación actual por dominio, el cual se puede visualizar en la Tabla 1-8.

OBJETIVOS DE CONTROL Y CONTROLES		
A.5	Política de Seguridad	El Distrito Zonal cuenta con un documento de política de seguridad, pero no cuenta con un cronograma de revisiones al documento.
A.6	Aspectos Organizativos de la Seguridad de la Información	El Distrito Zonal cuenta con el apoyo de la dirección con respecto a la seguridad de la información, pero no existe el mismo compromiso por parte de los demás departamentos.
A.7	Gestión de Activos	Dentro del Distrito Zonal se cuenta con un inventario de los activos, sin embargo no se realiza una correcta clasificación de los mismos y tampoco se maneja un adecuado sistema de etiquetado de la información.
A.8	Seguridad Ligada a los Recursos Humanos	En el Distrito Zonal, las responsabilidades y funciones de las personas contratadas, no concuerdan con las tareas realizadas dentro de la organización; Talento Humano, es el departamento responsable de la contratación de nuevos empleados, no realiza una revisión de los antecedentes de las personas, no realiza las capacitaciones necesarias para tratar de concientizar a los empleados de la importancia de un adecuado manejo de la información.
A.9	Seguridad Física y Ambiental	Ésta cuenta con un servicio de guardiana, tanto en el acceso a la organización como a los departamentos, con lo que respecta a la seguridad ante desastres naturales, el Distrito Zonal cuenta con un Plan de Contingencia, ya que en caso que se produzca una catástrofe, se pueda recuperar y seguir prestando los servicios en el menor tiempo posible.

OBJETIVOS DE CONTROL Y CONTROLES		
A.10	Gestión de Comunicaciones y Operaciones	Los procesos se encuentran documentados, sin embargo no se cuenta con un proceso de Gestión de Cambios, lo que puede ser perjudicial para la organización. De la misma manera no se realizan las capacitaciones necesarias al personal, pero no se cuenta con una adecuada gestión frente a códigos maliciosos que los empleados pudieran ejecutar sin darse cuenta.
A.11	Control de Acceso	El Distrito Zonal cuenta con políticas de control de acceso, nadie puede ingresar a los departamentos sin antes haberse identificado con el personal de vigilancia que se encuentra en las instalaciones, referente a los controles de acceso a los sistemas de Software, no existe un correcto manejo de las contraseñas, esto debido a que; para los empleados esto puede generar molestias o simplemente no cuentan con una adecuada capacitación sobre el cuidado y responsabilidad con las que estas credenciales deben manejarse.
A.12	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	El Distrito Zonal para su adecuado funcionamiento utiliza algunos Sistemas, los cuales son implementados gracias a la Subsecretaria de Educación, vale recalcar que el Distrito no pude acceder al código fuente de los mismos, así como tampoco puede decidir o implementar formas para proteger la información dentro de los sistemas.
A.13	Gestión de Incidentes de Seguridad de la Información	Debido a una posible falta de capacitación, no existe una adecuada comunicación entre departamentos, lo que provoca inconvenientes relacionados con eventos de seguridad, no se notifican posibles puntos débiles o falencias localizadas, pero cada departamento cuenta con un responsable, sobre el cual recaen sanciones en caso de fallos, y también es el responsable de realizar la recopilación de evidencias que permitan identificar futuros inconvenientes, pero lo cual por el momento no es realizado en ningún departamento.
A.14	Gestión de la Continuidad del Negocio	El Distrito Zonal cuenta con un plan de contingencia, el mismo asegura que se pueda levantar lo servicios en caso de desastre, de esta forma resguarda la información para así poder cumplir con los objetivos de Calidad establecidos por la Organización.
A.15	Cumplimiento	No se maneja ningún tipo de control frente al uso de software crackeado, esto debido a la falta de asignación de presupuesto por parte de las entidades superiores, tampoco se manejan licencias de ningún tipo para los sistemas empleados ni se protegen los datos de carácter personal, no se controla el uso indebido de los recursos empleados

OBJETIVOS DE CONTROL Y CONTROLES		
		para el tratamiento de la información ni para las herramientas de Auditoría de los sistemas de información.

Tabla 1-8 Objetivos de Control

Fuente: Los Autores

1.3.3.1 Resumen de la Situación Actual

Luego de haber realizado un análisis de los controles propuestos por la norma INE-ISO/IEC 27001:2011, se puede concluir que la Dirección Distrital de la Zonal N° 6 “Eloy Alfaro”, tiene clara la importancia de la información que manejan, sin embargo, no se puede decir lo mismo de todos los departamentos que conforman el Distrito, algunos de los empleados no le dan la debida importancia, tanto a la información como a las claves de acceso a los sistemas que manejan, lo que puede provocar inconvenientes en caso de fallos. Así también el Distrito cuenta con la debida documentación, como es el caso de Planes de Contingencia, pero existe falta de comunicación, esto debido a que el personal desconoce la existencia de toda esta documentación.

Mediante entrevistas realizadas al Jefe del Departamento de TIC’s, se pudo identificar varios incidentes que se han producido dentro de las instalaciones; como por ejemplo: fallos de energía, produciendo pérdida de información de los empleados, debido a que no tienen precaución al momento de guardar su trabajo, los cortes de energía de forma violenta también pueden causar daños a los equipos físicos.

Otro incidente que se produce, es la fuga de información, esto debido a que no existen políticas que garanticen la seguridad de la información almacenada en la nube, puesto que el personal, sube la información de la organización a sus cuentas personales de Dropbox o Google Drive, lo ideal debe ser que, cuente con su propio servidor en la nube, el mismo que le permitirá almacenar información de manera segura.

Es por este motivo que, surge la necesidad de elaborar un Sistema de Gestión de la Seguridad de la Información, el mismo que permitirá concientizar al personal que labora en el Distrito Zonal No.6 “Eloy Alfaro” sobre la importancia de su trabajo dentro de la organización, la necesidad de administrar adecuadamente sus contraseñas y cumplir con las normativas propuestas por la Dirección, así como también, debe existir una adecuada comunicación entre departamentos, esto con el fin de poder dar seguimiento y solución a problemas que se pueden generar dentro de los departamentos que conforman el Distrito.

CAPÍTULO 2. DESARROLLO DEL PLAN DEL SGSI

2.1 ANÁLISIS DE RIESGOS

En esta sección se procederá a realizar el análisis de los riesgos para el Departamento de TIC's del Distrito Zonal No. 6 "Eloy Alfaro", a continuación se procederá a dar la definición de análisis de riesgos según varios autores.

"Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización" [4]

"Uso sistemático de la información para identificar las fuentes y evaluar el riesgo" [2]

El análisis de riesgos consiste en la identificación de activos de la organización, los mismos que pueden ser clasificados tomando en cuenta el tipo de activo. Una vez identificado los activos críticos se identifican las amenazas a los que se encuentran expuestos así como las posibles consecuencias que podrían darse en caso de materializarse.

2.1.1 COMPARACIÓN DE METODOLOGÍAS DE ANÁLISIS DE RIESGOS.

En esta sección se procederá a describir varias metodologías de análisis de riesgos, definiendo de forma breve que es cada una de estas.

2.1.1.1 MAGERIT [4]

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), es una metodología de análisis y gestión de riesgos elaborada por la CSAE (Consejo Superior de Administración Electrónica) que estima que la gestión de riesgos es la base fundamental en las guías de un buen gobierno.

Es adaptable a organizaciones, tanto públicas como privadas, que dependen de un crecimiento de las Tecnologías de Información que ayuden a la consecución de sus

objetivos de servicios. La razón por la que existe MARGERIT está relacionada con la generalización de medios electrónicos, informáticos y telemáticos, que brindan beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

MAGERIT ayuda a los que trabajan con información mecanizada y a los sistemas informáticos que la tratan, ya que si la información o los servicios que se prestan gracias a ella son valiosos, MARGERIT les permitirá saber cuánto de este valor está en juego y ayudará a protegerlo. MAGERIT fue actualizada a su versión 3 en el 2012.

Esta versión 3 se ha estructurado en dos libros y una guía de técnica:

- Libro I: Método.
- Libro II: Catálogo de elementos.
- Guía de Técnica: Recopilación de técnicas de diferente tipo que pueden ser de utilidad para la aplicación del método.

2.1.1.2 Metodología BAA [5]

Ésta metodología fue desarrollada por el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), con el objetivo de proteger los activos de información importantes para las organizaciones, esto mediante la realización de un análisis de riesgos, actualmente la seguridad de los activos para las organizaciones es de vital importancia, ya que el funcionamiento de las mismas depende de la reputación que esta tenga frente a sus clientes, la seguridad que le ofrece a su información y la credibilidad de la misma.

Las siglas de esta metodología fueron tomadas de los principales procesos que maneja para realizar el Análisis

- Beneficio para el Atacante.
- Accesibilidad para el Atacante.

- Anonimidad del Atacante.

A partir de lo anterior, se ha dado el nombre de “BAA” a esta metodología de análisis de riesgos, lo cual tiene su origen en el Beneficio para el atacante, la Accesibilidad para el atacante y la Anonimidad del atacante.

El objetivo de la metodología es realizar una clasificación de los datos personales en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección.

2.1.1.3 Metodología DAFP [6]

Tomando en cuenta que el Tema de Administración de Riesgos es muy importante para las entidades públicas, el Estado Colombiano estableció una metodología llamada DAFP (Metodología para el Departamento Administrativo de la Función Pública). DAFP tiene como objetivo, fortalecer la implementación y desarrollo de la política de la administración de riesgos, a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de la misión y objetivos Institucionales de las entidades de la Administración Pública.

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad. Con el fin de asegurar dicho manejo, es importante que se establezca el entorno de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos:

- Contexto estratégico.
- Identificación de riesgos.
- Análisis de riesgos.
- Valoración de riesgos.
- Políticas de Administración de Riesgos.

Gracias a la implementación de la metodología DAFP, se ha podido generar una visión sistemática de la administración y evaluación de riesgos, consolidándose en un Ambiente de Control adecuado a la entidad y un Direccionamiento Estratégico que fije la orientación clara y planeada de la gestión, dando las bases para el adecuado desarrollo de las Actividades de Control.

2.1.2. SELECCIÓN DE LA METODOLOGÍA DE ANÁLISIS DE RIESGOS

En la Tabla 2-9 se muestra una comparación de las metodologías antes mencionadas.

CARACTERISTICAS	MAGERIT	BAA	DAFP
Constante Participación de la Dirección	x		x
Cuenta con documentación necesaria	x	x	
Cuenta con una guía de aplicación del método	x	x	
Aplicable para activos de TI	x		x
Aplicable para el análisis de riesgos en el aspecto Legal	x		
Prepara a la Organización para procesos de Auditoría	x		x
Propone ejemplos como guía de uso	x	x	x
Adaptable a cualquier tipo de empresa	x		
Conocimiento de la metodología por parte de los autores.	x		
Mayor madurez	x		
Compatibilidad con la NTE ISO/IEC 27005	x		
Cuenta con un reconocimiento a nivel mundial	x		
Analiza factores Internos y Externos a la Organización	x	x	
Cuenta con un método sistemático para analizar riesgos	x	x	x
Cuenta con un sistema que permite identificar amenazas	x		
Permite monitorizar el Riesgo después de su Gestión.			x
Propone listas de medidas a implementar para mitigar		x	

CARACTERISTICAS	MAGERIT	BAA	DAFP
el riesgo			
Cuenta con un procedimiento para identificar medidas de seguridad	x	x	x
Cuenta con una clasificación por tipo de dato	x	x	x

Tabla 2-9 Comparación de Metodologías

Fuente: Los Autores.

Tomando como base la tabla anterior, donde se realizó la comparación de algunas metodologías para el análisis de riesgos, se puede destacar lo siguiente:

- MAGERIT gestiona riesgos con respecto a recursos de TI; como son riesgos relacionados a hardware, software, redes así también ayuda en el análisis de riesgos legales.
- MAGERIT cuenta con tres libros donde se explica la metodología, esta documentación cuenta con secciones donde se ejemplifica los pasos a seguir, lo cual ayuda mucho a su implementación y a su entendimiento.
- MAGERIT es adaptable a cualquier tipo de organización, es decir es aplicable al Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro", siendo esta una Institución Pública.
- La primera versión de MAGERIT fue desarrollada en el 1997, en la actualidad está en la versión tres, por esta razón es una metodología que tiene madurez y es utilizada en varios lugares del Mundo, gracias a esto MAGERIT es compatible con la NTE ISO/IEC 27005 y la Norma ISO 31010.
- La metodología que usa MAGERIT es completa, analiza factores tanto internos como externos a la Organización, también implementa un procedimiento el cual me permite identificar las posibles medidas a tomar. Por estas razones los autores utilizarán la metodología de análisis de riesgos MAGERIT.

2.1.3. DESCRIPCIÓN DE LA METODOLOGÍA MARGERIT [4]

Tomando en cuenta la importancia del Análisis de Riesgos para las organizaciones, se creó la Metodología MAGERIT, la cual con su implementación persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de la información de la existencia de riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de Tecnologías de la Información y Comunicación.
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Para realizar un adecuado Análisis de Riesgos, MAGERIT implementa los pasos descritos en la Tabla 2-10:

PASOS	DESCRIPCIÓN
1. Caracterización de Activos.	El objetivo de esta sección es identificar los activos relevantes para la organización y valorar la importancia de los mismos.
2. Identificación de amenazas y vulnerabilidades.	En esta sección se identificará las amenazas relevantes o todas las cosas que pueden ocurrir, caracterizándolas por la probabilidad de ocurrencia y el daño causado; previo a este paso, debemos realizar una identificación de vulnerabilidades a las que se encuentran expuestos los activos críticos seleccionados.
3. Determinar las salvaguardas o contramedidas.	En esta sección se debe detallar las salvaguardas seleccionadas las cuales tienen que ser eficaces frente al riesgo.
4. Estimar el impacto	Para poder valorar el impacto se debe definir como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo	Para poder valorar el riesgo se debe definir como el impacto ponderado con la tasa de ocurrencia, o expectativa de materialización de la amenaza.

Tabla 2-10 Pasos para el Análisis de Riesgos según MAGERIT.

Fuente: Libro I MAGERIT.

2.1.4. ANÁLISIS DE RIESGOS EN EL CASO DE ESTUDIO

En la siguiente sección se procederá a realizar el análisis de riesgos para el Departamento de TIC's, del Distrito Zonal No.6 "Eloy Alfaro", como se menciona anteriormente se utilizará la Metodología MAGERIT para realizar este análisis.

2.1.4.1 Caracterización de los activos

Para poder realizar la identificación de los activos, se los ha categorizado en dos tipos: Activos Primarios los cuales se dividen en; actividades y procesos del Negocio y Activos de Soporte los cuales se dividen en: Hardware, Software, Redes, Personal, Ubicación y Estructura de la organización. Dichos activos pudieron ser identificados gracias a entrevistas realizadas con el Jefe del Departamento de TIC's del Distrito Zonal N°6 "Eloy Alfaro".

- ***Activos Primarios:*** este tipo de activos son importantes para la organización debido al valor que tienen, en caso de fallo o de pérdida de estos activos, es posible que se puedan paralizar los servicios, causar daños económicos, sanciones legales o incluso existe la posibilidad de que la organización no pueda volver a prestar servicios.
- ***Activos de Soporte:*** si bien están en otra categoría, al igual que los primeros son importantes, ya que gracias a estos activos, los Activos Primarios pueden funcionar. Muchos de estos activos no tienen un valor económico definido, ya que para la organización son más importantes no por el valor económico. Por ejemplo, el recurso humano es valorado por el conocimiento que posee, al igual que la ubicación, ya que esta última proporciona seguridad a los empleados y activos en general.

2.1.4.2 Identificación de los Activos

Luego de haber realizado un análisis junto con el Director Distrital y el Jefe del Departamento de TIC's, se ha identificado que el activo importante para la organización es el Sistema que Administra la información almacenada de las

Carpetas Compartidas de todos los departamentos que conforman el Distrito Zonal, es por ello que se llegó a una decisión conjunta, la cual categoriza a dicho activo como crítico para el funcionamiento del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro" y sobre el cual se va a enfocar el trabajo desarrollado a lo largo de este documento. Para ver un inventario de los Activos de Hardware identificados se puede observar la Tabla 1-2, ubicada en la sección 1.2.1.

2.1.4.3 Sistema de Almacenamiento de Carpetas Compartidas.

El Sistema de Almacenamiento de Carpetas Compartidas, es un servidor donde se guarda toda la información que necesitan los diferentes Departamentos del Distrito Zonal, para poder realizar los procesos que permitan mantener la certificación de la norma ISO 9001:2005.

Todos los Departamentos cuentan con una carpeta compartida, donde se deposita la información que proviene de Atención Ciudadana (es el Departamento encargado de atender a toda la ciudadanía, escuchar sus requerimientos y transferirlos al Departamento indicado para dar solución a los problemas presentados), estas carpetas tienen permisos solo de lectura, el único departamento capaz de modificar dicha documentación es el Departamento de TIC's, los respaldos de esta información son importantes puesto que sirve como evidencias cuando se realizan auditorias que pretenden mantener la certificación de la norma ISO 9001:2005.

El flujo de almacenamiento de la Información es el siguiente:

1. El Usuario se acerca al Departamento de Atención Ciudadana a presentar sus incidentes, el empleado llenará un documento donde especifique el proceso que se necesita realizar y el Departamento encargado de ello.
2. Se escanean todos los documentos necesarios junto con la definición del proceso y el Departamento encargado de su solución.
3. La documentación escaneada es almacenada en el Servidor de las Carpetas Compartidas dentro del Departamento de TIC's, de esta forma cuando el usuario se dirija al Departamento asignado, la persona que dará solución al

problema podrá acceder a la carpeta compartida de su Departamento, y podrá visualizar la documentación que facilitó el usuario, de esta forma se podrá dar solución a los errores presentados.

4. Dependiendo del Departamento asignado para la solución del problema, los documentos escaneados son almacenados en la carpeta compartida del Departamento. El usuario se puede dirigir al Departamento asignado con los documentos físicos.
5. El encargado de cada Departamento, para poder atender a la ciudadanía deberá acceder a la carpeta compartida, donde podrá visualizar la documentación necesaria.

En la Figura 2-8 se puede visualizar el proceso descrito anteriormente.

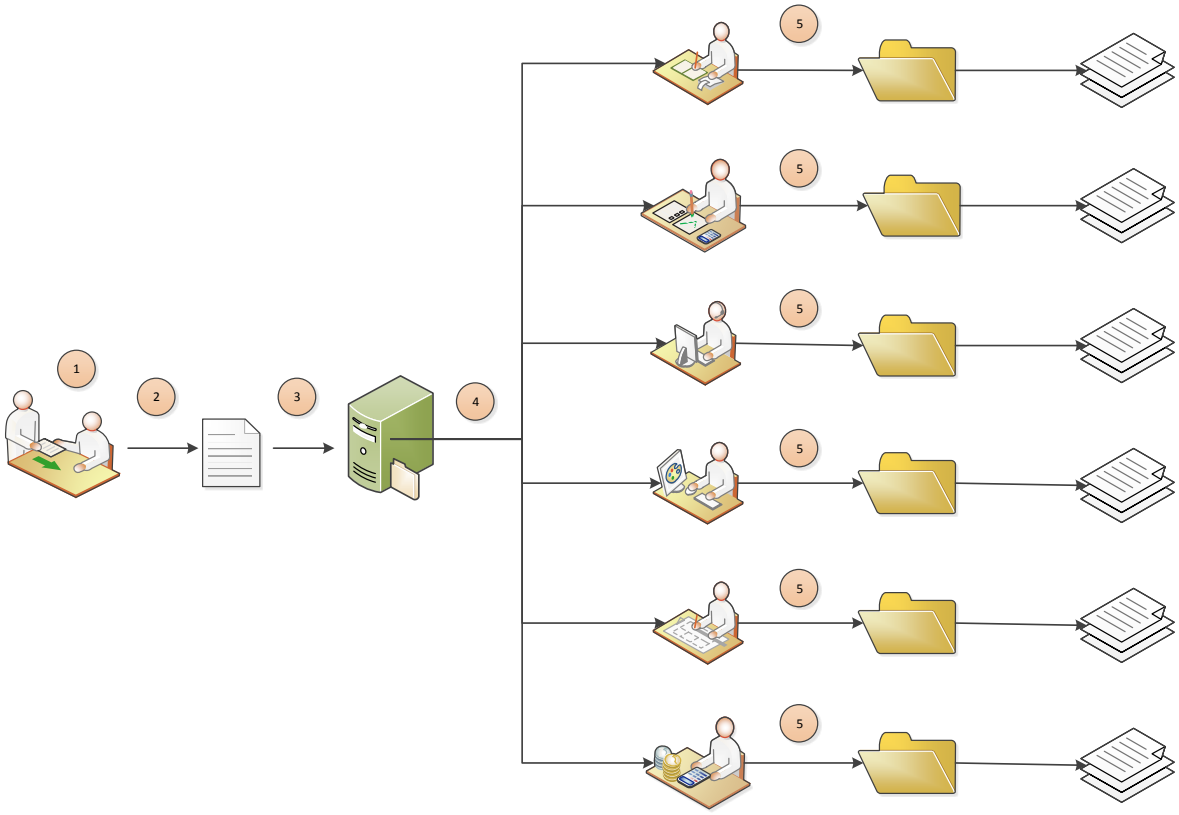


Figura 2-8 Flujo del Sistema de Carpetas Compartidas

Fuente: Los Autores

En caso de ser necesario el personal que labora en la Organización podrá almacenar documentos que visualicen las soluciones que se dieron a los problemas presentados.

Es importante recalcar que todos los documentos almacenados dentro del Servidor de Carpetas Compartidas deben seguir lineamientos, los cuales se establecerán en la Política de Uso de Información.

2.1.4.4 Identificación Vulnerabilidades

Una vulnerabilidad es una debilidad o defecto en la implementación u operación de un activo o control, la cual puede ser materializada por la ocurrencia de una amenaza. Para poder determinar las vulnerabilidades existentes dentro del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro", se han realizado entrevistas con el Jefe del Departamento y el personal que labora allí, de la misma forma se han utilizado algunas herramientas como ayuda para determinar las vulnerabilidades existentes.

2.1.4.4.1 Análisis de Vulnerabilidades Lógicas

Para poder identificar las vulnerabilidades lógicas existentes en el Distrito Zonal No. 6, se ha realizado un hackeo ético no intrusivo a la red de la Organización, lo que significa que la Organización se encontraba informada de los análisis que se estaban realizando a la red, los cuales no afectarían el desempeño normal de las actividades cotidianas.

El hackeo ético fue realizado bajo un contexto de pruebas de Caja Blanca, es decir la Organización proporcionó toda la información necesaria del servidor, como direcciones IP, y las facilidades de acceso a la red en las que se encuentra el servidor para que se puedan ejecutar las herramientas seleccionadas. Cabe mencionar que los análisis realizados al servidor de la Organización, fueron desde las propias instalaciones y bajo la supervisión del Jefe del Departamento de TIC's, por lo cual los informes generados por las herramientas fueron entregados tal y como

se lo especificó en un acuerdo de confidencialidad firmado por los autores de este documento y el Director Distrital.

Nessus[5].- es un software que realiza un escaneo de vulnerabilidades, consiste en un daemon “nessud”, el cual realiza el escaneo, y el “nessus” es el cliente el cual muestra el avance de los escaneos.

La herramienta fue utilizada para analizar el servidor de Documentación, el mismo que brindó un informe con las vulnerabilidades encontradas.

Para poder analizar el servidor es necesario identificar la dirección IP del mismo, ya que la herramienta realiza el análisis por este medio, la IP analizada en este caso es la 10.96.xx.xx (por motivos de confidencialidad no se puede dar a conocer la dirección IP del servidor), la herramienta al final del análisis muestra un informe en el cual especifica que el servidor cuenta con un total de 63 vulnerabilidades.

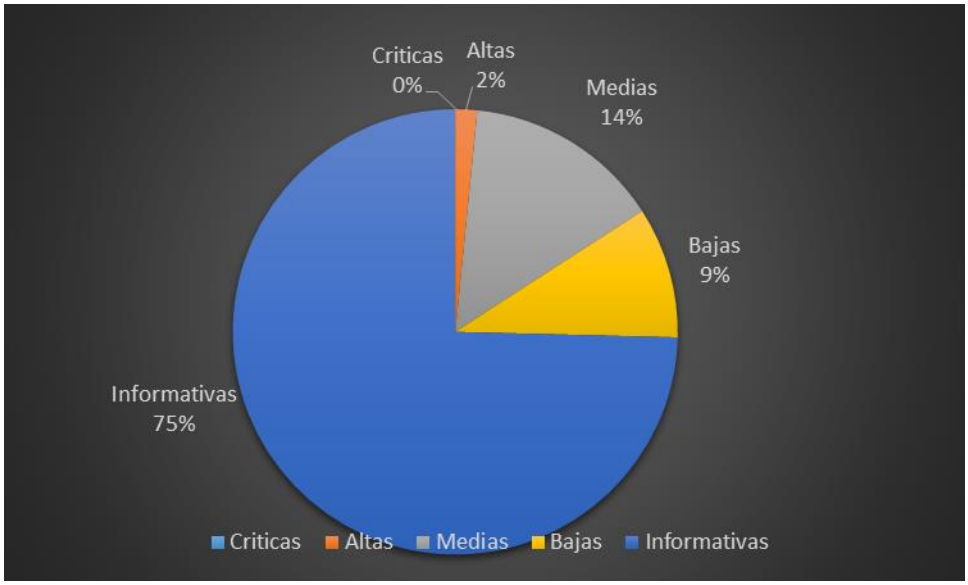


Figura 2-9 Resultados de análisis de vulnerabilidades del Servidor de Documentación

Fuente: Herramienta Nessus

[5] Fuente: http://www.tenable.com/products/nessus-vulnerability-scanner

Como se puede apreciar en la Figura 2-9, el porcentaje de vulnerabilidades a ser tratadas es del 16% (vulnerabilidades de nivel alto y nivel medio), del total general de vulnerabilidades encontradas. A continuación se presenta la Tabla 2-11, donde se puede visualizar un análisis de las vulnerabilidades encontradas por la herramienta Nessus.

SEVERIDAD	VULNERABILIDAD	ANÁLISIS
Alta	Versión desactualizada de software (Apache 2.2)	La versión de Apache permite la inyección de código malicioso, así como también se puede producir un ataque de negación de servicio para obtener información de credenciales sensibles.
Media	El certificado de la capa de conexión segura a Internet no pudo ser verificado.	El certificado de conexión a Internet no pudo ser verificado, lo que permitiría realizar ataques Man in the Middle.
Media	El certificado de la capa de conexión segura a Internet se encuentra auto firmado.	El certificado de conexión a Internet no se encuentra firmado por una entidad Autorizada.
Media	Eludir reglas de Firewall	Permite a los usuarios internos eludir reglas de Firewall mediante la utilización de puertos abiertos.
Media	El servidor DNS permite transferencias a zonas no permitidas.	El servidor DNS, no verifica el dominio de equipos permitiendo las conexiones remotas sin autorización.
Media	Servidor DNS responde a peticiones de terceros no autorizados.	El servidor DNS responde a conexiones externas, permitiendo así el acceso a información de la navegación de la Organización.
Media	El servidor acepta conexiones remotas con versiones de cifrado vulnerables.	La información que es transmitida por la red es fácil de vulnerar debido a la implementación de versiones de cifrado antiguas.
Media	Falla de desinfección del servidor al analizar código JavaScript malicioso.	Se permite la ejecución de código malicioso el cual permitirá tener fácilmente los accesos a la información del servidor.
Media	Conexiones inseguras	Se permiten conexiones las cuales pueden realizar pruebas en el servidor.
Media	El servidor presenta una vulnerabilidad de divulgación de información.	La versión de cifrado usada no protege adecuadamente la información transmitida por la red.

Tabla 2 -11 Análisis de las vulnerabilidades de la herramienta Nessus.

Fuente: Los Autores

NMap[6] es una herramienta que sirve para la exploración de red y realizar auditorías de seguridad, Nmap utiliza paquetes IP en formas originales para determinar qué equipos están disponibles en una red, que servicios (nombre y versión de la aplicación) ofrecen, que sistemas operativos ejecutan, que tipo de filtros de paquetes o cortafuegos se están utilizando. La herramienta fue utilizada en el Distrito Zonal No.6 “Eloy Alfaro” para analizar tres aspectos importantes:

1. Identificar puestos abiertos.
2. Información visible de los servicios que actualmente presta la organización.
3. Identificar información del sistema operativo del servidor.

Algunos de estos datos por motivo de seguridad el Jefe del Departamento de TIC’s ha solicitado no revelarlos.

VULNERABILIDAD	ANÁLISIS
Muestra el Sistema Operativo y la versión del servidor host.	Al mostrar la información del Sistema Operativo se puede explotar vulnerabilidades conocidas.
Puertos abiertos.	Presenta varios puertos abiertos, por los cuales se pueden realizar ataques maliciosos.
Servicios ejecutados.	Muestra información sobre los servicios que se están ejecutando en el servidor.

Tabla 2-12 Análisis de las vulnerabilidades de la herramienta NMap

Fuente: Los Autores.

Restricciones Técnicas.

Debido a cuestiones de seguridad, el Distrito Zonal N° 6 “Eloy Alfaro” solicitó firmar un acuerdo de confidencialidad, en el cual se especifica brindar absoluta reserva al informe de vulnerabilidades generado por la herramienta Nessus y la herramienta NMap.

Cabe mencionar que el Jefe del Departamento de TIC’s del Distrito Zonal N° 6 “Eloy Alfaro” cuenta actualmente con la herramienta Nessus en su equipo, esto para realizar un Análisis de Vulnerabilidades lógicas de la Organización cuando sea requerido, es por esto que únicamente se permitió ejecutar solo UNA herramienta

[6] Fuente: https://nmap.org/man/es/

adicional para Hackeo ético, y por solicitud expresa del Jefe del Departamento de TIC’s del Distrito Zonal, se utilizará la herramienta NMap.

La herramienta NMap cuenta con múltiples funcionalidades, el Distrito Zonal No.6 “Eloy Alfaro” limitó la utilización de la misma para obtener información sobre puertos abiertos, servicios ejecutados y versión del sistema operativo, cabe recalcar que por petición del mismo Distrito no se puede mostrar a detalle cada uno de ellos.

Análisis de Resultados

Luego de analizar las vulnerabilidades lógicas identificadas con la ayuda de las herramientas antes mencionadas, se puede mencionar que la manera en cómo se está administrando el servidor no es la adecuada, esto debido a que no cuenta con las debidas actualizaciones o parches para los servicios que allí se encuentran ejecutando, lo que puede provocar que personas mal intencionadas ataquen al servidor y provoquen incidentes como:

- Denegación de Servicios.
- Ataques Man in the Middle.
- Phishing.

Al mostrar información y la versión del sistema operativo del servidor en donde se están ejecutando los servicios, facilita a los atacantes explotar vulnerabilidades conocidas para estos sistemas o versiones en específico.

El contar con puertos abiertos en el servidor, facilita a los atacantes ingresar al servidor y causar daños al mismo, es necesario que se configure de manera adecuada el Firewall para que este tipo de incidentes pueda ser evitado.

Conclusiones de las Vulnerabilidades Lógicas.

- Se encuentra visible mucha información referente al servidor como por ejemplo el sistema operativo y la versión del mismo, puertos abiertos y

servicios ejecutados, la mala utilización de este tipo de información puede atentar a la integridad del Distrito Zonal No.6 “Eloy Alfaro”.

- Existen vulnerabilidades que pueden facilitar la ejecución de ataques maliciosos, por parte de personal externo o interno a la Organización.
- Debido a las restricciones que se tuvieron con el acceso al servidor, no se pudo aprovechar la totalidad de las funcionalidades de las herramientas.
- La utilización de software desactualizado, genera vulnerabilidades que pueden afectar el desarrollo normal de las actividades de la Organización.

2.1.4.4.2 Identificación de Vulnerabilidades Físicas

Para poder identificar las vulnerabilidades físicas que se presentan dentro de la organización se ha empleado Ingeniería Social, lo cual, mediante varias entrevistas con el personal que labora en la organización y con el Jefe del Departamento de TIC’s, han permitido tener una visión más clara de cómo se desarrollan las actividades cotidianas.

En coordinación con el Director Distrital y el Jefe del Departamento de TIC’s del Distrito Zonal No. 6 “Eloy Alfaro”, se ha llegado al acuerdo de realizar una visita semanal a las instalaciones de la organización, esto con el objetivo de lograr generar un ambiente de confianza entre el personal y los autores de este documento, para que de esta manera se logre obtener información más clara y verídica de cómo se encuentra actualmente la organización a nivel físico.

Adicionalmente se ha empleado una herramienta que permite identificar vulnerabilidades de Seguridad de TI de la organización, esto se lo realiza mediante la implementación de un CheckList al personal y al Jefe del Departamento de TIC’s del Distrito Zonal, esta herramienta se detalla a continuación:

MSAT[7].- La herramienta de Evaluación de Seguridad de Microsoft, es una herramienta gratuita diseñada para ayudar a las organizaciones a evaluar los puntos débiles de su entorno de seguridad de TI. Esta herramienta basa su análisis en preguntas de seguridad referentes a distintos temas como son: el personal, la infraestructura, las aplicaciones y las operaciones de la Organización; una vez realizado el análisis pertinente, la herramienta mostrará un informe con la evaluación detallada, y la lista de acciones recomendadas para las vulnerabilidades encontradas. El checklist completo se encuentra en el Anexo 3.

A continuación se realiza un análisis sección por sección de los aspectos que MSAT analiza para identificar las vulnerabilidades de la Organización.

- **Área de Infraestructura:**

En esta sección se tratan temas relacionados con el perímetro de la Organización (seguridad de la red y seguridad física), con la autentificación de los usuarios (autentificación de usuarios internos y externos), y con la gestión y control de incidentes. En la Figura 2-10 se muestra los porcentajes.

Figura 2-10 Seguridad de la Infraestructura

Fuente: Los Autores

En porcentaje de no cumplimiento es alto, puesto que se tiene deficiencias en:

[7] Fuente: https://technet.microsoft.com/es-es/library/cc185712.aspx

- Defensa del perímetro puesto que no se tiene un adecuado uso de antivirus, acceso remoto, y una arquitectura segura de la red.
- Autentificación puesto que no se tiene una adecuada gestión de acceso de usuarios tanto internos como externos a la Organización.

El porcentaje de cumplimiento se debe a temas relacionados con la utilización de bloqueos de red y una adecuada documentación de los procesos.

- **Área de Aplicaciones:**

En esta sección se trata temas relacionados con la implantación y utilización del software existente, con el almacenamiento y comunicación de datos. En la Figura 2-11 se muestra los porcentajes.

Figura 2-11 Seguridad de las Aplicaciones

Fuente: Los Autores

El porcentaje de no cumplimiento es alto puesto que se tiene deficiencias en:

- **Implantación y utilización de software:** puesto que se utiliza software no licenciado, no se mantiene registros de utilización y el personal no tiene un procedimiento sobre el adecuado mantenimiento de los mismos.
- **Almacenamiento y comunicación de datos:** no existe un adecuado procedimiento para clasificar la información al momento de almacenarla.

El porcentaje de cumplimiento se debe a que la Organización realiza back ups de la información de forma regular, y mantiene procedimientos documentados de este proceso.

- **Área de Personal:**

En esta sección se tratan temas relacionados con los requisitos y evaluaciones al personal, directivas y procedimientos en relación con terceros, y formación y conocimiento de los empleados. En la Figura 2-12 se muestra los porcentajes.

Figura 2-12 Seguridad del personal

Fuente: Los Autores

El porcentaje de no cumplimiento se debe a que existen falencias en:

- **Directivos y procedimientos:** no existen procedimientos adecuados al momento de establecer permiso a los diferentes usuarios, así como en el proceso de contratación del mismo.
- **Formación y conocimiento:** no existe el personal suficiente con los conocimientos requeridos para la Organización.

El porcentaje de cumplimiento se debe a que si existe la capacitación necesaria con respecto a la seguridad de la información pero existe falta de compromiso por parte del personal.

- **Área de Operaciones:**

En esta sección se trata temas relacionados con el entorno (seguridad de la empresa en relación con los procedimientos y procesos operativos), directivas de seguridad, actualizaciones y revisiones, copias de seguridad y recuperación de información. En la Figura 2-13 se muestra los porcentajes.

Figura 2-13 Seguridad en las Operaciones

Fuente: Los Autores

El porcentaje de no cumplimiento es bajo puesto que únicamente se tiene deficiencias en:

- **Directivas de seguridad**: puesto que no se tiene procedimientos adecuados para la eliminación de datos.
- **Actualización y revisiones**: no se tiene procedimientos claros para la actualización e instalación de software.

El proceso de cumplimiento es alto puesto que la Organización tiene los procedimientos bien documentados y establecidos, así como todo lo referente a back ups de la información de la Organización.

Después de haber realizado en análisis a los resultados obtenidos se pudo determinar las vulnerabilidades físicas mostradas en la Tabla 2-13.

VULNERABILIDAD	DESCRIPCIÓN
Fugas en el Aire Acondicionado en la sala de Servidores.	El sistema de Aire Acondicionado en la sala de servidores presenta fugas, lo cual puede afectar el funcionamiento de los mismos.
Falta de protección en ventanas.	Al momento el Distrito Zonal no cuenta con una adecuada protección en las ventanas de las instalaciones.
No existen procedimientos en caso de sismos.	No existen procedimientos que especifiquen que se debe realizar en caso de producirse un fenómeno natural de esta magnitud.
Transferencias de contraseñas en claro.	No se realiza una adecuada Gestión de las contraseñas.
Arquitectura insegura de la red.	Existe un desconocimiento de la arquitectura de la red.
Tráfico sensible sin protección.	No existe control de la información que los empleados manejan dentro de la Organización.
Líneas de comunicación sin protección.	No se controla a los usuarios que se encuentran conectados en la red de la Organización.
Copia no controlada de documentos.	No se contrala al personal la manera de almacenar o administrar la información de la Organización.
Almacenamiento de documentos y medios sin protección.	Los documentos son almacenados sin importar su nivel de confidencialidad.
Falta de políticas para desechar documentos.	No se cuenta con procedimientos para la eliminación de documentos importantes para la organización.
Falta de políticas para la recepción de documentos.	No se cuenta con procedimientos para la recepción de documentos.
Limpieza inadecuada por parte del personal.	Al momento de realizar la limpieza de las instalaciones, los encargados no tienen el cuidado necesario que garantice la seguridad de los equipos.
Descarga y uso no controlado de software.	El personal puede instalar software de cualquier tipo ya que los usuarios no se encuentran limitados.
Asignación errada de los derechos de acceso.	No existe una adecuada gestión de credenciales de acceso para el personal.
Mantenimiento insuficiente.	No se realiza un adecuado mantenimiento de los equipos, lo que puede provocar perdida de información sensible de la organización.
El servidor muestra fallas en la conexión.	Existen falencias con la conexión a otros equipos.
Ausencia de políticas sobre la limpieza de escritorio y de pantalla.	Los empleados no manejan adecuadamente su entorno de trabajo.
Gestión inadecuada de la	No existe un control de tráfico de red de la

VULNERABILIDAD	DESCRIPCIÓN
red.	Organización.
Asignación errada de roles y funciones.	No existe un correcto proceso de contratación de personal.
Gestión deficiente de contraseñas.	Los usuarios no saben administrar las contraseñas de manera adecuada.
Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.	Cuando un puesto de trabajo es abandonado no existe un control para salvaguardar la información del equipo.
Falta de software licenciado.	No se cuenta con licencias de los productos adquiridos.
Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Utilización de software licenciado que atenta contra la propiedad intelectual y derechos de autor del mismo.
Entrenamiento insuficiente sobre el funcionamiento del Sistema.	No existen capacitaciones adecuadas para el personal.
Ausencia de asignación adecuada de responsabilidades en la seguridad de la información.	No existe un correcto compromiso de los empleados acerca de la seguridad de la información.
Ausencia del personal.	No se cuenta con personal suficiente que permita realizar un correcto control de las disposiciones referentes a la seguridad de la información.

Tabla 2-13 Análisis de Vulnerabilidades Físicas

Fuente: Los Autores

Restricciones Técnicas

La utilización de esta herramienta fue solicitada por el Jefe del Departamento de TIC's del Distrito Zonal N° 6 "Eloy Alfaro", esto debido a que se cuenta con una constante interacción con el personal que labora dentro de la Organización, cubriendo así todas las necesidades del proyecto realizado.

Análisis de Resultados

Después de ejecutar la herramienta dentro del Distrito Zonal No.6 "Eloy Alfaro" y obtener el informe pertinente, se pudo evidenciar resultados que reflejan existencia

de áreas donde hace falta la implementación de buenas prácticas, estas áreas son las relacionadas con la Infraestructura y con el manejo de aplicaciones, considerando que entre las necesidades primordiales está la adecuada gestión de las contraseñas de los diferentes usuarios, ya que el acceso al servidor por cualquier personal no autorizado, pone en riesgo la integridad de la información allí almacenada.

Otro punto a considerar, es asegurar el adecuado funcionamiento de los equipos, ya que por mala utilización del Internet y uso inadecuado de software, los equipos pueden fallar y detener las actividades diarias del Distrito Zonal.

Dentro de las áreas donde se tiene un mayor porcentaje de cumplimientos son las áreas de operación y personal, ya que existen procedimientos definidos para la realización de las diferentes actividades, pero hace falta concientización del personal en temas relacionados con la seguridad de la Información.

Conclusiones de Vulnerabilidades Físicas

- Luego realizar un análisis a las visitas realizadas a la Organización, se llegó a la conclusión que referente Seguridad física y ambiental el Distrito Zonal No.6 “Eloy Alfaro” se encuentra en un nivel aceptable, cabe recalcar que la única vulnerabilidad encontrada fue la falta de mantenimiento a los equipos.
- El Distrito Zonal No. 6 “Eloy Alfaro” cuenta con un Servicio de Guardianía (2 Niveles, Acceso a las instalaciones, acceso a las Oficinas de Atención ciudadana primer piso).
- Existe un control para el acceso del personal debidamente autorizado a los diferentes Departamentos.
- Cuenta con Controles Biométricos para registrar el ingreso del Personal.
- Cuentan con puertas que tienen un adecuado control de acceso hacia las oficinas.
- Cuenta con un adecuado sistema de suministro eléctrico en el caso que se produzcan fallos.

Para poder visualizar un informe de vulnerabilidades identificadas en el Distrito Zonal No. 6 “Eloy Alfaro” se puede revisar el Anexo 4.

2.1.4.5 Identificación de Amenazas

Las amenazas son actos que pueden producirse de manera intempestiva, causando daños, tanto físicos como económicos a los activos de una organización, estas amenazas pueden producirse por causas naturales o por actos deliberados del personal administrativo, técnico o de apoyo.

Tipos de Amenazas [8]**:** Conjuntamente con el Jefe del Departamento de TIC’s, se ha logrado identificar seis tipos de amenazas que pueden afectar al activo crítico “Sistema de Almacenamiento Carpetas Compartidas”, las cuales se muestran en la Tabla 2-14.

TIPO.	DESCRIPCIÓN.
Daño Físico	Este tipo de amenazas tienen que ver con daño en los equipos por causas externas, por ejemplo fuego o agua, las mismas que al producirse ocasionan molestias o incluso pérdida de los equipos tecnológicos.
Eventos Naturales	Este tipo de amenazas están presentes en todas las organizaciones que se encuentran en zonas con un alto índice de erupciones volcánicas y movimientos sísmicos, son fenómenos naturales inevitables con los cuales las organizaciones deben convivir.
Pérdida de los servicios esenciales.	Este tipo de amenazas se caracteriza por los agentes externos que involucra, son amenazas producidas por individuos mal intencionados, los mismos que buscan causar daños a la empresa o robar información importante para la organización.
Fallas Técnicas	Estas amenazas son producidas por incumplimiento de los acuerdos de niveles de servicio por parte de proveedores externos, falta de mantenimientos o por equipos obsoletos que han cumplido con su ciclo de vida útil.
Acciones no Autorizadas	Estas amenazas se producen por la utilización de software no licenciado, el cual provoca falencias o debilidades en los sistemas debido a la falta de actualizaciones o soporte por parte de los creadores, otro motivo por el cual se producen estas amenazas es por la mala manipulación o por no poseer la autorización de manipular los equipos de la organización, sea por una mala distribución de tareas o por empleados mal intencionados que pretendan causar daños a la organización.

TIPO.	DESCRIPCIÓN.
Compromiso de las Funciones	Este tipo de amenazas se produce por la falta de interés por parte de la Alta Dirección, no se brinda un adecuado apoyo económico para la realización adecuada de capacitaciones al personal, o por una inadecuada selección de personal para desempeñar funciones dentro de los departamentos.

Tabla 2-14 Tipos de Amenazas

Fuente: Los Autores

Después de haber realizado un análisis a las encuestas realizadas al Jefe del departamento de TIC's y al personal que labora con él; y tomando en cuenta la tipología descrita anteriormente se pudieron obtener las siguientes amenazas:

- El Fuego o el Agua son amenazas latentes dentro de la organización, puesto que se está expuesto a inclemencias del tiempo o a desastres naturales.
- Los Fenómenos Sísmicos son una constante amenaza para la organización, esto debido a que la ciudad donde se localiza la organización se encuentra dentro del Cinturón de Fuego del Pacífico.
- La pérdida o robo de los equipos de la organización, así como una manipulación inadecuada del Hardware como del Software y una mala administración de las redes de comunicación pueden provocar que la información de la organización se vea afectada, ésta puede ser adulterada o robada por empleados mal intencionados o por personas externas que puedan tener acceso a esos equipos o a la información.
- La falta de mantenimiento en los equipos o un mal funcionamiento de los mismos pueden provocar irregularidades al momento de realizar las tareas diarias de la organización.
- La utilización de software no licenciado o pirata provoca fallas de seguridad, como puertas traseras en los equipos de la organización.

Para poder observar de mejor manera todas las amenazas localizadas en el Distrito Zonal N°6, se puede visualizar el Anexo 5.

2.1.4.6 Estimación del riesgo.

En esta sección se identificará el riesgo existente sobre el activo crítico identificado, para esto se tomará en cuenta la probabilidad de ocurrencia y el impacto que se puede tener sobre la Organización.

Valoración y escalas de la probabilidad.

La probabilidad es la posibilidad que una amenaza explote una vulnerabilidad. Para poder determinar la probabilidad que una amenaza explote una vulnerabilidad, se ha utilizado una valoración cualitativo y cuantitativa, la valoración cualitativa se ha utilizado por facilidad de entendimiento para el personal, y la valoración cuantitativa se la ha utilizado para poder realizar los cálculos relacionados con el riesgo, los valores utilizados se podrán visualizar en la Tabla 2-15.

VALOR	ESCALA	TIEMPO
5	Muy frecuente	A diario
4	Frecuente	Mensualmente
3	Normal	Una vez al año
2	Poco frecuente	Cada varios años
1	Muy poco frecuente	Siglos

Tabla 2-15 Valoración de la Probabilidad

Fuente: Los Autores

Valoración y escalas del impacto.

Para poder identificar el impacto que podría producirse sobre el activo crítico en caso de que las amenazas identificadas se materialicen y exploten las vulnerabilidades con las que convive la organización, se ha decidido, conjuntamente con el Jefe del Distrito Zonal No. 6, evaluar tres aspectos importantes, la Confidencialidad, Integridad y Disponibilidad del activo crítico en caso de ejecutarse la amenaza.

Estos factores fueron elegidos por la importancia que tienen, ya que cada uno de estos aspectos es importante para que la organización pueda prestar un buen servicio y que logre alcanzar los objetivos de la misma.

- **Confidencialidad:** se refiere a que la información crítica o importante, no puede estar disponible para todas la personas, por lo contrario esta información solo debe llegar a ser vista por las personas autorizadas.
- **Integridad:** la información debe ser veraz y confiable para que los procesos que involucren a esta información puedan ejecutarse de manera adecuada.
- **Disponibilidad:** la información debe estar disponible para los usuarios en el momento que ellos la necesiten, este aspecto se ve reflejado en los Acuerdos de Niveles de Servicio (SLA) firmado con terceros o con los clientes dependiendo el tipo de organización.

Para poder cuantificar el impacto sobre el activo, se ha determinado realizarlo mediante entrevistas con el Jefe del Departamento de TIC's del Distrito Zonal No. 6, para lo cual se ha decidido establecer una valoración específica para cada aspecto, que permite a los autores calcular el impacto de manera adecuada, la cual se puede visualizar en la Tabla 2-16.

ESCALAS DE IMPACTO	VALOR
SI	1
NO	0

Tabla 2-16 Escala de Impacto

Fuente: Los Autores

Las escalas a implementar para calcular el impacto se basan en una respuesta simple, si la amenaza afecta o no a los aspectos establecidos, la respuesta deberá ser un **sí** o **no**, por lo cual los resultados serán 1 y 0 respectivamente, los valores de cada aspecto van a ser sumados, lo cual, al ser tres aspectos los analizados daría un total de **3** como valor máximo y será cualificado como **Impacto Alto;** y un **cero** como valor mínimo, al dar el valor de **cero** significa que no afecta en nada al activo crítico,

por lo que en realidad no representa una amenaza real para el activo, por ende se eliminan estas amenazas y se tomará como valor mínimo **1** y la cualificación será de **Impacto Bajo.**

Para identificar el impacto de las amenazas localizadas dentro del departamento de TIC's del Distrito Zonal N°6 vamos a utilizar la siguiente tabla, la cual califica el impacto en Bajo, Medio y Alto.

VALOR	IMPACTO
3	Alto
2	Medio
1	Bajo

Tabla 2-17 Cualificación del Impacto

Fuente: Los Autores

Como se muestra en la Tabla 2-17, se tomará en consideración 3 niveles de impacto sobre la organización, los mismos que serán detallados a continuación:

- **Alto:** este nivel de impacto causa daños severos a la continuidad de la organización, provocando pérdida de información crítica y confidencial, lo que conlleva a una suspensión indefinida de las actividades de la organización.
- **Medio:** este nivel de impacto provoca que la organización deje de prestar sus servicios por un corto periodo de tiempo, hasta que sus procesos puedan volver a ser implementados normalmente.
- **Bajo:** este nivel de impacto no provoca daños mayormente significativos a la organización, se puede seguir brindando servicios ya que estos no resultan afectados al igual que la credibilidad de la empresa.

2.1.4.7 Determinación del Riesgo.

Para la determinación de la severidad del riego, se tomará en cuenta 3 categorías, las mismas que serán definidas mediante la siguiente ecuación:

Riesgo = Probabilidad * Impacto.

La cual permitirá localizar al riesgo en las categorías mostradas en la Tabla 2-18:

RIESGOS	VALOR
Riego Alto	6-15
Riesgo Medio	3-5
Riesgo Bajo	1-2

Tabla 2-18 Niveles del Riesgo

Fuente: Los Autores

- **Riesgo Alto:** pertenecen los riesgos que tiene como resultado de la ecuación valores entre 6-15, en esta categoría se localizan los riesgos que podrían afectar severamente la continuidad del negocio y provocar pérdidas representativas a la Organización.
- **Riesgo Medio:** pertenecen los riesgos que tienen como resultado de la ecuación valores entre 3 y 5, aquí se localizan los riesgos que pueden afectar menormente los objetivos de la Organización.
- **Riesgo Bajo:** pertenecen los riesgos que tienen como resultado de la ecuación valores iguales a 1 y 2, este tipo de riesgos en caso de materializarse no causaran daño a la Organización, sin interrumpir sus actividades y sin causar daño a los usuarios.

2.1.4.8 Plan de tratamiento de Riesgos.

De acuerdo a la sección 2.1.3 donde se describen a la Metodología MAGERIT, se muestra que dicha metodología presenta las siguientes opciones de tratamiento del riesgo las cuales se pueden visualizar en la Tabla 2-19.

OPCIÓN	DESCRIPCIÓN
Eliminación	La eliminación de la fuente de riesgos es una opción frente a un riesgo que no es aceptable. En un sistema se puede eliminar varias cosas, siempre que no

OPCIÓN	DESCRIPCIÓN
	afecten los objetivos de las Organizaciones, eliminar estos activos supone reorientar la misión. Más viable es prescindir de otros componentes no esenciales, que están presentes para cumplir con los objetivos establecidos, esta opción puede tomar diferentes formas: • Eliminar ciertos tipos de activos. • Reordenar la arquitectura del sistema. La decisión de eliminar las fuentes de riesgo requiere realizar un nuevo análisis de riesgos sobre el sistema modificado.
Mitigación	La mitigación del riesgo se refiere a reducir el impacto causado por una amenaza o reducir la probabilidad de que una amenaza se materialice. En ambos casos lo que se hay que hacer es ampliar o mejorar el conjunto se salvaguardias.
Compartición	La compartición del riesgo se refiere a transferir el riesgo, como la transferencia puede ser parcial o total se habla de compartir el riesgo. Hay dos formas de compartir el riesgo: • Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten las responsabilidades técnicas y legales. • Riesgo cuantitativo: se comparte por medio de la contratación de seguros.
Financiación	La financiación se refiere a aceptar riesgos, la Organización deberá reservar fondos para el caso de que el riesgo se concrete y haya que responder por las consecuencias. Normalmente esta opción no modifica nada del sistema.

Tabla 2-19 Opciones de Tratamiento del Riesgo

Fuente: Libro I MAGERIT. [4]

Una vez identificado las posibles opciones de tratamiento del riesgos, así como también los niveles del mismo, los autores junto con el Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro", y la Dirección Distrital toman la decisión de tratar los Riesgo con nivel Alto (valores de 6-15) aplicando la opción de mitigar los mismos. De la misma forma los riesgos con nivel medio (valores 3-5) y los riesgos de nivel bajo (1-2), serán aceptados por parte de la Dirección Distrital aplicando la opción de Financiarlos.

Para poder evidenciar la resolución adoptada por la Organización para Tatar los Riesgos, se puede revisar los Documentos Habilitantes adjuntos en los Anexos de este Proyecto. En la Tabla 2-20 se muestra la justificación de las opciones tomadas en cuenta.

OPCIONES DE TRATAMIENTO	JUSTIFICACIÓN
Mitigación	Se mitigarán los riesgos puesto que con la implementación de los controles indicados en la NTE INE-ISO/IEC 27001 se podrá reducir la probabilidad de que la amenaza se materialice sin la necesidad de la intervención de partes externas, y sin alterar el buen funcionamiento del Departamento de TIC's ayudándolos a cumplir sus objetivos.
Financiación	Después de haber realizado un análisis con la Dirección Distrital y el Jefe de Departamento, se llegó a la conclusión que el Distrito Zonal, puede aceptar los riesgos medios y bajos, a pesar que la metodología MAGERIT menciona que la Organización deberá reservar fondos para el caso de que el riesgo se concrete, el Distrito Zonal al ser una entidad pública no puede asignar recursos económicos para los diferentes procesos, pero la Dirección Distrital asumirá con responsabilidad las consecuencias en caso que el riesgo se materialice.

Tabla 2-20 Opciones de Tratamiento de Riesgos que se consideraron

Fuente: Los Autores

En la Tabla 2-21 se muestra la justificación de las opciones que NO se han tomado en cuenta.

OPCIONES DE TRATAMIENTO	JUSTIFICACIÓN
Eliminación	No se toma en consideración esta opción puesto que el activo es de suma importancia para la organización, su eliminación puede afectar el funcionamiento del Departamento de TIC's evitando que todos los objetivos propuestos por el mismo sean cumplidos.
Compartición	No se puede tomar en cuenta esta opción puesto que esto implicaría la contratación de seguros y la distribución de responsabilidades legales. Estos son proceso que se encuentra fuera del Alcance del Distrito Zonal No.6 "Eloy Alfaro", al ser una Institución Pública estos procesos están a cargo de la Sub-Secretaría de Educación, lo cual se encuentra fuera del alcance del SGSI.

Tabla 2-21 Opciones de Tratamiento de Riesgos que no se consideraron

Fuente: Los Autores.

2.1.4.9 Matriz de Riesgos.

Una matriz de riesgos en una herramienta que ayuda en la documentación y evaluación del riesgo de una institución, la matriz de riesgos nos permite efectuar una evaluación cualitativa y cuantitativa de los riesgos y la determinación del perfil de los mismos en los proceso. [8]

La matriz de riesgos identificada para el activo crítico "Sistema de Almacenamiento de Carpetas Compartidas" cuenta con el siguiente formato:

- **Tipo de Amenaza:** se especifican los tipos de amenazas encontradas para el activo crítico, la descripción de cada tipo de amenazas se encuentran detalladas en la sección 2.1.4.5.
- **Amenaza:** se especifica, todas las amenazas que se pudieron encontrar, luego de haber realizado entrevistas con el Jefe del Departamento de TIC's y

[8] Fuente: http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf

el personal que labora en él, cada amenaza se encuentra agrupada según su tipo, y el detalle de las amenazas encontradas se ubica en la sección 2.1.4.5.

- **Vulnerabilidades:** se especifica todas las vulnerabilidades encontradas después de haber realizado encuestas al personal que labora en el Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro", y después de haber ejecutado las herramientas Nessus, MSAT y visitas a la Organización, el detalle de las vulnerabilidades encontradas se encuentran detallada en la sección 2.1.4.4.
- **Probabilidad:** en esta sección se cuantifica el valor de la probabilidad de que una amenaza explote una vulnerabilidad, según la valoración definida en la sección 2.1.4.6 Valoración de la Probabilidad.
- **Impacto:** en esta sección se cuantifica el valor del impacto que se puede tener en caso de que una amenaza explote una vulnerabilidad, el impacto se ha cuantificado según la valoración definida en la sección 2.1.4.6 Valoración del Impacto.
- **Riesgo:** después de haber evaluado y cuantificado los valores de la probabilidad y del impacto, se procede a cuantificar el valor del riesgo y así poder identificar cuales seria los riesgos a tratar.

Una vez definido el formato a utilizar en la matriz de evaluación de riesgo, se procederá a completar la misma, en base al criterio de los autores y del Jefe del Departamento de TIC's, considerando toda la información hasta hoy recopilada mediante observaciones, documentación y entrevistas realizadas. En la Tabla 2-22 se puede visualizar la matriz de riesgos completa.

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	PROBABILIDAD	IMPACTO				RIESGO
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	
Daño Físico	Daño por agua	Fugas en el Aire Acondicionado en la sala de Servidores	2	0	0	1	1	2

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	PROBABILIDAD	IMPACTO				RIESGO
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	
		Falta de protección en ventanas.	2	0	0	1	1	2
Eventos Naturales	Fenómenos Sísmicos	No existe procedimientos en caso de sismos	1	0	0	1	1	1
Perdida de los Servicios Esenciales	Espionaje remoto	Transferencias de contraseñas en claro.	2	1	1	1	3	6
		Arquitectura insegura de la red	4	1	1	1	3	12
	Escucha encubierta	Tráfico sensible sin protección.	2	1	1	0	2	4
		Puertos abiertos	2	1	1	0	2	4
		Líneas de comunicación sin protección	2	1	0	0	1	2
	Hurto de medios o documentos	Copia no controlada de documentos	4	1	0	0	1	4
		Almacenamiento de documentos y medios sin protección.	4	1	1	0	2	8
	Recuperación de Medios Reciclados o desechados	Falta de políticas para desechar documentos.	5	1	0	0	1	5
	Datos provenientes de fuentes no confiables	Falta de políticas para la recepción de documentos.	3	1	1	0	2	6
		El certificado de la capa de conexión segura a Internet no pudo ser verificado.	2	1	1	0	2	4

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	PROBABILIDAD	IMPACTO				RIESGO
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	
		Conexiones Inseguras	2	0	1	1	2	4
		El servidor acepta conexiones remotas con versiones de cifrado vulnerables.	2	1	1	0	2	4
		El certificado de la capa de conexión segura a Internet se encuentra auto firmado.	2	1	1	0	2	4
		Falla de desinfección del servidor al analizar código JavaScript malicioso.	1	0	1	0	1	1
	Manipulación con hardware	Limpieza inadecuada por parte del personal.	4	1	0	1	2	8
	Manipulación con software	Descarga y uso no controlado de software.	5	1	1	1	3	15
		Asignación errada de los derechos de acceso.	3	1	1	1	3	9
Fallas Técnicas	Falla del equipo	Mantenimiento insuficiente.	4	0	0	1	1	4
	Mal funcionamiento del equipo	Ausencia de políticas sobre la limpieza de escritorio y de pantalla	5	1	1	1	3	15

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	PROBABILIDAD	IMPACTO				RIESGO
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	
	Saturación del sistema de información	Gestión inadecuada de la red.	5	1	1	1	3	15
	Mal Funcionamiento de Software	Servidor DNS responde a peticiones de terceros no autorizados.	2	1	0	0	1	2
		Eludir reglas de Firewall	5	1	1	1	3	15
		El servidor DNS permite transferencias a zonas no permitidas.	2	1	1	0	2	4
		Versión desactualizada de software (Apache 2.2)	1	1	1	1	3	3
		El servidor presenta una vulnerabilidad de divulgación de información.	2	1	0	0	1	2
	Incumplimiento en el mantenimiento del sistema de información	Asignación errada de roles y funciones.	4	1	1	1	3	12
Acciones no Autorizadas	Uso no autorizado del equipo	Gestión deficiente de contraseñas	5	1	1	1	3	15
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.	4	1	1	0	2	8
	Uso de software	Falta de software	5	1	1	1	3	15

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	PROBABILIDAD	IMPACTO				RIESGO
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	
	falso o copiado	licenciado.						
		Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	5	1	1	0	2	10
Compromiso de las funciones	Error en el uso	Entrenamiento insuficiente sobre el funcionamiento del Sistema	5	0	0	1	1	5
	Negación de acciones	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información.	5	1	1	1	3	15
	Incumplimiento en la disponibilidad del personal	Ausencia del personal.	4	0	0	1	1	4

Tabla 2-22 Matriz de Riesgos

Elaborado por: Los Autores

De la matriz de evaluación del riesgo se obtuvo como resultado un total de 16 riesgos que alcanzaron el nivel de riesgos altos con valores de 6-15, los cuales serán mitigados de acuerdo a lo acordado con el Director Distrital, ente encargado de realizar la toma de decisiones.

2.1.4.10 Selección de Controles.

Después de obtener los riesgos a ser tratados, se procederá a seleccionar los controles adecuados de la norma NTE INE-ISO/IEC 27001:2011 Anexo A, los cuales

tendrán como objetivo reducir la probabilidad de que una amenaza se materialice y deberán ser eficaces frente a los riesgos. En la Tabla 2-23 se muestra los controles seleccionados, para ver la matriz completa ver el Anexo 6.

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	ACCIÓN	CONTROLES
Pérdida de los Servicios Esenciales	Espionaje remoto	Transferencias de contraseñas en claro.	Mitigar	A.12.5.4 Fugas de Información A.12.3.2. Gestión de claves
		Arquitectura insegura de la red	Mitigar	A.13.1.2 Notificación de los puntos débiles de seguridad
	Hurto de medios o documentos	Almacenamiento de documentos y medios sin protección.	Mitigar	A.15.1.3 Protección de los documentos de la organización A.6.1.5 Acuerdo de confidencialidad. A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información 8.2.2 Concienciación, formación y capacitación en seguridad de la información 10.7.1 Gestión de soportes extraíbles 10.7.3 Procedimientos de manipulación de la información
	Datos provenientes de fuentes no confiables	Falta de políticas para la recepción de documentos.	Mitigar	A.15.1.3 Protección de los documentos de la organización A.6.1.5 Acuerdo de confidencialidad. A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información
	Manipulación con hardware	Limpieza inadecuada por parte del personal.	Mitigar	A.13.2.1 Responsabilidades y procedimientos 10.10.5 Registro de fallos

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	ACCIÓN	CONTROLES
	Manipulación con software	Descarga y uso no controlado de software.	Mitigar	A.10.10.2 Supervisión del uso del sistema A.7.1.3 Uso aceptable de los activos A.11.5.6 Limitación del tiempo de conexión A.10.4.1 Controles contra el código malicioso 10.4.2 Controles contra el código descargable en el cliente
		Asignación errada de los derechos de acceso.	Mitigar	A.13.2.1 Responsabilidades y procedimientos. A.11.1.1 Política de control de acceso A.11.2.2 Gestión se privilegios A.8.3.3 Retirada de los derechos de acceso
Fallas Técnicas	Mal funcionamiento del equipo	Ausencia de políticas sobre la limpieza de escritorio y de pantalla	Mitigar	A.13.2.1 Responsabilidades y procedimientos A.11.5.4 Uso de los recursos del sistema A.7.1.3 Uso aceptable de los activos A.9.2.4 Mantenimiento de equipos 10.7.2 Retirada de soportes A.11.3.3 Política de puesto de trabajo despejado y pantalla limpia
	Saturación del sistema de información	Gestión inadecuada de la red.	Mitigar	A.10.6.1 Controles de red A.10.6.2 Seguridad de los servicios de red
	Mal funcionamiento del software	Eludir reglas de Firewall	Mitigar	A. 10.6.1 Controles de red A. 10.6.2 Seguridad de los servicios de red A. 11.4.2 Autenticación de usuarios para conexiones externas
	Incumplimiento en el mantenimiento	Asignación errada de roles y funciones.	Mitigar	A. 10.1.3. Segregación de tareas

TIPO DE AMENAZA	AMENAZA	VULNERABILIDADES	ACCIÓN	CONTROLES
	del sistema de información			
Acciones no Autorizadas	Uso no autorizado del equipo	Gestión deficiente de contraseñas	Mitigar	A. 11.2.1 Registro de Usuario A. 11.2.2 Gestión de Privilegios A. 11.2.3 Gestión de Contraseñas de Usuarios A. 11.5.2 Identificación y autenticación de usuarios A. 11.5.3 Sistema de Gestión de Contraseñas
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.	Mitigar	A 11.3.1 Uso de Contraseñas A. 11.3.2 Equipo desatendido A. 11.3.3. Política de puesto de trabajo despejado y pantalla limpia A. 11.5.5 Desconexión automática de sesión A. 11.5.6 Limitación del tiempo de conexión
	Uso de software falso o copiado	Falta de software licenciado.	Mitigar	A. 15.1.1 Identificación de la legislación aplicable
		Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Mitigar	A. 15.1.2 Derechos de propiedad intelectual
Compromiso de las funciones	Negación de acciones	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información.	Mitigar	A.6.1.2 Coordinación de la seguridad de la Información. A. 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información 6.1.8 Revisión independiente de la seguridad de la Información. A. 13.2.1 Responsabilidades y procedimientos

Tabla 2-23 Selección de Controles a implementar

Fuente: Los Autores

Después de haber realizado el análisis respectivo se pudo determinar que hay varios controles identificados, los cuales serán agrupados para la realización de las políticas necesarias con el fin de reducir la probabilidad de la materialización del riesgo.

2.1.4.11 Aplicabilidad de los Controles

Después de realizar el análisis de riegos, se determinaron los controles que el Distrito Zonal No.6 “Eloy Alfaro” ya aplica en la actualidad, también se podrá visualizar los controles que los autores conjuntamente con el Jefe del Departamento de TIC’s se seleccionaron para aplicarlos.

Controles Utilizados, en la Tabla 2-24 se mostrará los controles que ya están siendo utilizados dentro del Distrito Zonal No. 6 “Eloy Alfaro”, la primera columna es el código del control, seguido por su nombre y finalmente la justificación de la utilización del mismo.

A.5 POLÍTICA DE SEGURIDAD		
A.5.1.1	Documento de política de seguridad de la información	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que cuenta con un documento de política de seguridad.
A.5.1.2	Revisión de la política de seguridad de la información	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto ya cuenta con un documento de política de seguridad la cual tiene un cronograma definido de las revisiones al documento.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1.1	Compromiso de la dirección con la seguridad de la información.	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que se cuenta con el apoyo de la Dirección respecto a la seguridad de la información.
A.6.1.6	Contacto con las autoridades	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control ya que mantienen estrecha comunicación con la Dirección Distrital, la cual

		ayuda a llevar un mejor control de los proceso que se realizan dentro de la Institución.
A.7 GESTIÓN DE ACTIVOS.		
A.7.1.1	Inventario de activos	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control ya se tiene un inventario de todos los activos que hay dentro de la Institución, además este inventario es actualizado con regularidad, verificando el custodio del activo y el estado del mismo.
A.7.1.2	Propiedad de los activos	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que todos los activos tiene un custodio definido, este custodio está presente en el inventario, cada uno de los custodios es asignado al ingreso de nuevos activos a la Organización.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		
A.8.2.1	Responsabilidades de la alta dirección	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que son ellos quienes gestionan el acceso del nuevo personal, son ellos quienes empiezan el proceso de la contratación de nuevos empleados.
A.8.2.3	Proceso disciplinario	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que existen procesos definidos y políticas disciplinarias en caso de omitir alguno de ellos.
A.8.3.1	Responsabilidad del cese o cambio	El presente control se aplica dentro de la Organización puesto que existen procesos donde se indican que todo el personal al momento de retirarse debe devolver los activos de a su cargo, así como las credenciales utilizadas.
A.8.3.2	Devolución de activos	El presente control se aplica dentro de la Organización puesto todo el personal al momento de retirarse de la Organización debe devolver los activos a su cargo, verificando el estado de los mismos.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL		

A.9.1.1	Perímetro de seguridad física	El Distrito Zonal No.6 “Eloy Alfaro” cuenta con la seguridad necesaria, como el servicio de guardias, los cuales son los encargados de proteger el perímetro del Distrito.
A.9.1.2	Controles físicos de entrada	El Distrito Zonal No.6 “Eloy Alfaro” cuenta con todo tipo de controles para el acceso a los diferentes departamentos. Estos controles con lectores biométricos y le existencia de guardias que se aseguran que las personas que ingresan sean las autorizadas.
A.9.1.3	Seguridad de oficinas, despachos e instalaciones	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que cuenta con áreas seguras y protegidas, la Organización cuenta con accesos biométricos, puestas con seguros, extintores, mangueras contra incendios, señalización en caso de emergencias.
A.9.1.5	Trabajo en áreas seguras	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que las áreas donde el personal desempeñan sus labores diarios, están protegidas con extintores, puestas con seguros, accesos biométricos.
A.9.2.1	Emplazamiento y protección de equipos	El Distrito Zonal No.6 “Eloy Alfaro” cumple con este control puesto que todos los equipos de la Organización se encuentran protegidos.
A.9.2.2	Instalaciones de suministro	El Distrito Zonal No.6 “Eloy Alfaro” cumple con este control puesto que se tiene un UPS que ayuda a asegurar los equipos ante fallas eléctricas.
A.9.2.3	Seguridad del cableado	El Distrito Zonal No.6 “Eloy Alfaro” cumple con este control puesto que mantiene el cableado estructurado de forma correcta, mediante las conexiones eléctricas por medio de la pared.
A.9.2.6	Reutilización o retirada segura de equipos	El Distrito Zonal No.6 “Eloy Alfaro” cumple con este control puesto que cuando un empleado sale de Organización se realiza un borrado total de los discos de los equipos.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A 10.1.1	Documentación de los procedimientos de operación	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que todos los procedimientos se encuentran adecuadamente documentados y almacenas, estoy procedimientos se encuentran disponibles tanto en archivos físicos como

		digitales en el servidor del Alfresco.
A 10.2.2	Supervisión y revisión de los servicios prestados por terceros	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que los servicios que se vayan a implementar de terceros es analizado por el Director Distrital y la Sub Secretaria de Educación, sin la previa autorización de las autoridades no se puede adquirir servicios de terceros.
A 10.5.1	Copias de seguridad de la información	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que se realizan copias de seguridad de toda la información de forma periódica, la cual es almacenada por la Subsecretaria de Educación.
A 10.8.4	Mensajería electrónica	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto mantiene políticas en el momento de intercambiar información por cualquier medio, especialmente con los mensajes de correo electrónico.
A 10.9.3	Información públicamente disponible	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que al ser una Institución Pública toda la información debe estar disponible a los usuarios que la necesiten.
A.10.10.4	Registros de administración y operación	Este control ya se aplica puesto que la Organización tiene debidamente detallado y documentado todos los procesos de la parte administrativa.
A.10.10.6	Sincronización del reloj	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que todos los equipos de la Organización se encuentran sincronizados, incluyendo el reloj del acceso biométrico y el reloj de los servidores.
A.11 CONTROL DE ACCESO		
A.11.4.3	Identificación de los equipos en las redes	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que el jefe del Departamento de Tics es quien administra las personas y equipos que se encuentran

A.11.7.1	Equipos portátiles y comunicación móviles	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que se tiene políticas que controlan el uso de portátiles y comunicación móviles
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
A 12.2.1	Validación de los datos de entrada	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que se controla la procedencia y la integridad de los datos que van a ser ingresados a la Organización.
A 12.2.3	Integridad de los mensajes	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que se valida al origen de la información y el uso que se le dará a la misma.
A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A 13.2.2	Aprendizaje de los incidentes de seguridad de información	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto existen mecanismos para cuantificar los incidentes y brindar soluciones de raíz, para evitar futuros problemas.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A 14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que ya cuenta con un documento de continuidad del negocio, dentro de este documento se consideran aspectos de la seguridad de la información, que para la Organización son suficientes dentro del documento.
A 14.1.4	Marco de referencia para la planificación de la continuidad del negocio	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que se tiene un único marco de referencia, es decir se tiene un único modelo, al cual se tiene que regir todos los Departamentos. De esta forma se mantiene la consistencia de la Organización.

A 14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	El Distrito Zonal No.6 “Eloy Alfaro”, aplica este control puesto que la Organización cuenta con un documento de Continuidad del Negocio, para la creación del mismo se necesitó de la realización de prueba, en caso de presentar algún tipo de inconsistencia de los datos se necesita de revisión del mismo.
A.15 CUMPLIMIENTO		
	No Aplica	

Tabla 2-24 Controles Utilizados

Fuente: Los Autores

Controles Seleccionados en la Tabla 2-25 se mostrará los controles que se van a utilizar en el desarrollo del Plan del Sistema de Gestión de la Seguridad de la Información, la primera columna es el código del control, seguido por su nombre y finalmente la justificación de la utilización del mismo.

A.5 POLÍTICA DE SEGURIDAD		
	No aplica	
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1.2	Coordinación de la seguridad de la información	El presente control se aplicará para poder coordinar la seguridad de la información entre los diferentes Departamento, así se creará conciencia sobre la seguridad de la información.
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	El presente control se aplicará para poder establecer un compromiso por parte de los usuarios, ante la ausencia de asignación de responsabilidades en la seguridad de la información.

A.6.1.5	Acuerdos de confidencialidad	El presente control se aplicará para mitigar la perdida de información causada por el hurto de medios o documentos. Además me ayudará a asegurar la integridad de los datos y el cuidado de los mismos.
A.6.1.8	Revisión independiente de la seguridad de la información	Este control se aplica pues que la revisión de documentos referentes a la seguridad de la información se las realizará de forma independiente Departamento por Departamento.
A.7 GESTIÓN DE ACTIVOS.		
A.7.1.3	Uso aceptable de los activos	El presente control se aplicará con la finalidad de establecer políticas sobre el adecuado uso de los activos evitando las descargas, la instalación de software indebido y promoviendo la limpieza de escritorio y de pantalla limpia.
A.7.2.1	Directrices de clasificación	El presente control se aplicará para poder mitigar la fuga de información causada por el mal manejo de la información. Además me ayudará a asegurar la integridad de los datos
A.7.2.2	Etiquetado y manejado de la información	El presente control se aplicará para asegurar la integridad de la información en caso de hurto de medios o documentos. Además me ayudará a asegurar la integridad de los datos
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		
A.8.2.2	Concienciación, formación y capacitación en seguridad de la información	Este control se aplica para poder asegurar la calidad de la información mediante la concienciación de la importancia de ella.

A.8.3.3	Retirada de los derechos de acceso	Este control se aplicará con la finalidad de gestionar de una manera adecuada la salida de los usuarios de la Organización, revocando los permisos y accesos que cada uno de ellos tengan
A.9 SEGURIDAD FÍSICA Y AMBIENTAL		
A.9.2.4	Mantenimiento de los equipos	Este control se aplicará con la finalidad de mitigar el mal funcionamiento de los equipos, implementando una política para el mantenimiento de los equipos.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A 10.1.3	Segregación de tareas	El presente control se aplicará para mitigar las fallas técnicas evitando la asignación errada de roles y responsabilidades sobre los diferentes sistemas existentes en la Organización.
A 10.4.1	Controles contra el código malicioso	El presente control se aplicará para tener un adecuado control de los activos evitando la ejecución de código malicioso.
A 10.4.2	Controles contra el código descargable en el cliente	El presente control se aplicará para tener un adecuado control de los activos evitando la descarga de código por parte de los empleados, y usuarios en general.
A 10.6.1	Controles de red	El presente control se aplicará para poder mitigar las fallas técnicas, asegurando la gestión adecuada de la red, además me permitirá evitar resolución de DNS.
A 10.6.2	Seguridad de los servicios de red	El presente control se aplicará para poder mitigar las fallas técnicas, asegurando la gestión adecuada de la red, además me permitirá evitar resolución de DNS.
A 10.7.1	Gestión de soportes extraíbles	Este control se aplicará para poder gestionar de manera adecuada toda la información, evitando el uso inadecuado de soportes extraíbles.

A 10.7.2	Retirada de soportes	Este control se aplicará para poder gestionar la retirada de soportes de manera adecuada.
A 10.7.3	Procedimientos de manipulación de la información	Este control ayudará a la Organización a establecer procedimientos para manipular de la información de manera adecuada.
A.10.10.2	Supervisión del uso del sistema	El presente control se aplicará con la finalidad de controlar las descargas y el uso no controlado de software.
A.10.10.5	Registro de fallos	El presente control se aplicará con la finalidad de mantener un registro de fallos, de estos problemas se podrá proponer soluciones de raíz.
A.11 CONTROL DE ACCESO		
A.11.1.1	Política de control de acceso	El presente control se aplicará con la finalidad de establecer los lineamientos necesarios para gestionar los usuarios, con esto se podrá tener un control sobre los usuarios y los perfiles ligados a estos.
A.11.2.1	Registro de usuario	Este control se aplicará con la finalidad de mitigar las acciones no autorizadas por el uso de los equipos, ayudando a tener un mejor control de los permisos de los usuarios a la información.
A.11.2.2	Gestión de privilegios	Este control se aplicará con la finalidad de establecer una política que me ayuda a gestionar los usuarios de forma adecuada y ordenada, evitando acciones no autorizadas y el mal uso de los equipos.
A.11.2.3	Gestión de contraseñas de usuario.	Este control se aplicará con la finalidad de mitigar las acciones no autorizadas a los equipos gracias a la gestión deficiente de las contraseñas.
A.11.3.1	Uso de contraseñas	Este control se aplicará con la finalidad de mitigar el uso no autorizado de los equipos, estableciendo contraseñas que puedan evitar el mal uso de la información y la fuga de la misma.

A.11.3.2	Equipo de usuario desatendido	Este control se aplicará para evitar los equipos desatendidos, es decir ayudará a que solo los usuarios permitidos puedan acceder a los diferentes equipos de lo Organización.
A.11.3.3	Política de puesto de trabajo despejado y pantalla limpia	Este control se aplicará con la finalidad de mitigar las fallas técnicas y evitar el mal funcionamiento de los equipos a causa de la sobre carga de datos, además ayudará a evitar acciones no autorizadas a causa de la falta de terminación de sesión de cada usuario.
A.11.4.2	Autenticación de usuario para conexiones externas	Este control se aplicará con la finalidad de evitar el mal funcionamiento del software gracias a una adecuada autentificación se los usuarios que requieran hacer conexiones remotas.
A.11.5.2	Identificación y autenticación de usuario	Este control se aplicará para poder tener una gestión eficiente de contraseñas, evitando el uso no autorizado de usuarios con actividades maliciosas.
A.11.5.3	Sistemas de gestión de contraseñas	Este control se aplicará para poder tener un adecuado sistema de gestión de contraseñas, ayudando desde la creación de usuarios, hasta la eliminación de los mismos. De esta forma evitar acciones no autorizadas.
A.11.5.4	Uso de los recursos del sistema	El presente control se aplicará para poder establecer políticas sobre la limpieza de escritorio y de pantalla, de esta forma asegurando el adecuado funcionamiento de los equipos.
A.11.5.5	Desconexión automática de sesión	Este control permitirá evitar la fuga de información gracias al bloqueo automático de la sesión de cada usuario, ayudando a resguardar la integridad de los datos dentro de los diferentes equipos de la Organización.
A.11.5.6	Limitación del tiempo de conexión	El presente control se aplicará con la finalidad de tener un mejor uso sobre los activos, evitando fugas de información, y las acciones no autorizadas dentro de los equipos a causa de la ausencia de la terminación de la sesión.

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
A 12.3.2	Gestión de claves	El presente control se aplicará para mitigar el espionaje remoto y ayudar a tener un mejor control sobre los permisos de cada usuario, con la finalidad de asegurar la integridad de la información que se maneja, en especial de la información más crítica para la Organización
A 12.5.4	Fugas de información	El presente control se aplicará con la finalidad de mitigar el espionaje remoto evitando la transferencia de contraseñas en claro.
A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A 13.1.2	Notificación de los puntos débiles de seguridad	El presente control se aplicará para mitigar el espionaje remoto evitando la arquitectura insegura de la red.
A 13.2.1	Responsabilidades y procedimientos	El personal debe tener muy claro las responsabilidades dentro de la organización al igual que los procedimientos existentes, de esta forma tendrán clara, la forma adecuada de manipular el hardware y el software evitando causar pérdidas a la Organización, con la aplicación de este control se pretende evitar el mal funcionamiento de los equipos. Además se pretende establecer un compromiso antes las funciones y las responsabilidades de cada usuario ante la seguridad de la información.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
	No aplica	
A.15 CUMPLIMIENTO		

A 15.1.1	Identificación de la legislación aplicable	El presente control se implementará para asegurar que la organización cuente con software propietario que requiere de licencias.
A 15.1.2	Derechos de propiedad intelectual (IPR)[Intellectual Property Rights]	El presente control se implementará para asegurar que la organización cuente con software propietario que requiere de licencias.
A 15.1.3	Protección de documentos de la organización	El presente control se aplicará para poder mitigar el hurto de medios o documentos, implementando procedimientos para un adecuado almacenamiento de documentos y medios. Además me ayudará a asegurar la integridad de la información verificando el origen de los datos.

Tabla 2-25 Controles Seleccionados.

Fuente: Los Autores

2.2. ELABORACIÓN DE LA DOCUMENTACIÓN BASE DEL PLAN DE SGSI.

Esta sección está dedicada a la realización del Plan del Sistema de Gestión de la Seguridad de la Información, para la realización del mismo es necesario seguir algunas fases la cuales están asociadas a entregables, los cuales se explicaran con más detalle en las siguientes secciones.

2.2.1 DESCRIPCIÓN DEL SERVIDOR ALFRESCO COMO HERRAMIENTA DE APOYO.

La norma ISO/IEC 27001:2011, establece que todos los documentos que forman parte del Plan del Sistema de Gestión de la Seguridad de la Información deben estar protegidos y controlados, de la misma forma se deben establecer procedimientos que permitan mantener disponibles los documentos para su revisión por parte del personal que labora en la organización. Para poder cumplir con esto lineamientos, se va a utilizar el Servidor Alfresco el cual permitirá:

- Revisar y actualizar toda la documentación referente al Plan del Sistema de Gestión de Seguridad de la Información.
- Llevar un control de cambios que se realicen sobre la documentación, identificando cuando se realizó la última modificación.
- Asegurar que los documentos se puedan identificar con facilidad y sean entendibles para todo el personal.
- Asegurar que la distribución y los permisos de acceso a los documentos sean controlados.

Se ha tomado la decisión de usar el Servidor Alfresco como herramienta de almacenamiento de los documentos por dos razones:

1. El Distrito Zonal ya cuenta con un servidor de Alfresco el cual se encuentra ubicado en la Subsecretaría de Educación, el Jefe del Departamento de TIC's es el encargado de su administración dentro del Distrito Zonal No.6 "Eloy Alfaro", además los empleados de la Organización ya tiene un conocimiento previo de su funcionamiento.
2. La herramienta Alfresco, es un software de código abierto y según como se establece en el Decreto 1014 en el artículo uno, que dice: se establece como política pública para las Entidades de Administración pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos. [8]. Alfresco es una buena oportunidad para considerar dicho Decreto.

2.2.1.1 Definición y Funcionalidades del Alfresco.

Alfresco es un sistema de gestión de contenidos de código abierto, con más de 1.700 clientes en todo el mundo, conformados por un 70% de empresas y un 25% de organismos de administración pública, con un porcentaje menor de entidades financieras y medios de comunicación [9]. Los beneficios del Servidor Alfresco al ser implementado dentro de un Organización son [10]:

- Organizar y facilitar la gestión de contenido, sea estos documentos ofimáticos, presentaciones, imágenes, videos, etc.

- Gestionar el ciclo de vida de los contenidos, crear, compartir, versionar, aprobar, publicar, retirar, archivar información.
- Provee un repositorio Fuente basado en últimas tecnologías y estándares altamente escalables, disponibles y extraíbles.

Las principales funciones del Alfresco incluyen [11]:

- **Espacio de Trabajo:** Alfresco ofrece espacios de trabajo identificados con permisos para los diferentes usuarios. Además ofrece espacios inteligentes programando límite de espacio de almacenamiento, tipos de archivos a ser almacenados.
- **Multilingüismo y versiones:** Alfresco es completamente multilingüe, la interfaz cuenta de 25 idiomas, los documentos pueden traducirse en varios idiomas. Además incluye un gestor de versiones de los contenidos, cada modificación de un contenido es un cambio en el Alfresco, que aparecerá en el historial y será archivado para poder volver a una versión anterior.
- **Metadatos:** se puede consultar una ficha detallada de un documento que reúne el conjunto de información propia del documento y de sus versiones. Se almacenan metadatos como fechas, usuarios, listas, etc.
- **Formato de archivo:** Alfresco es capaz de gestionar todo tipo de documentos, desde archivos de texto simple a archivos binarios pasando por documentos ofimáticos.
- **Bloqueo de Documentos:** Alfresco integra un mecanismo de check-in/ check-out[9] que permite restringir los accesos a los documentos. Si un usuario desea realizar una modificación en un documento, deberá extraer una copia del trabajo de este documento (check-out) que bloqueará automáticamente el documento y creará una copia accesible únicamente para el usuario, que haya realizado la extracción para que pueda realizar las correcciones.

[9] Check- in / Check out es el proceso por el cual se ingresan datos en el servidor y se registra la acción automáticamente, check out bloquea la acción en caso de que se requiera una copia del Documento.

2.2.1.2. Estructura del Repositorio Alfresco

Como se especificó en la sección anterior, se utilizará el servidor Alfresco para el almacenamiento los documentos del Plan del Sistema de Gestión de la Seguridad de la Información, para ellos es importante mencionar el flujo donde se encontrarán los diferentes archivos. La siguiente figura muestra la ubicación de los archivos dentro del Servidor Alfresco.

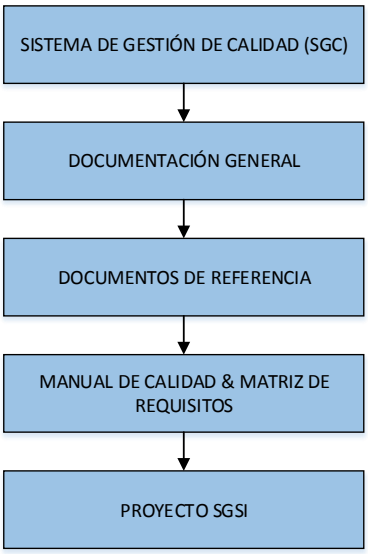


Figura 2-14 Flujo para la Documentación dentro del Servidor Alfresco

Fuente: Los Autores

Los documentos estarán disponibles para los usuarios dependiendo de los permisos de cada uno, por ejemplo: el Director Distrital y el Jefe del Departamento de TIC's podrán acceder a toda la documentación del SGSI, mientras que el resto de empleados podrán tener accesos solo a las políticas del Plan del Sistema de Gestión de la Seguridad de la Información.

En la Tabla 2-26 se muestra la estructura del repositorio de los ficheros, propuesta por los autores del proyecto, para el almacenamiento de los documentos que forman parte de la Planificación del SGSI.

FASES DEL PLAN DE GESTIÓN DE SEGURIDADES DE LA INFORMACIÓN	ENTREGABLES DE LA NORMA.	ESTRUCTURA SGSI EN EL REPOSITORIO ALFRESCO

FASES DEL PLAN DE GESTIÓN DE SEGURIDADES DE LA INFORMACIÓN	ENTREGABLES DE LA NORMA.	ESTRUCTURA SGSI EN EL REPOSITORIO ALFRESCO
Obtención de la aprobación de la dirección para iniciar un proyecto de SGSI	Aprobación de la dirección para la iniciación del proyecto de SGSI	Documentos Habilitantes
Definición del alcance, límites y políticas del SGSI	El alcance y límites del SGSI	Alcance del SGSI
	Política del SGSI	Controles
Realización del análisis de requerimientos de la seguridad de la información	Requerimientos de seguridad de la información	Alcance del SGSI
	Activos de información	No aplica, Identificación de activos se encuentra en la sección 1.3.
	Resultados de la evaluación de la seguridad de la información	Plan de evaluación y tratamiento de riesgos
Realización de la evaluación del riesgo y planificación del tratamiento del riesgo	Aprobación escrita de la dirección para la implementación del SGSI	No aplica
	Plan de tratamiento del riesgo	Plan de evaluación y tratamiento de riesgos
	Declaración de aplicabilidad incluyendo los objetivos de control y los controles seleccionados	Controles
Diseño del SGSI	Plan final de implementación del proyecto de SGSI	Controles (en esta sección se encuentran las 12 Políticas Creadas para la Organización)

Tabla 2-26 Estructura de Ficheros para el Repositorio Alfresco

Fuente: Los Autores

2.2.1. DESCRIPCIÓN DEL PLAN DEL SGSI.

Como se menciona en la sección 1.3.2, una de las características más relevantes que brinda la norma ISO/IEC 27001:2011, es que se adapta al modelo PDCA, aclarando que el proyecto se centra en la fase de Planificación, las otras fases que son la implementación, verificación y mejoramiento del plan quedan a criterio del Distrito Zonal No.6 “Eloy Alfaro”. Según la NTE INEN-ISO/IEC 27001:2011 la fase de

Planificación define las políticas, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la Organización. [3]

2.2.1.1 Fases y Entregables de la norma NTE INEN-ISO/IEC 27003:2012.

La finalidad de la norma NTE INEN-ISO/IEC 27003:2012, es proveer una guía práctica en el desarrollo del plan de implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de una Organización, de acuerdo con la Norma INEN-ISO/IEC 27001:2011.

El proceso descrito dentro de esta norma Internacional, ha sido diseña para proveer soporte a la implementación de la Norma ISO/IESC 27001:2011 [13]. El plan de gestión de seguridad de la información según la norma NTE INEN-ISO/IEC 27003:2012 consta de cinco fases, cada una con sus respectivos entregables, las mismas que pueden ser visualizadas en la Figura 2-15.

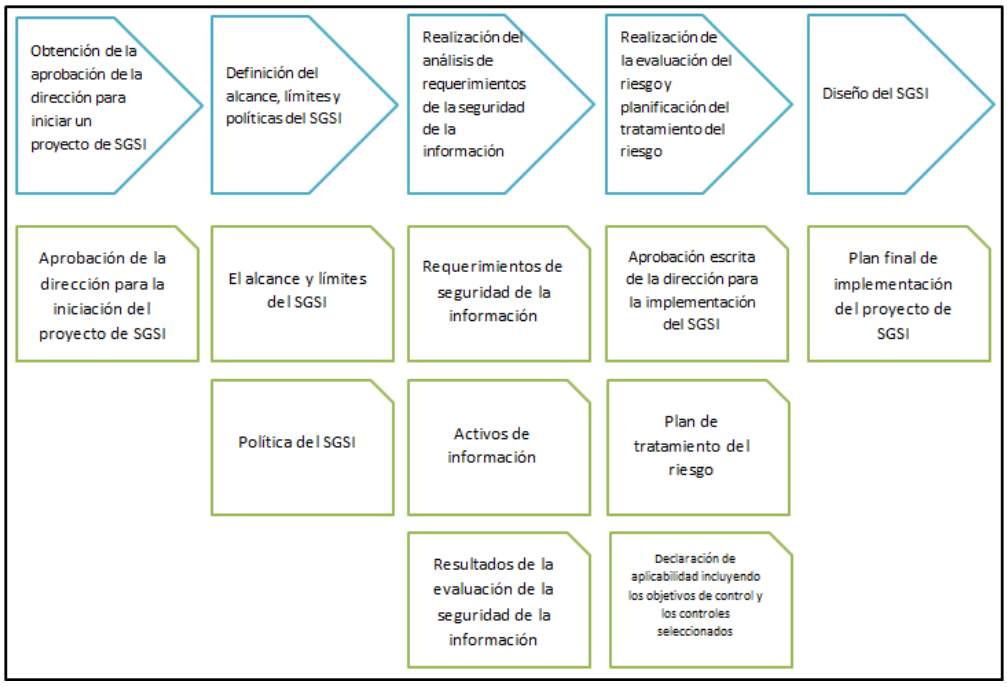


Figura 2-15 Fases de la Planificación del SGSI.

Fuente: Norma NTE INEN-ISO/IEC 27003:2012

A continuación se procede con la descripción de cada una de las fases, y que es lo que se pretende conseguir con la realización de cada una de ellas.

FASE	DESCRIPCIÓN.
Aprobación de la dirección para la iniciación del proyecto	En esta fase se pretende conseguir la autorización y el compromiso de la Dirección Distrital para poder inicial con la realización del Plan del Sistema de Gestión de Seguridad de la Información.
Definir el alcance del SGSI, límites y políticas del SGSI	Se busca definir el alcance y los límites Organizacionales referentes al activo crítico identificado, también se busca establecer los objetivos que se pretende alcanzar con la realización del proyecto.
Realizar el análisis de los requerimientos de seguridad de la información	Esta fase consiste en el análisis de la situación actual de la organización para identificar los requerimientos de seguridad de la información y los activos de información críticos a ser considerados en el SGSI
Realizar la evaluación del riesgo y la planificación del tratamiento del riesgo	Consiste en definir la metodología de evaluación del riesgo en base a la cual se seleccionarán los controles pertinentes para su mitigación. Los entregables de esta fase son la aprobación de la dirección para la implementación del SGSI, el plan de tratamiento del riesgo y la declaración de aplicabilidad de los controles seleccionados.
Diseño del SGSI	Esta fase corresponde con la fase “Hacer” del modelo PHVA y consiste en el diseño de la seguridad organizacional en base a las opciones de tratamiento del riesgo seleccionadas, los requerimientos de registro y documentación y el diseño de controles. Se tiene como entregable el plan de implementación del proyecto de SGSI.

Tabla 2-27 Fases de la Planificación del SGSI.

Fuente NTE INEN-ISO/IEC 27003:2012

2.2.2 DESCRIPCIÓN DE LOS ENTREGABLES.

Después de haber realizado en análisis de riesgos y haber identificado los controles a implementar para mitigar la materialización del riesgo, se procederá a la realización de las Políticas que van a componer el Plan de Seguridad de la Información. Las políticas a realizar agruparan varios controles o pueden tener un solo control.

Las políticas definidas son las siguientes:

- Política de Contraseñas y Claves.
- Política de Control de Acceso.
- Política de Gestión de Red.
- Política de Puesto de Trabajo despejado y Pantalla Limpia.
- Política de Responsabilidades de los Usuarios.
- Política de Supervisión y Uso de Sistemas de Información.
- Política de Uso de Activos.
- Política de Autentificación de Usuarios.
- Política de Mantenimiento de Equipos.
- Política para la Gestión de Usuarios.
- Política para la Regulación Legales.
- Política para el Uso de la Información.

Adicionalmente se cuenta con entregables, que forman parte de la norma ISO 27003:2012 y que servirán para la realización del Plan del Sistema de Gestión de la Seguridad de la Información.

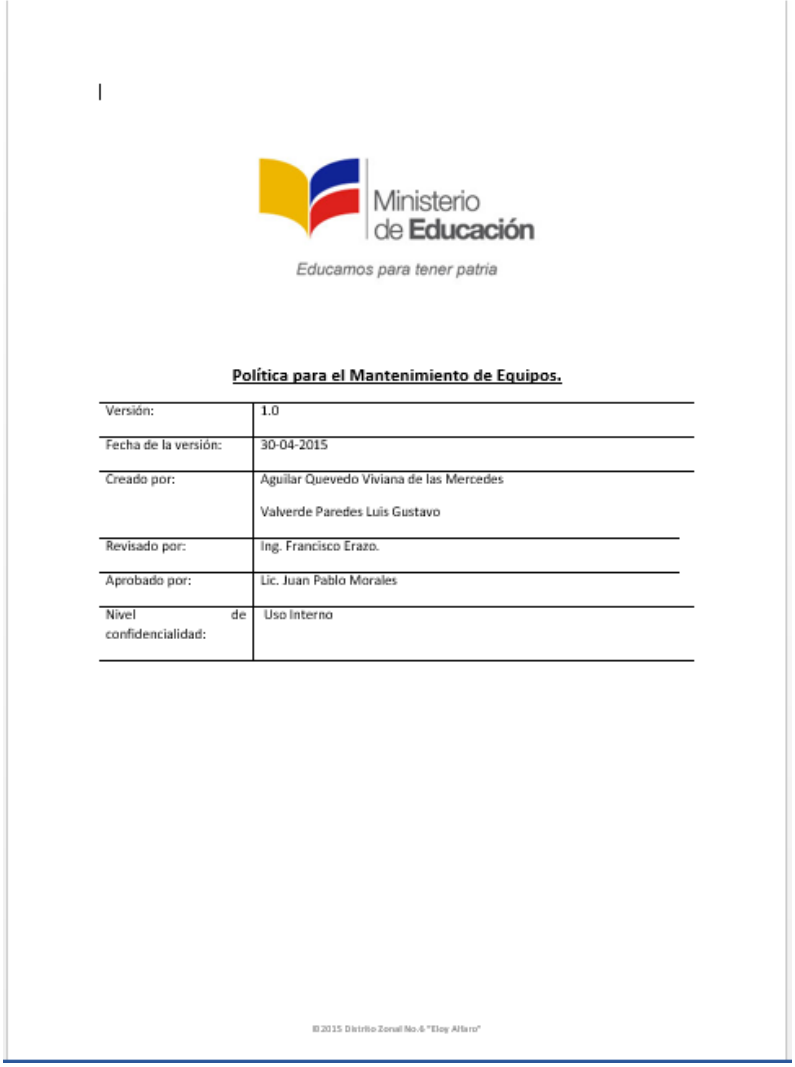
- Plan de Proyecto.
- Política del SGSI.
- Alcance y Límites del SGSI.
- Metodología de Evaluación de Riegos.
- Informe de Evaluación de Riesgos.
- Plan de Tratamiento de Riesgos.
- Declaración de Aplicabilidad.
- Procedimiento para el Control de Documentos y Registros.
- Gestión de Incidentes.
- Requisitos de la Seguridad de la Información.

2.2.2.1 Modelo de Documento de Política

Es necesario que se elabore un formato para el Documento de Políticas desarrolladas para el Distrito Zonal N°6 “Eloy Alfaro”, ya que todas las políticas deben cumplir con un estándar aprobado por la Dirección, por lo tanto, los autores del presente proyecto han desarrollado un formato para la creación y aprobación de las políticas que van a ser almacenadas en el repositorio Alfresco, para que de esta manera puedan ser accedidas por el personal que forma parte de la Organización y puedan cumplir con las normas implantadas para mejorar la Seguridad de la Información sensible del Distrito Zonal.

El Documento para la elaboración de Políticas está estructurado de la siguiente manera:

En la Primera Hoja del documento, se coloca el Logo que representa a la Organización en mención, seguido de una tabla en la que se específica la versión del Documento, la fecha en la cual fue realizada esa versión del Documento, los creadores de ese Documento de Política, el nombre del encargado de Revisar que la Política cumpla con las normativas bajo las cuales se maneja el Distrito Zonal, se especifica también el nombre de la persona encarga de Aprobar la Política, para que esta pueda ser almacenada en el Repositorio Alfresco, y por último se especifica el Nivel de Confidencialidad del documento para filtrar a los usuarios que tienen acceso a dicho documento. En la Figura 2-16 se puede observar de mejor manera el formato de carátula para el Documento de Política diseñado para el Distrito Zonal N° 6.



Ministerio de Educación

Educamos para tener patria

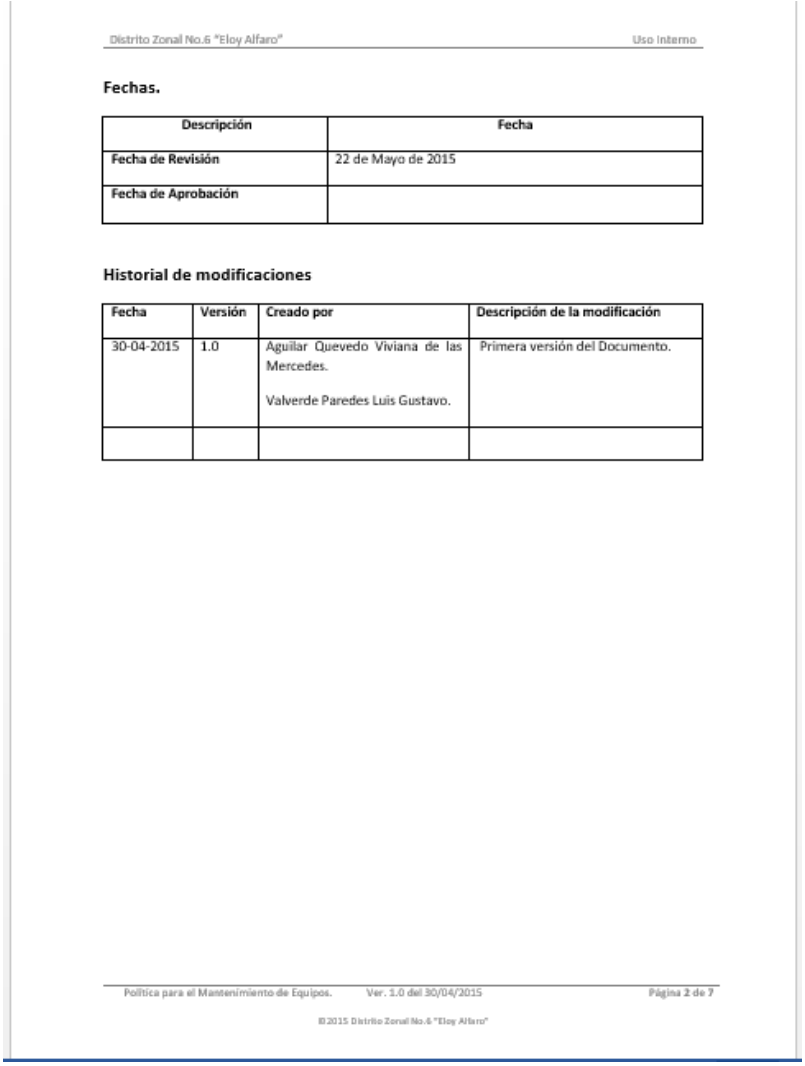
Política para el Mantenimiento de Equipos.

Versión:	1.0
Fecha de la versión:	30-04-2015
Creado por:	Aguilar Quevedo Viviana de las Mercedes Valverde Paredes Luis Gustavo
Revisado por:	Ing. Francisco Erazo.
Aprobado por:	Lic. Juan Pablo Morales
Nivel de confidencialidad:	Uso Interno

Figura 2-16 Carátula Documento de Política

Fuente: Los Autores

En la siguiente hoja del documento se tiene dos tablas, la primera especifica la fecha en la cual la política fue Revisada por el responsable del proceso y la fecha en la cual fue Aprobada dicha política. En la segunda tabla se cuenta con un Historial de Modificaciones, para lo cual se debe registrar la fecha en la cual dicha política fue modifica, la versión a la que fue modificada la política seguido de los responsables de haber creado dicha modificación en la política y por último se debe colocar una Descripción clara y concisa de las modificantes que se realizaron en la política. En la Figura 2-17 se muestra la imagen que describe de mejor manera las tablas mencionadas anteriormente con un ejemplo de cómo se debe llenarla.



Distrito Zonal No.6 "Eloy Alfaro" Uso Interno

Fechas.

Descripción	Fecha
Fecha de Revisión	22 de Mayo de 2015
Fecha de Aprobación	

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
30-04-2015	1.0	Aguilar Quevedo Viviana de las Mercedes. Valverde Paredes Luis Gustavo.	Primera versión del Documento.

Política para el Mantenimiento de Equipos. Ver. 1.0 del 30/04/2015 Página 2 de 7

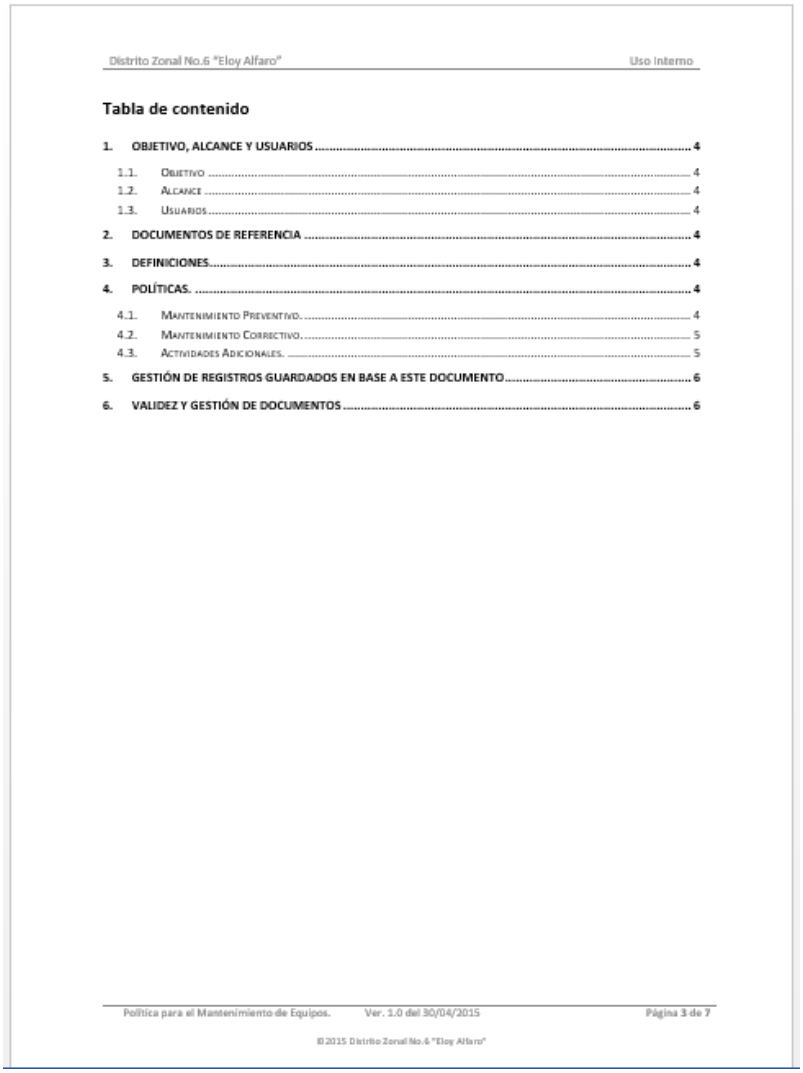
©2015 Distrito Zonal No.6 "Eloy Alfaro"

Figura 2-17 Historial de modificaciones del Documento de Política

Fuente: Los Autores

En la siguiente página se encuentra la tabla del contenido, en la cual se especifican los temas tratados en el documento y en donde se encuentran dichos temas dentro del documento.

En la Figura 2-18 se muestra la imagen en el cual se cuenta con un ejemplo de la Tabla de Contenido de una Política creada Para el Distrito Zonal N° 6 “Eloy Alfaro”.



Distrito Zonal No.6 "Eloy Alfaro" Uso Interno

Tabla de contenido

Política para el Mantenimiento de Equipos. Ver. 1.0 del 30/04/2015 Página 3 de 7

©2015 Distrito Zonal No.6 "Eloy Alfaro"

Figura 2-18 Tabla de Contenido de una Política

Fuente: Los Autores

Luego de la Tabla de contenido procedemos al desarrollo del documento en sí, para ello se lo ha dividido en secciones, en la primera sección se deben definir ciertos aspectos importantes que permiten entender de mejor manera el documento, estos aspectos son:

- El Objetivo.
- El Alcance.
- Los Usuarios que van a tener acceso a ese Documento.

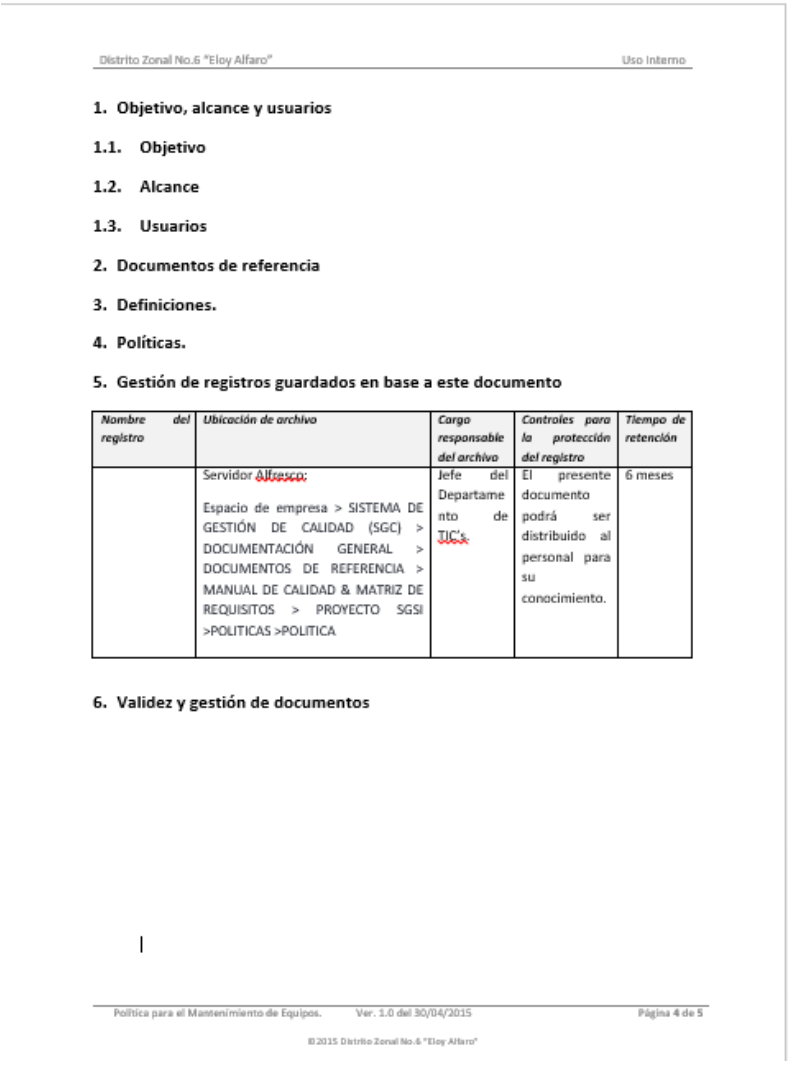
En la segunda sección se especifican los Documentos que sirvieron de Referencia para desarrollar el actual, cada uno consta de ciertas entradas que deben cumplir para poder ser desarrollados.

La tercera parte del Documento puede variar, esto se debe a que en ciertos documentos puede o no ser necesario realizar una aclaración de ciertos términos que pueden ser no tan comunes y necesitan de una explicación previa, en otros casos se procede con el Desarrollo mismo de la Política como tal, esto significa que se especifican las actividades que deben ser desarrolladas por el personal para garantizar una adecuada Seguridad de la Información.

En la siguiente sección se muestra un cuadro que corresponde a la Gestión de registros guardados en base a este documento, lo que significa que debemos especificar la dirección exacta en el repositorio en donde va a ser almacenada la política, para que pueda ser accedida por los empleados.

Para finalizar en la última sección debemos especificar el período de validez que tiene la política y de la frecuencia con la que tiene que ser revisada, para verificar si se ameritan o no cambios a dicha política y quienes son los encargados de dicha gestión.

En la Figura 2-19 se puede observar de mejor manera el formato que se debe seguir para desarrollar el Documento de Política.



Distrito Zonal No.6 "Eloy Alfaro" Uso Interno

1. Objetivo, alcance y usuarios

1.1. Objetivo

1.2. Alcance

1.3. Usuarios

2. Documentos de referencia

3. Definiciones.

4. Políticas.

5. Gestión de registros guardados en base a este documento

Nombre del registro	*Ubicación de archivo*	*Cargo responsable del archivo*	*Controles para la protección del registro*	*Tiempo de retención*
	Servidor Alfresco: Espacio de empresa > SISTEMA DE GESTIÓN DE CALIDAD (SGC) > DOCUMENTACIÓN GENERAL > DOCUMENTOS DE REFERENCIA > MANUAL DE CALIDAD & MATRIZ DE REQUISITOS > PROYECTO SGSI >POLITICAS >POLITICA	Jefe del Departamento de TIC's.	El presente documento podrá ser distribuido al personal para su conocimiento.	6 meses

6. Validez y gestión de documentos

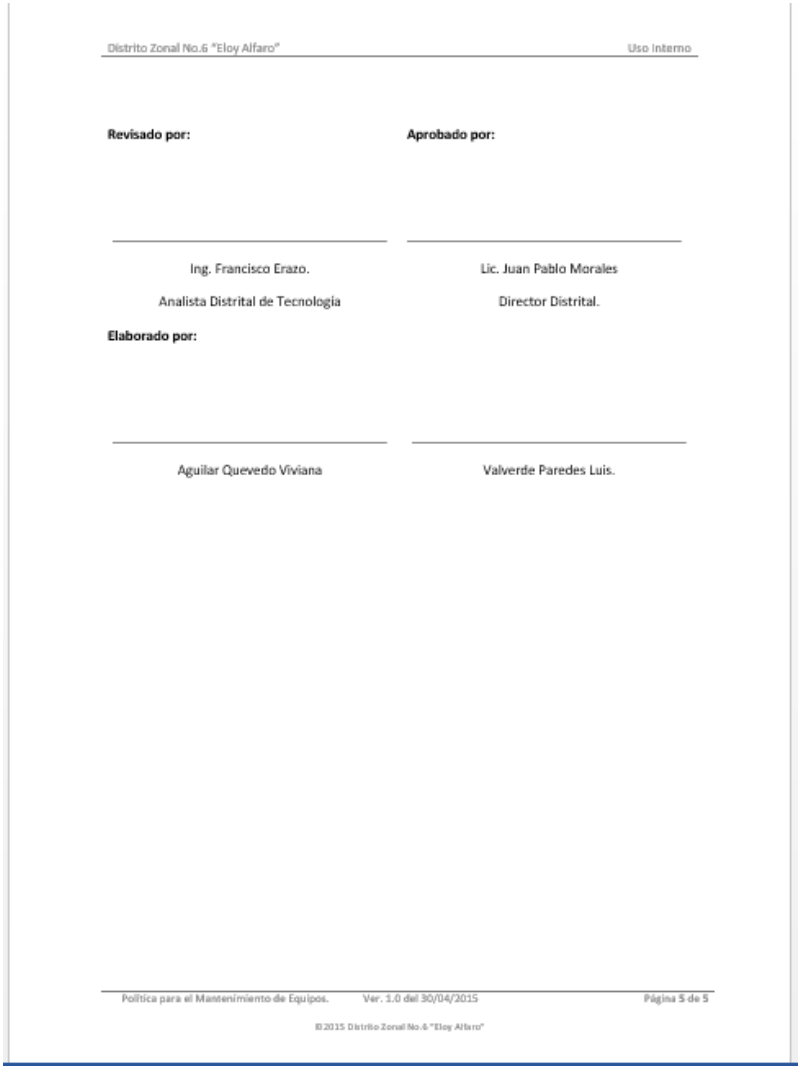
Política para el Mantenimiento de Equipos. Ver. 1.0 del 30/04/2015 Página 4 de 5

©2015 Distrito Zonal No.6 "Eloy Alfaro"

Figura 2-19 Contenido del Documento de Política

Fuente: Los Autores

Al final del desarrollo de la política se tiene un registro de las personas involucradas tanto en el desarrollo, la revisión y la aprobación del Documento, el mismo que cuenta con un espacio para que cada uno de los involucrados pueda colocar su firma tal y como se muestra en la Figura 2-20.



Distrito Zonal No.6 "Eloy Alfaro" Uso Interno

Revisado por: **Aprobado por:**

Ing. Francisco Erazo. Lic. Juan Pablo Morales

Analista Distrital de Tecnología Director Distrital.

Elaborado por:

Aguilar Quevedo Viviana Valverde Paredes Luis.

Política para el Mantenimiento de Equipos. Ver. 1.0 del 30/04/2015 Página 5 de 5

©2015 Distrito Zonal No.6 "Eloy Alfaro"

Figura 2-20 Firmas de Desarrollo, Revisión y Aprobación del Documento de Política

Fuente: Los Autores

2.2.2.2 Descripción de la Documentación base del SGSI.

En esta sección se procede a describir cada uno de los entregables necesarios para realizar el Plan de Seguridad de la Información.

2.2.2.2.1 Plan de Proyecto.

En este documento se explica la importancia de la realización del Proyecto del plan del Sistema de Gestión de la Seguridad de la Información para la Organización, con la finalidad de obtener el apoyo, aprobación y el compromiso por parte de la

Dirección para el desarrollo del presente proyecto, así como también se explican los beneficios a largo plazo y las responsabilidades de cada uno de los involucrados.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 7.

2.2.2.2.2 Alcance y límites del SGSI.

En el presente documento se define alcance y los límites del SGSI. El alcance de este proyecto es:

"La Planificación del Sistema de Gestión de la Información se lo realizará en Distrito Zonal No.6 "Eloy Alfaro", ubicado en la Av. Upano y Pedro de Céspedes, específicamente a la información que almacena el Departamento de TIC's la cual es necesaria para la ejecución de los diferentes procesos que garantizan la calidad de los servicios que ofrece. Es importante definir el personal que se encuentra inverso dentro de esta Planificación del SGSI, los cuales serán, todos los empleados de la organización, con diferentes responsabilidades cada uno de ellos, como es el Director Distrital, quien será el encargado de la aceptación de todo lo referente al SGSI; el jefe del Departamento de TIC's, quien será el encargado de la revisión de todo lo relacionado al SGSI; el personal quienes serán los encargados de poner en práctica todas la políticas de seguridad necesarias para un adecuado manejo de la información.

El punto de enfoque será en Sistema de Carpetas Compartidas, el cual es uno de los activos más importantes para el Departamento, en el cual se almacena información que tiene que cumplir con la integridad, disponibilidad y confidencialidad de la información para así garantizar y ayudar que los objetivos de la empresa se cumplan en su totalidad."

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 8.

2.2.2.2.3 Políticas del SGSI.

Dentro del documento de Políticas del SGSI, se describe los objetivos del proyecto, leyes y reglamentos que rigen a la Organización. Tomando en cuenta que el proyecto está dirigido al Distrito Zonal No. 6 "Eloy Alfaro", y que es una entidad pública, ésta tiene que acatar dichos reglamentos y estatutos que le imponga la Subsecretaria de Educación y el Ministerio de Educación, tenemos que tener claro cuáles son las leyes que los rigen, como por ejemplo: la Constitución del Ecuador, Código de planificación de finanzas, Ley Orgánica de transparencia al acceso de la Información, etc.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 9.

2.2.2.2.4 Metodología de Evaluación de Riesgos

El presente documento tiene como finalidad brindar una visión de cuál es la metodología que se seleccionó para poder realizar el análisis de riesgos, en este caso de la Metodología de Análisis y Gestión de Riesgos MAGERIT. Se mostrará cuáles son los pasos a seguir para la realización del análisis.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 10.

2.2.2.2.5 Informe de Evaluación de Riesgos

El presente documento tiene como finalidad mostrar la ejecución de las diferentes herramientas que se utilizaron para el análisis de vulnerabilidades existentes dentro

de la Organización. Se muestra a detalle el proceso que se realizó con el análisis de resultados de los mismos.
Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 4.

2.2.2.2.6 Plan de tratamiento del riesgo

Dentro del plan de tratamiento del riesgo, se especifican los pasos a seguir para que el personal dentro del Distrito Zonal No.6 "Eloy Alfaro", en caso de ser necesario, puedan realizar un análisis adecuado, se presenta la selección de los controles a utilizar, seguido de la justificación de cada uno de ellos, se sugiere el tiempo de revisión del Plan del SGSI, así como también el tiempo para la realización de Auditorías Internas, para finalizar se muestra un plan de capacitación a los empleados.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No. 6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 11.

2.2.2.2.7 Declaración de aplicabilidad.

Dentro del documento de aplicabilidad, se especifican cuáles han sido los controles seleccionados para poder tratar las vulnerabilidades encontradas, así como también se mencionan cuáles son los controles que están siendo utilizados actualmente por el Distrito Zonal No.6 "Eloy Alfaro", para finalizar se justifican cuáles son los controles que no se utilizarán en este proyecto.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 12.

2.2.2.2.8 Procedimiento para el control de Documentos y Registros.

El presente documento tiene como finalidad determinar los procedimientos que el Distrito Zonal No.6 debe realizar para gestionar de mejor manera los documentos y Registros, de la misma manera se especificará el periodo de validez que tienen los documentos y procedimientos para retirarlos en caso de ser necesario.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 13.

2.2.2.2.9 Gestión de Incidentes.

Este documento tiene como finalidad garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta a dichos aspectos, para de esta manera mitigar las posibles consecuencias en el caso de que los eventos puedan afectar la operatividad de la Organización.

Este documento está dirigido al Director Distrital y al Jefe del Departamento de TIC's del Distrito Zonal No.6 "Eloy Alfaro." El documento completo se encuentra en el Anexo 14.

2.2.2.2.10 Requisitos de la Seguridad de la Información.

El objetivo de realizar el análisis de requerimientos de seguridad de la información es el de identificar activos de información importantes para la Organización, así como también identificar el estado actual de la misma con un enfoque de la seguridad de la información para de esta manera identificar el nivel de protección que la Organización desea dar a la Información.

Los pasos a realizar en esta etapa son los siguientes:

- Identificación de la Organización. (sección 1.1)
- Identificación de activos. (sección 1.2)

- Clasificación de activos. (no aplica[10])
- Identificación de la Situación Actual de la Organización. (sección 1.3.3)
- Identificar el nivel de protección que la Organización desea dar a la Información. (sección 1.3.3.1)

2.2.2.3 Descripción de las políticas.

En esta sección de describen las políticas desarrolladas para mitigar los riesgos identificados en la Organización.

2.2.2.3.1 Política de Contraseñas y Claves.

Esta política tiene como finalidad, establecer normas para la adecuada creación de claves para los usuarios, así como también el adecuado uso de las mismas, de esta forma se podrá garantizar la confidencialidad de la información, logrando la continuidad de la Organización. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 15.

2.2.2.3.2 Política de Control de Acceso.

Esta política tiene como finalidad, establecer normas para la adecuada gestión para la creación de usuarios así como también para brindar acceso a los diferentes sistemas.

Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 16.

2.2.2.3.3 Política de Gestión de Red.

Esta política tiene como finalidad asegurar la adecuada gestión de la red, su configuración y su adecuada utilización, de esta forma se espera asegurar la integridad de la información que pertenece a la Organización. Este documento se

[10] Esta actividad no aplica, puesto que el Director Distrital y el Jefe del Departamento de TIC’s seleccionan el activo crítico a tratar.

está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 17.

2.2.2.3.4 Política de Puesto de Trabajo despejado y Pantalla Limpia.

Esta política tiene como finalidad, establecer normas hacia los usuarios para que estos puedan tener su puesto de trabajo despejado y tengan normativas para poder tener la pantalla limpia. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 18.

2.2.2.3.5 Política de Responsabilidades de los Usuarios.

Esta política tiene como finalidad, establecer normas que deberán de seguir los empleados que se encuentran dentro del Distrito Zonal No.6 “Eloy Alfaro”, así como también los procedimientos que se tiene que seguir, con el propósito de garantizar la continuidad de las diferentes operaciones. En esta sección se definen las responsabilidades tanto del Jefe del Departamento de TIC’s como del personal en General. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 19.

2.2.2.3.6 Política de Supervisión y Uso de Sistemas de Información.

Esta política tiene como finalidad establecer normas referentes al uso adecuado de los diferentes sistemas, haciendo referencia al uso adecuado de los recursos disponibles, evitando la descarga de código malicioso que pueda poner en riesgo la integridad de la información. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 20.

2.2.2.3.7 Política de Uso de Activos

Esta política tiene como finalidad establecer normas para el adecuado uso de los activos, es decir establece reglas para que los diferentes usuarios aprendan a tener un adecuado uso con los activos de la Organización. De esta forma se podrá asegurar el adecuado funcionamiento de los activos existentes. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 21.

2.2.2.3.8 Política de Autentificación de Usuarios.

Esta política tiene como finalidad asegurar la integridad de la información cuando usuarios, tanto internos como externos se conectan al sistema que se está utilizando dentro del Distrito Zonal No.6 “Eloy Alfaro”. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 22.

2.2.2.3.9 Política de Mantenimiento de Equipos.

Esta política tiene como finalidad, establecer normas para el adecuado mantenimiento de los equipos que se encuentran dentro del Distrito Zonal No.6 “Eloy Alfaro”, con la finalidad de garantizar la continuidad de las operaciones Administrativas del mismo. Dentro de esta política se habla del mantenimiento correctivo y preventivo de los equipos de cómputo.

Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 23.

2.2.2.3.10 Política para la Gestión de Usuarios.

Esta política tiene como finalidad establecer lineamientos para la correcta gestión de los usuarios que laboran o que se integren a la Organización. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 24.

2.2.2.3.11 Política para la Regulación Legales.

Esta política tiene como finalidad, establecer normas sobre las diferentes regulaciones legales que se tiene que seguir dentro de la Organización, es decir hace referencia sobre el uso de software licenciado adulterado y las posibles sanciones que los usuarios pueden tener en caso de hacerlo. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 25.

2.2.2.3.12 Política para el Uso de la Información.

El presente documento tiene como finalidad, garantizar el uso adecuado de la información que se maneja dentro del Distrito Zonal No.6 “Eloy Alfaro”. En esta sección se especifica la forma en la que se clasifica y etiqueta la información. Este documento se está dirigido al todo el personal interno del Distrito Zonal No.6 “Eloy Alfaro.” El documento completo se encuentra en el Anexo 26.

2.3 GUÍA DE IMPLEMENTACIÓN.

El personal que está a cargo de la ejecución de las actividades de la implementación son el Director Distrital y el Jefe del Departamento de TIC’s, recalcando que se pueden añadir otras actividades dependiendo de las necesidades de la Organización.

Para la implementación del plan, se debe seguir una secuencia de actividades, las cuales se muestran a continuación:

1. Identificación del marco legal: Investigación sobre todas las normas, leyes y reglamentos vigentes en el Ecuador así como las que rigen a la Organización. (ver anexo 27)
2. Determinar la situación actual del Distrito Zonal No 6. “Eloy Alfaro” referente a la seguridad de la información, esta actividad se realizó con la ayuda de encuestas realizadas al Jefe del Departamento de TICS, con base a los controles del anexo A de la norma ISO/EC 27001, (ver sección 1.3.3)
3. Aprobación del plan de seguridad por parte del Director Distrital.

4. Definir una metodología para el análisis de riesgos, (ver sección 2.1.3)
5. Identificación de los activos de información, se caracteriza a los activos de información como activos primarios y activos de soporte, de los activos identificados se realiza la valoración de los mismos y se identifica el de mayor criticidad, (ver sección 2.1.4.2).
6. Análisis de las vulnerabilidades tanto físicas como lógicas existentes relacionadas al activo de información, (ver sección 2.1.4.4).
7. Análisis de las amenas existentes relacionadas al activo de información y que puedan explotar las vulnerabilidades encontradas, (ver sección 2.1.4.5).
8. Definir los criterios de valoración y escalas para la probabilidad e impacto del riesgo, en caso de que una amenaza explote una vulnerabilidad y la materialice, (ver sección 2.1.4.6).
9. Evaluar al riesgo en base a los valores especificados de probabilidad e impacto, en este caso se utilizó una matriz para poder hacer más fácil la evaluación, (ver sección 2.1.4.6).
10. Establecer una propuesta de tratamiento del riesgo, identificando cuales son las acciones a tomar ante ellos, en nuestro caso se definen las acciones de eliminar, mitigar, compartir, y financiar, de las cuales en el presente proyecto se consideró el mitigar y financiar los riesgos, (ver sección 2.1.4.7).
11. Aplicar la propuesta de tratamiento del riesgo, con la selección de controles de seguridad definidos en la norma ISO/IEC 27001, (ver sección 2.1.4.10).
12. Elaboración de los documentos base para el SGSI.
    - 12.1 Elaboración del Plan de Proyecto (ver Anexo 7)
    - 12.2 Elaboración del Documento de Alcance y Límites del SGSI, (ver Anexo 8).
    - 12.3 Elaboración de la Política del SGSI, (ver Anexo 9).
    - 12.4 Elaboración de la Metodología de Evaluación de Riesgos, (ver Anexo 10).
    - 12.5 Elaboración del Informe de Evaluación de Riesgos, (ver Anexo 4).
    - 12.6 Elaboración del Plan de Tratamiento de Riegos, (ver Anexo 11).

12.7 Elaboración de la Declaración de Aplicabilidad del SGSI, (ver Anexo 12).

12.8 Elaboración de los Procedimientos para el Control de Documentos y Registros, (ver Anexo 13).

12.9 Elaboración del documento de Gestión de Incidentes, (ver Anexo 14).

13. Elaboración de la Política de Contraseñas y Claves, (ver Anexo 15).
14. Elaboración de la Política de Control de Acceso, (ver Anexo 16).
15. Elaboración de la Política de Gestión de Red, (ver Anexo 17).
16. Elaboración de la Política de Puesto de Trabajo despejado y Pantalla Limpia, (ver Anexo 18).
17. Elaboración de la Política de Responsabilidades de los Usuarios, (ver Anexo 19).
18. Elaboración de la Política de Supervisión y Uso de Sistemas de Información, (ver Anexo 10).
19. Elaboración de la Política de Uso de Activos, (ver Anexo 21).
20. Elaboración de la Política para Autentificación de Usuarios, (ver Anexo 22).
21. Elaboración de la Política para el Mantenimiento de equipos, (ver Anexo 23).
22. Elaboración de la Política para la Gestión de Usuarios, (ver Anexo 24).
23. Elaboración de la Política para la Regulaciones Legales, (ver Anexo 25).
24. Elaboración de la Política para el Uso de la Información, (ver Anexo 26).
25. Elaboración de otras políticas, las políticas realizadas son en base a los controles seleccionados, en caso de realizar otro análisis de riesgos y seleccionar nuevos controles, estos deberán ser parte de nuevas políticas, la selección de nuevos controles será realizado según las necesidades de la Organización.
26. Capacitación al personal.
27. Implementación de las políticas de seguridad establecidas.

2.4 ANÁLISIS DE LA FACTIBILIDAD DE LA APLICACIÓN DEL PLAN DEL SGSI.

El análisis de factibilidad, busca presentar al Jefe Distrital los recursos necesarios para poder implementar el proyecto dentro del Distrito Zonal No. 6 “Eloy Alfaro”. Este análisis se basa en 3 aspectos que son fundamentales para que el Sistema de Gestión de la Seguridad de la Información pueda ser aplicado, los aspectos son:

- Factibilidad Técnica.
- Factibilidad Operativa.
- Factibilidad Económica.

Es necesario que la organización disponga de los 3 aspectos tomados en cuenta para que el SGSI pueda ser implementado de manera adecuada dentro de la organización. Cada aspecto tomado en cuenta será tratado con mayor detenimiento en las siguientes secciones.

2.4.1. FACTIBILIDAD TÉCNICA

En esta sección se identifica los recursos técnicos requeridos para que se pueda implementar el SGSI en la organización, así como también identifica la disponibilidad de los equipos y la capacidad de procesamiento de los mismos para poder implementar el plan. En la tabla 2-28 se encuentran los requisitos del sistema.

CARACTERÍSTICAS	CAPACIDAD	DISPONIBILIDAD EN EL DEPARTAMENTO DE TIC’S
Sistema Operativo	Windows 2008 Server R2 Enterprise	Si
Disco Duro	1 TB	Si
Memoria (RAM)	6 GB	Si
Procesador	Intel Xeon 2.3 GHz	Si
Tarjeta de Red	1000 Mbps	Si

Tabla 2-28 Requisitos para el Sistema de Gestión Documental Alfresco

Fuente: Los Autores

El servidor es necesario para implementar el sistema para gestión documental Alfresco y poder colocar allí la documentación del proyecto para que el personal pueda accederlos.

El Distrito Zonal No. 6 actualmente cuenta con un servidor de Documentación el mismo que almacena toda la información de los procesos que realiza la organización, así como también almacena el sistema Alfresco que actualmente se encuentra implementado en la organización.

Es necesario también contar con otro tipo de equipos que permitan proteger a la organización y que ayude a la misma a cumplir con los objetivos de seguridad. En la tabla 2-29 se encuentran los requerimientos físicos.

CARACTERÍSTICAS	DISPONIBILIDAD DE LA ORGANIZACIÓN
Sistema contra incendios	Actualmente la organización cuenta con un extintor en la entrada al cuarto de servidores, el mismo que cuenta con detectores de humo.
Lectores Biométricos	Al momento el Distrito Zonal cuenta con lectores biométricos en el ingreso a las instalaciones, el mismo que nos ayuda a tener un control de los empleados que laboran en la organización.
Servicio de Guardianía	El Distrito Zonal cuenta con un servicio de guardianía que se encuentra ubicado en una caseta en la entrada a las instalaciones.
UPS	Al momento se ha implementado un UPS que permite evitar daños en los equipos debido a los cortes de energía inesperados.

CARACTERÍSTICAS	DISPONIBILIDAD DE LA ORGANIZACIÓN
Sistema de Aire acondicionado	El cuarto de servidores actualmente se encuentra con un adecuado sistema de Aire Acondicionado que permite brindar una adecuada refrigeración al Servidor.

Tabla 2-29 Requerimiento de Equipos Físicos contra Acceso no Autorizado.

Fuente: Los Autores

Referente al acceso a la red, el Distrito Zonal No. 6 “Eloy Alfaro” cuenta con un Sistema llamado Zentyal, que permite gestionar los permisos de navegación a los usuarios de la organización y el ancho de banda asignado para la navegabilidad.

Según el análisis realizado al Distrito Zonal No. 6, se puede evidenciar que cumple con los requisitos técnicos necesarios para implementar el Sistema de Gestión de la Seguridad de la Información en la organización sin ningún inconveniente, y no existe la necesidad de adquirir nuevos equipos.

2.4.2. FACTIBILIDAD OPERATIVA

El análisis de la factibilidad operativa, busca identificar si el Distrito Zonal No. 6 “Eloy Alfaro” cuenta con el personal necesario y capacitado para poder implementar el SGSI en la Organización, para poder definir el número de personas necesarias para poder realizar la Implementación del SGSI dentro de la Organización se ha realizado una Matriz de Carga de Trabajo Laboral, la misma que se puede visualizar en el Anexo 28, en la cual se identifica el número total de horas hombre necesarias para realizar la implementación del SGSI.

Al momento de realizar las entrevistas al personal, al Jefe del Departamento de TIC’s y al Director Distrital, se pudo evidenciar el apoyo y compromiso por parte de la dirección para la implementación del SGSI en la Organización, lo cual facilita el proceso de implementación.

Actualmente el personal que labora en el Departamento de TIC’s del Distrito Zonal No.6 se encuentra capacitado en temas de Seguridad de la Información y se han aplicado varios controles con temas referentes a la misma, por lo cual se facilita la implementación de nuevos controles.

Por otro lado, el personal que labora en los demás Departamentos no se encuentra familiarizado con temas de seguridad de la información, aunque actualmente se han implementado controles como el Sistema Biométrico, no se tiene un adecuado compromiso del personal, por lo cual es necesario realizar charlas que permitan concientizar al personal de lo importante de su trabajo dentro de la organización.

Para ayudar al proceso de concientización al personal, se han creado políticas que deben ser implementadas de manera adecuada y a las cuales todo el personal de la organización debe tener acceso, es recomendable que la organización realice una inversión y se adquiera la norma NTE ISO-IEC 27001:2011; donde se encuentran controles que pueden ser adoptados por la organización para mejorar la seguridad de la información.

Cabe mencionar que el proceso de creación del Sistema de Gestión de la Seguridad de la Información se encuentra detallado en este documento, el mismo que tiene un orden lógico que se debe seguir para poder crear e implementar el SGSI en la organización, es importante aclarar que el presente documento, fue desarrollado específicamente para un activo critico identificado por la organización como fundamental para el funcionamiento de la misma.

Dentro del análisis de la factibilidad operativa se considera la realización de charlas y capacitaciones, las cuales se especifica en el Documento del Plan de Tratamiento de Riesgos.

2.4.3. FACTIBILIDAD ECONÓMICA

El análisis de factibilidad económica, pretende presentar un estimado de los recursos económicos necesarios para poder implementar el Sistema de Gestión de la Seguridad de la Información en el Distrito Zonal No.6 “Eloy Alfaro”; cabe mencionar que los beneficios planteados con la implementación del SGSI en la organización no son económicos, sino que se pretende ahorrar costos de recuperación en el caso de que un evento inesperado afectase el activo crítico de la Organización.

Un aspecto importante necesario de mencionar es que, los recursos necesarios para proteger al activo crítico NO deben sobrepasar el valor del mismo, teniendo claro esto se procede a identificar los recursos necesarios para la implementación del SGSI en la organización mostrados en la Tabla 2-30.

RECURSO	COSTO
Servidor para el Sistema de Gestión Documental	$5000
Firewall	$7000
Lectores Biométricos	$300
Sistema de Suministro Eléctrico (UPS)	$7000
Antivirus	$2000
Licencias	$10600
Sistema de Aire Acondicionado	$800
Capacitaciones	$2000
Personal para la Implementación	$16000
NTE INE-ISO/IEC 27000	$170
NTE INE-ISO/IEC 27001	$150
NTE INE-ISO/IEC 27003	$180
NTE INE-ISO/IEC 27005	$180
TOTAL	$51380

Tabla 2-30 Recursos Económicos Estimados Para la Implementación del SGSI

Fuente: Los Autores

Basándose en cotizaciones realizadas de los recursos requeridos para la implementación del SGSI en el Distrito Zonal, se determina que el recurso económico estimado que se necesita para la implementación del Sistema es de $51380 dólares americanos.

Es importante mencionar que el Distrito Zonal N° 6 “Eloy Alfaro”, actualmente cuenta con ciertos recursos necesarios para la implementación del SGSI los cuales se detallan en la Tabla 2-31.

RECURSO	COSTO ESTIMADO	COSTO DE IMPLEMENTACIÓN
Servidor para el Sistema de Gestión Documental	$5000	$0
Firewall	$7000	$0
Lectores Biométricos	$300	$0
Sistema de Suministro Eléctrico (UPS)	$7000	$0
Antivirus	$2000	$1950
Licencias	$10600	$10582
Sistema de Aire Acondicionado	$800	$0
Capacitaciones	$2000	$2000
Personal para la Implementación	$16000	$16000
NTE INE-ISO/IEC 27000	$170	$170
NTE INE-ISO/IEC 27001	$150	$150
NTE INE-ISO/IEC 27003	$180	$180
NTE INE-ISO/IEC 27005	$180	$180
TOTAL	$51380	$31212

Tabla 2-31 Recursos Económicos Esperados Para la Implementación del SGSI.

Fuente: Los Autores

Una vez identificados los recursos con los que actualmente cuenta el Distrito Zonal No.6 “Eloy Alfaro” (marcados con valor 0 en la Tabla 2-31), para la implementación del Sistema de Gestión de la seguridad de la información, el recurso económico necesario para la implementación se estima que esta alrededor de los $31212 dólares americanos, este presupuesto debe ser entregado al Director Distrital, el mismo que debe aprobarlo e incluirlo en la Planificación anual de Recursos necesarios por la organización para el siguiente año.

El tiempo de implementación estimado para el SGSI es de un año, el personal a cargo de esta tarea es el Jefe del Departamento de TIC’s, el mismo que cuenta con

una certificación en Seguridad de la Información y con la experiencia de haber Desarrollado e Implementado un proyecto previo.

Para realizar el análisis de la Factibilidad Económica, se han realizado varias cotizaciones, una de estas cotizaciones, propuesta por empresa de Antivirus, menciona que por la adquisición de sus licencias se brindan las capacitaciones referentes a Seguridad de la Información de forma gratuita, donde ellos proponen su propio plan de capacitación al personal, los autores proponen un plan de capacitación el cual se encuentra en el Anexo 29.

CAPÍTULO 3. EVALUACIÓN DEL PLAN SGSI.

3.1 VALIDACIÓN DEL PLAN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Una vez realizado el Plan de Seguridad de la información, con la documentación necesaria para el SGSI y las Políticas que servirán para mitigar el impacto del riesgo, se procederá a implementar una de ellas.

La selección de la política a implementar se la realizó junto con el Director Distrital y el Jefe del Departamento de TIC's, esta selección se la realizó en base a las necesidades de la Organización, ya que se desea incrementar el rendimiento de los equipos y de los procesos que se realizan en ellos, para de esta manera asegurar un correcto funcionamiento de los mismos y evitar una futura perdida de información o un retraso en las actividades diarias de la Organización (Ver Documentos Habilitantes).

3.1.1 DESCRIPCIÓN DEL ESCENARIO.

El Distrito Zonal No.6 "Eloy Alfaro", cuenta con diez Departamentos distribuidos en el edificio de la Organización, ubicado en la Avenida Napo y Av. Upano, el Distrito Zonal cuenta con 65 equipos distribuidos en los diferentes departamentos, debido a

que el Distrito tiene bajo su cargo más de 88 Instituciones, la cantidad de personas en busca de ayuda es alta, por esta razón los equipos necesitan estar en correcto funcionamiento; debido a la falta de mantenimiento, en este momento los equipos no se encuentran 100% funcionales, presentándose problemas al momento de la atención a la ciudadanía y en diversas ocasiones la perdida de información, por daños en los equipos y por la presencia de virus.

Esta situación se debe a que el Distrito Zonal no cuenta con políticas necesarias de Mantenimiento para sus equipos; por ende la política a implementar ayudará a la Organización a establecer lineamientos tanto para el mantenimiento preventivo, como para el mantenimiento correctivo y así ayudará a cumplir sus objetivos.

3.1.2 PERIODO DE VALIDACIÓN.

La implementación de la política de Mantenimiento de Equipos dentro del Distrito Zonal No. 6 “Eloy Alfaro” será implementado en dos etapas.

- La primera etapa denominada como “Etapa de prueba”, abarca un periodo de tiempo de tres semanas, (15 días laborables), en esta etapa la política se encuentra en un proceso de depuración, se corrigen inconsistencias en la misma, así como también se definen encargados de realizar los mantenimientos y se planifican fechas para realizarlo.
- La segunda etapa denominada “Etapa de implementación”, abarca un periodo de tiempo tres semanas, (15 días laborales), en el cual se aplica la planificación realizada de los mantenimientos, para finalizar con el análisis de los resultados obtenidos, para la revisión final de la misma.

3.1.3 PROCEDIMIENTO DE IMPLEMENTACIÓN DE LA POLÍTICA PARA EL MANTENIMIENTO DE EQUIPOS.

1. El Director Distrital será el encargado de la realizar la aprobación que permita implementar la Política para el Mantenimiento de Equipos en la Organización.

2. El Jefe del Departamento de TIC’s, será el encargado de distribuir la política al resto de la Organización, esta distribución puede ser a travez de cualquier medio existente en el Distrito Zonal.
3. Una vez distribuida la Política para el Mantenimiento de equipos, se procede a la implementación de la misma para lo cual se debe tener en consideración que existen dos tipos de mantenimiento, los usuarios deberán considerar los siguientes aspectos.

   3.1 Mantenimiento Preventivo.

   - El Jefe del Departamento de TIC’s deberá realizar una planificación para el mantenimiento de los equipos de toda la organización, dicha planificación deberá considerar los lineamientos establecidos en la Política para el Mantenimiento de Equipos, una vez terminada la planificación, esta deberá ser autorizada por el Director Distrital.
   - La planificación tendrá que ser distribuida al resto de los Departamento de la Organización.
   - Se procederá a dar inicio con la actividad de mantenimiento de equipos, según lo establecido en la planificación.
   - Dentro del mantenimiento de los equipos se debe considerar la limpieza tanto física como lógica de los equipos.
   - Una vez terminada la actividad el usuario deberá asegurarse del estado de su equipo.

   3.2 Mantenimiento Correctivo.

   - Para la realización del mantenimiento correctivo, es necesario que el usuario que haya detectado alguna anormalidad en su equipo, realice la solicitud pidiendo la revisión del mismo; la solicitud tiene que seguir los lineamientos establecidos dentro de la Política para el Mantenimiento de Equipos.

- Una vez que la solicitud haya llegado al Departamento de TIC's, este deberá analizarla y dar una respuesta con el día, la hora y el nombre de la persona designada para realizar el mantenimiento.
- Una vez terminada la actividad el usuario deberá asegurarse del estado de su equipo

3.2 ANÁLISIS DE RESULTADOS.

Para poder verificar la efectividad de la política implementada dentro del Distrito Zonal No. 6 "Eloy Alfaro" se procederá a realizar un análisis de la situación de la Organización antes de implementar la Política de Mantenimiento de Equipos, y la será comparada con los resultados brindados por el personal, luego de haber implementado la política, para esto se aplicará una encuesta al personal que labora dentro de la Organización y se considerarán aspectos especificados en la Tabla 3-32.

PREMISA	PORCENTAJE DE SATISFACCIÓN
Horarios Adecuados para el mantenimiento de los equipos.	30 %
Notificación con anticipación de la realización de Mantenimiento	20%
Correcto funcionamiento de los equipos	30%
Cumplimiento de los objetivos de la Organización.	40%
Rapidez en la realización de las actividades de mantenimiento.	50%
Cantidad de Inconvenientes por problemas en los equipos	70%

Tabla 3-32 Análisis de la situación antes de la implementación de la política

Fuente: Los Autores

El siguiente análisis hace referencia a la situación en la cual se encontraba la Organización antes de la implementación de la Política de Mantenimiento de equipos.

- **Horarios Adecuados para realizar el Mantenimiento de los equipos**: antes de la implementación de la política se lo realizaba en cualquier horario, con preferencia en las horas de almuerzo, lo que provocaba inconvenientes para el resto de empleados ya que estas actividades solían interferir en el desarrollo de sus tareas diarias.
- **Notificación con anticipación de la realización del Mantenimiento:** antes de la implementación de la política, el Departamento de TIC's notificaba al personal al inicio de la planificación de las actividades, lo que ocasionaba problemas, ya que la mayoría de empleados no recordaban los días en los que se iban a realizar las actividades.
- **Correcto funcionamiento de los equipos:** antes de la implementación de la política, los equipos no funcionaban de forma adecuada, lo que causaba retrasos al momento de atender a la ciudadanía.
- **Cumplimiento de los objetivos de la Organización:** antes de la implementación de la política, debido al mal funcionamiento de los equipos, no se podía atender a la ciudadanía como de manera adecuada, ya que esta atención se tornaba demasiado lenta ocasionando molestias a los usuarios, uno de los objetivos de la Organización es tener una adecuada atención y buen trato a la ciudadanía, por lo cual este objetivo no se estaba cumpliendo.
- **Rapidez en la realización de las actividades de mantenimiento:** como se mencionó anteriormente debido a que las actividades de mantenimiento se realizaban en horarios de trabajo, este interrumpía con las actividades diarias lo que causaba malestar en los usuarios.
- **Cantidad de Inconvenientes por problemas de los equipos:** el mal funcionamiento de los equipos ocasiona quejas por parte de la ciudadanía, es por eso que este campo tiene un valor alto.

Para poder calcular el porcentaje de cumplimiento luego de haber aplicada la política de Mantenimiento de Equipos, se ha generado una encuesta para el personal, los

resultados de esta encuesta se muestran en la Tabla 2-33, la encuesta puede ser visualizada en el Anexo 30.

PREMISA	PORCENTAJE DE SATISFACCIÓN
Horarios Adecuados para el mantenimiento de los equipos.	80 %
Notificación con anticipación de la realización de Mantenimiento	90%
Correcto funcionamiento de los equipos	80%
Cumplimiento de los objetivos de la Organización.	80%
Rapidez en la realización de las actividades de mantenimiento.	70%
Cantidad de Inconvenientes por problemas en los equipos	30%

Tabla 3-33 Análisis de la situación después de la implementación de la política.

Elaborado por: Los Autores

El siguiente análisis hace referencia a la situación luego de haber implementado la Política de Mantenimiento de equipos.

- **Horarios Adecuados para realizar el Mantenimiento de los equipos:** para la implementación de la política, fue necesario la realización de un Plan de Mantenimiento por parte del Departamento de TIC's, en la cual se determinó los horarios para la realización del mantenimiento, y se especificó que los horarios de mantenimiento se realizarán después de las jornadas de trabajo.
- **Notificación con anticipación de la realización del Mantenimiento:** uno de los puntos a considerar dentro de la política, es dar a conocer al personal los días y horas en la que se van a realizar los mantenimientos, por ende se procedió con la notificación vía correo electrónico, dos días de anticipación y se le recordará el día previo a la realización de la actividad, lo que permite a los usuarios planificar su tiempo y generar respaldos de su información en caso de presentarse algún inconveniente.
- **Correcto funcionamiento de los equipos:** una vez realizado el mantenimiento de los equipos, estos se desempeñaban con mayor eficacia,

por lo que las tareas se realizaban en menor tiempo generando que la ciudadanía se sienta satisfecha con el tiempo de respuesta por parte del personal.

- **Cumplimiento de los objetivos de la Organización:** gracias a la implementación de la política de mantenimiento de los equipos, los equipos funcionaron de mejor manera permitiendo una atención más rápida a los usuarios, aumentando el número de peticiones ciudadanas resueltas.
- **Rapidez en la realización de las actividades de mantenimiento:** gracias a una adecuada planificación de los mantenimientos a realizarse en los equipos, esta tarea se realizó en menor tiempo, ya que ningún usuario requería el equipo por lo cual el proceso de mantenimiento se realizó de manera ininterrumpida en cada equipo.
- **Cantidad de Inconvenientes por problemas de los equipos:** después de la implementación de la política de mantenimiento de equipos, el número de incidentes disminuyó satisfactoriamente, puesto que ya no se presentaba problemas como virus o saturación del disco.

3.2.1 ANÁLISIS DE LA APLICABILIDAD DEL PLAN.

Con el análisis de la aplicabilidad de Plan, se pretende mostrar la situación actual de la Organización y la situación esperada luego de la aplicación de los controles seleccionados dentro del Plan de Seguridad de la Información; se tomará en cuenta el análisis de Factibilidad de la Aplicación del SGSI, el cual ayuda a determinar con qué recursos cuenta la Organización y los que hacen falta para su implementación.

Se realizará un análisis cuantitativo del estado de cumplimiento de los controles seleccionados, con este análisis se permitirá determinar las mejoras que se obtendrán con la implementación del Plan de Seguridad de la Información dentro del Distrito Zonal No. 6 “Eloy Alfaro”.

En la Taba 2-34 se muestra la comparación de los porcentajes de cumplimiento tanto el actual como el esperado después de la implementación de los controles

seleccionados, para determinar el porcentaje de cumplimiento esperado se aplicará la ecuación planteada en la sección 1.3.3 del presente documento. Para la realización de la tabla se utilizarán los dominios del Anexo A de la norma ISO/IEC 27001:2011, la valoración de los mismos se encuentran en el Anexo 2.

DOMINIO		PORCENTAJE DE CUMPLIMIENTO ACTUAL.	PORCENTAJE DE CUMPLIMIENTO ESPERADO.
A.5	Política de Seguridad	100%	100%
A.6	Aspectos Organizativos de la Seguridad de la Información	18.18%	54.54%
A.7	Gestión de Activos	40%	100%
A.8	Seguridad Ligada a los Recursos Humanos	44.44%	66.66%
A.9	Seguridad Física y Ambiental	61.54%	69.24%
A.10	Gestión de Comunicaciones y Operaciones	21.88%	53.13%
A.11	Control de Acceso	8.00%	60.00%
A.12	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	12.50%	25.00%
A.13	Gestión de Incidentes de Seguridad de la Información	20.00%	60.00%
A.14	Gestión de la Continuidad del Negocio	60.00%	60.00%
A.15	Cumplimiento	0%	30.00%

Tabla 3-34 Comparación de la Situación Actual de la Organización.

Elaborado por: Los Autores

- El dominio A.5 Política de Seguridad cuenta con dos controles, en la actualidad la Organización cumple con ambos, razón por la cual cumple en un 100%, la Organización a pesar de tener políticas de seguridad de la información y de ser revisar de forma periódica, no abarca la totalidad de la información, y el personal que labora en la Organización tampoco las implementa, hace caso omiso a la existencia de las mismas, poniendo en riesgo la integridad y la disponibilidad de la información, cabe recalcar que la Política de Seguridad no está completa ya que no abarca situaciones como contraseñas, accesos de usuarios, entre otras, es por eso que se realizó el presente proyecto.
- El dominio A.6 Aspectos Organizativos de la Seguridad de la Seguridad de la Información cuenta con once controles, en la actualidad la Organización cumple con dos (porcentaje de 18.18%), después del análisis de riesgos se estableció la implementación de cuatro controles más (porcentaje del 54.54%). Este dominio tiene ese porcentaje puesto que el Distrito Zonal No. 6 “Eloy Alfaro” no tiene relaciones con terceros, por lo tanto ese tipo de controles no aplica para esta organización, los controles que se pudieron aplicar tienen relación con la Organización Interna y las responsabilidades que tienen los usuarios ante la seguridad de la Información.
- El dominio A.7 Gestión de Activos cuenta con cinco controles, en la actualidad la Organización cumple con dos (porcentaje de 40%), después del análisis de riesgos se estableció la implementación de tres controles más (porcentaje del 100%). Los activos de información son muy importantes para la Organización es por este motivo que se tomó especial interés en la aplicaciones de controles que me ayuden definir responsabilidades sobre los activos, sobre su buen uso, así también es importante tener presente los lineamientos necesarios para una buena clasificación y etiquetado de la información.
- El dominio A.8 Seguridad Ligada a los Recursos Humanos cuenta con nueve controles, en la actualidad la Organización cumple con cuatro (porcentaje de 44.44%), después del análisis de riesgos se estableció la implementación de dos controles más (porcentaje del 66.66%). Debido a que el Distrito Zonal no forma

parte del proceso de contratación de personal, puesto que esta actividad es realizada por el Ministerio de Educación no se consideran controles de la sección previo al empleo, los controles que se toman en cuenta son los que se establecerán durante el empleo ya que la finalidad de esta implementación es establecer responsabilidades de los empleados de la Organización caso contrario establecer procesos disciplinarios.

- El dominio A.9 Seguridad Física y Ambiental cuenta con trece controles, en la actualidad la Organización cumple con ocho (porcentaje de 61.54%), después del análisis de riesgos se estableció la implementación de un control más (porcentaje del 69.24%). Después de realizar al análisis de la situación actual de la Organización se pudo determinar que el Distrito Zonal No.6 “Eloy Alfaro” cuenta con áreas seguras, cuenta con controles físicos de entrada como puertas con lectores de tarjetas, la Organización posee personal de seguridad que controlan el acceso de personal, el único control que se aplicará de este dominio es la de mantenimiento de quipos puesto que es necesaria para un correcto desempeño de los equipos, cabe recalcar que no es necesario la implementación de políticas que controles el uso de equipos fuera de la Organización, puesto que si un funcionario tiene que salir del Distrito, todo lugar a donde baya tiene la obligación de brindar los recursos necesarios al empleado.
- El dominio A.10 Gestión de Comunicaciones y Operaciones cuenta con treinta y dos controles, en la actualidad la Organización cumple con siete (porcentaje de 21.88%), después del análisis de riesgos se estableció la implementación de diez controles más (porcentaje del 53.13%). Dentro de este dominio se implementan controles tanto para establecer responsabilidades y procedimientos de operaciones que aseguren el funcionamiento correcto de los recursos de la Organización. Se establecen controles que ayuden a resguardar los equipos contra código malicioso o la instalación de software indebido, también se implementarán políticas para la adecuada gestión de las redes asegurando así la integridad de la información y la disponibilidad de la misma.

- El dominio A.11 Control de Acceso Información cuenta con veinte y cinco controles, en la actualidad la Organización cumple con dos (porcentaje de 08%), después del análisis de riesgos se estableció la implementación de trece controles más (porcentaje del 60%). Este dominio ayudará a asegurar el adecuado control de los empleados de la Organización mediante una adecuada Gestión, es decir mediante un control al momento de crear, modificar y eliminar usuarios dentro de la Organización.
- El dominio A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información cuenta con diez y seis controles, en la actualidad la Organización cumple con dos (porcentaje de 12.5%), después del análisis de riesgos se estableció la implementación de dos controles más (porcentaje del 25%). Este dominio tiene una orientación para brindar seguridad a fuentes de software, es decir brinda seguridad al momento de realizar desarrollo de software, pero el Distrito Zonal No 6. “Eloy Alfaro” no realiza desarrollo, es por esto que no se aplican controles de este dominio.
- El dominio A.13 Gestión de Incidentes de Seguridad de la Información cuenta con cinco controles, en la actualidad la Organización cumple con uno (porcentaje de 20%), después del análisis de riesgos se estableció la implementación de dos controles más (porcentaje del 60%). Con la aplicación de los controles establecidos en este control se pretende generar responsabilidades relacionadas a la seguridad de la información por parte de los empleados, estos deberán notificar de cualquier tipo de incidente que ponga en riesgo la seguridad de la información.
- El dominio A.14 Gestión de la Continuidad del Negocio cuenta con cinco controles, en la actualidad la Organización cumple con ninguno tres (porcentaje del 60%), después del análisis de riesgos se estableció que no es necesario la implementación más controles (porcentaje del 60%). El Distrito Zonal No. 6 “Eloy Alfaro” ya cuenta con un plan de continuidad del negocio, es por esto que no se aplican controles de esta sección. La continuidad del negocio viene establecido por el Ministerio de Educación.

- El dominio A.15 Cumplimiento cuenta con diez controles, en la actualidad la Organización no cumple con ninguno (porcentaje del 0%), después del análisis de riesgos se estableció la implementación de tres controles (porcentaje del 30%). La aplicación de los controles establecidos en este dominio ayudarán a la Organización a establecer políticas sobre el uso de software licenciado si es necesario, caso contrario se podrá utilizar software libre. Con la aplicación de estos controles también se podrá respetar el derecho de propiedad intelectual y valorar el esfuerzo de los demás.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES.

4.1 CONCLUSIONES.

- El Distrito Zonal N° 6 “Eloy Alfaro” actualmente posee una política de Seguridad y un plan de contingencia, sin embargo el personal que labora dentro de la organización desconoce de su existencia, esto se debe a que no existe una adecuada comunicación entre los departamentos y a la falta de compromiso de los mismos, así como tampoco existen procesos de concientización la personal que les haga caer en cuenta el rol fundamental que desempeñan dentro de la organización.
- El derecho intelectual dentro de la organización, no está amparado por ninguna política actualmente, puesto que no se está utilizando software licenciado en la gran mayoría de equipos que se encuentran dentro de la organización.
- El Distrito Zonal No. 6 “Eloy Alfaro”, al tener bajo su cargo los sectores de Lloa, La Mena, Chilibulo, La Magdalena, Solanda, La Argelia, Chimbacalle, la Ferroviaria y San Bartolo, maneja información importante para cada una de las instituciones educativas ubicadas en dichos sectores, al tener que almacenar datos, tanto de los estudiantes como del personal administrativo, los encargados

de dicha actividad no poseen un adecuado conocimiento en temas de Seguridad de la Información, que les permita darse cuenta del impacto negativo que podría producirse, si esta información fuera manipulada por personal no autorizado.

- Los controles que actualmente son implementados dentro del Distrito Zonal N° 6 “Eloy Alfaro”, no logran mitigar todos los riegos identificados a los cuales se encuentra expuesta la organización, esto se debe a la falta de conocimiento del personal o al poco interés que este tiene. Luego de haber realizado el análisis a la organización, se pudo identificar que el mayor riesgo que afecta al Distrito Zonal N°6 “Eloy Alfaro”, es la pérdida de información que sufren los empleados, esto debido a un mal funcionamiento que tienen los equipos.
- Existe un compromiso por parte de la Dirección Distrital, la misma que apoyó en el desarrollo de este proyecto, para la creación y la futura implementación de un Sistema de Gestión de la Seguridad de la Información, esto debido a que la nueva administración entiende la necesidad de implementar controles, que aseguren la continuidad de los procesos y la integridad con la cual son manejados.
- Se desarrolló este proyecto con la Norma NTE ISO\IEC 27001:2011, puesto que ésta norma internacional puede ser aplicada a cualquier tipo de organización sin importar su tamaño, y debido a que sirve de apoyo y guía al momento de desarrollar la documentación base de este SGSI.
- La realización del Proyecto permitió generar un mayor conocimiento de la Norma NTE ISO\IEC 27001, 27003 y 27005; puesto que fue necesario realizar una investigación previa a la realización del proyecto,
- La implementación de herramientas de software así como Ingeniería Social, para realizar la identificación de las vulnerabilidades físicas de la Organización fue de ayuda para generar vínculos con el personal que labora en el Distrito Zonal No.6 “Eloy Alfaro”, de esta manera la obtención de datos se facilitó debido a la confianza generada.
- La constante participación del personal al momento de realizar la identificación de vulnerabilidades, ayudó a generar un mejor análisis de las mismas, puesto que el

personal es el encargado de realizar las actividades diarias en la organización y es el que conoce de las fortalezas y debilidades existentes.

4.2 RECOMENDACIONES

- Realizar charlas de concientización al personal que labora dentro del Distrito Zonal N° 6 “Eloy Alfaro” sobre temas de Seguridad de la Información, para que de esta manera se logre generar conciencia del papel importante que desempeñan dentro de la organización, y de cuan importantes pueden llegar a ser como individuos para la misma.
- La Dirección Distrital debe tener en cuenta la importancia de una adecuada comunicación entre departamentos, es por ello que la Dirección Distrital debe involucrarse más y fomentar la comunicación, esto para afianzar lazos que ayuden a la organización a alcanzar los objetivos planteados.
- Para realizar un adecuado análisis de riesgos se debe emplear una metodología de Análisis de Riegos que pueda adaptarse a las necesidades del proyecto, por lo cual el Distrito Zonal N° 6 “Eloy Alfaro” debería considerar la implementación de la metodología de Análisis y Gestión de Riesgos MAGERIT, que sirve de guía base para realizar un correcto Análisis de Riesgos como se especifica en la sección 2.1.3 de este documento.
- La Organización deberá adquirir las Normas de la Familia ISO 27000, especialmente la norma ISO/IEC 27001 donde se especifican los requisitos que

se necesitan para poder elaborar un Sistema de Gestión de la Seguridad de la información, así como la norma ISO/IEC 27003 que proporciona una guía de implementación del Sistema de Gestión de la Seguridad de la Información, puesto que estas ayudaran al momento de realizar las capacitaciones al personal para implementar el SGSI dentro de la organización.

- Crear un repositorio dentro del gestor documental Alfresco, que actualmente posee el Distrito Zonal N°6 “Eloy Alfaro”, para almacenar todos los documentos a ser publicados del Sistema de Gestión de la Seguridad de la Información, para que el personal que labora en la organización pueda acceder cuando surjan dudas, o se presenten inconvenientes al momento de implementar un control.
- Fijar periodos de validez, revisión y mejora de los documentos que forman parte de este proyecto, ya que de esta manera se puede verificar que tan efectivas son las políticas implementadas o si es necesario mejorar o dejar de implementar alguna.
- Para poder contar con una perspectiva más amplia de las vulnerabilidades lógicas a las cuales se encuentra expuesta la Organización, ésta debe utilizar herramientas adicionales que permitan verificar los resultados obtenidos con las herramientas actuales.

BIBLIOGRAFÍA

[1] Ministerio de Educación , «Manual de Calidad. MINEDUC-MC-001,» Versión 2.0, Quito, 2014.

[2] M. d. Educación., «Ministerio de Educación.,» Ecuador ama la vida, [En línea]. Available: http://educacion.gob.ec/. [Último acceso: 07 Mayo 2015].

[3] I. E. d. Normalización., «Norma Técnica Ecuatoriana INEN-ISO/IEC 27000:2012,» Primera Edición. , Quito - Ecuador, 2012.

[4] I. E. d. Normalización, «Norma Técnica Ecuatoriana INEN-ISO/IEC 27001:2011,» Primero Edición, Quito - Ecuador, 2011.

[5] C. J. M. J. Amutino Miguel, MAGERIT Version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método, Madrid-España: Ministerio de Hacienda y Administraciones Públicas, 2012.

[6] I. F. d. A. a. l. Información, «Metodología de Análisis de Riesgo BAA,» México, 2013.

[7] Departamento Administrativo de la Función Pública, «Guía para la administración del riesgo,» Dirección de control Interno y Racionalización de

Trámites, Colombia, 2011.

[8] I. E. d. Normalización, Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27005:2012, Quito- Ecuador: INEN, 2012.

[9] A. Pública., «Decreto 1014.,» Rafael Correa Delagado. Presidente Constitucional de la República, Quito , 2007.

[10] C. Alfresco, «ALFRESCO,» Alfresco Documentation, Enero 2008. [En línea]. Available: http://docs.alfresco.com/. [Último acceso: 09 Mayo 2015].

[11] LAVA, «ALFRESCO,» MagmaSoft Innovando Tecnología, Abril 2009. [En línea]. Available: http://www.imaginar.org/taller/dgd/pres/4_Alfresco.pdf. [Último acceso: 09 Mayo 2015].

[12] Alfresco, «Smile Open Source Solutions,» Enero 2009. [En línea]. Available: http://www.upf.edu/arxiu-gestiondocumental/_pdf/presentacion_contenidos_empresa.pdf. [Último acceso: 09 Mayo 2015].

[13] I. E. d. Normalización, Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27003:2012, Quito - Ecuador, 2012.

[14] J. C. Migue Angel Amutio, MAGERIT- Versión 3.0 Metodología de Análsis y Gestión de Riesgos de los Sistemas de Información, Libro II Catálogo de Elementos., Madrid - España: Ministerio de Hacienda y Administración Pública, 2012.

[15] J. C. Miguel Angel Amutio, MAGERIT- Versión 3.0 Metología de Análisis y Gestión de Riesgos de los Sisteas de Información. Libro III Guía de Tecnicas., Madrid - España: Ministerio de Hacienda y Administración Públicas, 2012.

GLOSARIO

Aceptación del Riesgo: decisión de la organización de aceptar un riesgo.

Activo: se define como cualquier cosa que representa valor para la organización.

Amenaza: acción mal intencionada que busca explotar una vulnerabilidad.

Ataque: intento de causar daño a un activo o a los activos de la organización.

Confidencialidad: propiedad que tiene la información para ser expuesta al personal con la autorización necesaria.

Control de Acceso: actividad en la que la organización asegura la integridad, confidencialidad y disponibilidad de los activos.

Control: medio de gestión del riesgo, también conocido como salvaguardias o contramedidas.

Declaración de aplicabilidad: descripción de los controles a utilizar y los utilizados con su respectiva justificación.

Disponibilidad: se define como la característica que deben tener los activos para poder ser accedidos cuando sea necesario.

Evento: ocurrencia de un grupo de circunstancias.

Impacto: posible daño que puede causar la ejecución de un riesgo.

Información: grupo de datos procesados importantes para la organización.

Integridad: que la información sea correcta y no haya sido manipulada.

Plan: programa en el que se detalla las actividades y los recursos necesarios para llevar a cabo una idea.

Política: normativas planteadas por la organización para cumplir con un fin específico.

Procedimiento: forma especificada para realizar una actividad.

Proceso: conjunto de actividades interrelacionadas.

Registro: documento que provee evidencias de las actividades realizadas.

Riesgo: probabilidad que una amenaza explote una vulnerabilidad.

Seguridad de la Información: asegurar la confidencialidad, disponibilidad e integridad de la información.

Vulnerabilidad: debilidad que posee un activo.

ANEXOS.

Anexo 1. Inventario del Distrito Zonal No. 6

Anexo 2. Matriz de evaluación del estado de cumplimiento

Anexo 3. MSAT-Cuestionario Evaluación

Anexo 4. Informe de Vulnerabilidades

Anexo 5. Identificación de Amenazas

Anexo 6. Matriz de Tratamiento de Riego

Anexo 7. Documento-Plan-de-Proyecto

Anexo 8. Documento-de-Alcance-y-Límites-del-SGSI

Anexo 9. Documento-de-Política-del-SGSI

Anexo 10. Metodología de Evaluación de Riesgo

Anexo 11. Documento-de-Tratamiento-de-Riesgos

Anexo 12. Documento-de-Aplicabilidad_SGSI

Anexo 13. Documento de Control de Documentos y registros

Anexo 14.Documento Gestión de Incidentes

Anexo 14.1.Registro de Incidentes

Anexo 15. Política de Contraseñas y Claves

Anexo 16. Política de Control de Acceso