UNIVERSIDAD SEÑOR DE SIPÁN

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN (SGSI) DE ACUERDO CON LA NORMA ISO/IEC 27001. CASO DE ESTUDIO: UNIDAD DE GESTIÓN EDUCATIVA LOCAL 01

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:
Bach. Llanos Guillén Enrique Guillermo

Asesor:
Bravo Ruiz Jaime Arturo

Línea de Investigación:
Tecnologías de la información

Pimentel – Perú
Año 2019

Aprobación de la Tesis

Presidente del jurado de tesis

Secretario del jurado de tesis

Vocal del jurado de tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Telef: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DEDICATORIA

"A mis hijos……..

A la memoria de mi hermano……. y

A mi señora madre".

Con todo cariño a mis queridos hijos Romina, Ángel, D'stefano, Camila y Wendy, por el constante apoyo y amor que me brindan cada día.

A mi madre, por confiar en mí, por cada palabra y cada gesto de cariño motivándome a culminar mi carrera, por impulsarme con valor y amor para tomar grandes decisiones

A Yovana por su permanente apoyo y amor.

A mi familia, hermanos, amigos que se identificaron conmigo y me dieron una voz de aliento en mis momentos difíciles.

Para todos los mencionados les dedico el presente trabajo que fue realizado con mucha dedicación y cariño.

Enrique Llanos Guillen

AGRADECIMIENTO

A la U.S.S, como institución que me dio la oportunidad de crecer personal y académicamente y a cada uno de los profesores que me enseñaron y fueron formando en mí, espíritu de compromiso con la profesión y con el país.

Enrique Llanos Guillen

ÍNDICE

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Telef: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Telef: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE DE TABLAS

RESUMEN

El proyecto de investigación consiste en desarrollar un Sistema de Gestión de Seguridad de la Información, dentro del contexto de la norma ISO/IEC 27001, a fin de proteger y salvaguardar los activos informáticos ubicados en la Unidad de Gestión Educativa Local Nº 01.

El desarrollo de este sistema permitirá diseñar e implementar estrategias de seguridad y operaciones, asimismo como supervisar y evaluar los resultados con la meta de ser garantes de la privacidad, disponibilidad e integridad de los sistemas de información de la mencionada dependencia gubernamental.

Durante el progreso del método de Seguridad de la Información, se efectuará la definición del alcance y el desarrollo de la estrategia basado en un modelo espiral Plan-Do-Check-Act (PDCA), para la mejorar consecuentemente dicha área.

El método que se empleará para la obtención de datos será por medio de la observación directa, entrevistas y cuestionarios, con la finalidad de ejecutar el estudio y la evaluación de las amenazas potenciales a los activos de información.

Posteriormente los resultados del examen y evaluación de los riesgos permitirán diseñar y aplicar estrategias de seguridad y procedimientos adecuados permitiendo cumplir con la finalidad principal del trabajo investigativo.

Palabras clave: seguridad, centro de datos, riesgo, sistemas de información, SGSI, confidencialidad, integridad, disponibilidad.

ABSTRACT

he research project consists in developing an Information Security Management System, within the context of ISO / IEC 27001, in order to protect and safeguard the computer assets located in Local Education Management Unit No. 01.

The development of this system will allow the design and implementation of security strategies and operations, as well as monitoring and evaluating the results with the goal of guaranteeing the privacy, availability and integrity of the information systems of the aforementioned government agency.

During the progress of the Information Security method, the definition of the scope and development of the strategy based on a spiral Plan-Do-Check-Act (PDCA) model will be carried out, to consequently improve said area.

The method that will be used to obtain data will be through direct observation, interviews and questionnaires, in order to carry out the study and the evaluation of potential threats to information assets.

Subsequently, the results of the examination and risk assessment will allow the design and application of appropriate safety strategies and procedures, allowing the main purpose of the research work to be fulfilled.

Keywords: security, data center, risk, information systems, ISMS, confidentiality, integrity, availability.

INTRODUCCIÓN

La Unidad de Gestión Educativa Local Nº01, es una entidad pública del sector educación, cuya misión es ser garante de los derechos y servicios educativos de alta calidad a la población poder alcanzar sus potencialidades y favorecer el desarrollo de forma imparcial, en consonancia con la democracia y basada en resultados desde perspectivas de igualdad e interculturalidad. Cuenta con un centro de datos, en donde se procesan sistemas de información, cuya revisión física y lógica de la seguridad permitió identificar los riesgos, amenazas y vulnerabilidades, lo cual sirvió para proponer las acciones correctivas necesarias para la solidez de la información. Este es un activo de gran importancia para los negocios y por lo tanto necesita ser resguardado adecuadamente utilizando las normas ISO/IEC 27001.

El objetivo de este proyecto es de proteger los activos informáticos y tecnológicos usados para su resguardo y procesamiento, de potenciales riesgos, dentro o fuera de la institución, premeditadas o eventuales, consiguiendo robustecer la fiabilidad de los datos.

Del mismo modo, se debe responder por la aplicación de las medidas de seguridad, identificando los recursos, sin que necesariamente deba realizarse la asignación de tiempo y dineros adicionales. Preservar las Políticas de Seguridad constantemente, con el fin de asegurar su eficacia en las nuevas tecnologías que la Ugel necesita para cubrir el crecimiento en los últimos años.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Situación problemática

La información es un recurso de valor incalculable para cualquier entidad y como tal debe ser debidamente resguardada. Las estrategias para su resguardo permiten protegerla de amenazas, a fin de salvaguardar la integridad, seguridad y confidencialidad de la misma, asegurando la continuidad de los servicios. La información está relacionada no solamente con los datos informáticos, sino con todas aquellas operaciones que reflejan las actividades de la organización, las cuales pueden ser objeto de vulnerabilidad y en consecuencia producir algún perjuicio en el normal funcionamiento de las organizaciones e inclusive causar daños severos e irreparables en la misma. En vista de esta realidad, diferentes empresas se vieron obligadas a adoptar políticas orientadas a la preservación de la información, así como a mejoramiento sistemático de su seguridad.

En este orden de ideas, se encuentra el caso de México, dónde según (Espinoza, 2013) en la Asociación Nacional de Concesionarios de Grupo Volkswagen México "se halló un problema de seguridad, debido a la subordinación de operación por sistemas concentrados con la red, ya que las aplicaciones transitaban de manera descontrolada por la red sin ningún mecanismo de control". (p. 41) Más adelante, especifica el autor que:

> Los constantes ataques de virus y de seguridad degradaban su red de datos hasta dejarla inoperante, por lo que decidieron buscar alternativas que no solo se basaran el en robo de información y daño a la infraestructura tecnológica, si no que abarquen todos los procesos y patrones requeridos para que las operaciones no se vieran afectadas. Por este motivo se implementó junto con TI América, un proyecto exhaustivo de seguridad, con el cual fue posible lograr beneficios a corto y mediano plazo, a través de la reducción de gastos de operación, aumento productivo y, esencialmente, mejoras en los servicios al consumidor. (p.42)

Otro caso donde se evidenció la relevancia de la seguridad en las organizaciones empresariales fue en Terpel, una de las empresas del ramo de combustibles más grandes de Colombia, la misma cuenta con sedes en Chile, Panamá y Ecuador. El volumen de sus operaciones exigía poseer una solución la cual le garantizara la protección de toda la información interna y externa, así como ofrecer seguridad y confidencialidad a todos sus clientes y socios de negocio. En esta empresa, de acuerdo con (Zambrano, (s.f)

> El panorama de vulnerabilidad en esta institución era un blanco fácil para la empresa Terpel, desde la información que circula en la red, las transacciones millonarias de dinero y transacciones con los clientes por diferentes canales. Con 150 mil ocurrencias de seguridad por día, un reducido número de eficacia en su localización, Spoofing, Spam y la perpetración en la data informática hacían propensa a Terpel a los accesos ilegales, operaciones fraudulentas o cualquier suceso no autorizado en la red que conllevara pérdidas irremediables a la institución. Decidió implementar un sistema de seguridad de la información, apoyándose en la experiencia de una empresa especializada como "Digiware". El resultado obetenido fue que toda la información de la institución posee, niveles óptimos de confianza, lo que ha implicado que ya no existe negación del servicio en las operaciones comerciales de la empresa que puedan desencadenar colapsos o incidentes negativos en la red tal como ocurría con anterioridad. (p. 2)

Ya concretamente en el Perú, se encuentra la situación del negocio Atento, dedicado a los servicios de telecomunicaciones, la cual en el año 2011 decide aplicar soluciones de seguridad para la información, lo cual permita gestionar las mismas, este plan llegó a término en diciembre del 2014. Luego de una exigente auditoría, la institución obtuvo la certificación ISO 27001:2005 conferida por la entidad española que brinda la Normativa y Certificación – AENOR. Posteriormente se acreditan la certificación ISO 27001:2013, la cual garantiza la excelencia en privacidad, probidad y disponibilidad, avalando que los consumidores acreditados obtengan acceso regulado a la información. Asimismo, aseguraron las características de la información de la clientela y de su organización Además, impulsar las actividades para salvaguardar la información dentro de las organizaciones, perfeccionando su imagen y fomentando la cordialidad en el amparo de la información. (Atento, s.f).

Dentro de este mismo marco de las organizaciones que requieren la protección de su información, se encuentra la (UGEL) que es un órgano del estado sin propósitos de lucro, encargada de ejecutar la mayor autoridad administrativa de la UGEL de Lima Metropolitana. Está encargada de gestionar la educación básica regular, especial, alternativa de técnica y producción y de ejercer la supervisión del servicio de educación ofertado por las instituciones. Dentro de sus funciones se puede mencionar:

La UGEL ejercer supervisión, así como regularizar la aplicación de las mejoras correspondientes. Ofrecer la asesoría académica, administrativa y logística a los colegios estatales que se encuentran bajo su jurisdicción.

Resolver de manera prioritaria los procesos administrativos correspondientes. Proponer a la DRELM, la implementación de enlaces educativos. Aplicar que garanticen la transparencia, ética del funcionario público y combatir la corrupción, dentro de sus competencias y la normativa vigente. Inducir convenios de cooperación, que ayuden a optimizar la calidad del aprendizaje educativo. (Ministerio de Educación Perú, 2019)

Esta dependencia estadal, se encuentra estructurada de la siguiente manera: el equipo de logística conformado por el área de control institucional, cuya función principal realizar el control del gobierno, según la normativa del Sistema Nacional de Control. Seguidamente se encuentra el área de Asesoría Jurídica, la cual se encarga de emitir opinión y asesorar acerca de asuntos de orden jurídico de competencia de la UGEL de Lima Metropolitana. Por último, está el Área de Planificación y Presupuesto, cuya función principal es desarrollar y conducir la ejecución del seguimiento y análisis de los planes y presupuestarios de la UGEL de Lima Metropolitana, siguiendo la normativa correspondiente.

Está conformado también por la Unidad de Apoyo, la cual a su vez se divide en el área administrativa, que se encarga de orientar, llevar a cabo, y hacer el seguimiento de los sistemas de administración y suministro, área contable y de recurso económicos de la UGEL de Lima Metropolitana. En esta misma dependencia, se halla el Área de Recursos Humanos encargada de gestionar y supervisar todo lo relacionado con el personal que se encuentre bajo su competencia.

Finalmente, se encuentran sus líneas organizativas, la primera de ellas es el Área de Gestión de Educación Básica Regular y Especial, encargada de la planificación, ejecución y seguimiento, de las actividades relacionadas con la educación básica regular y especial, en los institutos educativos dentro de su jurisdicción. La segunda, tiene la misma función dentro del área educativa básica alternativa y técnico productiva, en los institutos bajo su competencia dentro del marco legal vigente. La tercera tiene la función de realizar los procedimientos de autorización a cargo de la UGEL, la cual es el área activa en la creación y funcionamiento instituciones educativas de carácter básicas y técnico-productivas, públicas y privadas. (Ministerio de Educación Perú, 2019)

Tal como puede observarse, las funciones de esta dependencia oficial son múltiples e importantes para el normal desenvolvimiento de una de las actividades más relevantes para el país como lo es la educación. En este sentido, se entiende que se maneja gran cantidad de información que refleja las actividades de esta estatal, la misma debe ser protegida, pues incluso al no tratarse de una empresa privada o con fines de lucro, tiene a su cargo partidas de dinero y transacciones dirigidas al pago del personal a su cargo, tanto internamente como la nómina externa que conforma el personal docente a su cargo. Así mimo, tiene a su cargo información jurídica de carácter confidencial y que solo debe ser manejada por los organismos competentes y personas encargadas. Sin embargo, a través de un proceso de observación, se pudo constatar que en la dependencia gubernamental educativa, no existen medidas para necesarias para salvaguardar la información de ataques informáticos, robos, pérdida de documentos entre otros, lo que convierte a esta importante dependencia en un ente vulnerable ante las derivaciones que se puedan suscitar luego de la pérdida o un mal manejo de la información. Por lo antes descrito, se hace necesaria la implementación de un Sistema de Seguridad de la Información. Respecto a esta problemática, la norma ISO/IEC 27001 contiene las alternativas de solución necesarias.

1.2 Formulación del Problema

Actualmente, la Unidad de Gestión Educativa Local 01, no posee ningún mecanismo y/o sistema que permita brindar seguridad hacia los activos informáticos, debido a la falta

de capacidades del personal para poder afrontar las nuevas tecnologías y los riesgos que están expuestos.

¿En qué medida la implementación de un sistema de gestión de seguridad de la información basado a la norma ISO/IEC 27001 mejorará la seguridad y garantizará el acceso supervisado a los sistemas y activos informáticos en la Unidad de Gestión Educativa Local 01?

1.3 Delimitación de la Investigación

El presente trabajo de investigación se llevó a cabo en la Unidad de Gestión Educativa Local Nº1 – San Juan de Miraflores, Lima - Perú, El periodo en el cual se realizó esta investigación comprende el periodo setiembre del 2017– julio del 2018.

1.4 Justificación e Importancia

Este estudio se justifica desde diferentes aspectos el económico, por causa de los peligros a los que se exponen los activos informáticos, la caída de unos de estos activos, causa la perdida de información e interrupción de los servicios, ocasionando una gran pérdida económica invaluable a la entidad. En este contexto se propone desarrollar e implementar un SGSI a fin de garantizar continuidad de los servicios.

Tiene además justificación académica considerando que la investigación y el aporte como estudiante, servirá como fuente futura de consulta para realizar distintas investigaciones.

Justificación tecnológica, puesto que los activos informáticos son de suma relevancia dentro de la Ugel.

La disponibilidad y seguridad de la información son aspectos importantes para mantener la imagen institucional lo cual conlleva el logro de las metas institucionales. El SGSI contribuye en la gestión de políticas y procesos relacionados con los objetivos de la Ugel01, la implementación de un SGSI permite que el personal de tecnologías de la UGEL

Nº01 podría reconocer las amenazas informativas y activos, encontrándose en condiciones de asumirlo, minimizarlo y controlarlo mediante una metodología definida y documentada.

En este sentido, la investigación adquiere justificación social por cuanto aplicar un SGSI en las diferentes entidades públicas genera resultados positivos en la mejora de los servicios orientados a los ciudadanos y usuarios internos, a fin de brindar una atención de calidad.

1.5 Limitaciones de la Investigación

El tamaño de la muestra: El presente estudio de investigación abarcará solo los activos informáticos de la Unidad de Gestión Educativa local Nº01. Por ser una entidad del estado, se maneja información clasificada, por lo tanto pueden existir restricciones a la información.

1.6 Objetivos

1.6.1 Objetivo General

Desarrollar un sistema de gestión seguridad de la Información de acuerdo con la norma ISO/IEC 27001 en la Unidad de Gestión Educativa Local 01.

1.6.2 Objetivos Específicos

a. Diseñar un sistema de gestión seguridad de la información de acuerdo a la norma ISO/IEC 27001 en la Unidad de Gestión Educativa Local 01.

b. Implementar y ejecutar los pasos para la puesta en marcha del SGSI en la Unidad de Gestión Educativa Local 01.

c. Supervisar y analizar el sistema de gestión seguridad de la información de acuerdo con la norma ISO/IEC 27001 en la Unidad de Gestión Educativa Local 01.

d. Evaluar los resultados de la implementación y aplicar las mejoras continuas del sistema de gestión seguridad de la información de acuerdo con la norma ISO/IEC 27001 en la Unidad de Gestión Educativa Local 01.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes Nacionales

Como primer antecedente del presente estudio se encuentra el trabajo de (Ampuero, 2011), titulado Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. El objetivo fue diseñar un sistema de gestión de seguridad de información para una compañía de seguros que abarque lo necesario para impedir inconvenientes en este organismo. Para el cumplimiento de este objetivo se utilizaron estándares y buenas prácticas reconocidas mundialmente para el desarrollo de las etapas del diseño del (SGSI) y de esta forma garantizar la implementación en cualquier compañía de este rubro.

Los resultados obtenidos indicaron que para ofrecer un nivel estándar de seguridad a la compañía, todo SGSI debe estar basado en buenas prácticas dirigidas a seguridad de la información que demuestren las consideraciones a seguir distintos aspectos. Por último, indica el autor como resultado de su investigación que es inútil poseer un SGSI que tenga en cuenta todos los peligros y controles para disminuirlos o poseer la tecnología posible para salvaguardar la información de la empresa si no se le brinda la importancia debida a la seguridad de la información de parte de la alta gerencia y no se llevan a cabo las políticas y establecidas por parte de los encargados de la seguridad.

Como segundo antecedente, se encuentra la investigación realizada por (Espinoza H. , 2013) titulada Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo Para lograr los objetivos planteados, se tomó en consideración un enfoque en la seguridad de la empresa, tomando en cuenta las fases de sus procesos de producción, los cuales se dividen a su vez en 4 subprocesos que son

Planeamiento, Manufactura, Calidad y Bodegas e Inventarios. En estos subprocesos está ligada información fundamental para la empresa, como "recetas" de productos, sistematización de manufactura, tipos de pruebas de calidad de producto, etc. Esto debe estar protegido en forma adecuada con el fin de impedir que dicha información se extravíe o vaya a personas no autorizadas.

Como último antecedente nacional, se encuentra el trabajo realizado por (Aguirre, 2014), titulado Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Para llevar a cabo dicha investigación se trabajó con una institución pública para efectos de estudio, con el propósito de desarrollar y diseñar una solución de seguridad adaptado a la normativa implicada para la organización y que sirva de referente para la aplicación de dicho sistema. Por consiguiente, se efectuaron conversaciones con la alta gerencia por medio de las cuales se definió el alcance y políticas para la organización enfocada en los procesos institucionales prioritarios de dicha institución, seguidamente se efectuaron entrevistas a fin poder identificar y precisar los activos importantes de la organización, se igual manera se pudo identificar los peligros potenciales a los cuales estos estaban expuestos. Finalmente, se redactó un documento en el cual se estableció que controles de la NTP ISO/IEC 17799:2007 podían aplicarse dentro de la empresa, con base en el trabajo implementado.

2.1.2 Antecedentes Internacionales

Como primer estudio internacional, se encuentra el trabajo realizado por (Tola, 2016) este trabajo fue efectuado en la Universidad Gustavo Galindo en Ecuador, con la finalidad de obtener el título de Ingeniero en electricidad y computación. El citado proyecto de titulación estableció la información pertinente para la aplicación de un Sistema de Gestión de Seguridad de la Información, basado en la norma IO 27001:2005, para asegurar la protección de los activos de información y otorgar confianza a los clientes de A&C Group S.A. La norma adoptó una perspectiva por procesos para instaurar, maniobrar, inspeccionar, examinar, conservar y mantener un SGSI. El objetivo general fue Lograr la implementación de un Sistema de Gestión de Seguridad de la Información, con base en ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa A&C Group S.A. Al finalizar la investigación, los autores pudieron concluir que es

fundamental determinar los objetivos y políticas del sistema de gestión de seguridad de la información, debido a que los mismos van marcando la ruta que debe seguir la organización para dirigirse adecuadamente, conservar la privacidad, integridad y el manejo de la información, por consiguiente es importante la participación de los altos ejecutivos. Igualmente indicaron que Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, están fundados en la prevención, por ende es básico identificar los peligros a los que están sometidos los activos para así impedir pérdidas económicas u operacionales.

Como segundo trabajo internacional se encuentra el realizado por (Aguirre R. Z., 2015) titulado estudio para la implementación del sistema de gestión de seguridad de la información para la Secretaria de Educación Departamental de Nariño basado en la norma ISO/IEC 27001. El citado trabajo se planteó con el propósito de minimizar el impacto y la probabilidad de las amenazas y riesgos potenciales a que ve expuesta el área financiera mediante un diagnóstico de la seguridad informática y de la información que ayude a la implementación de un SGSI basado en la norma ISO/IEC 27001 en la Secretaría de Educación de Nariño. Como conclusión de este estudio se obtuvo que es importante optimizar la documentación y mantenerla actualizada de forma explícita para cada uno de los sistemas de información. Para organizar todos los requerimientos del estatuto, la normativa y los contratos de ley. Se debe guardar la propiedad intelectual, así como utilizar programas de procesamiento de datos originales, salvaguardar los registros del espacio financiero contra pérdidas, destrozos, adulteraciones, accesos y divulgación no autorizada así como el uso de controles de cifrado de la información.

Como último antecedente internacional, se encuentra la investigación realizada por (Maya, 2006) titulado plan de implementación del SGSI basado en la norma ISO 27001:2013. El referido estudio describe los objetivos, la trascendencia, la posibilidad del SGSI y la metodología necesaria para la planificación, identificación y desarrollo del modelo de seguridad de la información para la organización Textilera S.A, basado en la norma ISO 27001:2013; comenzando con el análisis de la organización desde la perspectiva de los procesos de ejecución, de la seguridad, identificación de vulnerabilidad y amenazas, con la aplicación metodológica de gestionar los riesgos de seguridad de la información,

planeación del tratamiento de riesgos y reproducción del marco documental del sistema de gestión de seguridad de la información para Textilera S.A.

Al término de la investigación la autora concluye que tras implementar un sistema de gestión de seguridad de la información SGSI, se completará un mecanismo de mejora de recursos baja en los costes lo que permitirá a Textilera S.A lograr las metas planteadas. Estas mejoras permitirán lograr la madurez fijada por la organización, de igual forma facilitará un mejor acercamiento para realizar la certificación del SGSI por medio de la norma ISO 27001:2013. - Un SGSI proviene cambios de procesos y estructuras, sin embargo logra que la integridad, confiabilidad y disponibilidad estén situadas como uno de los mayores activos dentro de la organización y para Textilera S.A esto es de vital importancia para su crecimiento.

2.2 Estado del Arte

El estado del arte reseñado en la presente investigación resume hechos sucedidos recientemente sobre las acciones primordiales abarcadas en la etapa de establecimiento de un SGSI en algunas empresas dedicadas a diferentes rubros. Como primera experiencia se resume el trabajo realizado por (Céspedes, 2016) este trabajo se relacionó con la protección de la confidencialidad de la Corte de Lambayeque, la cual se vio implicada en distintas ocurrencias, como en el caso de la investigación del órgano de control OCMA del año 2009 donde se detectaron distintas irregularidades en el sistema de expedientes jurídicos como consecuencia de fallas en el uso de los sistemas de información, se realizó la auditoria a dichos sistemas, (Diario la Republica, 2013)

Otra experiencia que representa un valioso aporte al presente estudio es la investigación realizada por (Moscaiza, 2018), este trabajo se enfocó en el diseño de un modelo de gestión de la seguridad de la Información en la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013, considerando el desarrollo, normas y problemas internos de esta clase de bancos, las cuales tienen aspectos que demuestran la necesidad de reorientar sus procesos hacia una segura gestión de riesgos, así como, la conciliación a los requisitos de regulación actuales, lo que permite que se conserve la disposición, confiabilidad e integridad de los datos. En este sentido, dicho estándar describió la forma

eficaz en cómo la institución financiera tratará los peligros de seguridad de información, en consonancia con los logros institucionales y los objetivos de control que promueve la normativa del sistema de gestión. Asimismo, explica el Plan de Seguridad en donde se encontrarán los principales proyectos que el SGSI necesita.

Como conclusión en este estudio se obtuvo que valorar activos de información en la Cooperativa de Ahorro y Crédito ABC, consintió en que dicha institución pudo reconocer los componentes fundamentales para los propósitos de rentabilidad financiera, contribuyendo con las personas encargadas de la administración de los activos, así como la continuidad y categorización. Con este resultado puede indicarse que la CAC optimizó en gran medida la representación de sus activos en relación a su principio, respondiendo de este modo a una gestión de riesgos eficaz.

Dicho análisis además permitió clasificar los riesgos prioritarios de seguridad de los activos de información en la Cooperativa de Crédito y Ahorro ABC con una eficacia mejorada respecto al estado inicial. Con este resultado puede indicarse que la Cooperativa superó la gestión de sus amenazas potenciales con relación a su valor inicial de 22.22% ya que tenía un menor análisis debido a que no existían métodos establecidos. En el referido diseño se han clasificado ordenamientos para tratar riesgos de seguridad de información, resguardando sus procesos y finalidades financieras por medio de la selección de controles del Anexo A de la norma ISO 27001:2013, considerando el enfoque más favorable para enfrentar cualquier riesgo y su peligro potencial.

2.3 Bases teórico científicas

2.3.1 Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO/IEC 27001, un sistema de gestión de seguridad de información es un cúmulo de tareas, acciones y recursos que instituye la directiva con la finalidad de direccionar y contribuir con la seguridad de la información y asegurar el continuo de la operatividad empresarial. Esta operación se debe realizar a través de un proceso sistémico, establecido, normado y que sea del dominio de toda la empresa. Este procedimiento es el

que constituye un SGSI, el cual se puede considerar, por comparación con la norma universal ISO 9001, como el sistema de calidad para la seguridad de activos de información.

Es válido resaltar que certificar un estatus de protección completa es prácticamente imposible, inclusive al momento de poseer un presupuesto sin restricciones. El fin del sistema de gestión de la seguridad de la información es, por consiguiente, garantizar que los peligros de la seguridad de los activos de la información sean del dominio público, asumidos, gestionados y reducidos por la entidad de una manera establecida, sistemática, constituida, comunicable, eficaz y consustanciada con las conmutaciones que se provoquen en las amenzas y el ámbito tecnológico. (ISO/IEC 27000, 2013)

2.3.2 Seguridad de información

Comprende aquellas medidas que permiten la prevención y reacción del ser humano, instituciones y sistemas de tecnología para salvaguardar y proteger la integridad de la información. (ISO/IEC 27000,2013)

2.3.3 Descomposición de la definición

Al hablar de SGSI, según ISO/IEC 27001, se refiere al mantenimiento de su privacidad, confianza y disponibilidad. Del mismo modo, se relaciona con los sistemas inherentes a su tratamiento interno de la empresa. De este modo, estos tres conceptos conforman los pilares para un SGSI:

a) Confidencialidad: se mantiene de forma hermética la información, asimismo el acceso es totalmente restringido.

b) Integridad: la información mantiene su fidelidad y se encuentra completa.

c) Disponibilidad: la información se encuentra disponible para las personas y entidades autorizadas a su acceso.

Para certificar que la seguridad de los activos es agenciada de manera correcta, debe estar basada en un proceso sistémico. Uno de los objetivos fundamentales de los sistemas de información es promover la toma de decisiones. Cuando un encargado tiene que tomar una decisión solicita la información, que le permita minimizar las dudas. No obstante, aunque

todos la usen, no todos los encargados recolectan la misma información: esto va a depender de diversos factores, por ejemplo la experiencia en el área, formación profesional, compromiso, etc. De igual manera, los responsables necesitan recolectar mayor o menor información lo que dependerá de su aversión a afrontar riesgos potenciales.

Figura 1: integración de confidencialidad, integridad, Información y disponibilidad

2.3.4 Fases para la Implementación de un SGSI

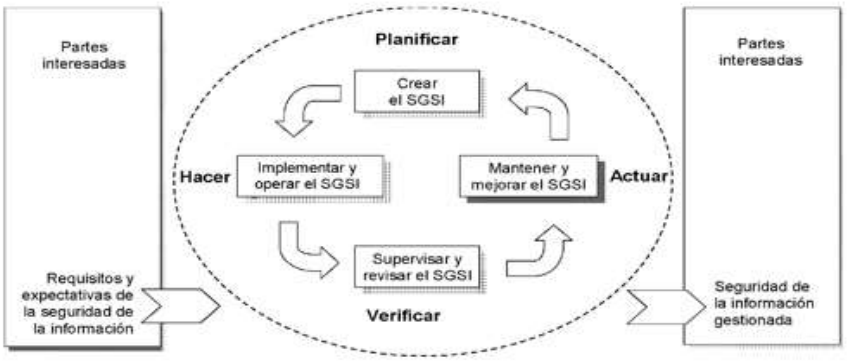


Figura 2 Modelo PDCA aplicado al proceso ISMS

Los resultados de la aplicación de este ciclo proveen a la organización un mejor proceso competitivo, de los productos y servicios, mejorando la calidad, mermando los costos, mejorando la productividad, aumentando la participación del mercado y subiendo la rentabilidad de la institución.

2.3.4.1 Fase Plan: Establecer el SGSI

Durante esta fase, se deben realizar los siguientes pasos: Definir las metas del SGSI a efectos del negocio, la organización, su ubicación, recursos tecnológicos, agregando datos y justificación de cualquier falta.

Delimitar una estrategia de seguridad que: comprenda el marco universal y las metas de seguridad de la información dentro de la empresa. Tome en cuenta consideraciones de tipo legal o convenidos relacionados a la seguridad de la información. Esté enlazada con el entorno estratégico de gestión de riesgos de la empresa en el que se determine y mantenga el SGSI.

Así mimo, se debe establecer una metodología de evaluación del peligro de la información adecuada para el SGSI y los requerimientos del negocio, además de instaurar los criterios de aceptación del riesgo y delimitar los estados de riesgo aceptable. Lo más importante de esta metodología es que la resultante se pueda comparar y divulgar (hay cuantiosas metodologías adaptadas para evaluar riesgos, sin embargo es totalmente aceptable elegir una propia).

Identificar los riesgos: Identificar los activos que están dentro del alcance del SGSI y a sus encargados directos, determinados como propietarios. Clasificar las amenazas respecto a los activos. Equiparar las debilidades que se puedan aprovechar basada en las amenazas. Identificar los efectos en la privacidad, integridad y disponibilidad de los activos. Analizar y valorar los riesgos: Hacer el seguimiento del impacto en el negocio de una falla de seguridad que represente una pérdida de confidencialidad, integridad o disponibilidad de un activo de información. Evaluar de forma realista la posibilidad de un incidente de seguridad relacionado con las amenazas, vulnerabilidad, efecto en los activos y los controles que ya estén implantados. Estimar los niveles de riesgo. Determinar, de acuerdo a criterios de aceptación de riesgo anteriormente establecidos, si el riesgo es admisible o requiere de tratamiento.

Por último clasificar y evaluar las opciones de resolución de los peligros para: implementar controles apropiados. Admitir el riesgo, cumpliendo con las políticas y juicios

determinados. Evitar el riesgo, por ejemplo a través de la cesantía de las actividades que lo causan. Transmitir el peligro a terceros, por ejemplo empresas aseguradoras o que provean servicios de outsourcing. Delimitar una declaración de aplicabilidad que involucre: Las metas de control y registros elegidos, las razones para su selección.

2.3.4.2 Fase Do: Implementar y utilizar el SGSI

Esta fase consiste en trazar un plan para tratar los riesgos identificando las acciones, activos, y metas en la gestión de los riesgos de seguridad de la información. Instaurar la planificación para el procesamiento de procesamiento de amenazas, con el propósito de lograr los objetivos de control clasificados, esto debe incluir asignación de recursos, compromisos y deberes prioritarios. Aplicar controles preseleccionados que conduzcan a las metas de control. Delimitar un sistema de métricas que promueva la obtención de resultados repetibles y equiparables para cuantificar la eficiencia de los controles o sus grupos. Gestionar capacitación en cuanto a la seguridad de la información a todo el personal. Ejecutar las operaciones del SGSI. Agenciar los recursos indispensables determinados al SGSI para mantener la seguridad de la información. Aplicar procedimientos que permitan detectar con rapidez responder incidentes de seguridad.

2.3.4.3 Fase Check: Monitorizar y revisar el SGSI

Durante este periodo la empresa debe: Realizar ordenamientos de monitoreo y chequeo para: Revelar de forma temprana los déficit en los efectos creados por el proceso de información. Clasificar resquicios e incidencias. Apoyar a la directiva a delimitar si lo desarrollado por los responsables y aparatos tecnológicos para garantizar la seguridad de los activos se ejecutan respecto a lo planeado. Develar y advertir ocurrencias de seguridad a través de indicador. Delimitar si las actividades desarrolladas para solucionar resquicios de seguridad dieron resultados.

Chequear continuamente el buen funcionamiento del SGSI, cumpliendo con las estrategias metas del SGSI, los avances en materia de seguridad, incidencias, indicadores de eficiencia, explicaciones y detalles de las implicaciones. Cuantificar la efectividad de los controles para la verificación que conlleva los requerimientos de seguridad.

Monitorear continuamente en periodos planeados las valoraciones de riesgo, los residuos y estándares factibles, considerando los cambios probables que se hayan producido en la organización, los aspectos tecnológicos, las metas y procedimientos de negocio, los riesgos valorados, la certeza de los controles aplicados y el ámbito exterior – requisitos jurídicos, obligaciones laborales, etc. Efectuar continuamente auditorías internas del SGSI en intervalos planificados. Analizar el SGSI de parte de la dirección por periodos para ser garantes que el alcance delimitado siga siendo el apropiado y que las mejoras en el proceso del SGSI son evidentes. Reestablecer los planeamientos de seguridad en función de las conclusiones y nuevos productos hallados durante las acciones de monitorización y revisión. Reconocer acciones e incidencias que puedan comprometer la eficacia o el rendimiento del SGSI.

2.3.4.5 Fase Act: Mantener y mejorar el SGSI

En dicho momento la empresa instaura los cambios y progresos cada vez que se requiera con el fin de optimizar el SGSI, efectuara todas las labores de prevención y corrección apropiadas basadas en la norma ISO 27001 y a las lecciones asimiladas durante las vivencias propias y de otras empresas. En esta fase se debe comunicar a todas las partes involucradas de cada control o acción realizada, con el fin de lograr los objetivos establecidos en este trabajo de investigación.

2.4 Definición de términos básicos

Amenaza: Escenario u ocurrencia que causa perjuicios en un área.

Análisis de vulnerabilidades: Evaluación del periodo de la seguridad de un área o sus elementos a través el envío de evidencias y recolecta de los efectos.

Aplicación: Todo aquel programa computacional que se use como base en los procedimientos.

Auditoría: Procedimiento de analizar, inspeccionar y realizar un escrito sistemático de los eventos de organismo para determinar su valor.

Autorización: Acción de conceder la accesibilidad a terceros o procesos.

Confidencialidad: Requerimiento de seguridad que muestra la ruta a los recursos de sistema, debe estar conformando únicamente a los usuarios con acceso acreditado.

Control de acceso: Prohibir la accesibilidad a objetos de acuerdo a las autorizaciones de acceso del sujeto.

Dato: Es toda aquella información que se produce, envía, recepciona y tramitan internamente en la empresa.

Disponibilidad: Requisición de seguridad que sugiere que los datos y los servicios del sistema sigan funcionando y que las personas autorizadas tengan acceso a los recursos cuando y donde lo requieran, y de la forma en que lo necesiten.

Gestión de seguridad: Proceso que establece y mantiene en un sistema o red informática. Los periodos de este proceso engloban la precaución de problemáticas de seguridad, localización de intromisiones, indagación y respuesta. Fuente (ISO/IEC 27001)

Instalación: Es cualquier sitio donde se albergan los recursos de información. Este entorno puede ubicarse de forma interna y externa en la empresa.

Integración: En ingeniería de sistemas, mezcla de elementos en un ente vinculado.

Integridad: Requerimiento de seguridad que señala que la información debe protegerse ante posibles adulteraciones.

Personal: Son todas las personas que están implicadas en el acceso y el conducción de una u otra forma a los activos de información de la empresa.

Política de seguridad: Cúmulo de normas que señalan la ideología de una empresa con relación a la protección de su información y software informanticos.

Privacidad: poseer libertad de acceso sin la debida autorización.

Servicio: Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.

Seguridad: se refiere a cumplir los tres conceptos confidencialidad, integridad y disponibilidad.

Software libre: Código que otorga libertad a los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el mismo.

Tecnología: Es todo el hardware donde se maneje la información y las comunicaciones.

Vulnerabilidades: Debilidades en un sistema que se pueden usar para violenta las estrategias de seguridad.

CAPÍTULO III

MARCO METEDOLÓGICO

3.1 Tipo y diseño de la investigación

3.1.1 Tipo de la investigación

La clase investigativa desarrollada en el presente estudio es de tipo aplicada. Esta investigación puede definirse según el punto de vista de diferentes autores, tal es el caso de (Chávez, 2007), quien señala:

> El tipo de investigación aplicada tiene como propósito solucionar un problema en un espacio temporal breve, orientado a la implementación rápida por medio de acciones concretas para hacer frente al problema. Por ende, se orienta a la acción urgente y no al desarrollo teórico y sus resultados, a través de actividades exactas para hacer frente al problema. (p. 134)

En este sentido, (Hernández R. F., 2013) señalan que este tipo de estudio puede identificarse como "aquella que posee finalidades prácticas en el sentido de dar solución a

problemáticas detectadas en un área del conocimiento. Está vinculada a la visión de necesidades o problemas específicos y a la aspiración del investigador de solucionar estos" (p. 103) En la experiencia específica de la presente investigación, la finalidad es la creación de un sistema de gestión seguridad de la Información de acuerdo con la norma ISO/IEC 27001 en la UGEL 01, con lo cual se aplican los conocimientos accedidos en el área de ingeniería y se buscó la respuesta a un problema real en un contexto determinado.

3.1.2 Diseño de la investigación

Por la correlación de sus variables, el estudio corresponde al tipo de diseño cuasi experimental. Se aplicarán pruebas pre y post en el grupo de la investigación, considerando el siguiente diseño:

G O1 X O2

Donde:

G = Grupo de investigación (áreas de la Ugel)

X = Aplicación (SGSI)

O1 = Pre Observación

O2 = Post Observación

3.2 Población y muestra

La población de la presente investigación se encuentra constituido por ciento seis (106) empleados que laboran en la Unidad de gestión Educativa Local Nº01, de acuerdo a lo que se ilustra en el Tabla 1.

Tabla 1

Descripción de la Población

ENTIDAD : UNIDAD DE GESTION EDUCATIVA LOCAL - UGEL 01								
SECTOR : MINISTERIO DE EDUCACION								
ORGANOS O UNIDADES ORGANICAS	CLASIFICACIÓN							TOTAL
	FP	EC	SP - DS	SP - EJ	SP - ES	SP - AP	RE	
DIRECCIÓN GRAL	0	0	0	0	1	1	1	3

ORGANO DE CONTROL INSTITUCIONAL	0	0	1	0	1	1	0	3
OFICINA DE ASESORIA	0	0	1	0	1	1	0	3
PLANIFICACIÓN Y PRESUPUESTO	0	0	1	0	5	1	0	7
ADMINISTRACIÓN	0	0	1	0	4	26	0	13
RECURSOS HUMANOS	0	0	1	0	6	21	0	28
GESTIÓN DE LA EDUCACIÓN BÁSICA REGULAR Y ESPECIAL	0	0	0	0	0	0	13	13
GESTIÓN DE LA EDUCACIÓN BASICA ALTERNATIVA Y TÉCNICO PRODUCTIVA	0	0	0	0	0	0	5	5
SUPERVISIÓN Y GESTIÓN DEL SERVICIO EDUCATIVO	0	0	0	0	2	2	9	13
TOTAL	0	0	5	0	20	53	28	106
TOTAL OCUPADOS	101							
TOTAL PREVISTOS	5							
TOTAL GENERAL	106							

Fuente: *CAP de la Ugel01 según RD Nº01371-2016-UGEL.01.SJM*

3.2.1 Muestra

Según (Hernández R. F., 2013) la muestra se define como "un subconjunto de la población". (p. 207) En la presente investigación, para delimitar el volumen de la muestra se implementó la siguiente fórmula:

$$n = \frac{z^2\, p*q*N}{E^2\,(N-1) + z^2\,(p*q)}$$

n: Tamaño de la muestra
N: N° de la población
Z: 1,96 para El 95% de confianza.
p: 0.5 Frecuencia esperada del factor a estudiar.
q: 1 -p
E: 0.05 Para el 5% de precisión o error admitido.

Desarrollo:

Datos: N= 106 usuarios

$$n = \frac{(1.96)^2\,(0.5 * 0.5)\,106}{(0.05)^2\,(126 - 1) + (1.96)^2\,(0.5*0.5)}$$

n= 83.25 = 83 **usuarios**

Muestra Óptima: = Muestra

1 + (Muestra / Población)

$$= \frac{83}{1 + (83 / 106)}$$

= 46.55 = **47 usuarios**

La muestra está conformada por 47 usuarios de la UGEL01.

3.3 Hipótesis

La implementación de un SGSI permitirá mejorar la seguridad y garantizará la accesibilidad a los sistemas de información y activos informáticos en la Unidad de Gestión Educativa Local 01.

3.4 Operacionalización

Variables de Investigación

Cuadro 1

Variable	Tipo	Dimensiones	Definición Conceptual	Indicadores	Datos para la Medición
Implementacion del SGSI en la Unidad de Gestión Educativa Local Nº 01	Dependiente	Gestion de Seguridad	Gestionar los lineamientos y mantenimiento del SGSI	Grado de cumplimiento de los lineamientos que soporten la implementación y mantenimiento del SGSI	1. Lineamientos que soportan la implementación y mantenimiento del SGSI 2. Documentación relacionada a la implementación y mantenimiento del SGSI
		Gestion de Riesgo	Identificar y monitorear permanentemente los posibles riesgos en los activos relevantes para la entidad.	obertura del SGSI en los Activos de Información	1. Evaluación de Riesgos 2. Tratamiento de Riesgos 3. Proyectos para el tratamiento de riesgos
		Gestion de Incidentes	Asegurar que los incidentes recurrentes sean solucionados a la brevedad. Asimismo, fortalecer el conocimiento del equipo de Seguridad de Información ante estos incidentes.	Número de incidentes recurrentes que fueron detectados y aprendidos	1. Listado de los incidentes de seguridad de información 2. Listado de los puntos débiles de seguridad (Vulnerabilidades) 3. Análisis de causa raíz de cada incidente 4. Acciones correctivas aplicadas a los incidentes 5. Base de datos centralizada y actualizada de Incidentes
Control del SGSI en la Unidad de Gestión Educativa Local Nº 01	Independiente	Control de Seguridad	Gestionar las medidas de seguridad de la información necesaria para el cumplimiento regulatorio de leyes, reglamentos, políticas y/o acuerdos con terceros	Grado de cumplimiento de las medidas de seguridad de la información	1. Número total de medidas requeridas para el cumplimiento de SGSI 2. . Número de medidas adoptadas en la entidad.
		Concientizaciòn	Capacitar y sensibilizar permanentemente a los trabajadores y terceros con respecto a su responsabilidad para mantener y asegurar el SGSI en la entidad.	Número de empleados que se encuentran concientizados, es decir los que realizaron el curso de concientización virtual y rindieron su respectivo examen de Seguridad de la Información	1. Número total de empleados dla entidad. 2. Número de empleados que realizaron el curso virtual y rindieron la evaluación.

Operacionalización de Variable

Fuente: elaboración propia

2.5 Métodos, técnicas e instrumentos de recolección de datos

3.5.1 Métodos y Técnicas para la recolección de datos

Observación directa**:** con el fin de identificar y obtener los contenidos más recientes que suceden en la UGEL Nº01.

Entrevista: esta técnica, permitió recaudar información del equipo de tecnologías de la información con propósito de analizar y clasificar los riesgos vinculados a los activos de Información.

Cuestionario: Se realizaron un conjunto de interrogantes, con el fin de recopilar toda la información de los empleados de las distintas áreas de la Ugel Nº01, importante relacionada con la seguridad de la información de dicha entidad.

3.5.2 Instrumentos de recolección de datos

Para (Hernández, 2010), el instrumento para medir es un "medio que usado por el investigador para sistematizar información o datos relacionados con las variables de estudio" (p. 200). Las técnicas e instrumentos de recolección de datos son cuantificables por lo cual el investigador recopila información para el logro de los objetivos.. (Barrera, 2000) Para obtener información el instrumento en función de los objetivos, con el fin de interrogar, a través de un cuestionario cerrado, dicho cuestionario cuenta con catorce (14) preguntas basadas en la aplicabilidad del SGSI ISO27001 como se indica en el Anexo "1", con el propósito de diagnosticar el estado vigente de la seguridad de la información en la UGEL 01. Asimismo se utilizó el software Mantis Bug Tracker desplegado como mesa de ayuda, para la recolectar la información relacionada a los incidentes reportados. Finalmente fue utilizada la herramienta de procesamiento MS Excel en su versión actual, la cual se utilizó como programa computacional de auditoria durante el análisis de riesgos en la UGEL Nº 01.

3.6 Procedimientos para la recolección de datos

Para recolectar información se hizo a través de la observación directa. Ésta se aplicó durante 30 días en el espacio de informática para realizar posteriormente análisis de la información recabada, el cual se basó en los procesos de almacenamiento, respaldo, seguridad de los sistemas de información, que se manejan en el centro de datos.

Se observó a los especialistas del equipo de tecnologías de la información a fin de conocer el procedimiento que utilizan en el proceso de manejo de incidentes, para su posterior análisis, recolecte información suficiente para diseñar e implementar política de

gestión de incidentes basada en la ISO27001, así como el seguimiento, consulta y tiempo de respuesta, entre otros.

Para aplicar mis entrevistas, fueron seleccionados un total de seis (06) trabajadores de diferentes jerarquías y áreas de trabajo, recolectando información acerca de la atención, el uso de los sistemas de información que brinda la entidad, logrando analizar y procesar dicha información para diseñar e implementar estrategias de seguridad de la información.

Asimismo se entrevistó a cinco (05) especialistas del equipo de tecnologías de la información, recolectando información acerca de los datos e información de valor, gestión de seguridad, gestión de riesgo, controles de seguridad, gestión de incidentes, logrando analizar y medir los indicadores alineados a los objetivos de este trabajo de investigación.

Para aplicar el cuestionario, se tomó la muestra óptima conformada por cuarentaisiete (47) usuarios de diferentes áreas de la Ugel Nº 01, se coordinó con la dirección de la Ugel Nº01 para aplicar el cuestionario en el ambiente del auditorio, el cual tuvo una duración de 60 minutos, conformado por catorce (14) preguntas referenciadas en el Anexo 1, con el fin de diagnosticar el estado actual de la seguridad de la información en la Unidad de Gestión Educativa Local Nº 01.

3.7 Plan de análisis estadístico de datos

Para presentar los datos que proceden del instrumento de recaudación, se implementó la estadística descriptiva, para lo cual se empleó el paquete informático SPSS, para el procesamiento y muestra de los resultados de la investigación a través de cuadros y gráficos estadísticos. (Hernández R., 2013), señala como “La utilización de bases estadísticas de frecuencias y porcentajes; integrados con cuadros y gráficos estadísticos con sus concernientes análisis” (p. 56)

Cuadro 2

Cuadro para el análisis de recolección de datos

Temas	Respuestas					Total	valor %
	SI	PARCIALMENTE	NO	NO APLICA	ASUME		
cobertura de politicas							
Organización de la Seguridad							
identificacion de activos							
Personal Capacitado							
Seguridad en la infraestructura							

Fuente: elaboración propia

3.8 Criterios éticos

La ingeniería en sistemas también debe apegarse a criterios éticos que garanticen que sus procedimientos estén encaminados hacia el beneficio común y que los conocimientos aplicados sean utilizados correctamente. Por lo antes descrito, la presente investigación se enmarca según lo expresado por (Torres, 2016) cuando señala: "Los ingenieros en sistemas de computación estarán vinculados durante todo su ejercicio en la enseñanza relacionada con la experiencia de su profesión y causarán un enfoque ético en la praxis de la misma, vinculándose a:

> 1. Aumentar su conocimiento en los avances y análisis, descripción, esbozo, desarrollo, mantenimiento y documentos relacionados, aunado a la administración del procesamiento. 2. Afianzar su habilidad para la creación de la información segura, fiable, útil y cualitativamente razonable a precios accesibles y en un tiempo flexible. 3. Desarrollar su destreza para documentar y redactar. 4. Actualizar de manera continua su discernimiento de los estándares importantes y del legado el sistema de información y la documentación con que se desenvuelve. 5. Mostrar que las vulneraciones personales del código inconsistentes con el ejercicio de la ingeniería en sistemas. (p. 12)

3.9 Criterios de rigor científico

(Guba, 1981) Propone como mínimo cuatros criterios elementales para conseguirlos, sobre los cuales se trabajará a posteriori. Luego se exponen detalladamente a cada uno de ellos:

3.9.1 Criterios de rigor valor de verdad

Validez interna: Valor de verdad: igualdad entre la situación real y los datos recabados.

Credibilidad: Se pretende la igualdad con las opiniones de los involucrados objetos de estudio.

3.9.2 Criterios de rigor aplicabilidad

Validez externa o transferibilidad: nivel en que pueden ser aplicados los resultados de una investigación a otros sujetos o entornos.

Transferibilidad: Se busca elaborar la información sobre el entorno que permitirán transferir las conclusiones a entornos análogos. No pretende aplicar sin condiciones.

3.9.3 Criterios de rigor Consistencia

Fiabilidad: nivel en que los instrumentos renuevan las mismas medidas en las mismas circunstancias

Dependencia – Variación rastreable: ¿Cómo ha avanzado una fuente de datos? ¿En qué medida el investigador es más preciso en su percepción de la realidad con el paso del tiempo?

3.9.4 Criterios de rigor Neutralidad

Objetividad: Grado en que la investigación está excluida de la influencia de la perspectiva del investigador.

Confirmabilidad: No se desea ocultar la subjetividad del investigador, no obstante se busca que los datos y las conclusiones sean validados por voces externas.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Resultados e Indicadores

Tabla 2

Indicador: Grado de cumplimiento de los lineamientos que soporten la implementación y mantenimiento del SGSI

Métricas (Medición)	Frecuencia	% del Universo Requerido	Criterios de Medición						Datos de la Medición Antes			
			Valor correcto		Valor aceptable		Valor fallido		Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
Cantidad de lineamientos implementados para el SGSI y mantenimiento del SGSI con la ayuda de documentacion relacionada	Trimestral	100%	=	100%	>=	80%	<	83%	10	3	30%	Fallido

Datos de la Medición Despues			
Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
10	8	80%	Aceptable

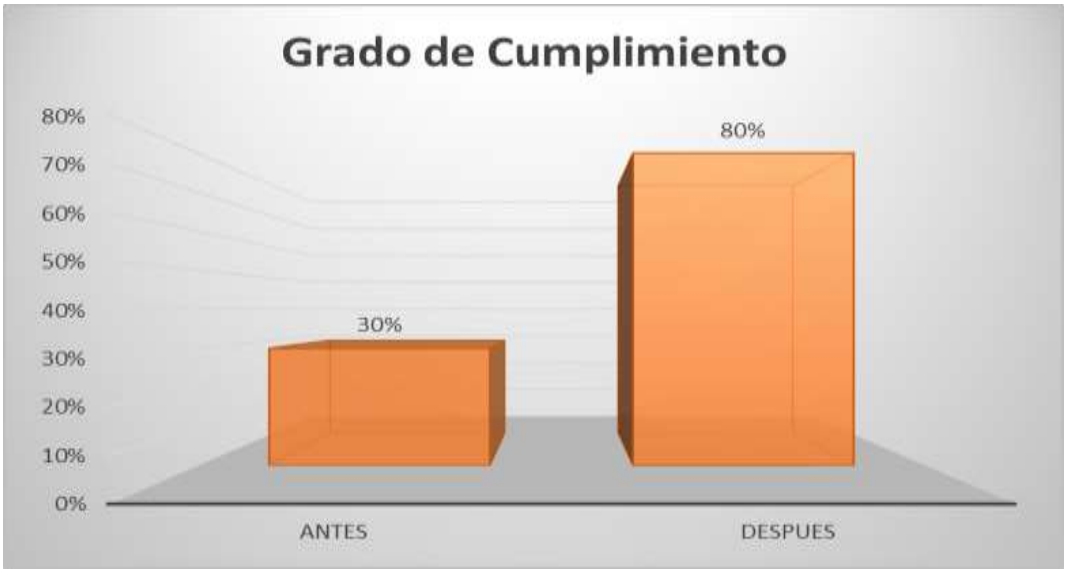


Figura 3 De los 10 lineamientos que soportan al SGSI, se venían cumpliendo 3 por lo tanto muestra un resultado de condición fallido por no superar los criterios de evaluación, posteriormente a la implementación del SGSI se incrementó a 8, evidenciando una mejora dando como resultado un criterio de medición aceptable.

Tabla 3

Indicador: Cobertura del SGSI en Activos de Información

Métricas (Medición)	Frecuencia	% del Universo Requerido	Criterios de Medición						Datos de la Medición Antes			
			Valor correcto		Valor aceptable		Valor fallido		Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
Número de proyectos implementados para mitigar riesgos	Semestral	100%	=	100%	>=	86%	<	86%	15	2	13%	Fallido

Datos de la Medición Despues			
Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
15	14	93%	Aceptable

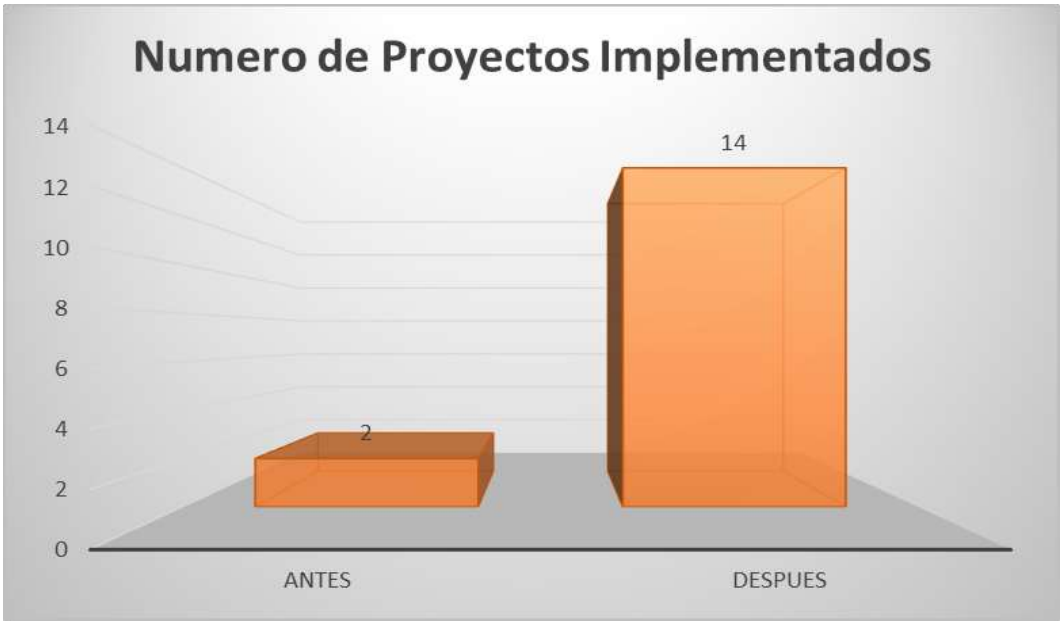


Figura 4 de los 15 proyectos propuestos a implementar se tuvo solo 2 antes del SGSI mostrando el estado fallido por no lograr un criterio de medición favorable, posteriormente se ha incrementado a 14 proyectos de los 15 propuestos dando un resultado aceptable por los criterios de medición.

Tabla 4

Indicador: Grado de cumplimiento de las medidas de seguridad de la información

Métricas (Medición)	Frecuencia	% del Universo Requerido	Criterios de Medición					Datos de la Medición Antes			
			Valor correcto		Valor aceptable		Valor fallido	Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
Número de medidas de cumplimiento de seguridad de la información que faltan implementar y difundir en la entidad	Semestral	100%	=	100%	>=	75%	< 75%	40	30	75%	Aceptable

Datos de la Medición Despues			
Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
40	40	100%	Correcto

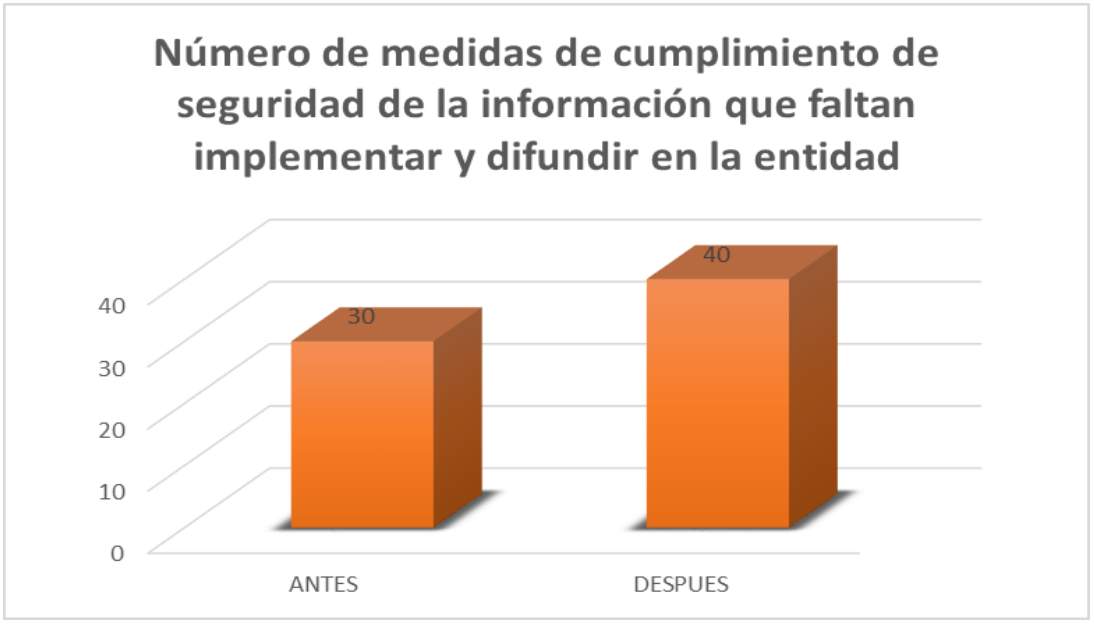


Figura 5 Como se muestra en el cuadro anterior, ya la entidad venia implementando medidas de seguridad con un resultado aceptable de acuerdo a los criterios de medición, posteriormente después del SGSI se incrementó al 100%, dando como un resultado correcto.

Tabla 5

Indicador: Número de empleados que se encuentran concientizados, es decir los que realizaron el curso de concientización virtual y rindieron su respectivo examen de Seguridad de la Información

Métricas (Medición)	Frecuencia	% del Universo Requerido	Criterios de Medición						Datos de la Medición Antes			
			Valor correcto		Valor aceptable		Valor fallido		Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
Número de empleados que realizaron el curso virtual y rindieron la evaluación dividido entre el número total de empleados dla entidad.	Semestral	100%	=	100%	>=	70%	<	80%	47	20	43%	Fallido

Datos de la Medición Despues			
Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
47	47	100%	Correcto

Figura 6 Como se muestra en el cuadro 4.1.4 y en la tabla 4.1.4, no existía o casi nula la capacitación sobre SGSI a los trabajadores de la UGEL, obteniendo un resultado fallido en los criterios de medición, posteriormente se llegó a la totalidad del 100% de efectividad arrojando como resultado en los criterios de evaluación aceptable.

Tabla 6

Indicador: Número de incidentes recurrentes que fueron detectados y aprendidos

Métricas (Medición)	Frecuencia	% del Universo Requerido	Criterios de Medición						Datos de la Medición Antes			
			Valor correcto		Valor aceptable		Valor fallido		Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
Número de nuevos incidentes de seguridad para los cuales el Análisis de Causa Raíz implementado en incidentes pasados se aplico dividido entre el número total de nuevos de incidentes.	Trimestral	100%	=	100%	>=	95%	<	95%	60	40	67%	Fallido

Datos de la Medición Despues			
Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
60	57	95%	Aceptable

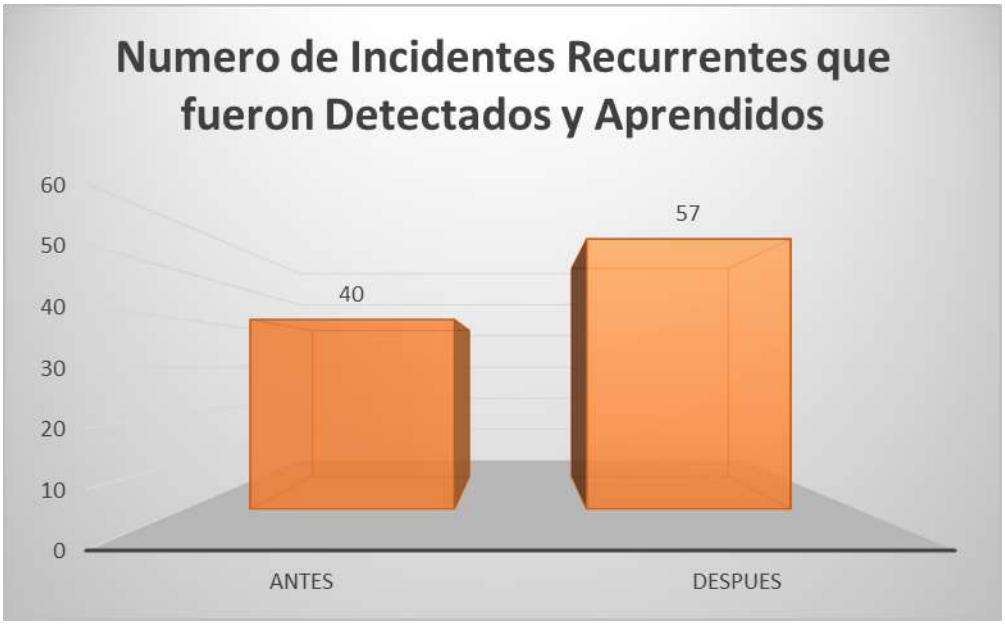


Figura 7 Como se muestra en el cuadro y en la tabla anteriores, tuvieron un 67% de efectividad en cuestión de los incidentes, ubicándose en los criterios de medición con la condición de fallido, el levantamiento de información se realiza cada 3 meses, en la última medición se superó la efectividad al 95% que representa unos 57 incidentes recurrentes, optimizando el servicio, por lo tanto como resultado de los criterios de medición es de condición aceptable.

4.2 Discusión de Resultados

Tabla 7

Resultados de los Indicadores

Indicador	Criterios de Medición						Datos de la Medición Antes				Datos de la Medición Despues			
	Valor correcto		Valor aceptable		Valor fallido		Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado	Valor # de Ocurrencias Esperadas	Valor # de Ocurrencias Efectivas	% Efectividad	Resultado
Grado de cumplimiento de los lineamientos que soporten la implementación y mantenimiento del SGSI	=	100%	>=	80%	<	83%	**10**	**3**	**30%**	**Fallido**	**10**	**8**	**80%**	**Aceptable**
Grado de cumplimiento de los proyectos establecidos para mitigar los riesgos de Seguridad de la Información	=	100%	>=	86%	<	86%	**15**	**2**	**13%**	**Fallido**	**15**	**14**	**93%**	**Aceptable**
Grado de cumplimiento de las medidas	=	100%	>=	75%	<	75%	**40**	**30**	**75%**	**Aceptable**	**40**	**40**	**100%**	**Correcto**
Número de empleados que se encuentran concientizados, es decir los que realizaron el curso de concientización virtual y rindieron su respectivo examen	=	100%	>=	70%	<	80%	**47**	**20**	**43%**	**Fallido**	**47**	**47**	**100%**	**Correcto**
Número de incidentes recurrentes que fueron detectados y aprendidos	=	100%	>=	95%	<	95%	**60**	**40**	**67%**	**Fallido**	**60**	**57**	**95%**	**Aceptable**

4.3 Resultados de los Indicadores

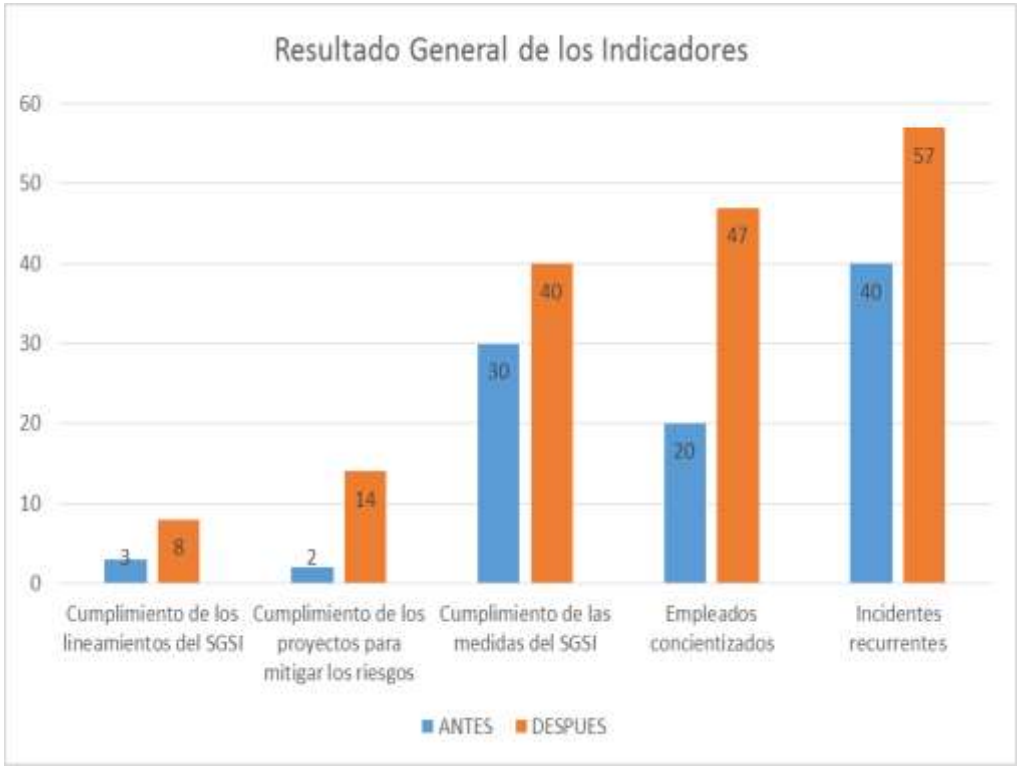


Figura 8 Resumen de indicadores

Resultado:

Establecer los lineamientos que soporten la implementación y mantenimiento del Sistema de Gestión de la Seguridad de la Información, en adelante "SGSI", en la entidad, garantizando la operatividad y efectividad de los Órganos u Oficinas del organismo e imagen de la organización, de acuerdo a la medición del indicador se evidencia que tiene un resultado aceptable.

Permitir a los trabajadores y terceros identificar y monitorear permanentemente los posibles riesgos de seguridad de la información relevantes para la entidad.

Definir, difundir y monitorear las medidas de seguridad de la información necesarias para el cumplimiento regulatorio de leyes, reglamentos, políticas y/o acuerdos con terceros vigentes relacionados a seguridad de la información.

Capacitar y sensibilizar permanentemente a los trabajadores y terceros con respecto a su responsabilidad para mantener y asegurar la seguridad de la información en la entidad.

Permitir a los trabajadores y terceros detectar, informar y gestionar eventos de seguridad de la información que puedan afectar la confidencialidad, disponibilidad e integridad de la información de la entidad.

Un aspecto muy importante también fue el de haber concientizado a los trabajadores lo cual importante que es la seguridad, que se deben cumplir las normas y políticas establecidas, logrando incrementar la eficiencia de la productividad de los trabajadores y por el bien de la institución.

Finalmente se puede determinar que en términos generales se logró la optimización de los recursos informáticos garantizando la confidencialidad integridad y disponibilidad de la información.

CAPÍTULO V

PROPUESTA DE INVESTIGACIÓN

5.1 Alcance del SGSI

Para la implementación, control, mantenimiento y la mejora continua al SGSI, la UGEL01 debe establecer los siguientes pasos:

a. Se debe identificar y clasificar de forma adecuada todos los activos informáticos tanto software como hardware asociándolos a la documentación respectiva.
b. Evaluar los posibles riesgos que pueden sufrir los activos informáticos por daño o pérdida de los mismos.
c. Seleccionar y aplicar los adecuados controles con el fin de minimizar los riesgos posteriormente gestionar los riesgos inaceptables.
d. Monitorear, dar continuidad y mejora continua a los controles relacionados a los activos informáticos en la UGEL01.

Para que la implementación del SGSI nos garantice la protección adecuada de los activos de informáticos de la UGEL01, en necesario que los pasos descritos anteriormente se ejecuten de forma permanente, con el fin de identificar algún comportamiento anómalo pudiendo identificar adecuadamente cambios en los riesgos.

5.1.1 Identificar los requisitos para la seguridad de los activos informáticos

Es importante iniciar la identificación adecuada de los requisitos para la seguridad de los activos informáticos fundamentándome en un contexto global basado en los objetivos generales, la estrategia de lineamiento, su tamaño y distribución geográfica de la organización.

A partir de esta información global, pasamos a identificar, en consecuencia, los requisitos del SGSI a través de:

a. La identificación adecuada de los activos informáticos con su valoración.
b. Identificar la carencia de la UGEL01 para procesar y almacenar la información.
c. La disposición legal, normativa y contractual.
d. Los requisitos de las áreas interesadas.

Llevar a cabo una evaluación metódica y análisis de los riesgos:

a. Las amenazas de seguridad constante a los activos informáticos.
b. Las causas de vulnerabilidad ante la posibilidad de que una advertencia de seguridad se materialice.
c. El poder de impacto de cualquier incidente de seguridad sobre los activos informáticos.

   d. Actualmente, ISO 27001 únicamente hace mención a la necesidad de identificar adecuadamente los riesgos relacionados a la falta de confidencialidad, integridad y disponibilidad de la información, después de realizar el análisis de riesgo a las consecuencias y la probabilidad de que ocurran, en consecuencia se debe cuantificar el riesgo. Asimismo se deberá definir al propietario del riesgo para su posterior gestión..

El gasto en controles de seguridad pertinentes debería ser proporcional al impacto calculado para el negocio y en base a la percepción de que el riesgo se materialice.

5.1.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Para llevar a cabo y gestionar un sistema de gestión de seguridad de la información en base a la ISO 27001, utilizare el ciclo continuo PDCA (Planificar, Actuar, Verificar y Hacer).

PDCA es una metodología que usare para aplicar un mejor nivel de gestión a través de los controles para los procesos y actividades ya sean internas y externas, de tal manera que nos permitirá aplicar la adecuada solución al problema y establecer una adecuada estrategia de mejora continua.

Esquema Base del Sistema de Seguridad

+ Documento sobre el alcance del SGSI
+ Listado Maestro - Oficina de Sistemas
+ Plan de tratamiento de Riesgos
+ Política de Seguridad de la Información SGSI
+ SOA

+ ST-PT-001 Mantenimiento Preventivo a la Infraestructura Informática
+ ST-PT-002 Mantenimiento Correctivo a la Infraestructura Informática
+ ST-PT-003 Inventario de Recursos Informáticos
+ ST-PT-004 Creación, Modificación o eliminación de Cuentas de Active Directory
+ ST-PT-005 Alta o Baja de Cuentas de Correo Electrónico
+ ST-PT-006 Alta o Baja de Usuario de Telefonía IP
+ ST-PT-007 Instalación de Cableado estructurado de Voz y Datos
+ ST-PT-008 Instalación de Antivirus Institucional
+ ST-PT-009 Actualización y Monitoreo de Antivirus Institucional
+ ST-PT-010 Respaldo y restauración de la información
+ ST-PT-011 Sistema de seguridad de vigilancia
+ ST-PT-012 Almacenamiento de archivos en el Servidor

+ ST-FT-001 Programa anual de mantenimiento preventivo
+ ST-FT-002 mantenimiento preventivo
+ ST-FT-003 mantenimiento correctivo
+ ST-FT-004 Inventario de Recursos Informáticos
+ ST-FT-005 Gestión de Cuentas de Usuario
+ ST-FT-006 Cableado Estructurado
+ ST-FT-007 Instalación de Antivirus
+ ST-FT-008 Programa de respaldo de la información
+ ST-FT-009 Respaldo de la información
+ ST-FT-010 Préstamo de equipo informático
+ ST-FT-011 Registro de Contraseñas

+ ST-DO-001 Política de Antivirus
+ ST-DO-002 Acceso físico al Centro de Datos
+ ST-DO-003 Uso de los Servicios y Recursos Informáticos
+ ST-DO-004 Respaldo de la Información
+ ST-DO-005 Contraseñas para Usuarios de Dominio
+ ST-DO-006 Recursos Compartidos
+ ST-DO-007 Préstamo de equipo Informático
+ ST-DO-008 Auditoria Interna
+ ST-DO-009 Uso de medios de almacenamiento removibles
+ ST-DO-010 Uso del Correo Electrónico
+ ST-DO-011 Inventario de Recursos Informáticos
+ ST-DO-012 Uso del Internet
+ ST-DO-013 Propiedad de la Información
+ ST-DO-014 Política de Contraseña
+ ST-DO-015 Cableado Estructurado de Voz yo Datos

5.1.3 Fases de la Implementación del Sistema de Seguridad

5.1.3.1 Plan (planificar): establecer el SGSI.

En esta fase se definen los objetivos que debemos alcanzar, además el método para logarlos, se identifican y analizan las causas y consecuencias del problema para prevenir las posibles fallas de seguridad, se definen los indicadores de control, asimismo se definen las personas involucradas en el proyecto.

Es así que se plantean un conjunto de elementos que permiten definir mecanismos de planificación en los aspectos de seguridad en la UNIDAD DE GESTIÓN EDUCATIVA LOCAL 01, estos mecanismos están definidos en:

a. **ST-PT-001 Mantenimiento Preventivo a la Infraestructura Informática**
   Procedimiento que permitirá mantener en condición operativa y continuidad funcional la infraestructura informática de la UGEL Nº1
   Ver detalle en:
   ST-PT-001 Mantenimiento Preventivo a la Infraestructura Informática

b. **ST-PT-002 Mantenimiento Correctivo a la Infraestructura Informática**
   Establecer el procedimiento para la atención y corrección de fallas en la infraestructura informática.
   Ver detalle en:
   ST-PT-002 Mantenimiento Correctivo a la Infraestructura Informática

c. **ST-PT-003 Inventario de Recursos Informáticos**
   Mantener actualizado el inventario de Recursos Informáticos, así como el monitoreo a instalaciones de aplicaciones no autorizadas.
   Ver detalle en:
   ST-PT-003 Inventario de Recursos Informáticos

d. ST-PT-004 Creación, Modificación o eliminación de Cuentas del Directorio

Procedimiento que permite a los usuarios validarse en el dominio de la red, asimismo controlar el acceso a los recursos establecidos y compartidos en la UGEL Nº01.

Ver detalle en:

ST-PT-004 Creación, Modificación o eliminación de Cuentas de Active Directory

e. ST-PT-005 Alta o Baja de Cuentas de Correo Electrónico

Brindar una herramienta de colaboración, que permitirá el intercambio de información entre las diferentes instancias, Proveedores y usuarios de la UGEL Nº1.

Ver detalle en:

ST-PT-005 Alta o Baja de Cuentas de Correo Electrónico

f. ST-PT-006 Alta o Baja de Usuario de Telefonía IP

Proporcionar una herramienta, con la cual los usuarios puedan comunicarse vía telefónica con otras entidades a fin de cumplir con sus actividades propias asignadas por la UGEL Nº1.

Ver detalle en:

ST-PT-006 Alta o Baja de Usuario de Telefonía IP

g. ST-PT-007 Instalación de Cableado estructurado de Voz y Datos

Proporcionar a los usuario de la UGEL Nº1, el procedimiento adecuado para implementar un tendido de red para los servicios de voz y datos

Ver detalle en:

ST-PT-007 Instalación de Cableado estructurado de Voz y Datos

h. ST-PT-008 Instalación de Antivirus Institucional

Mantener Protegida la Red de Datos de la UGEL Nº1 ante posibles amenazas de Virus

Ver detalle en:

ST-PT-008 Instalación de Antivirus Institucional

i. **ST-PT-009 Actualización y Monitoreo de Antivirus Institucional**

Mantener actualizada la Firma de Virus en los equipos Portátiles y PC de escritorio, así como detectar y eliminar amenazas de Virus

Ver detalle en:

ST-PT-009 Actualización y Monitoreo de Antivirus Institucional

j. **ST-PT-010 Respaldo y Restauración de la Información**

Procedimiento diseñado para garantizar la disponibilidad, seguridad y confidencialidad de la información, mediante la gestión de respaldo de la información

Ver detalle en:

ST-PT-010 Respaldo y restauración de la información

k. **ST-PT-011 Sistema de seguridad de vigilancia**

Establecer los pasos y recomendaciones a seguir para monitorear y garantizar el funcionamiento correcto del sistema de vigilancia.

Ver detalle en:

ST-PT-011 Sistema de seguridad de vigilancia

l. **ST-PT-012 Almacenamiento de archivos en el Servidor**

Establecer recomendaciones a seguir al momento de guardar información en el servidor de archivos de la UGEL Nº1.

Ver detalle en:

ST-PT-012 Almacenamiento de archivos en el Servidor Ugel

5.1.3.2 Do (hacer): implementar y utilizar el SGSI.

Fase en donde se ejecuta las tareas planificadas como el plan de acción para la mejora, a fin de obtener información para el posterior análisis

Es así que se propone con esta investigación tener en cuenta un conjunto de políticas, que deberán ser seguidas por los actores involucrados y teniendo en cuenta los activos afectados, las políticas diseñadas se encuentran descritas como:

a. ST-DO-001 Política de Antivirus

Política de cumplimiento para que los equipos de cómputo se conecten a la red, para garantizar la detección y prevención oportuna de código malicioso mediante el uso del software antivirus

Ver detalle en:

ST-DO-001 Política de Antivirus

b. ST-DO-002 Acceso físico al Centro de Datos

Establecer parámetros de seguridad para el acceso al Centro de Datos donde se encuentra toda la plataforma de servidores y servicios como también los equipos de comunicación.

Ver detalle en:

ST-DO-002 Acceso físico al Centro de Datos

c. ST-DO-003 Uso de los Servicios y Recursos Informáticos

Delinear el uso adecuado de los equipos informáticos de la UGEL Nº1

Ver detalle en:

ST-DO-003 Uso de los Servicios y Recursos Informáticos

d. ST-DO-004 Respaldo de la Información

Asegurar que la información contenida en los diferentes servidores de la UGEL Nº1, se respalde, a través de sistemas de almacenamiento, cumpliendo con lo establecido en esta política, a fin de garantizar su identificación, protección, integridad y disponibilidad de la información.

Ver detalle en:

ST-DO-004 Respaldo de la Información

e. ST-DO-005 Contraseñas para Usuarios de Dominio

Política en la cual se define la creación de contraseñas seguras y la frecuencia de cambio de las mismas dentro de los sistemas y equipos de la UGEL Nº1.

Ver detalle en:

ST-DO-005 Contraseñas para Usuarios de Dominio

f. ST-DO-006 Recursos Compartidos

Describir las políticas bajo las cuales los usuarios, harán uso de los Recursos Compartidos

Ver detalle en:

ST-DO-006 Recursos Compartidos

g. ST-DO-007 Préstamo de equipo Informático

Describir las políticas bajo las cuales los usuarios, podrán solicitar el Préstamo de equipo Informático.

Ver detalle en:

ST-DO-007 Préstamo de equipo Informático

h. ST-DO-008 Auditoria Interna

Establecer lineamientos sobre las prácticas de auditoria y monitoreo sobre las computadoras, sistemas y redes de la UGEL Nº1

Ver detalle en:

ST-DO-008 Auditoria Interna

i. ST-DO-009 Uso de medios de almacenamiento removibles

Establecer normas para el uso adecuado de medios de almacenamiento extraíbles así como la importancia de la misma para asegurar la fuga de información

Ver detalle en:

ST-DO-009 Uso de medios de almacenamiento removibles

j. ST-DO-010 Uso del Correo Electrónico

Establecer políticas y términos para la utilización de correo electrónico institucional

Ver detalle en:

ST-DO-010 Uso del Correo Electrónico

k. ST-DO-011 Inventario de Recursos Informáticos

Mantener actualizado y llevar el control de los activos Informáticos de la UGEL Nº1.

Ver detalle en:

ST-DO-011 Inventario de Recursos Informáticos

l. **ST-DO-012 Uso del Internet**

Establecer normas que aseguren el buen funcionamiento del Internet

Ver detalle en:

ST-DO-012 Uso del Internet

m. **ST-DO-013 Propiedad de la Información**

Establecer que la información que se procese en cualquier dispositivo informático de la UGEL Nº1 es propiedad de la misma

Ver detalle en:

ST-DO-013 Propiedad de la Información

n. **ST-DO-014 Política de Contraseña**

Con esta política se logra establecer un formato estándar para la creación de contraseñas fuertes, así como establecer el periodo de vigencia de las mismas.

Ver detalle en:

ST-DO-014 Política de Contraseña

o. **ST-DO-015 Cableado Estructurado de Voz y/o Datos**

Establecer los lineamientos a las especificaciones técnicas para la gestión y ejecución del cableado estructurado de la red para los servicios de voz y datos.

Ver detalle en:

ST-DO-015 Cableado Estructurado de Voz y Datos

5.1.3.3 Check (verificar): monitorizar y revisar el SGSI.

Después de implantada la mejora planificada, en un periodo de prueba se verifica y se controla los resultados.

De acuerdo a las políticas fijadas, se han diseñado parámetros de control y seguimiento, de acuerdo a estándares, permitiendo establecer líneas de acción directa, las cuales están definidas en:

a. **ST-FT-001 Programa anual de mantenimiento preventivo**

Formato de Control del Programa anual de mantenimiento preventivo

Ver detalle en:

ST-FT-001 Programa anual de mantenimiento preventivo

b. **ST-FT-002 mantenimiento preventivo**

Formato de Control del mantenimiento preventivo

Ver detalle en:

ST-FT-002 mantenimiento preventivo

c. **ST-FT-003 mantenimiento correctivo**

Formato de Control del mantenimiento correctivo

Ver detalle en:

ST-FT-003 mantenimiento correctivo

d. **ST-FT-004 Inventario de Recursos Informáticos**

Formato de Control del Inventario de Recursos Informáticos

Ver detalle en:

ST-FT-004 Inventario de Recursos Informáticos

e. **ST-FT-005 Gestión de Cuentas de Usuario**

Formato para el de la creación de cuentas de usuarios

Ver detalle en:

ST-FT-005 Gestión de Cuentas de Usuario

f. **ST-FT-006 Cableado Estructurado**

Formato de control del cableado estructurado

Ver detalle en:

ST-FT-006 Cableado Estructurado

g. **ST-FT-007 Instalación de Antivirus**

Formato de control de la instalación del antivirus

Ver detalle en:

ST-FT-007 Instalación de Antivirus

h. ST-FT-008 Programa de respaldo de la información

Formato de control de información a respaldar.

Ver detalle en:

ST-FT-008 Programa de respaldo de la información

i. ST-FT-009 Respaldo de la información

Formato de control del respaldo de la información

Ver detalle en:

ST-FT-009 Respaldo de la información

j. ST-FT-010 Préstamo de equipo informático

Formato de control de préstamo de equipos informáticos

Ver detalle en:

ST-FT-010 Préstamo de equipo informático

k. ST-FT-011 Registro de Contraseñas

Formato de control de registro de contraseñas

Ver detalle en:

ST-FT-011 Registro de Contraseñas

5.1.3.4 Act (actuar): mantener y mejorar el SGSI.

Después de analizar y comparar los resultados del funcionamiento de las actividades y de comprobar que la mejora implantada la mejora obtuvo un resultado satisfactorio en la etapa de prueba se debe registrar, para la implantación de forma definitiva la mejora.

Al finalizar la cuarta fase, se vuelve a la primera fase periódicamente para evaluar nuevas mejoras a implantar, por ello se han planificado un conjunto de documentos que permitirán implementar acciones de mejora continua, las cuales se encuentran descritas en:

a. Documento sobre el alcance del SGSI

Este documento forma parte del SGSI de la UGEL Nº1, que pertenece al sector educación del Perú y describe los procesos y las actividades implicadas en el marco del SGSI. Para asegurar la comprensión de las actividades de la Unidad de Gestión Educativa Local Nº1, este documento también incluye una descripción detallada del perfil de la entidad

Ver detalle en:

Documento sobre el alcance del SGSI

b. Listado Maestro - Oficina de Sistemas

Listado de todos los documentos creados para este SGSI

Ver detalle en:

Listado Maestro - Oficina de Sistemas

c. Plan de tratamiento de Riesgos

Salvaguardas para el tratamiento de riesgos

Ver detalle en:

Plan de tratamiento de Riesgos

d. Política de Seguridad de la Información del SGSI

Política se seguridad para la implementación del SGSI

Ver detalle en:

Documento de la política del SGSI

e. SOA

Declaración de la aplicabilidad SOA

Ver detalle en:

SOA

5.2 Análisis de Riesgos

5.2.1 Metodología

Durante la ejecución del proyecto se utilizará una metodología específica para cada una de las diferentes fases y etapas del mismo, las cuales aseguran que se contemple la totalidad de los aspectos relevantes para cada componente de revisión. La relación de metodología utilizada y el alcance de las mismas de resume a continuación:

Cuadro 3

Relación de metodología y alcance

NOMBRE	ALCANCE
MAGERIT	Metodología con el cual permite desarrollar un modelo de seguridad, lo que involucra el diseño de políticas y normas de seguridad.
COBIT5	Brinda una guía práctica de seguridad, con el fin de ayudar a las empresas a reducir sus riesgos aplicando una adecuada administración de seguridad.
ISO 27001	Estándar que propone el uso de los 11 objetivos de control que permiten realizar el diagnóstico de seguridad de la información.
ISO 17799	Esta norma permitirá realizar el análisis de riesgos mediante los pasos que brinda ISO, donde el principal estudio se hace en los activos de las empresas.

5.3 Desarrollo del análisis de riesgos

5.3.1 Identificación de los activo de la Ugel Nº 01

La identificación y clasificación de los activos de la Ugel, permitió que el alcance del SGSI considere la diferente clasificación de activos como:

a. Sistemas de Información
b. Licencias de software
c. Activos físicos
d. Servicios implementados
e. Personal de usuarios
f. Bienes Intangibles

5.3.2 La valoración de los activos y el establecimiento de dependencias entre activos

Se asigna valores a los activos, estos valores representan la importancia de los activos para la organización. La valoración escala podría ser una distinción entre bajo, medio y alto, o en más detalle: insignificante - baja - media - alta - muy alta. Se identificará las dependencias de los activos del resto de activos, ya que esto puede influir en los valores de los activos, además ayudará en la identificación de las amenazas relevantes y particularmente vulnerables.

5.3.3 Evaluación de amenazas

Se listaron los factores de riesgo relevantes a los pueden verse sometidos cada uno de los activos arriba nombrados. Evaluar la probabilidad de las amenazas, es decir la frecuencia de la amenaza (la frecuencia con que podría ocurrir, según la experiencia, las estadísticas, etc.). Las medidas de la probabilidad de las amenazas que ocurren en una escala, tales como alta, media o baja o en más detalle: Bajo, Poco Probable, Media, Altamente Probable, Casi Seguro.

5.3.4 Descripción de Consecuencias y Salvaguardas

Descripción de consecuencias y salvaguardas: se generó una descripción de las consecuencias que podría sufrir la Ugel Nº 01 si los activos son afectados por sus respectivas amenazas, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en qué grado son efectivas estas medidas.

5.3.5 Evaluación de la vulnerabilidad

Identificación de debilidades en el ambiente físico, la organización, procedimientos, personal, gestión, administración, hardware, software o comunicaciones entre equipos, que puede ser explotado por una fuente de amenaza para causar daño a los activos. Evaluar la gravedad de las vulnerabilidades es, en otras palabras, la facilidad con que pueden ser explotadas, utilizando una escala de alta, media y baja.

5.3.6 Evaluación de Riesgos

Identificar y evaluar los riesgos a los que los activos están expuestos, con el fin de seleccionar la seguridad apropiada y justificada. Los riesgos son una función de los valores de los activos, la probabilidad de amenazas que ocurre a causa de los impactos adversos potenciales de negocio, la facilidad de explotación de las vulnerabilidades de las amenazas identificadas, así como cualesquier inseguridad existente o todo lo que podría reducir el riesgo.

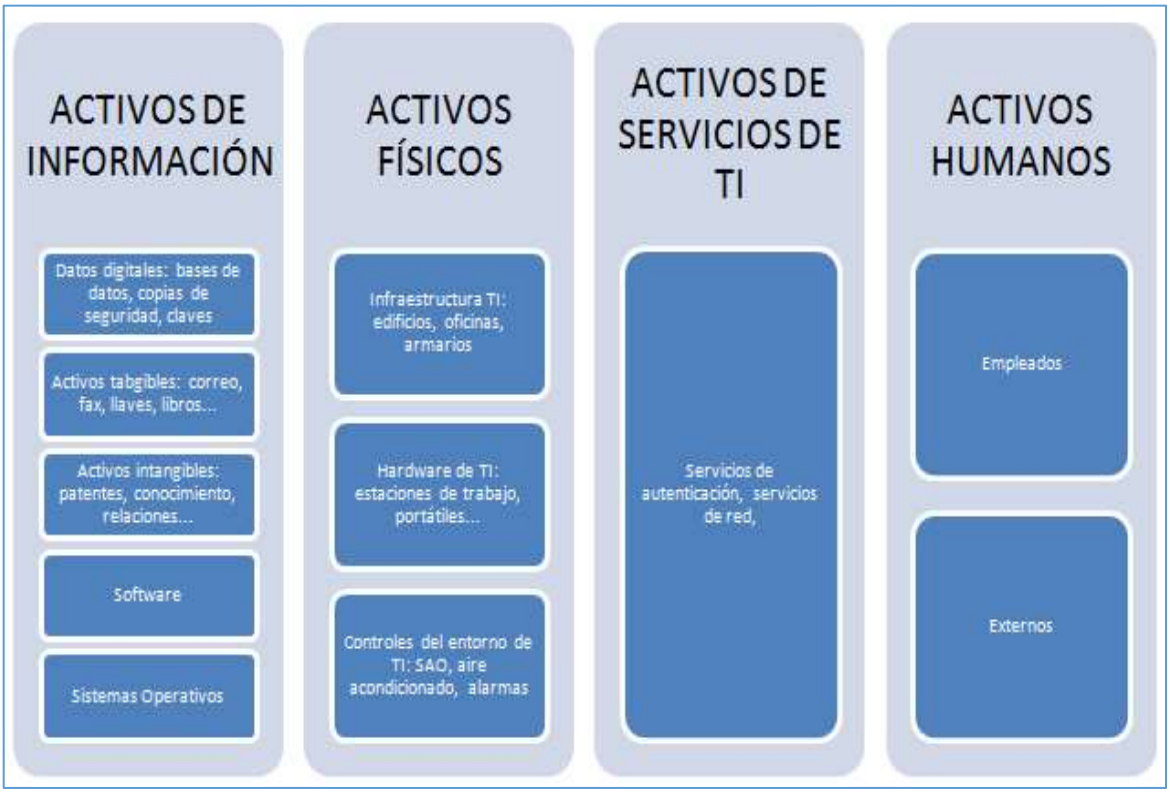
5.4 Activos

Se presentan los distintos Activos reconocidos en la Ugel Nº 01 **ISO 27001** Una de las primeras actividades necesarias para implantación de la norma ISO 27001 en una empresa es realizar una relación de recursos que recopile cuáles son los activos más importantes de la empresa. Debe identificarse el conglomerado de activos de la información, comprendiendo un activo como todo aquello que represente valor para la empresa. Estos activos son aquellos que quedan encasillados dentro de los procesos de selección para la determinación del alcance.

Un recurso vinculado con la seguridad de la información, se relaciona con cualquier información o sistema vinculado con el procedimiento de la misma que sea importante para la empresa. Todos los activos deben estar definidos, elaborando y conservando un inventario con los más relevantes. Activos de información, bases de datos, documentos, manuales, software, hardware, transacciones equipos de comunicaciones, servidores informáticos y de comunicaciones, ventajas importantes como por ejemplo calefacción, luminosidad, energía y aire acondicionado, los responsables que son quienes crean, divulgan y destruyen información. Esta se clasifica de la siguiente manera:

Cuadro 4

Clasificación de los activos



5.4.1 Activos encontrados en la Ugel Nº 01

A continuación se presentan los distintos Activos reconocidos en la Ugel Nº 01, asignando un valor a la importancia que tienen en la organización, ponderada en una escala del 1 al 5. Esta importancia es un valor subjetivo que refleja el nivel de Impacto que puede tener la Entidad si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos

Cuadro 5

Activos y sus Dependencias

DEPENDENCIAS	
BASE DE DATOS DE ERP	Data center
	Electricidad
	Red de Datos
	Servidor Data
	Windows Server 2008
	SQL server 2008
	Software Epicor 9.7
	Personal de Sistemas
	Consultores

DEPENDENCIAS	
INFORMACION DE FILES (PLANOS DE TODOS LOS PROYECTOS REALIADOS)	Data center
	Electricidad
	Red de Datos
	Servidor Files
	CenToS
	Personal de Sistemas
	Internet

DEPENDENCIAS	
BASE DE DATOS DE TELEFONIA IP	Data center
	Electricidad
	Red de Datos
	Servidor Telefonía IP
	CenToS
	Personal de Sistemas
	Personal Conectiva

DEPENDENCIAS	
INTRANET DE LA EMPRESA	Data center
	Electricidad
	Red de Datos
	Servidor Data
	Personal de Sistemas
	Personal Conectiva

DEPENDENCIAS

INFORMARMACION DE LIBROS CONTABLES	Data center
	Electricidad
	Red de Datos
	Servidor Telefonía IP
	CenToS
	Personal de Sistemas
	Personal Conectiva

DEPENDENCIAS

SERVIDOR DE BACKUP (veritas)	Data center
	Electricidad
	Red de Datos
	Personal de Sistemas

Tabla 8

Valoración del Impacto de Activos

VALORACIÓN DEL IMPACTO DE ACTIVOS										
		C		D			I			
DOM	ACTIVO	C1	C2	D1	D2	D3	I1	I2	VALOR	RIESGO
U	DATA CENTER	2	1	3	4	5	3	3	21	1638
U	AREAS DE SISTEMAS	1	2	1	2	3	2	2	13	468
COM	RED DE DATOS	5	5	1	2	3	5	5	26	1274
HW	SRVDATA	2	3	2	3	4	5	5	24	936
HW	SRVFILES	1	2	2	3	5	4	4	21	960
SW	SISTEMAS OPERATIVOS	1	1	3	3	3	3	3	17	459
SW	SISTEMA APLICATIVOS	1	1	2	3	4	4	4	19	722
S	INTERNET	1	1	1	2	3	4	4	16	784
S	FLUIDO ELECTRICO	1	1	2	2	4	5	5	20	440
OR	PERSONAL SISTEMAS	2	2	3	4	5	3	3	22	638
D	BASE DE DATOS DE ERP	4	5	2	3	5	4	4	27	1539
D	INFORMACION DE FILES (PLANOS DE TODOS LOS PROYECTOS REALIZADOS)	2	4	2	3	5	5	5	26	1820
D	BASE DE DATOS DE TELEFONIA IP	2	3	2	3	4	3	3	**20**	780
D	INTRANET (Unidad compartida)	4	5	4	5	5	5	5	**33**	2211
D	INFORMARMACION DE LIBROS CONTABLES	4	5	3	5	5	5	5	**32**	1760
D	BACKUP (VERITAS)	5	5	5	5	5	5	5	**35**	2310

Cuadro 6

Categorización de los Activos

CATEGORIAS	
[OR]	Personal.
[U]	Ubicación física.
[COM]	Red de Comunicaciones.
[HW]	Hardware.
[SW]	Software.
[S]	Servicios.
[D]	Datos-Información

Cuadro 7

Ámbitos de Probabilidades

AMBITOS	
C1	¿Que impacto tendría la divulgación de Información internamente?
C2	¿Que impacto tendría la divulgación de Información externamente?
D1	Información no disponible por 1 dia
D2	Información no disponible 1 semana
D3	Información no disponible 2 semanas
I1	¿Que impacto tendría la perdida de la Información? Sin que esta se pueda recuperar

Cuadro 8

Estimación de Impacto

IMPACTO	
0	No aplica
1	Insignificante
2	Baja
3	Media
4	Alta
5	Muy Alta

5.4.2 Valorización del Riesgo en Activos

Tabla 9
Data Center

DATA CENTER				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Condiciones inadecuadas de temperatura y/o humedad	21	5	3	315
Daños por agua	21	5	3	315
Corrupción o destrucción de la información	21	5	2	210
condiciones pesimas por degradación de los soportes de almacenamiento de la información	21	4	2	168
Errores del administrador	21	3	3	189
incidentes de falla por mantenimiento / actualización de equipos (hardware)	21	3	3	189
Corte del suministro eléctrico (apagones)	21	3	3	189
Interrupción de servicios de comunicaciones	21	3	1	63
			TOTAL	**1638**

Tabla 10
Área de sistemas

AREAS DE SISTEMAS				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Acceso no autorizado a personal que no sea del area.	13	3	2	78
Oficina sin señalizaciones	13	3	1	39
Infraestrucutra poco segura	13	3	1	39
Cables Expuestos	13	3	2	78
Incendios	13	2	3	78
Muebles inflamables	13	3	2	78
Robo / Hurto de información electrónica por personal del area	13	3	2	78
			TOTAL	**468**

Tabla 11
Red de datos

RED DE DATOS				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Acceso a la red por personal no autorizado	26	4	2	208
Virus, troyanos, spyware	26	4	1	104
Phishing	26	4	1	104
Correo electronico malicioso	26	4	3	312
Mala configuración del acceso inalambrica por encontrarse expuesta	26	3	1	78
Acceso no autorizado a la Red de datos	26	4	3	312
Difusión de software dañino	26	3	2	156
			TOTAL	**1274**

Tabla 12

Srvdata

SRVDATA				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado (aprovechando una debilidad)	24	3	1	72
incidentes por falla en el mantenimiento / actualización de equipos (hardware)	24	3	1	72
falta de recursos disponibles	24	4	2	192
Abuso de privilegios de acceso	24	4	2	192
incidentes por antivirus / actualización de equipos (software)	24	3	1	72
Errores del administrador	24	3	1	72
Corrupción o destrucción de la información	24	4	2	192
Robo / Hurto de información	24	3	1	72
			TOTAL	**936**

Tabla 13

Srvfiles

SRVFILES				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado (aprovechando una debilidad)	24	3	1	72
incidentes por falla en el mantenimiento / actualización de equipos (hardware)	24	4	1	96
falta de recursos disponible	24	4	1	96
Abuso de privilegios de acceso	24	3	1	72
incidentes por antivirus / actualización de equipos (software)	24	3	1	72
Errores del administrador	24	3	1	72
Corrupción o destrucción de la información	24	4	2	192
Robo / Hurto de información	24	4	3	288
			TOTAL	**960**

Tabla 14

Sistemas Operativos

SISTEMAS OPERATIVOS				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Errores de los usuarios	17	3	0	0
Corrupción o destrucción de la información	17	2	1	34
Mal manejo de sistemas y herramientas	17	2	0	0
Errores de mantenimiento / actualización de programas	17	1	0	0
Virus, troyanos, spyware	17	3	2	102
Phishing	17	4	2	136
Correo electronico malicioso	17	4	2	136
Robo / Hurto de información electrónica	17	3	1	51
			TOTAL	**459**

Tabla 15

Sistemas aplicativos

SISTEMA APLICATIVOS				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Errores de los usuarios	19	2	2	76
Corrupción o destrucción de la información	19	2	1	38
Mal manejo de sistemas y herramientas	19	2	1	38
Vulnerabilidades de los programas	19	3	2	114
Virus, troyanos, spyware	19	3	1	57
Phishing	19	3	2	114
Correo electronico malicioso	19	3	3	171
Robo / Hurto de información electrónica	19	3	2	114
			TOTAL	**722**

Tabla 16

Internet

INTERNET				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado al internet	16	3	2	96
Difusión de software dañino	16	2	0	0
Corrupción dibulgacion o destrucción de la información	16	2	1	32
Mal manejo de sistemas y herramientas	16	1	0	0
Análisis de tráfico	16	1	0	0
Incendios, Riadas, terremotos, rayos	16	3	2	96
Transmisión de contraseñas por teléfono, correo	16	4	5	320
Utilización de programas no autorizados / software 'pirateado'	16	4	3	192
Robo / Hurto de información electrónica	16	3	1	48
			TOTAL	**784**

Tabla 17

Fluido eléctrico

FLUIDO ELECTRICO				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado a tableros o llaves electricas	20	2	2	80
Ataque destructivo	20	3	1	60
Sobrecarga eléctrica	20	3	1	60
Averia de corriente (apagones)	20	3	1	60
Incendios	20	3	2	120
Robo / Hurto de información electrónica	20	3	1	60
			TOTAL	**440**

Tabla 18

Personal sistemas

PERSONAL SISTEMAS				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Capacidades para el manejo de sistemas y herramientas	22	2	0	0
Corrupción o destrucción de la información	22	2	1	44
Utilización de programas no licenciados	22	1	0	0
Manejo inadecuado de datos críticos	22	1	0	0
Mala administracion de creacion de contraseñas de acceso	22	3	2	132
Sobrepasar autoridades	22	4	2	176
perdida de dispositivos de almacenamiento	22	5	2	220
Robo / Hurto de información electrónica	22	3	1	66
			TOTAL	**638**

Tabla 19

Base de datos ERP

BASE DE DATOS DE ERP				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Acceso no autorizado a los backups DB	27	3	2	162
Alteración de la información en la DB	27	2	1	54
Corrupción o destrucción de la información	27	2	1	54
Modificación de la información	27	3	1	81
Corrupción o destrucción de la información	27	3	2	162
Averias en las restauraciones de los backups	27	5	3	405
Interupcion en las copias de Seguridad de la DB	27	5	4	540
Robo / Hurto de información electrónica	27	3	1	81
			TOTAL	**1539**

Tabla 20

Información de files (planos de los proyectos realizados)

INFORMACION DE FILES (PLANOS DE TODOS LOS PROYECTOS REALIZADOS)				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Errores de los usuarios	26	3	2	156
Inundacion, Sismo	26	3	2	156
Ataque físico y electrónico	26	4	3	312
Corrupción o destrucción de la información	26	3	2	156
Alteración de la información	26	2	2	104
malas condiciones para el almacenamiento de la información	26	3	2	156
Destrucción de información	26	4	2	208
Abuso de privilegios de acceso	26	4	3	312
Robo / Hurto de información electrónica	26	5	2	260
			TOTAL	**1820**

Tabla 21

Base de datos telefonía IP

BASE DE DATOS DE TELEFONIA IP				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado a telefonia IP	20	2	2	80
Alteración de la información	20	2	2	80
Corrupción o destrucción de la información	20	2	1	40
Modificación de la información	20	3	2	120
Corrupción o destrucción de la información	20	3	1	60
Averias en las restauraciones de los backups	20	3	2	120
Interupcion en las copias de Seguridad de la DB telefonia	20	3	2	120
Robo / Hurto de información electrónica	20	4	2	160
			TOTAL	**780**

Tabla 22

Intranet

INTRANET (Unidad compartida)				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado al intranet	33	4	2	264
Virus / Ejecución no autorizado de programas	33	3	2	198
Corrupción o destrucción de la información	33	3	2	198
Abuso de privilegios de acceso	33	4	3	396
Acceso no autorizado (aprovechando una debilidad)	33	3	2	198
Alteración de la información	33	3	2	198
ancho de banda no adecuado en relacion al uso	33	4	3	396
Sobrepasar autoridades	33	4	2	264
Robo / Hurto de información electrónica	33	3	1	99
			TOTAL	**2211**

Tabla 23

Información de libros contables

INFORMARMACION DE LIBROS CONTABLES				
AMENZAS	**IMPACTO**	**NIVEL DE AMENAZA**	**VULNERABILIDAD**	**NIVEL DE RIESGO**
Acceso no autorizado a los libros contables	32	4	2	256
Alteración de la información	32	3	1	96
Corrupción o destrucción de la información	32	3	1	96
Modificación de la información	32	3	2	192
Abuso de privilegios de acceso	32	3	1	96
Averias en las restauraciones de los backups	32	3	2	192
Interupcion en las copias de Seguridad	32	4	3	384
Robo / Hurto de información electrónica	32	3	2	192
Manipulación de la configuración	32	4	2	256
			TOTAL	**1760**

Tabla 24

Backup (veritas)

BACKUP (VERITAS)				
AMENZAS	IMPACTO	NIVEL DE AMENAZA	VULNERABILIDAD	NIVEL DE RIESGO
Acceso no autorizado a los backups	35	4	3	420
Alteración de la información	35	4	2	280
Corrupción o destrucción de la información	35	4	2	280
Modificación de la información	35	3	2	210
Abuso de privilegios de acceso	35	4	3	420
Averias en las restauraciones de los backups	35	4	2	280
Interupcion en las copias de Seguridad	35	4	3	420
Robo / Hurto de información electrónica	35	5	3	525
Manipulación de la configuración	35	3	3	315
falta de disponibilidad de recursos	35	4	3	420
			TOTAL	**2310**

5.4.3 Activos Ordenados según Riesgo

Tabla 25

DOM	ACTIVO	RIESGO
D	SERVIDOR DE BACKUP (IOMEGA)	**2310**
D	INTRANET DE LA EMPRESA	**2211**
D	INFORMACION DE FILES (PLANOS DE TODOS LOS PROYECTOS REALIADOS)	**1820**
D	INFORMARMACION DE LIBROS CONTABLES	**1760**
D	BASE DE DATOS DE ERP	**1539**
U	DATA CENTER	**1638**
COM	RED DE DATOS	**1274**
HW	SRVFILES	**960**
HW	SRVDATA	**936**
D	BASE DE DATOS DE TELEFONIA IP	**780**
S	INTERNET	**784**
SW	SISTEMA APLICATIVOS	**722**
OR	PERSONAL SISTEMAS	**638**
U	AREAS DE SISTEMAS	**468**
SW	SISTEMA BASE 01	**459**
S	FLUIDO ELECTRICO	**440**

5.4.4 Plan de Riesgo

Tabla 26

Salvaguarda

SALVAGUARDA	PRESUESTO $	ENERO	FEB	MAR	ABRIL	MAYO	JUN	JUL	AGO	SET	OCT	NOV	DIC
Implemenatcion de una Politica de Seguridad consientizacion a personal de la empresa Politica de Gestion de Contraseñas Politica de Acceso fisico al Data center Politica de Uso del Internet	500												
Implementacion de Firewall (Hardware) Politicas de Copias de Segruidad Politica de Restauracion de Backups Politica de Actualizacion de SistemaOperativos Politica de deterctor de Incedios	2900												
Implementacion de un DLP (Software) Uso adecuado del correo electronico Capacitacion en deteccion de Virus en PC.	1800												
Capacitacio sobre el uso de sistemas Capacitacion en los Correos Spam Prestamos de equipos Informaticos	200												
Implementar un sistema detector de incendios Implementar un sistema detector de humo Tener los extintores Operativos	2800												
Contratar personal de seguridad implementar sistemas de Video vigilancia implementar sistemas detector de metales en puerta	2600												

5.4.5 Salvaguardas

Tabla 27

AMENAZAS	VULNERABILIDADES	SALVAGUARDAS
Manejo inadecuado de datos críticos, falta de capacitación sobre riesgos	Ausenca de mecanismos de autenticacion	Implemenatcion de una Politica de Seguridad consientizacion al personal , Politica de Contraseñas, Politica de control del acceso al Data center Politica de Uso del Internet
Inundacion, Sismo Abuso de privilegios de acceso Red cableada expuesta para el acceso no autorizado	Configuracion de firewall Copias de respaldo inexistentes no hay un control con los backup	Implementacion de Firewall (Hardware) Politicas de Copias de Seguridad Politica y procedimiento de Restauracion de Backups Politica y procedimiento para la Actualizacion de SistemaOperativos , Politica procedimiento para el uso del detector de Incedios
Acceso no autorizado (aprovechando una vulnerabilidad)	Ausencia de mecanismo para prevencion de fuga de informacion	Implementacion de un DLP (Software) Uso adecuado del correo electronico Capacitacion en deteccion de Virus en PC.
Utilización de programas no autorizados / software 'pirateado'	falta de capacidades sobre normatividad y reglamentacion adecuada	Capacitacio sobre el uso de sistemas Capacitacion en los Correos Spam Prestamos de equipos Informaticos
Incendio por el mismo trabajo	ausencia de sistema deteccion de incendios	Implementar un sistema detector de incendios Implementar un sistema detector de humo Tener los extintores Operativos
El control de ingreso y salida del personal, camara obsoletas para vigilancia	falta de disposiciones y directivas no institucionales	Contratar personal de seguridad implementar sistemas de Video vigilancia implementar sistemas detector de metales en puerta

CONCLUSIONES

De acuerdo a los objetivos planteados, puedo detallar las siguientes conclusiones

a. Se logró diseñar un SGSI garantizando la operatividad y efectividad e imagen de la organización, se establecer el control adecuado de incidentes de seguridad. Representando el 80% con un resultado ACEPTABLE:

b. Se pudo determinar el alcance del cubrimiento a los activos críticos, los trabajadores y terceros tengan la capacidad de identificar y monitorear permanentemente los posibles riesgos, se logró el objetivo con un 93% de efectividad.

c. Se logró identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad, definir, difundir y monitorear las medidas de seguridad de la información con una efectividad del 100% minimizando los riesgos a los activos de la información.

d. Se logró las capacidades y sensibilización para que los trabajadores puedan controlar los incidentes de seguridad.

e. Se logró el objetivo de asegurar, que los incidentes de seguridad de información recurrentes sean solucionados a la brevedad. Asimismo, fortalecer el conocimiento del equipo de Seguridad de Información ante estos incidentes.

f. Se logró minimizar los riesgos asociados a los activos informáticos y se ha cumplido con el objetivo general.

RECOMENDACIONES

Al finalizar la investigación y al cumplir los propósitos de investigación planteados, el investigador se permite realizar las siguientes recomendaciones en espera de que sean consideradas para el desarrollo de futuros estudios parecidos:

a. Revisar y actualizar periódicamente el Anexo 2, donde se encuentra los controles de la norma ISO/IEC 27001, de acuerdo a lo que se dispone en seguridad de la información, lo que permitirá clasificar y diagnosticar los activos de información.

b. Verificar y actualizar permanentemente los compromisos y responsabilidades de seguridad, a fin de generar concientización sobre la SGSI.

c. Revisar y aplicar mejoras continuas, garantizando la sostenibilidad y continuidad del SGSI, lo que permitirá optimizar los procesos.

d. Se sugiere a la Universidad Señor Sipán estimular a los estudiantes a ejecutar investigaciones de este tipo, con el propósito de construir un perfil más metódico aplicando directamente lo aprendido durante la carrera de ingeniería hacia el desarrollo de sistemas de seguridad para empresas e instituciones.

e. A los estudiantes de la Universidad Señor Sipán que en próximos trabajos vinculados con el tema, se consideren los resultados del presente estudio como referencia para socavar en el desarrollo y creación de sistemas de seguridad de la información. De igual modo, se debe tomar en cuenta como eje principal el análisis con base en entrevistas, pues el mismo implica un amplio espectro para el logro de los objetivos concretos.

REFERENCIAS

Aguirre, M. D. (30 de Octubre de 2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* Lima, Lima , Perú : Pontificia Universidad Católica del Perú .

Aguirre, R. Z. (octubre de 2015). Estudio para la implementacion del sistema de gestión de seguridad de la informacion para la Secretaria de Educacion Departamental de Nariño basado en la NORMA ISO/IEC 27001. *estudio para la implementacion del sistema de gestion de seguridad de la informacion para la Secretaria de Educacion Departamental de Nariño Basado en la Norma ISO/IEC 27001*. Bogotá, Bogotá, Colombia: Universidad Nacional Abierta y a Distancia – Unad Escuela Ciencias Básicas, Tecnología e Ingeniería.

Barrera, J. H. (2000). *Metodologia de investigacion holistica.* Mexico: SYPAL.

Céspedes, M. A. (diciembre de 2016). "Implementación de la Norma Técnica Peruana 27001:2014 alineado a COBIT 5 con el desarrollo de un software de aplicación para automatizar el proceso de gestión de seguridad de la información de la Corte Superior de Justicia de Lambayeque". *"Implementación de la norma técnica peruana 27001:2014 alineado a cobit 5 con el desarrollo de un software de aplicación paraautomatizar el proceso de gestión de seguridad de la información de la corte superior de justicia de lambayeque*. Lambayeque, Chiclayo , Perú : Universidad Señor de Sipan.

Chávez, M. (2007). *Introducción a la investigación* . Maracaibo, Venezuela: Gráficas González .

Guba, E. (1981). *Criterios de credibilidad en la investigación naturalista". En GIMENO SACRISTÁN, J.y PÉREZ GÓMEZ, A. La Enseñanza: su teoría y su práctica.* . Madrid: Akal.

Hernández, R. F. (2010). Metodología de la Investigación (5ª Ed.). En R. F. Hernández, *Metodología de la Investigación* (pág. 500). Mexico: McGraw Hill Educación.

Hernández, R. F. (2013). *Metodología de la Investigación.* México : Macgrau Hill .

ISO/IEC 27000. (2013). *Sistema de Gestión de la Seguridad de la Información* . Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf: http://www.iso27000.es/download/doc_sgsi_all.pdf

Maya, P. A. (06 de junio de 2006). Plan de Implementación del SGSI Basado en la Norma Iso 27001:2013. *Plan de Implementación del Sgsi Basado en la NORMA ISO 27001:2013*. Cataluña, España: Universidad Autónoma de Barcelona.

Moscaiza, M. O. (febrero de 2018). Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013. *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013*. Lima, Lima, Perú: Universidad Peruana de Ciencias Aplicadas.

Tola, D. y. (2016). Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoría, aplicando La Norma ISO/IEC 27001". *Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*. Guayaquil, Ecuador: Facultad de Ingeniería en Electricidad y Computación Escuela Superior Politécnica del Litoral (ESPOL).

Torres, J. (24 de Mayo de 2016). *La ética en el ejercicio profesional* . Obtenido de Le ética en el ejercicio profesional : http://laeticaenelejercicioprofesional-jorge.blogspot.com/2016/05/codigo-etico-profesional-del-ingeniero.html

ANEXOS

ANEXO1

CUESTIONARIO BÁSICO BASADO EN LA APLICABILIDAD DEL SGSI

1. ¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?

   SI ____ NO ____

2. ¿Su computadora recibe mantenimiento de manera periódica?

   SI ____ NO ____

3. ¿Realiza copias de información (Backup) de su documentación diaria?

   SI ____ NO ____

4. ¿Qué procedimiento de control de acceso realiza al momento de ingresar a la computadora?

   - Ingreso de nombre de usuario y contraseña ____
   - Tarjeta inteligente ____
   - Lector de huellas dactilares ____
   - Ninguno ____

5. ¿Tiene conocimiento sobre el plan de inventario de equipos?

   SI ____ NO ____

6. ¿Tiene conocimiento sobre sistema para el control registros de incidentes?

   SI ____ NO ____

7. ¿Tiene conocimiento sobre un sistema para el control de préstamos de equipos?

   SI ____ NO ____

8. ¿Cuándo reporta un incidente o falla de su computadora, que tiempo se demoran en solucionar el incidente o arreglo de la misma?

   - 1 hora ____
   - 2 horas ____
   - 12 horas ____
   - 24 horas ____
   - Otros ____

9. ¿Ud. apaga o bloque su computadora cuando se mueve de su sitio o escritorio?

   SI ____ NO ____

10. ¿Con que frecuencia cambia su contraseña del equipo?

    - Nunca ____
    - Cada mes ____
    - Cada 3 meses ____
    - Cada 6 meses ____
    - Cada 12 meses ____

11. ¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?

    SI ____ NO ____

12. ¿Tiene alguna restricción para ingresar a los servicios de Internet?

    SI ____ NO ____

13. ¿Qué medida de seguridad o control aplica al momento de acceder a recursos compartidos en la red?

    - Ninguno ____
    - Nombre de usuario y contraseña ____

14. ¿Se lleva algún registro o bitácora de los incidentes de riesgo en cuanto al uso de los equipos y de la información de la Ugel01?

    SI ____ NO ____

ANEXO 2

CONTROLES DE LA ISO 27001

ISO 27001 POLITICA DE SEGURIDAD		
Información a Recaudar	*Controles*	*Evaluación*
La Ugel no cuenta con un documento de política de seguridad	La gerencia debe de aprobar un documento de política, esto se debe publicar y comunicar a todos los empleados y entidades externar relevantes	No cubierto
	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.	No cubierto
ISO 27001 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION		
Organización Interna		
Información a Recaudar	*Controles*	*Evaluación*
La gerencia cuenta con un apoyo mínimo en seguridad dentro de la Ugel Nº 01.	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la información.	Limitadamente Cubierto
	El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.	
No existe coordinación en actividades de seguridad en ninguna parte de la organización	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes	No cubierto
La organización no cuenta con una alta confidencialidad en sus activos de información	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.	Limitadamente Cubierto
No cuentan con personal asignado para la seguridad de la información	Se debe asignar de las responsabilidades de la seguridad de la información, claramente definidos para la protección de activos concretos y la realización de Procesos específicos de seguridad	Medianamente Cubierto
No existe contacto con grupos especializados en seguridad de la información	Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.	No Cubierto

Organización Externa		
Información a Recaudar	*Controles*	*Evaluación*
No realizan un análisis de riesgos que puedan perjudicar los activos de información de la Ugel Nº 01	Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.	No Cubierto
	Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.	No Cubierto
ISO 27001 GESTION DE LOS ACTIVOS		
Responsabilidad por los activos		
Información a Recaudar	*Controles*	*Evaluación*
No se encuentran claramente identificados todos los activos en la Ugel Nº 01.	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.	Limitadamente Cubierto
	Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de la organización.	
Clasificación de la información		
Información a Recaudar	*Controles*	*Evaluación*
No cuenta con una clasificación de activos en términos de valor, importancia.	La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.	No cubierto
ISO 27001 SEGURIDAD DE LOS RECURSOS HUMANOS		
Antes del empleo		
Información a Recaudar	*Controles*	*Evaluación*
No se cuenta con una documentación de roles y responsabilidades en seguridad de la información	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.	No cubierto
No se realiza ningún estudio de antecedentes ya que no hay un plan de estudio a nuevos empleados.	Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.	No cubierto
Existe un punto en el contrato donde especifica sus responsabilidades en la seguridad de la Ugel Nº 01.	Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.	Limitadamente Cubierto

Durante del empleo		
Información a Recaudar	*Controles*	*Evaluación*
La gerencia no permite que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.	La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.	No cubierto
No existe un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	No cubierto
ISO 27001 SEGURIDAD FISICA Y AMBIENTAL		
Áreas Seguras		
Información a Recaudar	*Controles*	*Evaluación*
Cuenta con perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.	Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.	Limitadamente Cubierto
No existen controles de entrada para personal autorizado.	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	No cubierto
No se aplica seguridad física en las oficinas, habitaciones y medios	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.	Limitadamente Cubierto
No cuentan con diseños de protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.	No cubierto
	Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.	
	Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.	

Seguridad del equipo		
Información a Recaudar	*Controles*	*Evaluación*
Los equipos están ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales y las oportunidades para el acceso no autorizado.	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	Limitadamente Cubierto
Los equipos se encuentran protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.	El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos. El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.	Limitadamente Cubierto
Los equipos son mantenidos correctamente para permitir su continua disponibilidad e integridad.	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.	Parcialmente cubierto
No se aplica seguridad al equipo fuera-dellocal tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.	Se debe aplicar seguridad al equipo fuera-dellocal tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.	No cubierto
Todos los ítems de equipo que contengan medios de almacenaje son chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.	Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.	Limitadamente Cubierto
Equipos, información o software no pueden ser sacados fuera de la propiedad sin previa autorización.	Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.	Parcialmente cubierto

ISO 27001 GESTION DE LAS COMUNICACIONES Y OPERACIONES		
Procedimiento y responsabilidades operacionales		
Información a Recaudar	*Controles*	*Evaluación*
Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.	
No se controlan los cambios en los medios y sistemas de procesamientos de la información.	Se deben de controlar los cambios en los medios y sistemas de procesamientos de la información.	
Planeación y aceptación del sistema		
Información a Recaudar	*Controles*	*Evaluación*
No se establecen los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas, tampoco se llevan a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.	Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.	
	Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.	No cubierto
Protección contra software malicioso y código móvil		
Información a Recaudar	*Controles*	*Evaluación*
No esta implementado controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.	No cubierto
Respaldo (back-up)		
Información a Recaudar	*Controles*	*Evaluación*
Se realizan copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.	Parcialmente cubierto

Gestión de seguridad de redes		
Información a Recaudar	*Controles*	*Evaluación*
No se tiene un mantenimiento en la arquitectura de redes. No se realizan modificaciones.	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.	No cubierto
No existe procedimientos para la gestión de medios removibles	Deben existir procedimientos para la gestión de medios removibles.	No cubierto
No se establecen los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.	Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.	Limitadamente Cubierto
	Se debe proteger la documentación de un acceso no autorizado.	No cubierto
Intercambio de información		
Información a Recaudar	*Controles*	*Evaluación*
Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.	Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.	No cubierto
Monitoreo		
Información a Recaudar	*Controles*	*Evaluación*
No se realizan monitores de eventos de seguridad de la información	Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.	No cubierto
	Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.	
	Se deben registrar las actividades del administrador y operador del sistema.	

ISO 27001 CONTROL DE ACCESO		
Requerimiento comercial para el control del acceso		
Información a Recaudar	*Controles*	*Evaluación*
No se tiene establecido, documentado y tampoco revisado la política de control de acceso en base a los requerimientos de seguridad y comerciales.	Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.	No cubierto
Gestión del acceso del usuario		
Información a Recaudar	*Controles*	*Evaluación*
No existe un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.	Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.	No cubierto
	Se debe restringir y controlar la asignación y uso de los privilegios.	
La asignación de claves se debe controlar a través de un proceso de gestión formal.	La asignación de claves se debe controlar a través de un proceso de gestión formal.	No cubierto
Responsabilidades del usuario		
Información a Recaudar	*Controles*	*Evaluación*
Los usuarios no siguen las buenas prácticas de seguridad en la selección y uso de claves.	Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.	No cubierto
No se asegura la protección apropiada al equipo desatendido	Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido	Limitadamente Cubierto
Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	No cubierto

Control de acceso a redes		
Información a Recaudar	*Controles*	*Evaluación*
No existe restricciones	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	No cubierto
Solo se autentifican con un usuario y clave	Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.	Limitadamente Cubierto
No existen restricciones en la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales.	Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales.	Limitadamente Cubierto
No se tiene implementado controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.	Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.	No cubierto
Control de acceso al sistema de operación		
Información a Recaudar	*Controles*	*Evaluación*
No se tiene centro en el acceso los servicios operativos mediante un procedimiento de registro seguro.	Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.	No cubierto
Los sistemas de manejo de claves son básicas y no son interactivas.	Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.	Limitadamente Cubierto
No hay restricción ni controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.	Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.	Limitadamente Cubierto

No se tiene control de sesiones.	Las sesiones inactivas deben cerrarse después de un período de inactividad definido.	No cubierto
Control de acceso a la aplicación e información		
Información a Recaudar	*Controles*	*Evaluación*
No hay restricciones en el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.	Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.	Limitadamente Cubierto
Computación móvil y tele-trabajo		
Información a Recaudar	*Controles*	*Evaluación*
No existe una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.	Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.	No cubierto
ISO 27001 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
Procesamiento correcto en las aplicaciones		
Información a Recaudar	*Controles*	*Evaluación*
El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.	El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.	Limitadamente Cubierto
ISO 27001 GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACION		
Reportes de evento y debilidades en la seguridad de la información		
Información a Recaudar	*Controles*	*Evaluación*
No se establece reporte de evento de la seguridad de información que está en respaldo de los canales gerenciales **.II.** No se realiza notaciones de apunte para los empleados.	Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.	Limitadamente Cubierto
	Se debe repetir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de la información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.	Limitadamente Cubierto

Gestión de incidentes y mejora en la seguridad de la información		
I. La empresa en la parte de gestión establecen un buen desempeño y el desarrollo de sus procesos son en menos tiempo posible esté buen manejo del pequeño sistema que utilizan. II .La empresa no maneja	Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	Limitadamente Cubierto
	Debe existir mecanismo para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.	Cubierto
	Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencias establecidas en la (s) jurisdicción (es) relevantes.	Limitadamente Cubierto

ANEXO 3

FORMATOS DEL ESQUEMA BASE DEL SISTEMA DE SEGURIDAD

MANTENIMIENTO PREVENTIVO A LA INFRAESTRUCTURA INFORMATICA

1. OBJETIVO

Establecer los mecanismos que permitan la ejecución de acciones orientadas a mantener en condiciones de operatividad y funcionalidad la infraestructura informática de la UGEL Nº1

2. ALCANCE

Este procedimiento aplica a todas las instalaciones y equipos informáticos para la realización de funciones propias de la UGEL Nº1

Se inicia desde la elaboración del calendario de mantenimiento preventivo hasta su ejecución y cumplimiento.

3. RESPONSABILIDADES

3.1. Responsable de Soporte Técnico

Es el responsable de elaborar el programa anual de mantenimiento preventivo a la Infraestructura Informática, ejecución del plan y llenado de registros correspondientes.

3.2. Responsable de la Oficina de Sistemas

Es el responsable de revisar y aprobar el programa anual de mantenimiento preventivo a la infraestructura Informática y verificar el cumplimiento del mismo.

4. DEFINICIONES Y ABREVIATURAS

4.1. Infraestructura Informática

Conjunto de programas y equipos que permiten mantener en operación las actividades que realiza la UGEL Nº1

4.2. Mantenimiento Preventivo

Son actividades necesarias para que el equipo opere de manera continua

4.3. Software

Equipamiento lógico o soporte lógico de un sistema informático

4.4. Hardware

Dispositivos y componentes físicos que realizan las tareas de entrada y salida de información en una computadora

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Elaboración de Programa Anual de Mantenimiento Preventivo

El Responsable de Soporte Técnico, es el encargado de elaborar a los 15 días de diciembre de cada periodo, el programa anual de mantenimiento preventivo, se deberá considerar los insumos a requerir para la ejecución del mismo.

La información del programa anual de mantenimiento preventivo, deberá ser actualizada en el Registro **ST-FT-001 Programa anual de mantenimiento Preventivo.**

6.2. Revisión de Programa anual de Mantenimiento Preventivo

El Jefe de la Oficina de Sistemas, es el encargado de revisar el programa anual de mantenimiento preventivo.

Si hay correcciones las envía al encargado de Soporte Técnico para las modificaciones correspondientes.

Si es conforme pasa a la siguiente actividad

6.3. Considerar materiales y equipos en el presupuesto anual de la Oficina de Sistemas

El jefe de la Oficina de Sistemas, considera los materiales y equipos necesarios para la realización de los trabajos de mantenimiento preventivo, el costo de materiales y/o equipos se deberá considerar en el presupuesto anual de la Oficina de Sistemas

6.4. Autorizar y liberar el Programa Anual de Mantenimiento Preventivo

El jefe de la Oficina de Sistemas, Autoriza y Libera el programa anual de mantenimiento Preventivo.

6.5. Envió de Reporte a Proveedor, para ejecución de mantenimiento preventivo a equipos arrendados

El encargado de Soporte Técnico envía un informe a los proveedores, indicando las fechas en las cuales se deberán ejecutar el mantenimiento preventivo a los equipos arrendados

6.6. Notificar a Responsables de Áreas, los trabajos a realizar

El responsable de Soporte Técnico, notifica con una semana de anticipación, por correo electrónico a los responsables de áreas, los trabajos a realizar de mantenimiento preventivo

En caso de haber algún impedimento para la realización del servicio, se coordinara una fecha oportuna.

6.7. Ejecuta Acciones de Mantenimiento Preventivo

El responsable de Soporte Técnico, realiza las actividades propias del mantenimiento preventivo, teniendo en cuenta las siguientes consideraciones

Para el caso de Software

6.7.1. El mantenimiento Preventivo a Software incluye:

6.7.1.1. Sistema Operativo, Desfragmentación de las unidades lógicas del Equipo y actualizaciones del Sistema Operativo, etc.

Para el caso de Hardware

6.7.2. El mantenimiento preventivo a Hardware incluye:

6.7.2.1. Equipo de Cómputo
6.7.2.2. Equipo de Comunicaciones
6.7.2.3. Periféricos
6.7.2.4. Teléfonos IP

6.8. Actualiza Información

El responsable de Soporte Técnico, captura la información en el registro **ST-FT-002 Mantenimiento preventivo a la infraestructura Informática.**

Fin de actividades

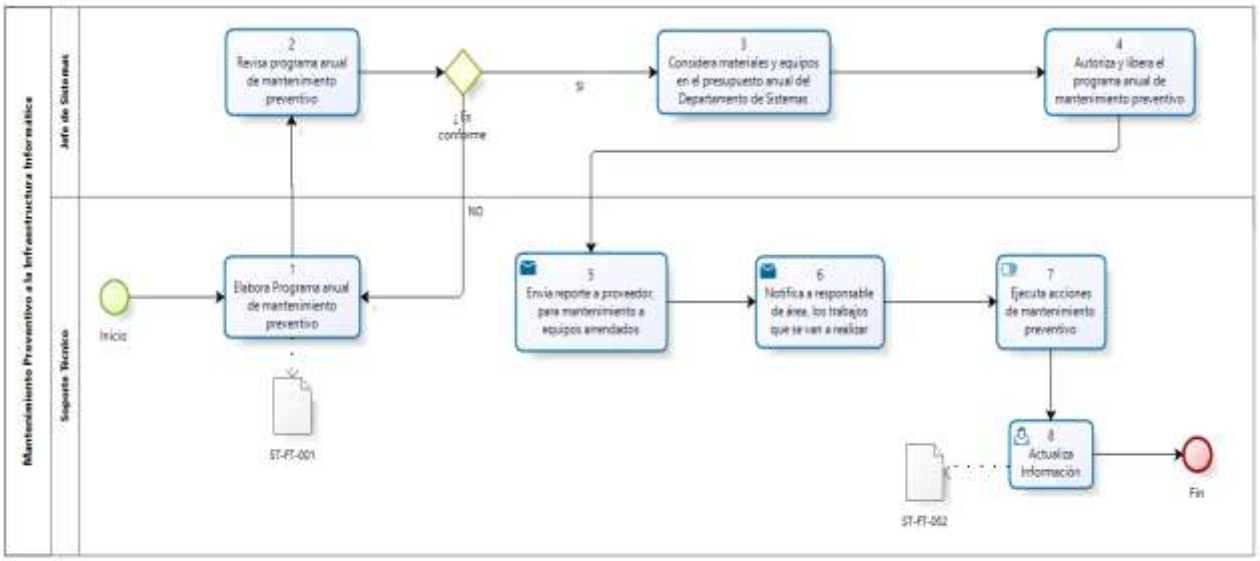
7. FORMATOS

7.1. ST-FT-001 Programa anual de Mantenimiento Preventivo a la Infraestructura Informática

7.2. ST-FT-002 Mantenimiento Preventivo a la Infraestructura Informática

8. ANEXOS

Diagrama de Flujo Mantenimiento Preventivo a la Infraestructura Informática



MANTENIMIENTO CORRECTIVO A LA INFRAESTRUCTURA INFORMATICA

1. OBJETIVO

Establecer el procedimiento para la atención y corrección de fallas en la infraestructura informática.

2. ALCANCE

Este procedimiento aplica a todas las instalaciones y equipos informáticos para la realización de funciones propias de La UGEL Nº1

Se inicia desde el reporte de falla por parte del usuario, el seguimiento y atención que se proporciona hasta la solución del problema y control de documentación.

3. RESPONSABILIDADES

3.1. Usuario

Es el responsable de comunicar a tiempo la falla presentada en su equipo informático asignado

3.2. Encargado de Soporte Técnico

Es responsable del cumplimiento de este procedimiento, así como la atención oportuna a las fallas presentadas en los diferentes equipos informáticos de la UGEL Nº1

3.3. Jefe de Sistemas

Es responsable de realizar las gestiones necesarias, para la elaboración de este procedimiento

4. DEFINICIONES Y ABREVIATURAS

4.1. Infraestructura Informática

Conjunto de programas y equipos que permiten mantener en operación las actividades que realiza la UGEL Nº1

4.2. Mantenimiento Correctivo

Son actividades necesarias para solucionar fallas o problemas existentes en los equipos informáticos.

4.3. Software

Equipamiento lógico o soporte lógico de un sistema informático

4.4. Hardware

Dispositivos y componentes físicos que realizan las tareas de entrada y salida de la información en una computadora

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Reportar Falla

El usuario es responsable de comunicar a la Oficina de Sistemas la falla en su equipo informático asignado

6.2. Recibir Información y atender solicitud de servicio

El Responsable de Soporte Técnico recibe información de la falla presentada y apertura una nueva solicitud de servicio informático, en el registro

ST-FT-003 Mantenimiento Correctivo a la Infraestructura Informática

6.3. Detectar causa del problema

El responsable de Soporte Técnico identifica la falla presentada en el equipo informático si puede repararlo, efectúa el mantenimiento correctivo, de lo contrario verifica si el equipo cuenta con contrato de servicio.

6.4. Realizar Mantenimiento Correctivo

El responsable de Soporte Técnico, una vez detectada la falla y sabiendo que es posible repararla, realiza las actividades de mantenimiento correctivo

6.5. Verificar si el equipo cuenta con contrato de servicio

El responsable de Soporte Técnico, verifica si el equipo que está presentando inconvenientes, cuenta con algún contrato de servicio.

Si cuenta con contrato, asigna informe a proveedor

De lo contrario, traslada el equipo a la Oficina de Sistemas para la revisión

6.6. Asignar Informe a Proveedor

El responsable de Soporte Técnico, una vez identificado que el equipo cuenta con contrato de servicio, asigna el informe al proveedor para que este deje operativo el equipo informático

6.7. Trasladar equipo informático a la Oficina de Sistemas

El Responsable de Soporte Técnico, traslada el equipo informático a la Oficina de Sistemas y deja un equipo de respaldo para que el usuario siga realizando sus actividades

6.8. Preparar informe Técnico

El responsable de Soporte Técnico, elabora un informe indicando los componentes o reparaciones que necesita el equipo informático

6.9. Gestionar Adquisición de Materiales y/o Reparación

El responsable del Departamento de Sistemas, realiza las gestiones de adquisición de materiales y/o reparación del equipo informático por un tercero

6.10. Retirar Componentes del Almacén Central

El responsable de Soporte Técnico, retira los componentes comprados del almacén central

6.11. Realizar Reparación y/o pruebas del equipo

El responsable de Soporte Técnico realiza la reparación del equipo y realiza pruebas para asegurar el correcto funcionamiento

6.12. Reinstalar el equipo

El responsable de Soporte Técnico, reubica el equipo en el área correspondiente

6.13. Actualizar Información

El responsable de Soporte Técnico una vez terminados los trabajos de reubicación del equipo, entrega al usuario un cuestionario para la evaluación en la atención del personal de Sistemas, hace firmar al usuario la conformidad del servicio y actualiza la información en el Registro

ST-FT-003 Mantenimiento Correctivo a la Infraestructura Informática

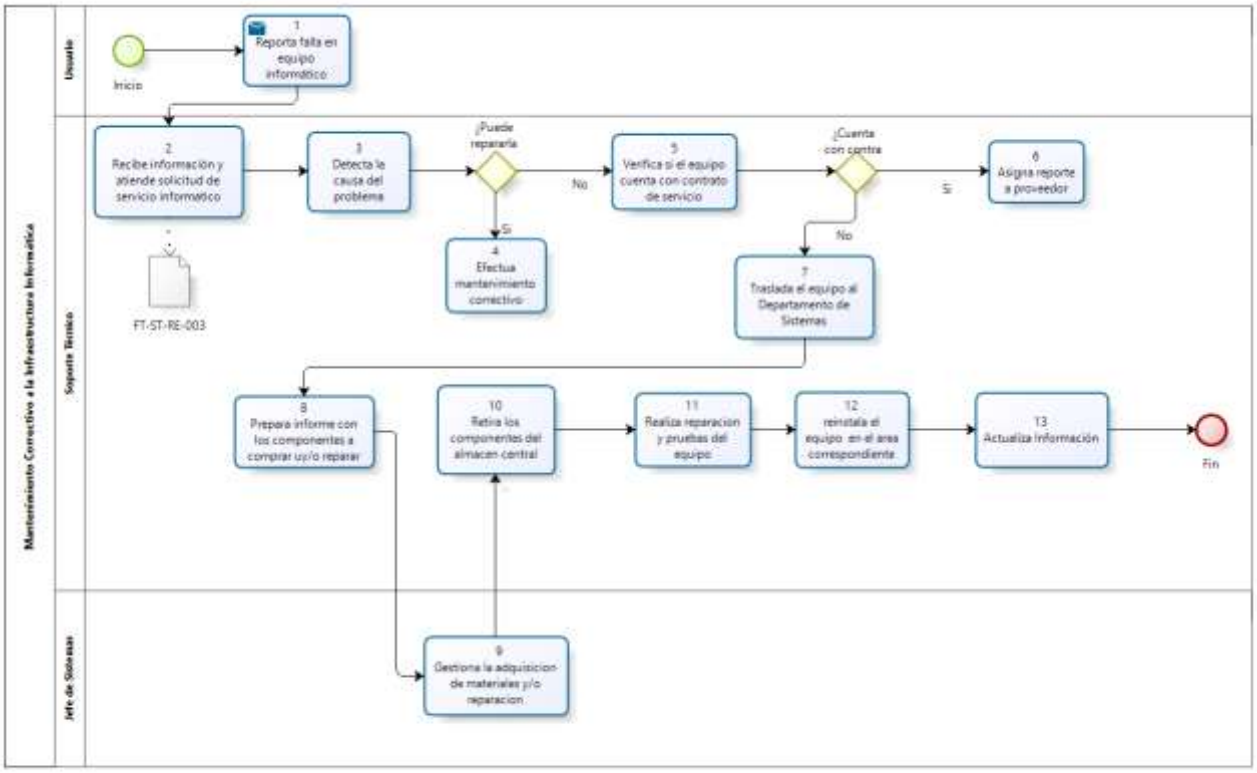
Fin de Actividades

7. FORMATOS

7.1. ST-FT-003 Solicitud de Servicios Informáticos

8. ANEXOS

Diagrama de Flujo Mantenimiento Correctivo a la Infraestructura Informática



INVENTARIO DE RECURSOS INFORMATICOS

1. OBJETIVO

Mantener actualizado el inventario de Recursos Informáticos, así como el monitoreo a instalaciones de aplicaciones no autorizadas.

2. ALCANCE

Aplica a todos los equipos informáticos de la UGEL Nº1, incluyendo los equipos en modalidad de alquiler.

3. RESPONSABILIDADES

3.1. Jefe de Sistemas

Es responsabilidad del Jefe de la Oficina de Sistema realizar las gestiones para mantener actualizado el parque de equipos informáticos con los que cuenta la empresa, ya sean por compra de activo o en modalidad de alquiler.

3.2. Soporte Técnico de Sistemas

Es responsable de realizar las actividades, para mantener actualizado los registros de inventario de recursos informáticos

4. DEFINICIONES Y ABREVIATURAS

4.1. Inventario de Recursos Informáticos

Sistema para el control y registro del inventario de recursos informáticos de La UGEL Nº1

4.2. Estación de Trabajo

Es una computadora que facilita a los usuarios el acceso a la red y ejecutar diversos aplicativos

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Solicita actualización de Recursos Informáticos

El Jefe de la Oficina de Sistemas solicita cada cuatro meses la actualización de los recursos informáticos de La UGEL Nº1

6.2. Imprimir Listado actual de Recursos Informáticos

El responsable de Soporte Técnico imprime el listado actual de equipos informáticos para iniciar las actividades de inventario

6.3. Revisar Hardware y Software en cada estación de trabajo

El responsable de Soporte Técnico inicia las actividades de inventario, captura la información correspondiente al Hardware y Software de los equipos pertenecientes a la red de datos de La UGEL Nº1, registra cualquier cambio en las características previamente configurada por la Oficina de Sistemas

6.4. Eliminar Software y aplicaciones no autorizadas

El Responsable de Soporte Técnico, si en la toma de inventario detecta aplicaciones no autorizadas, procede a eliminarlas, realizando un informe con los cambios encontrados

6.5. Colocación de sello de Seguridad

El Responsable de Soporte Técnico, deberá colocar un sticker de seguridad para evitar que el equipo pueda ser manipulado, en el deberá colocar la fecha del inventario, su nombre y firma

6.6. Elaborar Informe y Actualizar Registros

El encargado de Soporte Técnico una vez finalizado el inventario, elabora un informe especificando los cambios registrados en las estaciones de trabajo y procede a la actualización de la información en el Registro

ST-FT-004 Inventario de Recursos Informáticos

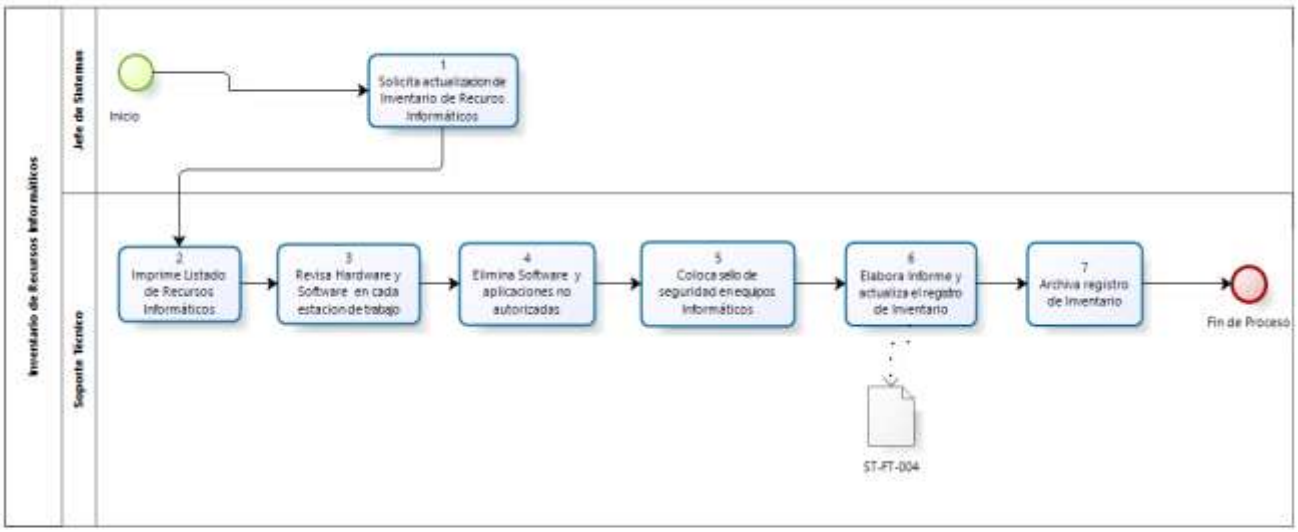
Fin de Actividades

7. FORMATOS

7.1. ST-FT-004 Inventario de Recursos Informáticos

8. ANEXOS

Diagrama de Flujo Inventario de Recursos Informáticos



CREACION, MODIFICACION O ELIMINACION DE CUENTAS DE ACTIVE DIRECTORY

1. OBJETIVO

Permitir que los usuarios tengan acceso a los recursos de la red de datos de La UGEL Nº1 y controlar el acceso a los recursos del Dominio..

2. ALCANCE

Este procedimiento aplica a todos los usuarios que requieran utilizar la red de Datos de La UGEL Nº1.

3. RESPONSABILIDADES

3.1. Departamento de Recursos Humanos

Comunicar el ingreso o baja de un usuario de La UGEL Nº1

3.2. Jefe de la Oficina de Sistemas

Verificar que se ejecute de forma correcta el procedimiento

3.3. Soporte Técnico de Sistemas

Realizar los trabajos para el alta, modificación o baja de los usuarios de La UGEL Nº1, en el Servidor de Dominio.

4. DEFINICIONES Y ABREVIATURAS

4.1. Active Directory

Es un servicio establecido, donde se crean los usuarios, equipos o grupos de trabajo pertenecientes a la red de La UGEL Nº1

4.2. DNS

Sistema de Nombres de Dominio, es un sistema de nomenclatura jerárquica para computadoras o recurso conectado a la red privada de La UGEL Nº1

4.3. Dominio

Es un repositorio de información estructurado sobre personas y recursos de una organización

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Recibir la solicitud de alta, modificación o baja de usuario

El Departamento de Recursos Humanos recibe la información de los nuevos ingresos de personal, modificación y/o baja del mismo.
Si es una modificación y/o baja del personal procede a informar al Jefe de la Oficina de Sistemas.
De lo contrario, llena la ficha para usuarios nuevos

6.2. Notificación de Modificación y/o Baja de Usuario

El Jefe de la Oficina de Sistemas, recibe la información proporcionada por Recursos Humanos, especifica a Soporte Técnico las actividades a realizar

6.3. Actualizar Cambios en el Active Directory

El responsable de Soporte Técnico actualiza la información en el Active Ditectory y actualiza información en el Registro ST-FT-005 Gestión de Cuentas

6.4. Llenado de Ficha para usuarios Nuevos

El Departamento de Recursos Humanos deberá llenar la ficha con los datos del personal que se estará incorporando a La UGEL Nº1 y que necesite utilizar algún recurso informático

6.5. Verificación de la Ficha para usuarios nuevos

El Jefe de la Oficina de Sistemas verifica que la ficha enviada por Recursos Humanos contiene todos los datos requeridos.

Si los datos son conformes, envía información a Soporte Técnico para la creación de la cuenta en el servidor de Dominio.

Caso contrario, devuelve la ficha al Departamento de Recursos Humanos para la actualización de los datos faltantes

6.6. Creación de Cuenta de Active Directory

El Responsable de Soporte Técnico, con los datos y especificaciones del Jefe del Departamento de Sistemas, crea la cuenta de Active Directory en el servidor de Dominio

6.7. Configurar Permisos de Cuenta de Usuario

El responsable de Soporte Técnico, asigna los permisos de la cuenta de usuario en el servidor de Dominio

6.8. Configurar Cuenta de usuario en equipo Informático

El responsable de Soporte Técnico, una vez creada la cuenta de usuario en el servidor de Dominio, procede a configurar la cuenta en el equipo informático asignado

6.9. Verificar que el equipo Informático este registrado en el Servidor de Dominio

El responsable de Soporte Técnico se encargara de verificar que la cuenta de usuario y el equipo informático se registre correctamente en el servidor de Dominio

Si está registrado, actualiza la información en el registro ST-FT-005 Gestión de Cuentas caso contrario vuelve a realizar las configuraciones para el registro

6.10. Actualización de Registro

El Responsable de Soporte Técnico, una vez terminada la configuración del equipo informático asignado al usuario, deberá de actualizar la información en el registro **ST-FT-005 Gestión de Cuentas**

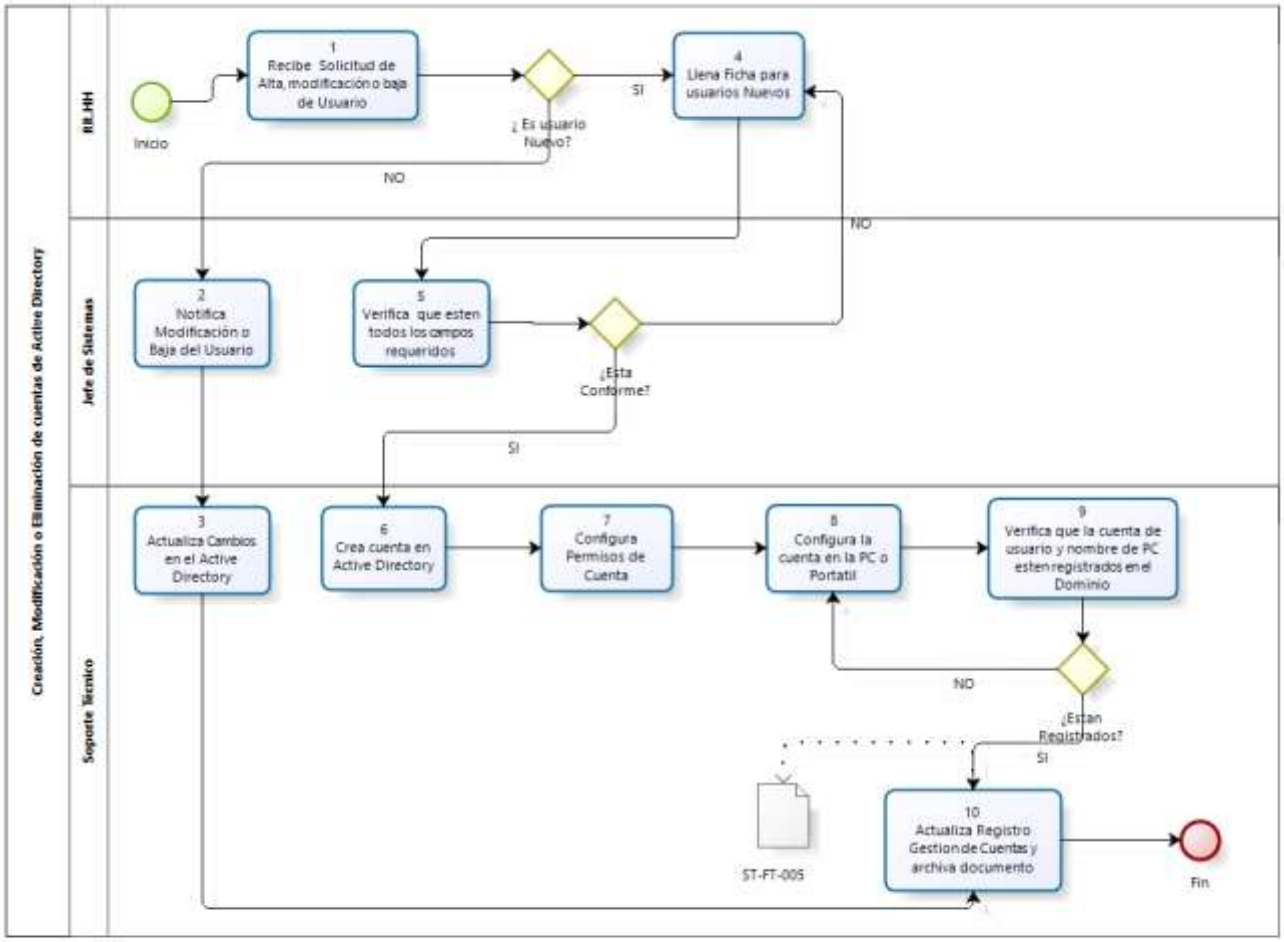
Fin de Actividades

7. FORMATOS

7.1. ST-FT-005 Gestión de Cuentas

8. ANEXOS

Diagrama de Flujo Creación, Modificación y/o Eliminación de Cuentas de Active Directory


Creación, Modificación o Eliminación de cuentas de Active Directory
RR.HH
Jefe de Sistemas
Soporte Técnico
Inicio
1
Recibe Solicitud de Alta, modificación o baja de Usuario
¿ Es usuario Nuevo?
SI
4
Llena Ficha para usuarios Nuevos
NO
2
Notifica Modificación o Baja del Usuario
5
Verifica que esten todos los campos requeridos
¿Esta Conforme?
NO
SI
3
Actualiza Cambios en el Active Directory
6
Crea cuenta en Active Directory
7
Configura Permisos de Cuenta
8
Configura la cuenta en la PC o Portatil
9
Verifica que la cuenta de usuario y nombre de PC esten registrados en el Dominio
NO
¿Estan Registrados?
SI
ST-FT-005
10
Actualiza Registro Gestion de Cuentas y archiva documento
Fin

ALTA O BAJA DE CUENTAS DE CORREO ELECTRONICO

1. OBJETIVO

Brindar una herramienta de colaboración, que permitirá el intercambio de información entre las diferentes instancias, Proveedores y usuarios de la UGEL Nº1.

2. ALCANCE

Este procedimiento aplica a todos los usuarios de la UGEL Nº1, que necesiten el intercambio de información con otras entidades.
Inicia con la solicitud de alta o baja de usuario perteneciente a la Red de la UGEL Nº1, hasta la creación o eliminación de la cuenta de correo electrónico.

3. RESPONSABILIDADES

3.1. Departamento de Recursos Humanos

Comunicar el ingreso o baja de un usuario de La UGEL Nº1

3.2. Jefe de la Oficina de Sistemas

Verificar que se ejecute de forma correcta el procedimiento

3.3. Soporte Técnico de Sistemas

Realizar los trabajos para el alta o baja de las cuentas de correo electrónico de la UGEL Nº1

4. DEFINICIONES Y ABREVIATURAS

4.1. Correo Electrónico

Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos

4.2. Servidor de Correo Electrónico

Realiza el proceso de envió de información entre los distintos usuarios conectados a la red de datos de La UGEL Nº1

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Recibir la solicitud de alta, modificación o baja de usuario

El Departamento de Recursos Humanos recibe la información de los nuevos ingresos de personal y/o baja del mismo.
Si es una baja del personal procede a informar al Jefe de la Oficina de Sistemas.
De lo contrario, llena la ficha para usuarios nuevos

6.2. Notificación Baja de Usuario

El Jefe de la Oficina de Sistemas, recibe la información proporcionada por Recursos Humanos, especifica a Soporte Técnico las actividades a realizar

6.3. Respaldo de Información

El encargado de Soporte Técnico procede a realizar el respaldo de la información contenida en el correo electrónico del usuario a dar de baja

6.4. Eliminar Cuenta de Correo Electrónico

El Responsable de Soporte Técnico, una vez resguardada la información, procede a eliminar la cuenta en el Servidor de Correos, actualiza la información en el Registro ST-FT-005 Gestión de Cuentas

6.5. Llenado de Ficha para usuarios Nuevos

El Departamento de Recursos Humanos deberá llenar la ficha con los datos del personal que haga necesite utilizar algún recurso informático

6.6. Verificación de la Ficha para usuarios nuevos

El Jefe de la Oficina de Sistemas verifica que la ficha enviada por Recursos Humanos contiene todos los datos requeridos.

Si los datos son conformes, envía información a Soporte Técnico para la creación de la cuenta en el servidor de Correo.

Caso contrario, devuelve la ficha al Departamento de Recursos Humanos para la actualización de los datos faltantes

6.7. Creación de Cuenta en el servidor de Correo

El responsable de Soporte Técnico, crea la cuenta de usuario en el Servidor de Correo

Si la cuenta necesita configurase en un equipo informático, procede a realizar la configuración.

Caso contrario envía un instructivo, con las indicaciones para acceder al correo vía web

6.8. Instructivo para acceder a Correo electrónico vía web

El responsable de Soporte Técnico envía un instructivo, indicando los parámetros y pasos para acceder al correo electrónico institucional desde la web.

6.9. Configurar Cuenta en Equipo Informático

El responsable de Soporte Técnico se encargara de configurar la cuenta de Correo electrónico en el dispositivo informático asignado

6.10. Pruebas de comunicación

El responsable de Soporte Técnico, una vez terminada la configuración de la cuenta de Correo electrónico en el equipo Informático asignado, procederá a realizar las pruebas de comunicación de envío y recepción de Correo electrónico.

Si las pruebas son correctas, actualiza el registro **ST-FT-005 Gestión de Cuentas**

Caso contrario vuelve a realizar las configuraciones en la cuenta

6.11. Actualizar Registro

El responsable de Soporte Técnico se encargara de actualizar la información en el registro **ST-FT-005 Gestión de Cuentas**

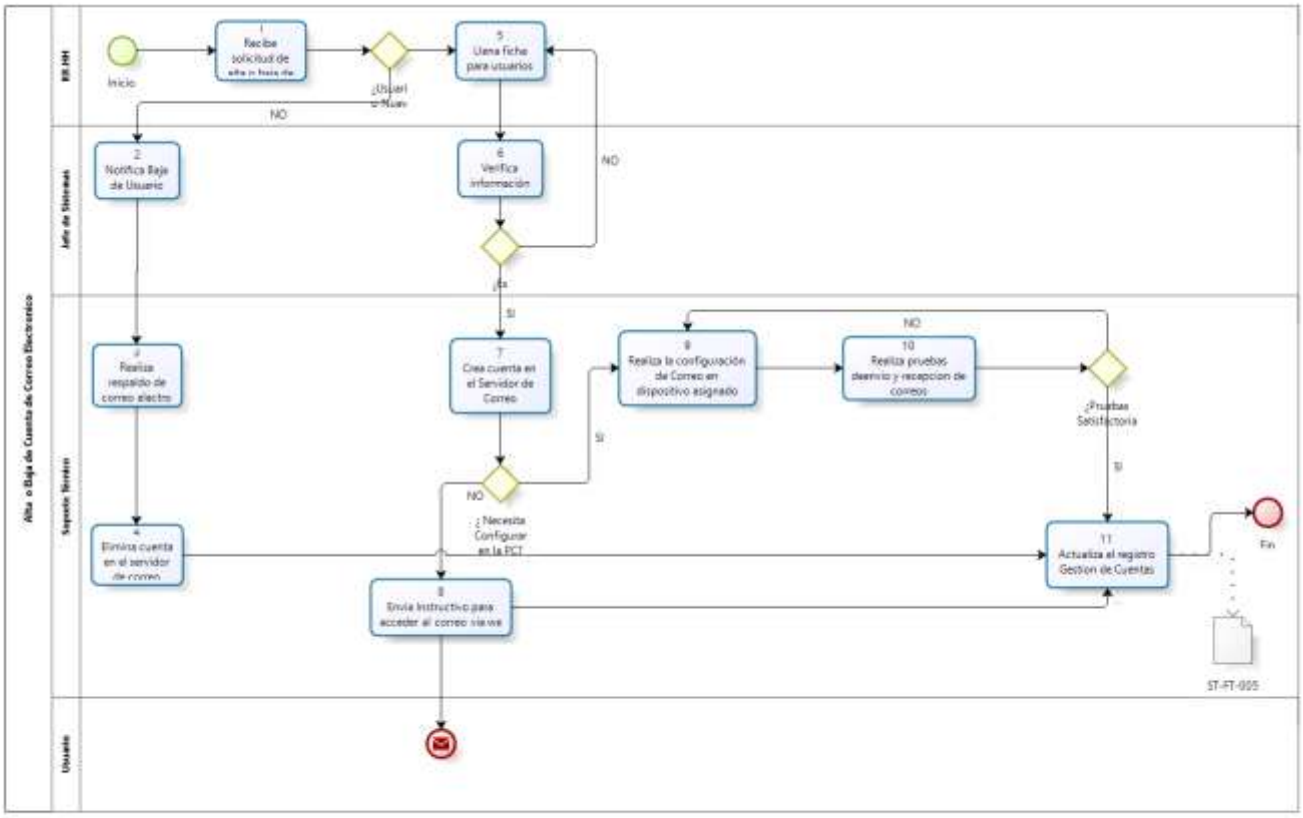
Fin de Actividades

7. FORMATOS

7.1. ST-FT-005 Gestión de Cuentas

8. ANEXOS

Diagrama de Flujo Alta o Baja de Cuentas de Correo Electrónico


Alta o Baja de Cuenta de Correo Electrónico
RR.HH
Jefe de Sistemas
Soporte Técnico
Usuario
Inicio
1
Recibe solicitud de
¿Usuari
o Nuev
NO
5
Llena ficha para usuarios
2
Notifica Baja de Usuario
6
Verifica información
NO
¿Es
SI
3
Realiza respaldo de correo electro
7
Crea cuenta en el Servidor de Correo
8
Realiza la configuración de Correo en dispositivo asignado
NO
10
Realiza pruebas deenvio y recepcion de correos
¿Pruebas Satisfactoria
SI
NO
SI
¿ Necesita Configurar en la PC?
4
Elimina cuenta en el servidor de correo
9
Envia Instructivo para acceder al correo via we
11
Actualiza el registro Gestion de Cuentas
Fin
ST-FT-005

ALTA O BAJA DE USUARIO DE TELEFONIA IP

1. OBJETIVO

Proporcionar una herramienta, con la cual los usuarios puedan comunicarse vía telefónica con otras entidades para la realización de sus Actividades propias de La UGEL Nº1

2. ALCANCE

Este procedimiento es aplicable a todos los usuarios que requieran el servicio de Telefonía IP

3. RESPONSABILIDADES

3.1. Departamento de Recursos Humanos

Comunicar el ingreso o baja de un usuario de La UGEL Nº1

3.2. Jefe de la Oficina de Sistemas

Verificar que se ejecute de forma correcta el procedimiento

3.3. Soporte Técnico de Sistemas

Realizar los trabajos para el alta y/o baja de los usuarios en el Servidor de Telefonía IP

4. DEFINICIONES Y ABREVIATURAS

4.1. Telefonía IP

Servicio que permite la comunicación telefónica utilizando el servicio de Internet

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Recibir la solicitud de alta, modificación o baja de usuario

El Departamento de Recursos Humanos recibe la información de los nuevos ingresos de personal y/o baja del mismo.
Si es una baja del personal procede a informar al Jefe del Departamento de Sistemas.
De lo contrario, llena la ficha para usuarios nuevos

6.2. Notificación de Baja de Usuario

El Jefe de la Oficina de Sistemas, recibe la información proporcionada por Recursos Humanos, especifica a Soporte Técnico las actividades a realizar

6.3. Eliminar Datos en anexo IP

El responsable de Soporte Técnico elimina datos del usuario a dar de baja, en el teléfono IP asignado

6.4. Inactivar Anexo Telefónico

El responsable de Soporte Técnico, una vez eliminado los datos del usuario, procede a inactivar el número de anexo hasta un nuevo ingreso de personal, Actualiza Registro Gestión de Cuentas y archiva documentación

6.5. Llenado de Ficha para usuarios Nuevos

El Departamento de Recursos Humanos deberá llenar la ficha con los datos del personal nuevo que se incorporara a la empresa y haga uso del servicio de Telefonía IP

6.6. Verificación de la Ficha para usuarios nuevos

El Jefe de la Oficina de Sistemas verifica que la ficha enviada por Recursos Humanos contiene todos los datos requeridos.

Si los datos son conformes, envía información a Soporte Técnico para la configuración de una cuenta y anexo Telefónico IP.

Caso contrario, devuelve la ficha al Departamento de Recursos Humanos para la actualización de los datos faltantes

6.7. Verificar Stock de Teléfono IP

El responsable de Soporte Técnico verifica si cuenta con Stock disponible de Teléfonos IP, Si cuenta con stock procede a verificar si hay un número de anexo disponible, de lo contrario, informa al Jefe de Sistema para que realice la adquisición del teléfono IP

6.8. Gestionar adquisición de Teléfono IP

El Jefe de la Oficina de Sistema es responsable de realizar las gestiones para la adquisición de un Teléfono IP en caso no hubiera disponibilidad del mismo

6.9. Verificar si hay número de anexo disponible

El responsable de Soporte Técnico es responsable de verificar si hay un número de anexo disponible, de haber número de anexo disponible procede a la activación del anexo, caso contrario, crea un nuevo número de anexo en el Servidor

6.10. Crear número de anexo en la central telefónica

El responsable de Soporte Técnico es responsable de crear un nuevo número de anexo en la central telefónica, cuando no haya un número de anexo disponible para su activación

6.11. Activar número de Anexo en la ventral telefónica

El responsable de Soporte Técnico es responsable de activar el número de anexo y configurar los datos del usuario en la central telefónica

6.12. Configurar Datos de usuario en el Teléfono IP

El responsable de Soporte Técnico es responsable de configurar el número de anexo y datos del usuario en el Teléfono IP asignado al usuario

6.13. Verificar Permisos del Usuario

El responsable de Soporte Técnico verifica si el usuario cuenta con permisos para llamadas externas, revisa según los datos proporcionados por el Jefe de la oficina de Sistemas, Si el usuario cuenta con permisos, procede a realizar las configuraciones en el servidor, caso contrario actualiza registro **ST-FT-005 Gestión de Cuentas**

6.14. Configurar Permisos para llamadas externas

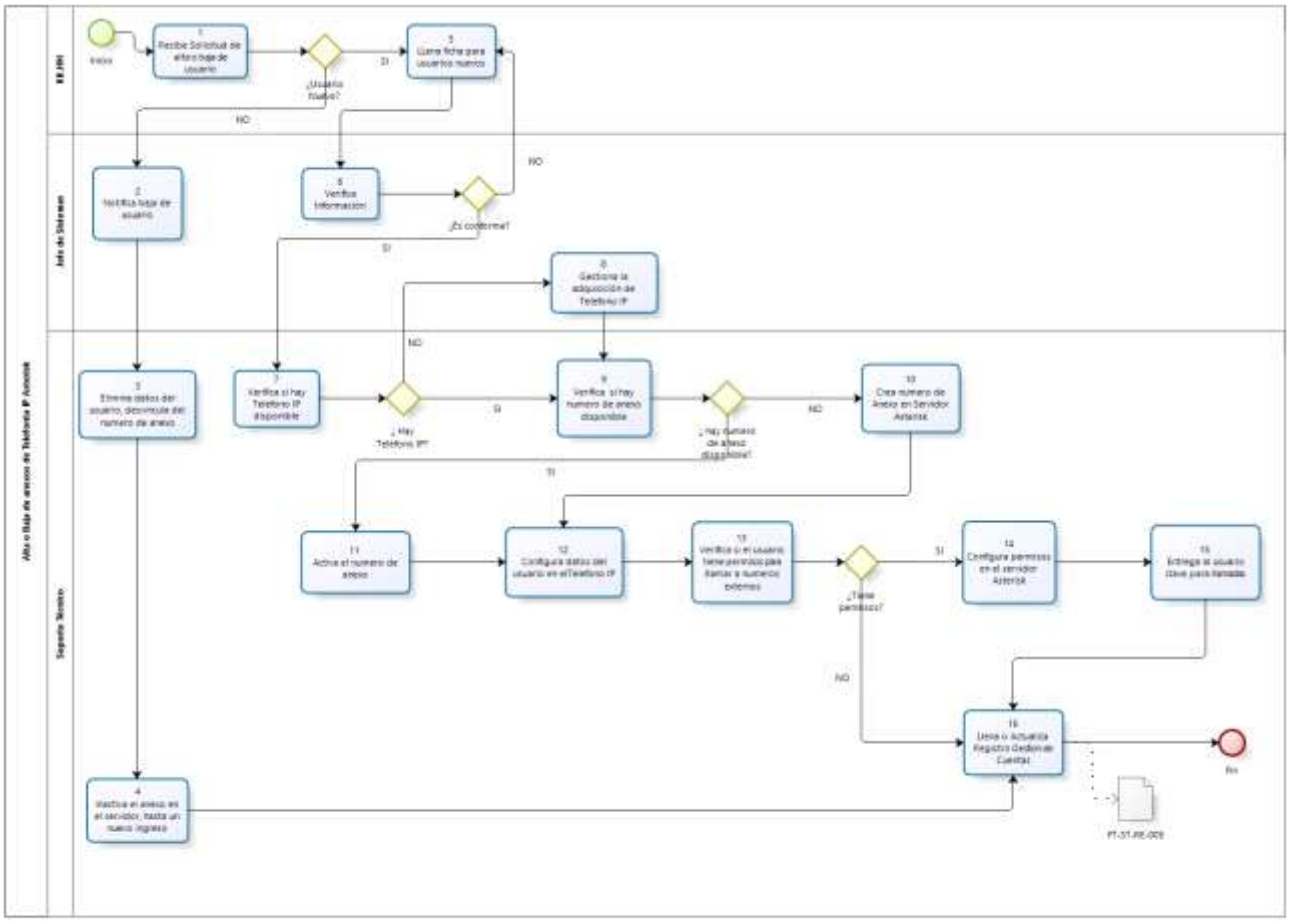
El responsable de Soporte Técnico es responsable de configurar los permisos que tendrá el usuario

7. FORMATOS

7.1. ST-FT-005 Gestión de Cuentas

8. ANEXOS

Diagrama de Flujo Alta o Baja de Usuario de Telefonía IP


Alta o Baja de anexos de Telefonía IP Asterisk
RR.HH
Jefe de Sistemas
Soporte Técnico
Inicio
1 Recibe Solicitud de alta o baja de usuario
¿Usuario Nuevo?
SI
NO
5 Llena ficha para usuarios nuevos
2 Verifica baja de usuario
6 Verifica información
¿Es conforme?
NO
SI
8 Gestiona la adquisición de Telefono IP
3 Elimina datos del usuario, desvincula del numero de anexo
7 Verifica si hay Telefono IP disponible
¿ Hay Telefono IP?
NO
SI
9 Verifica si hay numero de anexo disponible
¿ Hay numero de anexo disponible?
NO
10 Crea numero de Anexo en Servidor Asterisk
SI
11 Activa el numero de anexo
12 Configura datos del usuario en elTelefono IP
13 Verifica si el usuario tiene permisos para llamar a numeros externos
¿Tiene permisos?
SI
NO
14 Configura permisos en el servidor Asterisk
15 Entrega al usuario clave para llamadas
16 Llena o Actualiza Registro Gestion de Cuentas
Fin
4 Inactiva el anexo en el servidor, hasta un nuevo ingreso
FT-ST-RR-009

INSTALACION DE CABLEADO ESTRUCTURADO DE VOZ Y/O DATOS

1. OBJETIVO

Proporcionar a los usuario de la UGEL Nº1, la instalación de cableado estructurado para los servicios de Voz y Datos.

2. ALCANCE

Aplica a todos los usuarios que laboran en la UGEL Nº1 y que requieran el servicio de Voz y Datos.

3. RESPONSABILIDADES

3.1. Personal de la Empresa

Es el responsable de comunicar la necesidad de utilizar la Red de Voz y/o Datos

3.2. Jefe de Sistemas

Es responsable de verificar la factibilidad de la solicitud y realizar las gestiones necesarias para la implementación

3.3. Soporte Técnico

Es responsable de ejecutar los trabajos correspondientes al tendido de cableado Estructurado Voz y/o Datos, así como la actualización de registros que intervengan en el proceso.

4. DEFINICIONES Y ABREVIATURAS

4.1. Cableado Estructurado

Consiste en el tendido de cables de Red, con el propósito de implementar una Red de área local

4.2. Red

Conjunto de equipos y dispositivos conectados entre sí, con la finalidad de compartir y optimizar los recursos

5. DOCUMENTOS DE REFERENCIA

5.1. ANSI/TIA/EIA-568-B.2-1, Norma de telecomunicaciones para edificios comerciales

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Realiza Solicitud de Cableado Estructurado Voz y/o Datos

El usuario de la UGEL Nº1 solicita a la Oficina de Sistemas la necesidad de contar con un punto de Red para Voz y/o Datos

6.2. Recepcionar información

El responsable de recepcionar todas las solicitudes para un nuevo punto de red de Voz y/o Datos es el Jefe de la Oficina de Sistemas

6.3. Verificar si la solicitud es factible

El responsable de la Oficina de Sistemas es el encargado de verificar que la solicitud de un nuevo punto de Voz y/o Datos se pueda realizar.

Si es Factible, envía información a Soporte Técnico para que inicie los trabajos de instalación, de lo contrario notifica que no es posible realizar la solicitud.

6.4. Enviar Información a Soporte Técnico

El responsable de la Oficina de Sistemas es responsable de enviar la información con las especificaciones del trabajo a realizar.

6.5. Capturar información en el Sistema y apertura de solicitud

El responsable de Soporte Técnico, es responsable de capturar la información en el sistema con las especificaciones dadas por el Jefe de Sistemas

6.6. Elaborar Lista de Materiales

El responsable de Soporte Técnico, es el encargado de elaborar la lista de materiales a utilizar, en ella deberá especificar materiales, herramientas y/u otros componentes a utilizar

6.7. Verificar Stock de Materiales

El responsable de soporte técnico, verifica si cuenta con los materiales disponibles para realizar los trabajos de cableado estructurado.

Si cuenta con los materiales, ejecuta los trabajos, de lo contrario, notifica al Jefe de Sistema para que realice las gestiones necesarias

6.8. Gestión de Adquisición de materiales

El responsable de la Oficina de Sistemas, es el encargado de gestionar la adquisición de materiales faltantes, para la elaboración de los trabajos de cableado estructurado

6.9. Ejecución de los Trabajos

El responsable de Soporte Técnico, es el encargado de realizar los trabajos correspondientes a la instalación y pruebas de comunicación en el cableado estructurado

6.10. Realizar pruebas de comunicación

El responsable de Soporte Técnico, es el encargado de realizar las pruebas de comunicación, en el cableado estructurado

Si las pruebas son satisfactorias, actualiza registro Instalación de Cableado estructurado de Voz y/o Datos y archiva documentos, de lo contrario revisa la configuración y vuelve a ejecutar los trabajos de instalación

6.11. Actualizar Registros

El responsable de Soporte Técnico, es el encargado de actualizar la información correspondientes a la instalación de cableado estructurado de Voz y/o Datos en el registro **ST-FT-006 Cableado estructurado de voz y/o Datos**

6.12. Archivar Documentación

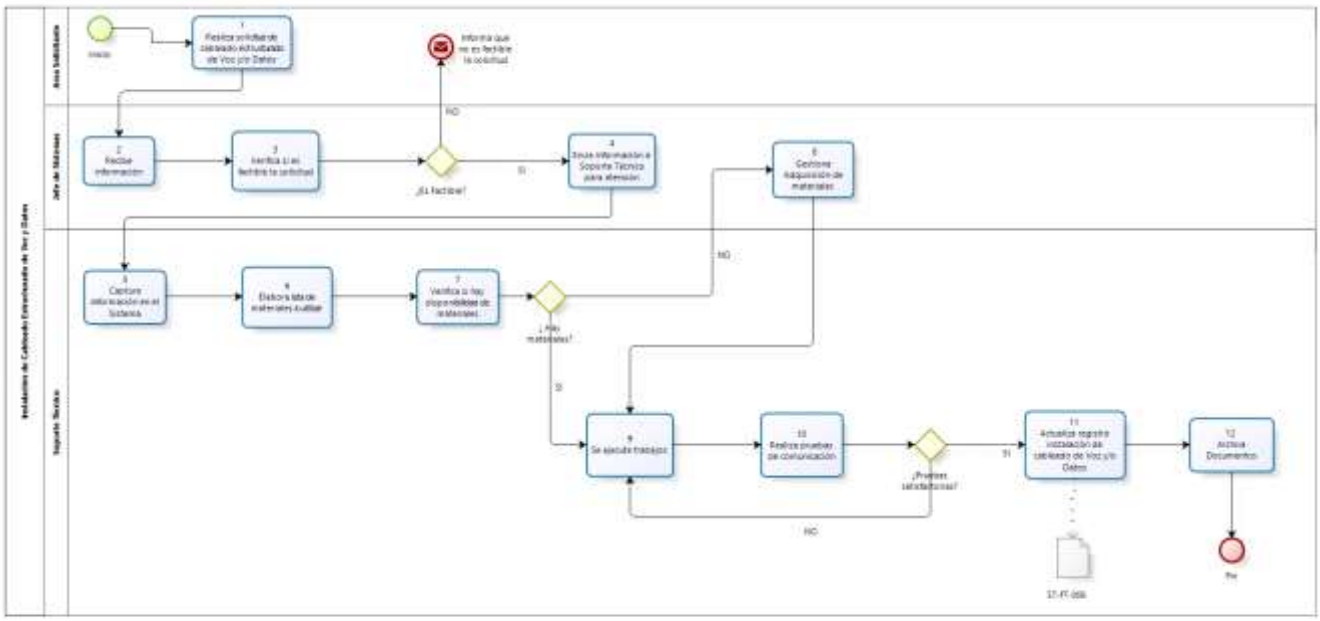
El responsable de Soporte Técnico, una vez finalizado todos los trabajos y actualizado los registros correspondientes, se encargara de archivar la documentación correspondiente al procedimiento de Cableado estructurado de Voz y/o Datos

7. FORMATOS

7.1. ST-FT-006 Cableado Estructurado de Voz y/o Datos

8. ANEXOS

Diagrama de Flujo Instalación de Cableado Estructurado de Voz y/o Datos



INSTALACION DE ANTIVIRUS INSTITUCIONAL

1. OBJETIVO

Mantener Protegida la Red de Datos de la UGEL Nº1 ante posibles amenazas de Virus

2. ALCANCE

Aplica a todas las PC de escritorio y Portátiles pertenecientes a la Red de Datos de la UGEL Nº1

3. RESPONSABILIDADES

3.1. Jefe de Sistemas

Gestionar la Adquisición del Software Antivirus

3.2. Soporte Técnico

Es responsable de realizar las actividades correspondientes a la Instalación del Software, así como la actualización de los registros correspondientes.

4. DEFINICIONES Y ABREVIATURAS

4.1. Antivirus

Es un programa que ayuda a proteger la computadora y/o Red de Datos contra amenazas de virus

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Gestionar la adquisición de Antivirus

El Jefe de Sistemas es responsable de realizar las gestiones para la adquisición de Antivirus, así como llevar el control de los contratos de proveedores del Software

6.2. Instalar Consola de Administración de Antivirus en el Servidor

Soporte Técnico es responsable de, realizar en coordinación con el Proveedor de la solución, la instalación de la consola de administración de antivirus, en ella deberán estar registrados todas las PC de escritorio y portátiles pertenecientes a la Red de Datos

6.3. Instalación Remota de Antivirus en PC de usuarios

Soporte Técnico es responsable de, realizar la instalación del Software en cada equipo de la red de Datos

6.4. Verificar la Instalación

Soporte Técnico es responsable de, verificar que la instalación remota del antivirus se haya efectuado correctamente, en caso de presentar algún inconveniente realizara la instalación de forma local, caso contrario actualiza el registro ST-FT-007 Antivirus Institucional

6.5. instalación de Antivirus en forma Local

Soporte Técnico es responsable de efectuar la instalación del Antivirus de forma local en aquellos equipos, que hayan presentado algún inconveniente con la instalación remota

6.6. Actualización de Registro de Antivirus

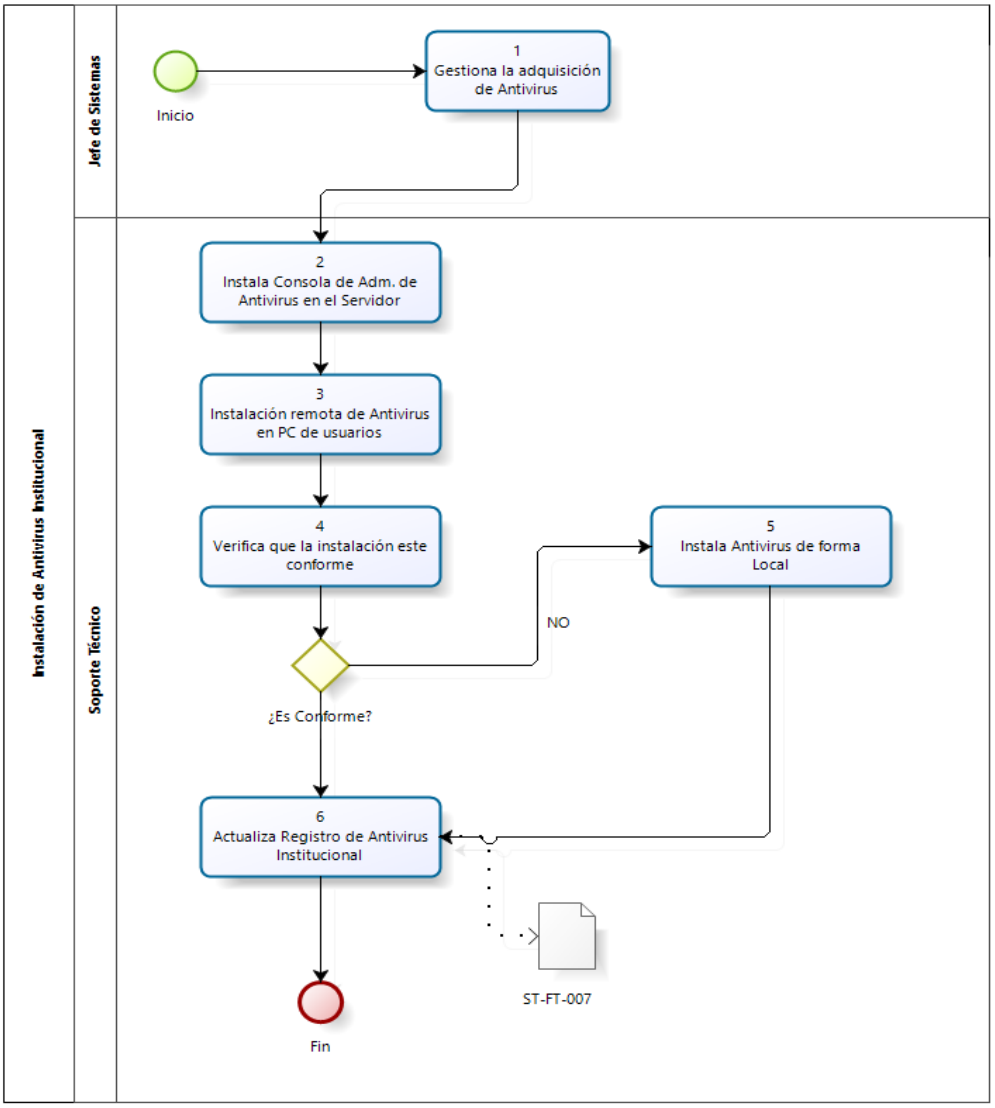
Soporte Técnico es responsable de actualizar el registro ST-FT-007 Antivirus Institucional

7. FORMATOS

7.1. ST-FT-007 Antivirus Institucional

8. ANEXOS

Diagrama de Flujo Instalación de Antivirus Institucional



ACTUALIZACION Y MONITOREO DE ANTIVIRUS INSTITUCIONAL

1. OBJETIVO

Mantener actualizada la Firma de Virus en los equipos Portátiles y PC de escritorio, así como detectar y eliminar amenazas de Virus

2. ALCANCE

Aplica a todas las PC de escritorio y Portátiles pertenecientes a la Red de Datos de la UGEL Nº1

3. RESPONSABILIDADES

3.1. Soporte Técnico

Es responsable de mantener actualizada la firma de virus y monitorear los equipos de cómputo ante posibles amenazas de Virus

4. DEFINICIONES Y ABREVIATURAS

4.1. Antivirus

Es un programa que ayuda a proteger la computadora y/o Red de Datos contra amenazas de virus

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Verificar que la firma de Virus está actualizada en las PC y Portátiles

El responsable de Soporte Técnico, verifica en la consola de administración, instalada en el servidor que la firma de Virus se encuentre actualizada en todas las PC y Portátiles de la UGEL

Si está actualizada, realiza el escaneo de virus, caso contrario aplica actualización

6.2. Aplicar Actualización

El responsable de Soporte Técnico, aplica la actualización de Firma de Virus a los equipos que no se hayan podido actualizar, mediante la consola de administración

6.3. Escaneo de Virus en la Red

El responsable de Soporte Técnico, realiza el escaneo de virus en los equipos conectados a la Red de Datos de la UGEL Nº1

Si encuentra una amenaza, aplica vacuna, caso contrario finaliza el procedimiento

6.4. Aplicar Vacuna

El responsable de Soporte Técnico, es el encargado de aplicar la vacuna a aquellos equipos que se haya detectado virus, si el virus es eliminado finaliza procedimiento, caso contrario, aísla el equipo de la Red de Datos

6.5. Aislar el Equipo infectado de la Red de Datos

El encargado de Soporte Técnico, aísla el equipo informático donde se haya detectado virus y este no pueda ser controlado

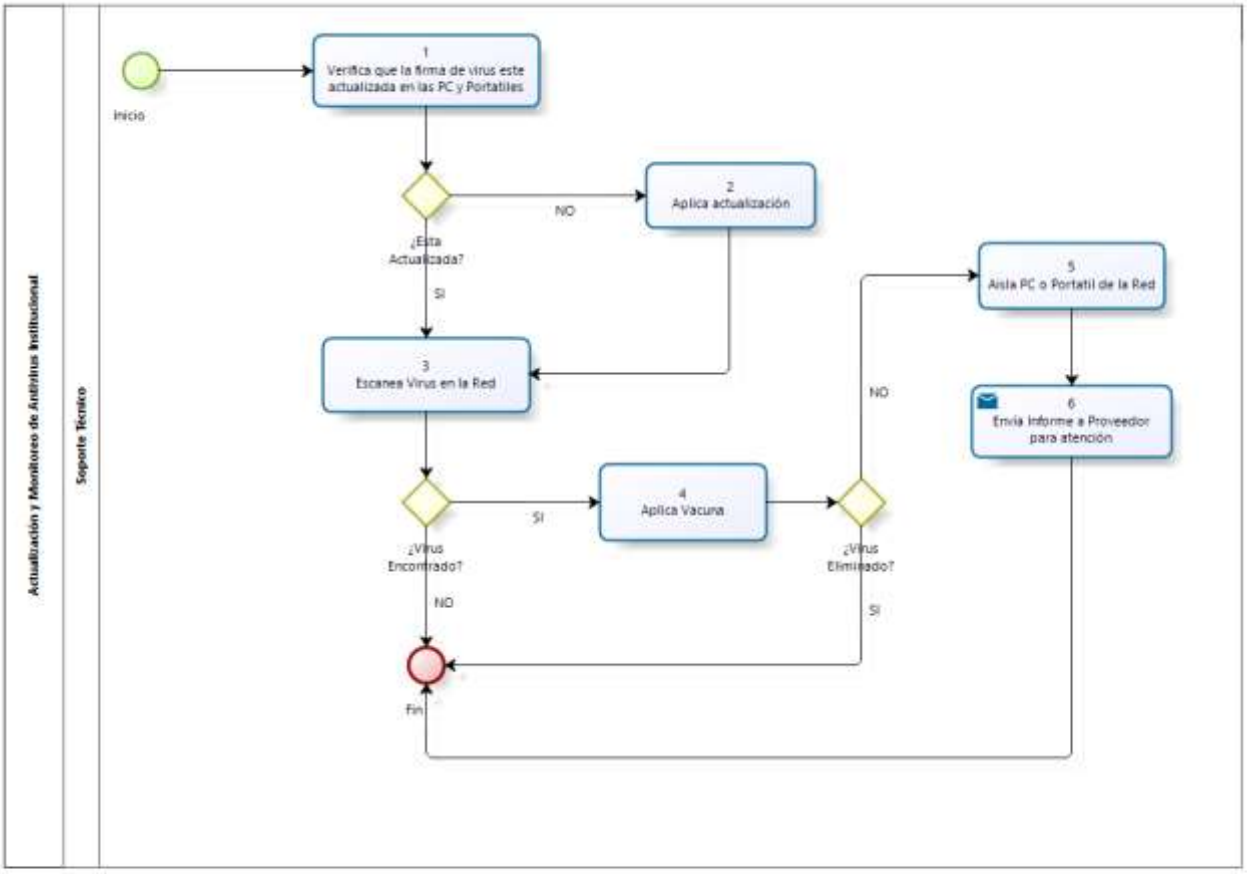
6.6. Enviar Informe a Proveedor de la Marca

El encargado de Soporte Técnico, prepara un informe en cual se detalla el problema presentado, ante la amenaza de virus, lo envía al proveedor de la marca y realiza las coordinaciones hasta que sea solucionado el problema, fin del procedimiento

7. FORMATOS

8. ANEXOS

Diagrama de Flujo Actualización y Monitoreo de Antivirus Institucional



RESPALDO DE LA INFORMACION

1. OBJETIVO

Garantizar la disponibilidad, seguridad y confidencialidad de la información, mediante la gestión de copias de la información

2. ALCANCE

Aplica a la información que se encuentre almacenada en los servidores de la UGEL Nº1

3. RESPONSABILIDADES

3.1. Jefe de Sistemas

Responsable del cumplimiento del procedimiento

3.2. Soporte Técnico

Es responsable de ejecutar las tareas relacionadas al respaldo y recuperación de la información.

4. DEFINICIONES Y ABREVIATURAS

4.1. Respaldo

Copia de información a un medio del cual se puede recuperar y restaurar la información

4.2. Restauración de la Información

Recuperar parte o la totalidad de información desde una copia de respaldo, la cual permitirá restaurar un sistema luego de un desastre

4.3. Repositorio

Deposito o almacén, un sitio centralizado donde se almacena y mantiene la información digital

5. DOCUMENTOS DE REFERENCIA

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Definir programa de respaldo

El jefe de sistema es el encargado de definir los aplicativos, información y mecanismos para la realización del respaldo de la información

6.2. Verificar tipo de respaldo

El responsable de soporte técnico, verifica el tipo de respaldo que se va a generar, si el respaldo es automático, programa en el sistema de backup los aplicativos y frecuencia en la cual se va a desarrollar, caso contrario ejecuta el respaldo manualmente.

6.3. Ejecutar Respaldo Manualmente

El responsable de soporte técnico es el encargado de realizar los respaldos de forma manual, beberá asegurar que no contenga errores, si contiene errores ejecuta nuevamente el respaldo, caso verifica si es respaldo es el último del mes

6.4. Programar los respaldo en el sistema de Backup

El encargado de soporte técnico es responsable de programar los respaldos de la información en el sistema de Backup, en el configurará la frecuencia y tipo de respaldo, solo aquellos aplicativos y/o información que su respaldo pueda realizarse de forma automática, según Registro ST-FT-008 Programa de Respaldo de la Información

6.5. Verificar si el respaldo contiene errores

El responsable de soporte técnico es el encargado de revisar el éxito en los respaldos, si contiene errores, volverá a programar en el sistema de Backup, caso contrario verifica si es el último respaldo del mes

6.6. Verificar si el respaldo es el último del mes

El responsable de soporte técnico es el encargado de verificar si el respaldo es el último del mes, si el respaldo es el último del mes, generara una copia adicional y la entregara al proveedor de resguardo externo, caso contrario registra bitácora de respaldo de la información

6.7. Generar copia adicional

El encargado de soporte técnico, es responsable de generar una copia adicional del respaldo siempre y cuando este sea la última copia del mes

6.8. Entregar copia a proveedor de resguardo externo

El encargado de soporte técnico es el encargado de entregar el dispositivo con la información correspondiente al cierre del mes

6.9. Registrar bitácora de respaldo de la información

El encargado de soporte técnico es responsable del llenado de la bitácora de los respaldos de la información, deberá llenar la bitácora en el registro **ST-FT-009 Respaldo de la Información**

6.10. Almacenar dispositivo en el Centro de Datos

El responsable de soporte técnico almacenara los dispositivos que contengan los respaldos de información en el Centro de Datos.

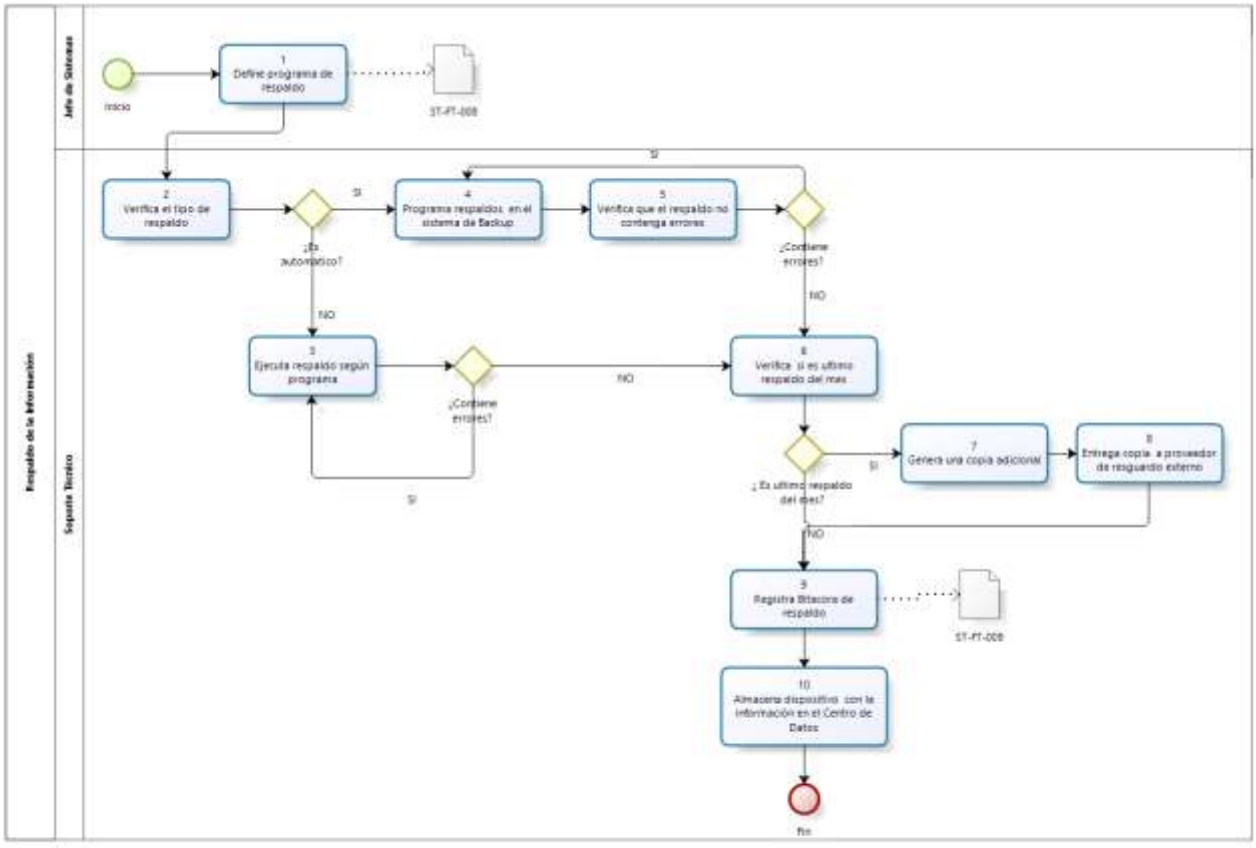
7. FORMATOS

ST-FT-008 Programa de respaldo de la información

ST-FT-009 Respaldo de la Información

8. ANEXOS

Diagrama de Flujo Respaldo de la Información



-

SISTEMA DE SEGURIDAD DE VIGILANCIA

1. OBJETIVO

Establecer los pasos y recomendaciones a seguir para verificar el correcto funcionamiento del sistema de vigilancia

2. ALCANCE

Este documento es aplicable al sistema de seguridad de vigilancia de la UGEL Nº1.

3. RESPONSABILIDADES

3.1. Jefe de Sistemas

Es el responsable de comunicar e implementar este procedimiento, así como de que no existan fallas ni inconvenientes con el sistema de seguridad.

3.2. Soporte Técnico

Es responsable de ejecutar las tareas relacionadas a la vigilancia de la información.

4. DEFINICIONES Y ABREVIATURAS

Ninguna

5. DOCUMENTOS DE REFERENCIA

Ninguna

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Definir programa de respaldo

A continuación se detallan las actividades a seguir:

Horarios de activación y desactivación de las alarmas:

• Hora de activación: 10:00 p.m.

• Hora de desactivación: 07:30 a.m.

6.2. Responsables de la desactivación:

Las personas responsables de la desactivación del sistema de alarmas son:

- Lucy Barrera. – Directora UGEL Nº1
- Juan Carlos Li. – Gerente de Planificación y Presupuesto
- Nilbert Salazar – Asistente de Tesorería
- Jorge Távara. – Jefe de Sistemas

Los jefes de área deben contar con el código de desactivación de cada una de las oficinas donde desempeñan sus labores.

Se debe de cambiar cada 03 meses como máximo las claves de activación y desactivación de las alarmas.

6.3. Razones de activación de las alarmas.

El único motivo por el cual se debe activar la alarma de seguridad de la UGEL Nº1 es exclusivamente en caso de robo.

Una razón adicional de activación sería en el caso de que el personal se quede laborando sobre el horario de activación de las alarmas. Se podría evitar esta activación proporcionando al encargado del área el código de desactivación.

6.4. Comunicación de activación de las alarmas.

En el caso de activación del sistema de alarmas se tendrá que comunicar exclusivamente vía telefónica a la Lic. Lucy Barrera-Directora de la UGEL Nº1, la razón de la activación.

6.5. Mantenimiento

El mantenimiento del sistema de seguridad es realizado por la Empresa BOXER, siendo el plazo recomendado cada 06 meses.

6.6. Generar copia adicional

El encargado de soporte técnico, es responsable de generar una copia adicional del respaldo siempre y cuando este sea la última copia del mes

6.7. Entregar copia a proveedor de resguardo externo

El encargado de soporte técnico es el encargado de entregar el dispositivo con la información correspondiente al cierre del mes

6.8. Registrar bitácora de los sucesos más relevantes

El encargado de soporte técnico es responsable del llenado de la bitácora de los sucesos más relevantes, deberá llenar la bitácora en el registro **ST-FT-011 Bitácora de incidentes.**

6.9. Almacenar dispositivo en el Centro de Datos

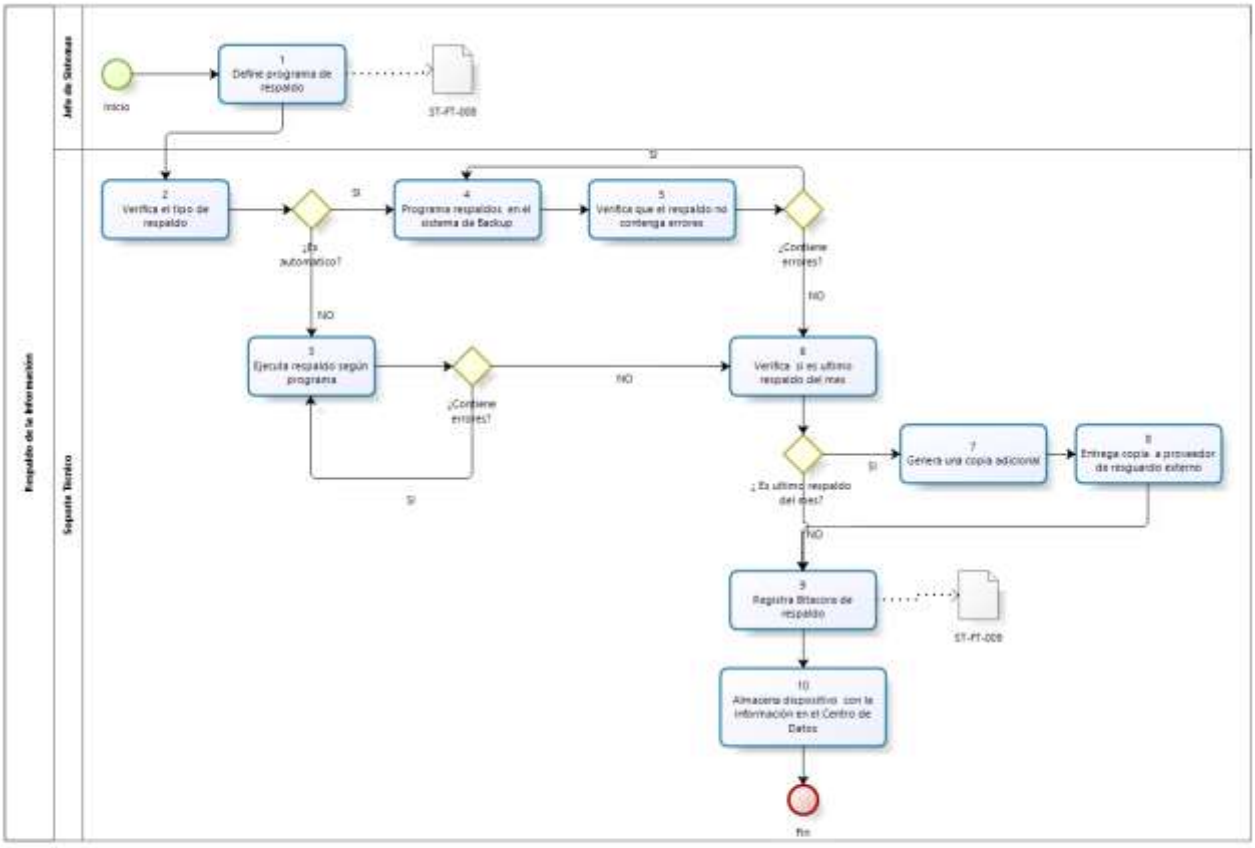
El responsable de soporte técnico almacenara los dispositivos que contengan los respaldos de información en el Centro de Datos.

7. FORMATOS

ST-FT-011 Bitácora de incidentes.

8. ANEXOS

Diagrama de Flujo vigilancia


Respaldo de la Información
Jefe de Sistemas
Soporte Técnico
Inicio
1 Define programa de respaldo
ST-PT-008
2 Verifica el tipo de respaldo
¿Es automático?
SI
NO
3 Ejecuta respaldo según programa
¿Contiene errores?
SI
4 Programa respaldos en el sistema de Backup
5 Verifica que el respaldo no contenga errores
¿Contiene errores?
SI
NO
6 Verifica si es ultimo respaldo del mes
¿Es ultimo respaldo del mes?
SI
7 Genera una copia adicional
8 Entrega copia a proveedor de resguardo externo
NO
9 Registra Bitacora de respaldo
ST-PT-009
10 Almacena dispositivo con la información en el Centro de Datos
fin

ALMACENAMIENTO DE ARCHIVOS EN EL SERVIDOR UGEL

1. OBJETIVO

Establecer recomendaciones a seguir al momento de guardar información en el servidor de archivos de la UGEL Nº1.

2. ALCANCE

Este documento es aplicable a las diferentes áreas que comprenden la organización de la UGEL Nº1.

3. RESPONSABILIDADES

3.1. Jefe de Sistemas

Es el responsable de comunicar e implementar este procedimiento, así como de que no se almacene información errada, se organice la información y se depure aquella que no tenga relación con documentos de la empresa.

3.2. Soporte Técnico

Es responsable de ejecutar las tareas relacionadas en el almacenamiento de la información en el servidor file (DATA).

4. DEFINICIONES Y ABREVIATURAS

Ninguna

5. DOCUMENTOS DE REFERENCIA

Ninguna

6. DESCRIPCION DE LAS ACTIVIDADES

6.1. Definir programa de respaldo

El servidor de archivos cuenta con dos unidades lógicas donde se almacena la información, las cuales son:

- Unidad “G”
- Unidad “Files”

Todos los usuarios tienen la obligación de guardar la información correspondiente al área donde desempeñen sus labores, teniendo en cuenta una serie de recomendaciones que se le brindan en la inducción a los sistemas.

6.2. Está prohibido almacenar información personal en el servidor de archivos.

6.3. Cada área tiene un directorio el cual se encuentra en la unidad “G”, donde se almacena la información de su trabajo.

6.4. La unidad “Files” es la unidad en la cual se guarda la información controlada y reservada a la que no todos los usuarios tienen acceso. Así mismo está prohibido almacenar información que no corresponda a esta carpeta, cambiar el nombre o guardar otro tipo de archivo.

6.5. Los usuarios no deberán cambiar la configuración establecida por el área de Sistemas, modificar las firmas electrónicas y fondos de pantallas.

6.6. Se prohíbe guardar información en la unidad “C” de la computadora que se le asigne al usuario.

6.7. No guardar carpetas ni documentos en el escritorio de las computadoras.

6.8. Se prohíbe modificar archivos de otros usuarios u otras áreas.

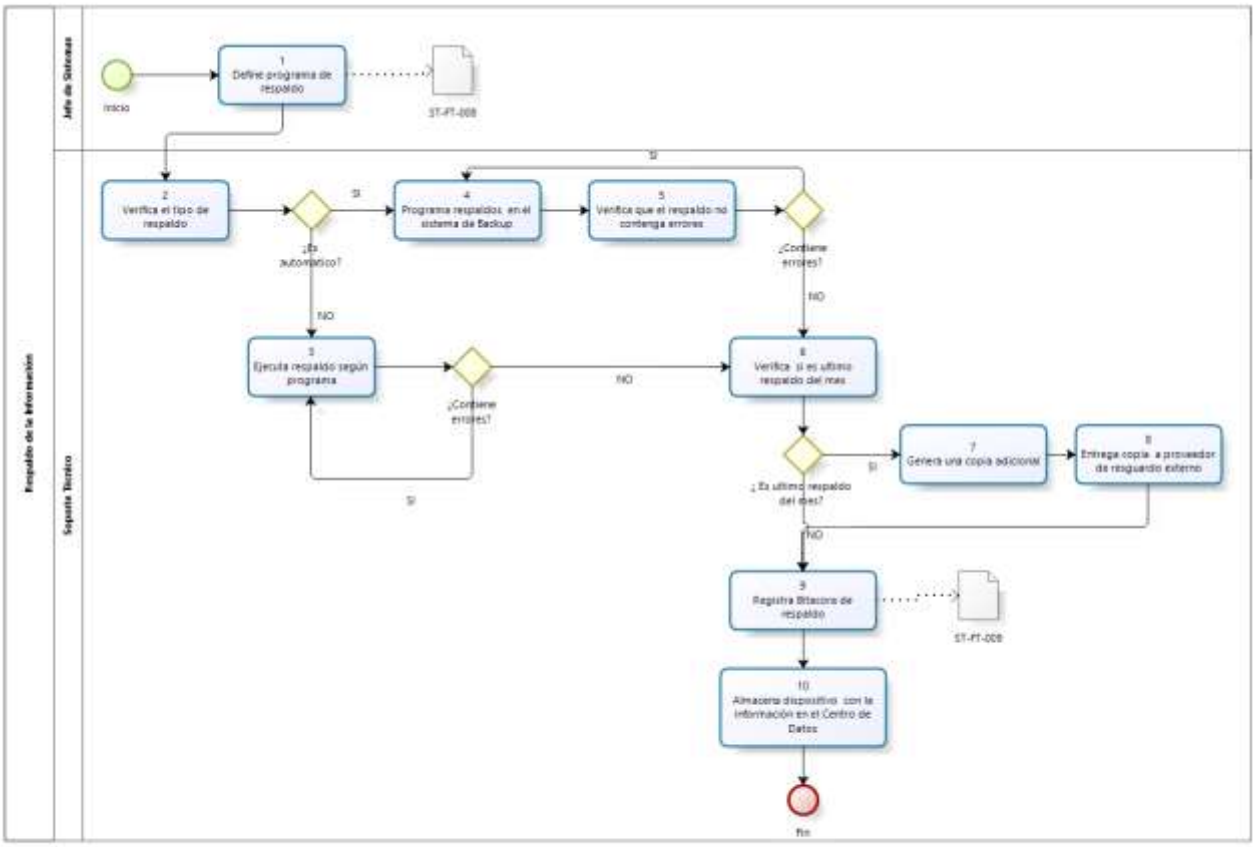
El responsable de soporte técnico almacenara los dispositivos que contengan los respaldos de información en el Centro de Datos.

7. FORMATOS

ST-FT-011 Bitácora de incidentes.

8. ANEXOS

Diagrama de Flujo almacenamiento de Archivos en el servidor files (DATA).



POLITICA DE ANTIVIRUS

1. OBJETIVO

Establecer los requerimientos que deben cumplir los equipos de cómputo conectados a la red, para garantizar la detección y prevención oportuna de código malicioso mediante el uso del software antivirus.

2. ALCANCE

Esta Política aplica a todos los equipos informáticos pertenecientes a la Red de Datos de la UGEL Nº1.

3. CONSIDERACIONES

3.1. Todos los equipos de cómputo conectados a la red, deberán tener instalada la Solución Antivirus.

3.2. Diariamente se realizará la actualización automática de las firmas de virus en el horario de 8:00 a.m.

3.3. Diariamente se realizará la exploración automática de los equipos en el horario de 12:40 p.m.

3.4. La oficina de Sistemas es responsable de:

3.4.1. Instalar la Solución antivirus en todas las computadoras de la institución.
3.4.2. Mediante la consola de administración del Antivirus, revisar diariamente que todos los equipos conectados a la Red, hayan actualizado la firma de virus correctamente.
3.4.3. Solucionar contingencias presentadas ante la amenaza de virus según procedimiento **Antivirus Institucional ST-PT-008.**
3.4.4. Realizar las gestiones necesarias para la adquisición o actualización de las licencias de uso.

3.5. Los usuarios de la institución deberán seguir las siguientes normas:

3.5.1. no deberá desinstalar la Solución Antivirus de su computadora ya que ocasionaría un riesgo de seguridad ante peligro de virus.

3.5.2. si el usuario hace uso de medios de almacenamiento, estos tendrán que ser rastreados por la Solución Antivirus.

3.5.3. El usuario deberá comunicarse con la Oficina de Sistemas en caso presente problemas de virus.

3.5.4. El usuario será notificado por la Oficina de Sistemas en los siguientes casos:

3.5.4.1. Cuando sea desconectado de la red con el fin de evitar la propagación de virus a otros equipos de la red.

3.5.4.2. Cuando sus archivos resulten con daños irreparables por causa de virus

3.5.4.3. Cuando viole las políticas de antivirus.

ACCESO FISICO AL CENTRO DE DATOS

1. OBJETIVO

Establecer parámetros de seguridad para el acceso al Centro de Datos donde se encuentran los servidores y equipos de comunicaciones.

2. CONSIDERACIONES

2.1. El acceso al centro de Datos es restringido solamente los empleados que laboran en la oficina de sistemas o personal que tenga que realizar alguna labor relacionada a sistemas acompañadas en todo momento por un representante de la oficina tendrán derecho de ingreso.

2.2. Solo el personal autorizado por el Jefe de Sistemas puede abrir los gabinetes de los servidores y el equipo que está dentro del centro de cómputo.

2.3. El acceso a los servidores, ya sea usando consola de administración local o una consola de administración remota es restringido a personal autorizado por el Jefe de Sistemas. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de servidores se considerara una violación de políticas de seguridad.

2.4. El acceso al centro de datos deberá ser registrado en la planilla de control de accesos que se encontrara al interior de la sala de sistemas, indicando la actividad realizada y la persona que lo acompaño.

2.5. No se permitirá el ingreso de personas con bebidas(café, gaseosas, entre otras)

2.6. El no seguir con lo dispuesto en esta política se considerara como falta grave para la entidad.

USO DE LOS SERVICIOS Y RECURSOS INFORMATICOS

1. OBJETIVO

Delinear el uso adecuado de los equipos informáticos de la UGEL Nº1.

2. CONSIDERACIONES

2.1. No está permitido el uso de los equipos informáticos para la realización de actividades ajenas a la institución.

2.2. Todas las estaciones de trabajo y portátiles deben de ser protegidas con un protector de pantalla desbloquearla por contraseña durante los momentos que el usuario no este atendiendo la terminal. El protector deberá activarse automáticamente a los 10 minutos de inactividad del equipo.

2.3. Los usuarios no pueden modificar el fondo de pantallas previamente configurado por la Oficina de Sistemas.

2.4. Los usuarios deberán contribuir al cuidado de los equipos informáticos asignados, no pueden alterarlos o modificarlos.

2.5. Contribuir al mantenimiento del orden en su estación de trabajo, no consumir ningún tipo de alimento o bebida.

2.6. Al finalizar la actividad laboral se deberá dejar correctamente apagado los ordenadores y equipos informáticos asignados.

2.7. Notificar a la oficina de sistemas las anomalías que detecten en los equipos, tanto Software como Hardware.

2.8. los usuarios en ningún caso podrán acceder físicamente al interior de los ordenadores u otro dispositivo informático que tengan asignado, solo el personal de la oficina de sistemas está autorizado a estas labores.

2.9. Está prohibido La destrucción, sustracción o traslado de cualquier dispositivo informático a personal no autorizado. De encontrar evidencia se considerara falta grave.

2.10. Está prohibido conectar cualquier dispositivo personal como (usb, cámaras, celulares, etc.) a los equipos asignados para sus labores.

2.11. Está prohibido manipular los mecanismos de seguridad instalados en cualquiera de los medios informáticos de la UGEL Nº1, de encontrar evidencia se considerara falta grave.

2.12. Los usuarios en ningún caso podrán borrar o desinstalar las aplicaciones, previamente configuradas por la oficina de sistemas.

RESPALDO DE LA INFORMACION

1. OBJETIVO

Asegurar que la información contenida en los diferentes servidores de la UGEL Nº1 sea resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

2. CONSIDERACIONES

2.1. Solo se realizara el respaldo de la información que se encuentre almacenada en los servidores de la UGEL Nº1.

2.2. Queda estrictamente prohibido almacenar, en las carpetas asignadas en el Servidor archivos de juego, música, información personal u cualquier otra información ajena a la institución.

2.3. Todo sistema deberá contar con la documentación de los procedimientos de respaldo y recuperación antes de entrar a producción.

2.4. Todos los respaldos deberán estar claramente identificados, con etiquetas que indiquen como mínimo los siguientes datos:

2.4.1. Equipo al que pertenece

2.4.2. Fecha y hora de ejecución

2.4.3. Frecuencia, la cual puede ser anual, mensual, semanal o diario

2.4.4. Numero de secuencia

2.4.5. Tipo de respaldo

2.4.6. Nombre del sistema o aplicativo

2.5. Todos los respaldos generados deberán ser llenados en el registro **Respaldo de la información ST-FT-009**

2.6. Los respaldos serán almacenados en una caja fuerte instalada en la sala de servidores, el Jefe de Sistemas y/o persona que el directamente asigne serán los encargados de enviar o retirar los mismos, según procedimiento **ST-PT-010 Respaldo de la Información.**

2.7. La única persona que tendrá acceso al área donde se encuentran los respaldos será el Jefe de la oficina de sistemas o persona que el directamente asigne entregándole la llave del lugar de resguardo.

2.8. Se contara de un espacio físico externo contratado en una empresa proveedora de resguardo externo en cajas de seguridad para almacenar una copia de los Tapes u otro medio almacenamiento.

2.9. El software de respaldo, deberá de estar configurado automáticamente para determinar el éxito o errores en el respaldo de la información.

2.10. El respaldo de la información contenido en los servidores, se efectuara a partir de las 21:00 horas**.**

CONTRASEÑAS PARA USUARIOS DE DOMINIO

1. OBJETIVO

Establecer un estándar para la creación de contraseñas robustas, la protección y la frecuencia de cambio de las mismas dentro de los sistemas y equipos de la UGEL Nº1.

2. CONSIDERACIONES

2.1. Todas las contraseñas de los sistemas de información, como sistema operativo, cuentas de aplicación, etc. Se deberán cambiar con una prioridad de tres meses.

2.2. Las contraseñas son personales no pueden ser comunicadas a otras personas.

2.3. Para la definición de contraseñas se consideraran las siguientes características:

2.3.1. tener una longitud mínima de 6 (seis) caracteres.

2.3.2. Debe de estar conformada con caracteres en mayúscula, minúscula, números y no alfa numéricos (@, $, #,%,&)

2.3.3. No deberá estar basada en información personal, nombres, etc.

2.4. No utilizar la misma contraseña para distintas cuentas de los sistemas y equipos de la UGEL Nº1.

2.5. No utilizar las funciones de recordar las contraseñas que poseen algunas aplicaciones (correo electrónico, sitios web de bancos, etc.)

2.6. No escribir las contraseñas en ningún documento.

RECURSOS COMPARTIDOS

1. OBJETIVO

Describir las políticas bajo las cuales los usuarios, harán uso de los Recursos Compartidos.

2. CONSIDERACIONES

2.1. Del uso General:

2.1.1. La oficina de sistemas proporciona el servicio de Servidor de Archivos, el cual estará estructurado por carpetas cuyos nombres serán los Departamentos que componen la UGEL Nº1.

2.1.2. Los permisos de los usuarios a las diferentes carpetas del Recurso Compartido será mediante el Registro **Gestión de Cuentas ST-FT-005**

2.1.3. La oficina de sistemas no tendrá intromisión en la manipulación de los archivos que se encuentren en las carpetas designadas.

2.1.4. Los usuarios que tengan permisos sobre los archivos compartidos son los responsables de la manipulación de la información.

2.1.5. Los respaldos de la información se realizara una vez a la semana de forma completa y diariamente se realizaran respaldos diferenciales.

2.2. Del uso Personal

2.2.1. queda estrictamente prohibido el uso de recursos compartidos para archivos de audio y video que queden fuera de los objetivos del negocio.

PRESTAMO DE EQUIPO INFORMATICO

1. OBJETIVO

Describir las políticas bajo las cuales los usuarios, podrán solicitar el Préstamo de equipo Informático.

2. CONSIDERACIONES

2.1. La Oficina de Sistemas pone a disposición de los empleados de la UGEL Nº1, el préstamo de equipos informáticos (proyector, cámara de video, computadora portátil) como herramientas de apoyo para las actividades laborales de cada una de las áreas de la institución.

2.2. El préstamo de los equipos informáticos se hace exclusivamente a los empleados de la UGEL Nº1.

2.3. La solicitud de reservación se realizara a través de correo electrónico a la Oficina de Sistemas con un día de anticipación.

2.4. La reservación tiene vigencia de 15 minutos exactos a partir de la hora indicada en la solicitud, transcurrido el lapso el equipo estará a disposición de quien lo solicite.

2.5. El usuario al recoger el equipo informático tendrá que firmar el registro FT-ST-RE-010 Préstamo Equipo Informático.

2.6. El tiempo máximo de préstamo para computadoras portátiles será de cinco días, para el caso de los demás dispositivos (proyector, cámara de video) tendrá máximo un día, en caso se requiera por más tiempo, el usuario deberá justificarlo por escrito a través de una solicitud firmada por su Gerencia de Área.

2.7. El préstamo de los equipos informáticos está sujeto a disponibilidad.

2.8. Al momento de la entrega del equipo informático, el solicitante será el total responsable del resguardo del mismo.

2.9. En caso de mal funcionamiento del equipo informático por manipulación del usuario, este deberá asumir los costos de reparación.

2.10. En caso de extravío por negligencia del usuario, este deberá asumir los costos por la reposición del equipo.

2.11. En caso de hurto o robo, el usuario deberá asumir deberá asumir los costos por la reposición del equipo.

AUDITORIA INTERNA

1. OBJETIVO

Establecer lineamientos sobre las prácticas de auditoria y monitoreo sobre las computadoras, sistemas y redes de la UGEL Nº1.

2. CONSIDERACIONES

2.1. La UGEL Nº1 por este medio provee su consentimiento para permitir realizar auditoria a las computadoras que se encuentren dentro del alcance del objetivo de la auditoria, para realizar actividades de inventario, escaneos y revisión de software y configuraciones instaladas.

2.2. Las actividades de auditoria se realizara a las 19:00 horas para no afectar las labores de los usuarios.

2.3. Los responsables de la auditoria interna son el Jefe de la Oficina de Sistemas y el Encargado de Soporte Técnico.

2.4. Los datos obtenidos en la auditoria deberán ser llenados en el registro **ST-FT-012 Auditoria de Sistemas**

2.5. Cualquier empleado que viole estas políticas será sancionado de acuerdo a los criterios establecidos.

USO DE MEDIOS DE ALMACENAMIENTO REMOVIBLE

1. OBJETIVO

Establecer normas para el uso adecuado de medios de almacenamiento extraíbles así como la importancia de la misma para asegurar la fuga de información.

2. CONSIDERACIONES

2.1. El uso de medios de almacenamiento removibles como (CD, DVD, USB, Memorias Flash, discos duros externos u otros medios de almacenamiento removible, estará autorizado para aquellos usuarios que la Gerencia de su Área lo asigne según Registro Gestión de Cuentas ST-FT-005.

2.2. La Oficina de Sistemas es responsable de implementar los controles necesarios para asegurar que solo los usuarios autorizados puedan hacer uso de los medios de almacenamiento removible.

2.3. Cualquier alteración a los controles de seguridad para dispositivos removibles se considerara como una falta grave.

2.4. Está terminantemente prohibido grabar en dispositivos extraíbles información de la empresa, a usuarios no autorizados. si el usuario encontrase activado los medios para conectar los dispositivos removibles, este tendrá que informar a la Oficina de Sistemas, de encontrar evidencia del uso de estos medios, se considerara falta grave.

USO DEL CORREO ELECTRONICO

1. OBJETIVO

Establecer políticas y términos para la utilización de correo electrónico institucional.

2. CONSIDERACIONES

2.1. La comunicación institucional realizada por Correo Electrónico, solo será a través de las cuentas asignadas.

2.2. El usuario es responsable del contenido de los mensajes enviados.

2.3. Se prohíbe él envió de mensajes que puedan crear un medio ofensivo sobre la raza, sexo, religión, política, nacionalidad, incapacidad u orientaciones personales, en general cualquier tipo de información que cause congestión en la red o interfiera con el trabajo de otros.

2.4. La Oficina de Sistemas bloqueara en forma automática la recepción de correos electrónicos desde aquellas direcciones que se han identificado como código malicioso o virus, en caso que el usuario necesite recibir correo electrónico desde alguna de estas direcciones, deberá comunicarse con el departamento de Sistemas para analizar y atender su solicitud.

2.5. Está prohibido él envió de información que se considere confidencial a cuentas de correo electrónico que no sean de la empresa.

2.6. No se pueden enviar cadenas, chistes o cualquier mensaje que no esté relacionado con los objetivos y razón del negocio.

2.7. Se puede enviar a través de la cuenta de correo electrónico datos adjuntos, siempre y cuando el tamaño máximo no exceda los 20Mb.

2.8. La dirección de correo electrónico se compondrá se la siguiente manera: inicial del primer nombre, seguido del apellido paterno ejemplo: José Castro jcastro@ugel01.gob.pe, si se diera el caso que haya dos usuarios que coincidan la inicial de su primar nombre y el apellido paterno se procederá a completar la dirección de correo electrónico con un elemento diferenciador, como la inicial del apellido materno o inicial del segundo nombre.

2.9. La Oficina de Sistemas es el único encargado en configurar la firma electrónica para cada usuario de correo electrónico, está prohibido cualquier modificación de la misma.

2.10. El tamaño del buzón para usuarios Vip será ilimitado y la configuración del protocolo de correo será IMAP, en el caso de usuarios comunes el protocolo de correo será POP.

INVENTARIO DE RECURSOS INFORMATICOS

1. OBJETIVO

Mantener actualizado y llevar el control de los activos Informáticos de la UGEL Nº1.

2. CONSIDERACIONES

2.1. La Oficina de Sistemas es el encargado de elaborar el inventario de los recursos informáticos.

2.2. La Oficina de Sistemas deberá realizar el inventario de los recursos informáticos cada cuatro meses.

2.3. El inventario a los Recursos informáticos, aplica tanto al Hardware y al Software de Cada equipo Informático.

2.4. La Oficina de Sistemas deberá de entregar una copia del último inventario realizado en el mes de diciembre, al área de logística para su control del inventario anual de activos de la UGEL Nº1.

2.5. La Oficina de Sistemas colocara un sello de seguridad en los equipos Informáticos, los cuales estarán debidamente identificados con su código de equipo.

2.6. Está prohibido remover el sello de seguridad, solo personal de la Oficina de Sistemas está autorizado a la manipulación del mismo.

2.7. La Oficina de Sistemas hará un informe a la Gerencia General sobre las diferencias y/o deficiencias encontradas.

2.8. Al finalizar la toma de Inventario de Recursos Informáticos, el responsable de soporte Técnico deberá actualizar el **Registro Inventario de Recursos Informáticos ST-FT-004.**

USO DEL INTERNET

1. OBJETIVO

Establecer normas que aseguren el buen funcionamiento del Internet.

2. CONSIDERACIONES

2.1. El acceso a internet debe de utilizarse para propósitos relacionados con actividades de la UGEL Nº1 de acuerdo a las funciones laborales del usuario.

2.2. Los sitios web con contenido sexual o pornográfico serán bloqueados automáticamente por el servidor Proxy.

2.3. El usuario no debe de bajar ningún programa, sin la debida autorización de la Oficina de Sistemas

2.4. La transmisión vía internet (escuchar música y ver videos) será bloqueado automáticamente por el Servidor Proxy.

2.5. Está prohibido el uso de páginas de redes sociales como: Facebook, chat, u similares.

2.6. Todos los equipos de cómputo están sujetos a monitoreo de las actividades que se realiza en internet.

2.7. Solo está permitido acceder al servicio de Internet por los medios físicos dispuestos por la Oficina de Sistemas, para el caso de los equipos portátiles cuando se encuentren fuera de la empresa si podrán conectarse a Internet por los medios disponibles en cada momento, sin embargo, el intercambio de información con la red local será únicamente a través de una conexión privada virtual.

PROPIEDAD DE LA INFORMACION

3. OBJETIVO

Establecer que la información que se procese en cualquier dispositivo informático de la UGEL Nº1 es propiedad de la misma.

4. CONSIDERACIONES

4.1. Los usuarios de cualquier equipo de cómputo de la UGEL Nº1 deben estar conscientes que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo de sus actividades laborales, son propiedad de la UGEL Nº1.

5. ACTIVIDADES PROHIBIDAS

5.1. Difundir información identificada como confidencial a través de medios que involucren el uso de Tecnología de la Información

5.2. Utilizar la infraestructura tecnológica de la UGEL Nº1 para conseguir o transmitir material con fines de lucro y/ o cualquier actividad personal.

5.3. Realizar actividades que contravengan la seguridad de los sistemas o generen interrupciones de la red de servicios.

5.4. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.

POLITICA DE CONTRASEÑAS

1. OBJETIVO

El objetivo fundamental de este documento es establecer un estándar para la creación de contraseñas fuertes, favorecer su protección, así como el cambio frecuente de las mismas.

2. CONSIDERACIONES

2.1. Todos los usuarios pertenecientes a la red de la UGEL Nº1 requieren de un nombre de usuario y contraseña para utilizar el equipo de cómputo que tiene asignado y servicios de red como correo electrónico, telefonía IP, etc. Su solicitud deberá realizarse tal y como se establece en el procedimiento Gestión de Cuentas **ST-FT-005**.

2.2. Todas las contraseñas y modificación de las mismas deberán ser registradas en el registro **ST-FT-011 Registro de Contraseñas,** solo personal de la Oficina de Sistemas tendrá acceso al mismo.

2.3. Las contraseñas de los usuarios deben de cumplirse con ciertos requerimientos de seguridad los cuales definirá la Oficina de Sistemas. Las contraseñas son personales y conocidas únicamente por el propio usuario el cual será responsable de toda actividad que realice con ella.

2.4. Por seguridad las contraseñas se cambian cada tres meses.

2.5. La Oficina de Sistemas se reserva el derecho de restablecer en cualquier momento la contraseña de cualquiera de los usuarios, si se detecta que ha sido comprometida.

2.6. Todas las computadoras de escritorio y portátiles deben de tener configurado el protector de pantalla con clave la cual se activara si el equipo se deja desatendido.

3. ACTIVIDADES PROHIBIDAS

3.1. Revelar la contraseña a personal no autorizado o permitir su uso a terceros para actividades ajenas a la UGEL Nº1.

3.2. Anotar la contraseña en libretas, cuadernos, etc. o cualquier medio físico que se encuentre a la vista de todos, la contraseña se tiene que aprender de memoria

CABLEADO ESTRUCTURADO DE VOZ Y/O DATOS

1. OBJETIVO

Describir los lineamientos aplicados para la gestión y ejecución del cableado estructurado de la Red de Datos de la UGEL Nº1.

2. CONSIDERACIONES

2.1. Especificaciones Técnicas de los materiales

2.1.1. Cable UTP:

2.1.1.1. El cableado Horizontal (desde los armarios hasta las rosetas) se realizara con cable UTP ***Categoría 6,*** de 4 pares con un diámetro por conductor de 23 AWG, con separador de pares con sección en cruz.

2.1.1.2. Las cubiertas de los cables deberán ser acorde a las normas internacionales de incendios, IEC-332-1, IEC-754-2, IEC-754-1, IEC-1034.

2.1.1.3. La asignación de colores a los pares se encuentran recogidos en la norma TIA, Categoría 6, 568B.

2.1.2. Conectores RJ45:

2.1.2.1. El conector de categoría 6 deberá cumplir la norma TIA/EIA-568-B

2.1.3. Rosetas:

2.1.3.1. las rosetas cumplirán con las especificaciones de la Categoría 6, TIA, Categoría 6,568-B

2.1.4. Canaletas:

2.1.4.1. La canalización del cableado para la sala de servidores se realizara con bandejas de canalización **metálicas**.

2.1.4.2. La canalización para oficinas se realizara con material plástico PVC.

2.1.5. Armarios:

2.1.5.1. Los armarios de la sala de servidores como los de distribución serán metálicos, aptos para rack de 19”

2.1.5.2. Cada armario tendrá su código de identificación.

2.2. Descripción de la Instalación

2.2.1. Cableado Horizontal:

2.2.1.1. El cableado horizontal deberá cumplir la norma ANSI/EIA/TIA 568-B

2.2.1.2. La longitud máxima de una conexión en par trenzado es de 90 metros

2.2.1.3. El cable del área de trabajo, que va desde la estación de trabajo hasta el punto de red instalado en la Roseta no deberá exceder los 3 metros.

2.2.1.4. La instalación de un nuevo punto de Red, para un usuario, deberá tener como mínimo dos puntos, uno para la red de datos y el otro para la Voz

2.2.1.5. Los extremos de cada cable y las rosetas, deberán tener un código único, con el cual podrá ser identificado dentro de la Red de la UGEL Nº1. La codificación será de la siguiente manera:

2.2.1.5.1. Código de Armario: dos dígitos

2.2.1.5.2. Área: Tres dígitos

2.2.1.5.3. Código de Roseta: dos dígitos

2.2.1.5.4. Código de Conector: un Dígitos

2.2.1.6. Las tomas deben de estar conectadas de acuerdo a la norma ***T568B***

2.2.2. Cableado Vertical

2.2.2.1. El cableado vertical de datos sirve para el enlace entre el armario principal y los armarios de distribución.

2.2.2.2. La codificación para el cableado vertical de datos será de la siguiente manera.

2.2.2.2.1. Letra identificativa del cableado vertical : V

2.2.2.2.2. Código de armario : 2 dígitos

2.2.2.2.3. Numero de Cable: 2 dígitos

2.2.2.3. Se colocara la misma nomenclatura en los dos extremos de cada enlace.

2.2.3. Documentación

2.2.3.1. Todo punto de red configurado, deberá estar documentado, no se considerara ninguna instalación terminada hasta que no se realicen las pruebas de comunicación y documentación.

2.2.3.2. Toda instalación de un nuevo punto de red de Voz y Datos deberá registrarse en el documento. **ST-FT-006 Cableado Estructurado de Voz y Datos.**

2.2.3.3. Toda solicitud para un nuevo punto de Red de Voz y Datos deberá realizarse según Procedimiento **ST-PT-007 Instalación de Cableado estructurado de Voz y Datos**

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

PROGRAMA ANUAL DE MANTENIMIENTO PREVENTIVO A LA INFRAESTRUCTURA INFORMÁTICA

FECHA:

AREA	CODIGO	DESCRIPCION	FECHA ULT. MANTENIMIENTO	MENSUAL	TRIMESTRAL	SEMESTRAL	ANUAL	EMPRESA EXTERNA	FECHAS PROGRAMADAS

ELABORADO POR:	APROBADO POR:
ENCARGADO DE SOPORTE TECNICO	**JEFE DEL DEPARTAMENTO DE SISTEMAS**
FIRMA	FIRMA

PERU Ministerio de Educación — UGEL N° 01 LIMA SUR

MANTENIMIENTO PREVENTIVO A LA INFRAESTRUCTURA INFORMÁTICA

FICHA N°

FECHA

PERSONAL DE SISTEMAS

NOMBRE Y APELLIDOS — CARGO

EMPRESA EXTERNA — TECNICO

DATOS DEL EQUIPO

CODIGO — USUARIO

DESCRIPCION — AREA

ACTIVIDADES REALIZADAS

HORA INICIO — HORA FIN

DESCRIPCION	ESTADO	OBSERVACIONES
ASPIRAR POLVO DEL EQUIPO	☐	
LIMPIEZA DE LA FUENTE DE PODER	☐	
LIMPIEZA DE VENTILADORES	☐	
LIMPIEZA DE LECTOR OPTICO	☐	
APLICAR LIMPIA CONTACTO	☐	
APLICAR REFRIGERANTE AL PROCESADOR	☐	
LIMPIEZA DEL MONITOR	☐	
LIMPIEZA DEL TECLADO Y MOUSE	☐	
ENSERADO DEL EQUIPO	☐	
OTRAS	☐	

RECOMENDACIONES

FIRMA DE SOPORTE TECNICO	**FIRMA DE USUARIO**

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

MANTENIMIENTO CORRECTIVO A LA INFRAESTRUCTURA INFORMÁTICA

FICHA N°

FECHA

DATOS DEL USUARIO

NOMBRE Y APELLIDOS | CARGO

CORREO ELECTRONICO | AREA

PERSONAL DE SISTEMAS

NOMBRE Y APELLIDOS | CARGO

DETALLE DEL PROBLEMA

ACTIVIDADES REALIZADAS

HORA INICIO | HORA FIN

SOLUCION:

ENCUESTA AL USUARIO

MARQUE CON "X" LA OPCION SELECCIONADA

1. ¿ LA ACTITUD DE LA PERSONA QUE LO ATENDIO FUE?
EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA ☐

2. ¿ EL TIEMPO PARA ATENDER SU REQUERIMIENTO FUE?
EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA ☐

3. ¿ LA EXPLICACION DE LA SOLUCION FUE?
EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA ☐

4. ¿ LA CALIDAD DE SERVICIO PROPORCIONADO POR EL SOPORTE TECNICO FUE?
EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA ☐

COMENTARIOS Y/O SUGERENCIAS

FIRMA DE SOPORTE TECNICO	**FIRMA DE USUARIO**

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

INVENTARIO DE RECURSOS INFORMATICOS

FECHA

EXPRESADOS EN NUEVOS SOLES

AREA

USUARIO

CARGO

CODIGO	DESCRIPCION	TIPO	DETALLE	FECHA ADQ.	OC	GUIA REMISION	IMPORTE

TOTAL INVENTARIO

FIRMA DE SOPORTE TECNICO	FIRMA DEL JEFE DE SISTEMAS

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

GESTION DE CUENTAS DE USUARIO

FICHA N° ____

1. DATOS DEL USUARIO (llenado por RR.HH)

DNI: ____

Nombres: ____ Apellidos: ____

Area: ____ Cargo: ____ Local: ____

Fecha Ingreso: ____

2. CARPETAS COMPARTIDAS DE RED (llenado por Gerencia del área)

2.1. Acceso a carpetas compartidas: SI NO

Nota: En caso de seleccionar la opción SI, tendrá acceso por defecto a la carpeta G:\Archivos Temporales (Lectura / Escritura)

2.2 Especificar las carpetas adicionales a las que tendrá acceso y el tipo de acceso

	Lectura	Lectura/ Escritura
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐

3. EMAIL CORPORATIVO (llenado por Gerencia del área)

3.1. Permitir envio a correos externos ☐

3.2. Permitir acceso a correo web (http://mail.fabtechsac.com) ☐

4. ACCESO A INTERNET (llenado por Gerencia del área)

4.1. Permitir acceso a Internet SI NO

Nota: En caso de seleccionar la opcion SI, tendra que especificar las paginas que desea ingresar

Página web	Tipos / Contenido	Sustento

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

CABLEADO ESTRUCTURADO DE VOZ Y/O DATOS

CABLEADO HORIZONTAL

CODIGO ARMARIO	CODIGO AREA	CODIGO ROSETA	CODIGO CONECTOR	TIPO	FECHA INSTALACION

CABLEADO VERTICAL

LETRA	CODIGO ARMARIO	N. CABLE	TIPO	FECHA INSTALACION

FIRMA DE SOPORTE TECNICO	**FIRMA DEL JEFE DE SISTEMAS**

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

INSTALACION DE ANTIVIRUS INSTITUCIONAL

ITEM	AREA	USUARIO	CARGO	NOM. EQUIPO	FECHA INSTALACION

FIRMA DE SOPORTE TECNICO	**FIRMA DEL JEFE DE SISTEMAS**

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

PROGRAMA DE RESPALDO DE LA INFORMACION

PERIODO

ITEM	NOMBRE APLICATIVO / ARCHIVO	SERVIDOR	RUTA	TIPO	FRECUENCIA	OBSERVACION

FIRMA DE JEFE DE SISTEMAS

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

RESPALDO DE LA INFORMACION

PERIODO

SERVIDOR:

APLICATIVO / ARCHIVO

RUTA

ITEM	FECHA / HORA	TIPO	FRECUENCIA	N° SECUENCIA	RESPONSABLE	OBSERVACION

FIRMA DE JEFE DE SISTEMAS

PERÚ | Ministerio de Educación | UGEL N° 01 LIMA SUR

PRESTAMO DE EQUIPO INFORMATICO

FICHA N°

DATOS DEL USUARIO

NOMBRE Y APELLIDOS | CARGO

CORREO ELECTRONICO | AREA

DATOS DEL PRESTAMO

FECHA DE PRESTAMO | FECHA DE DEVOLUCION

EQUIPOS

CODIGO	DESCRIPCION	MARCA	MODELO	DETALLE

MOTIVO:

ACUERDO

Mediante esta ficha se hace constar que se entregan y reciben en calidad de préstamo los bienes aquí relacionados.
El usuario asume el compromiso de devolución de los bienes en las mismas condiciones en que se reciben y en la fecha fijada; igualmente es responsabilidad del usuario la pérdida, daño o deterioro que pueda causar sobre los bienes relacionados, durante el periodo del préstamo

FIRMA DE SOPORTE TECNICO	FIRMA DE USUARIO

PERÚ Ministerio de Educación UGEL N° 01 LIMA SUR

REGISTRO DE CONTRASEÑAS

PERIODO

SERVIDOR: SERVICIO:

ITEM	AREA	USUARIO	FECHA	CONTRASENA INICIAL	FECHA 2	CONTRASENA MODIFICADA 2	FECHA 3	CONTRASENA MODIFICADA 3

UNIDAD DE GESTION EDUCATIVA LOCAL Nº1

DOCUMENTO SOBRE EL ALCANCE DEL SGSI

Código[1]	ST-F-DA-01
Versión:	01
Fecha de la versión:	15-06-2017
Creado por:	Enrique Llanos
Aprobado por:	Ing. Jorge Távara
Nivel de confidencialidad:	

[1] Fuente: Elaboración Propia de codificación de los documentos para la oficina de sistemas.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
10/05/2017	0.1	Enrique Llanos	Creación del documento de alcance del proyecto de sistema de gestión de seguridad de la información.

INDICE

1. Introducción

Este documento forma parte del Sistema de Gestión de Seguridad de la Información (SGSI) de la Unidad de Gestión Educativa Local Nº1, que pertenece al sector educación del Perú y describe los procesos y las actividades implicadas en el marco del SGSI. Para asegurar la comprensión de las actividades de la Unidad de Gestión Educativa Local Nº1, este documento también incluye una descripción detallada del perfil de la entidad.

2. Descripción del alcance

2.1. Perfil de la Unidad de Gestión Educativa Local Nº1

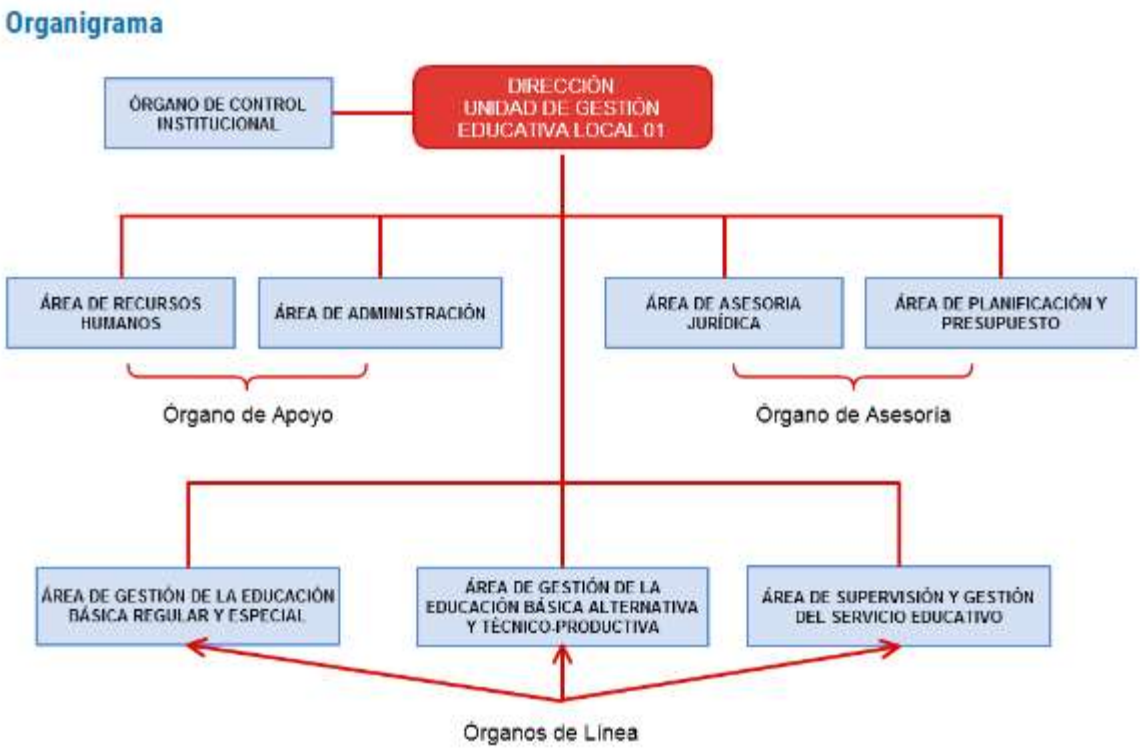
La Unidad de Gestión Educativa Local N° 01 del Distrito de San Juan de Miraflores es una instancia de ejecución descentralizada, con autonomía en el ámbito de su competencia, es responsable del desarrollo y administración de la educación que se ofrece en las Instituciones y Programas Educativos de su ámbito jurisdiccional y depende de la Dirección Regional de Educación de Lima Metropolitana (DRELM). Su jurisdicción territorial posee características heterogéneas en el aspecto demográfico, geográfico y económico, y está determinado mediante Ley 28044 página 26 del año 2003 y D.S. 023-2013-ED y comprende los siguientes distritos: San Juan de Miraflores, Villa María del Triunfo, Villa El Salvador, Pachacamac, Lurín, Punta Hermosa, Punta Negra, San Bartolo, Santa María del Mar, Pucusana y Chilca.

La Unidad de Gestión Educativa Local Nº01, es una entidad pública del sector educación, cuya misión es garantizar derechos, asegurar servicios educativos de calidad a la población para que todos puedan alcanzar su potencial y contribuir al desarrollo de manera descentralizada, democrática, transparente y en función a resultados desde enfoques de equidad e interculturalidad

2.2. Estructura Orgánica

2.2.1. Órganos de Dirección

2.2.2. Organigrama



3. Documentos de Referencia

- Norma ISO/IEC 27001, punto 4,3
- Documento del Plan del proyecto para la implementación de la norma ISO 27001.

4. Alcance del SGSI

El alcance está enfocado en la Oficina de Sistemas, en los procesos de Backup, Seguridad en los medios de comunicación.

4.1. Procesos

4.1.1. Planificación y Mantenimiento de HW y SW.

4.1.2. Procesamiento de Información.

4.1.3. Gestión de Proyectos

4.1.4. Operación de seguridad de información.

4.1.5. Atención de Requerimientos.

4.1.6. Backup.

4.2. Servicios

4.2.1. Servicio de Correo Corporativo.

4.2.2. Servicio de Telefonía IP.

4.2.3. Servicio de Datos (navegación en internet).

4.2.4. Servicio de Red Privada Virtual.

4.3.Unidades Organizativas

4.3.1. Área de Administración

4.3.2. Área de Almacén

4.3.3. Área de Planificación y Presupuesto

4.3.4. Área de Recursos Humanos

4.3.5. Área de Asesoría Jurídica

4.4. Ubicación

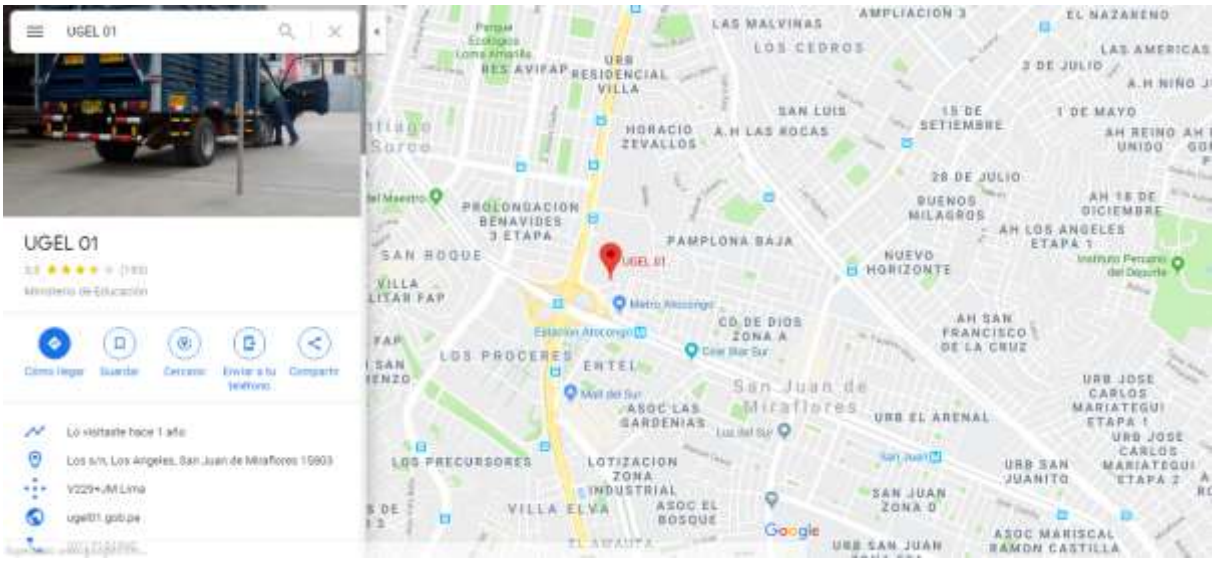


Figura1: Ubicación Geográfica de la Ugel Nº1

5. Redes e infraestructura de TI

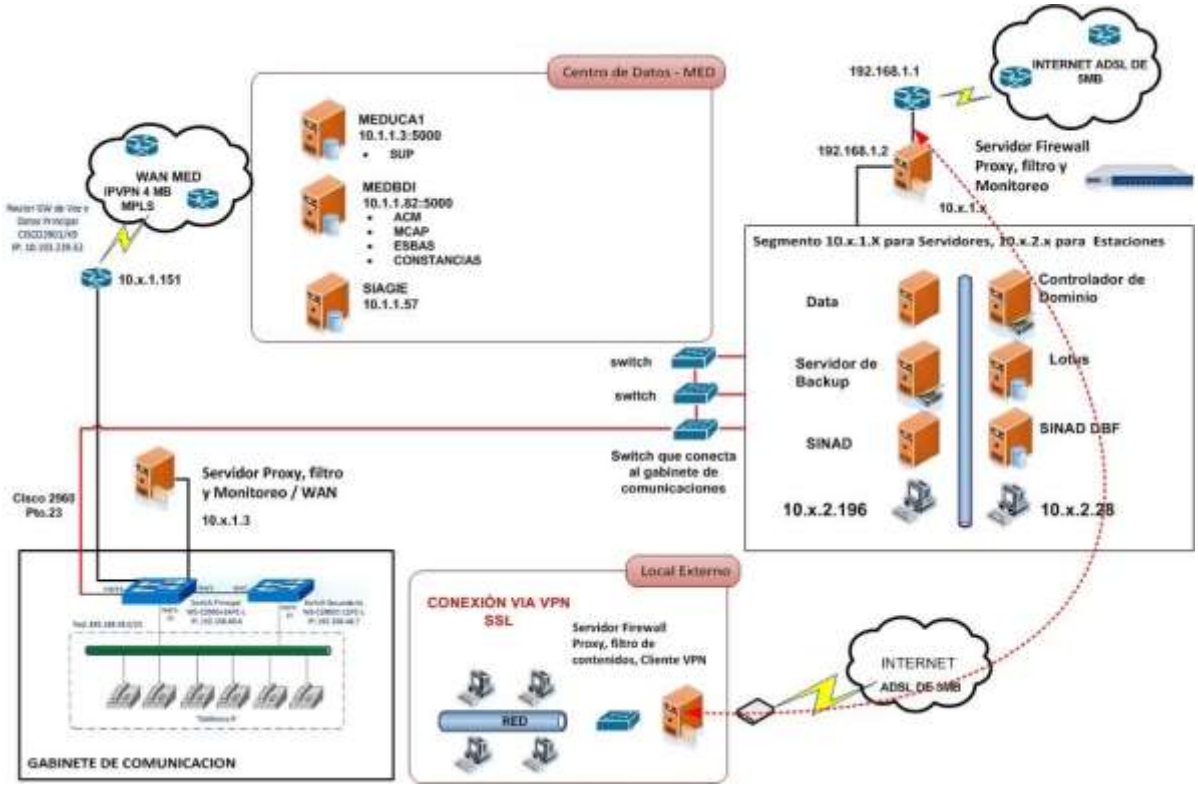


Figura 02[2]**.** Diagrama de Red de la UGEL Nº1

[2] Elaboración propia.

6. Activos de la Oficina de Sistemas

La Oficina de Sistemas cuenta con los siguientes activos de información en la Unidad de Gestión Educativa Local Nº1

DEPENDENCIAS	
BASE DE DATOS DE ERP	Data center
	Electricidad
	Red de Datos
	Servidor Data
	Windows Server 2008
	SQL server 2008
	Software Epicor 9.7
	Personal de Sistemas
	Consultores

DEPENDENCIAS	
INFORMACION DE FILES (PLANOS DE TODOS LOS PROYECTOS REALIADOS)	Data center
	Electricidad
	Red de Datos
	Servidor Files
	CenToS
	Personal de Sistemas
	Internet

DEPENDENCIAS	
BASE DE DATOS DE TELEFONIA IP	Data center
	Electricidad
	Red de Datos
	Servidor Telefonía IP
	CenToS
	Personal de Sistemas
	Personal Conectiva

DEPENDENCIAS	
INTRANET DE LA EMPRESA	Data center
	Electricidad
	Red de Datos
	Servidor Data
	Personal de Sistemas
	Personal Conectiva

DEPENDENCIAS	
INFORMARMACION DE LIBROS CONTABLES	Data center
	Electricidad
	Red de Datos
	Servidor Telefonía IP

	CenToS
	Personal de Sistemas
	Personal Conectiva
DEPENDENCIAS	
SERVIDOR DE BACKUP (veritas)	Data center
	Electricidad
	Red de Datos
	Personal de Sistemas

Tabla de Activos 1: Activos de la Oficina de Sistemas.

6.1.Categorías de los Activos de Información

Categoría de Activos

Tipo	Código	Categoría	Descripción	Responsable	Localización
Activo de Información	A1	Documentos de Sistema	Configuraciones, scripts, versiones	Jorge Távara	Oficina de Sistemas
	A2	Archivos de Data	Conversaciones Presenciales (Capacitaciones, Cursos Virtuales, contratos, acuerdos)	Jair Huarcaya	Oficina de Sistemas
	A3	Base de Datos	Base de Datos y documentos creados conservados en medio electrónicos (Videos)	Milagros Osores	Oficina de Sistemas
	A4	Información Escrita	Documentos creados y conservados en físico Contratos, Licencias, Manuales, Cotizaciones, Órdenes de Compra, Registros de Anteriores, Informes Anuales.	Jorge Távara	Oficina de Sistemas
Activos de Software	A5	Software de Aplicaciones	Sistema Operativo (Windows XP, Windows 7 Pro, Windows Server 2008 R2, Linux, etc.)	José Caro	Oficina de Sistemas
	A6	Software de Predios	Sistema de Instituciones Educativas del ámbito de la Ugel01	José Mechan	Oficina de Sistemas
	A7	Software de Caja	Sistema de flujo de entrada y salida de recursos (Ventas, Almacén, Facturas, Logística, Producción)	José Mechan	Oficina de Sistemas

	A8	Sistema de Agua	Sistemas con módulos de servicios	Jorge Acosta	Oficina de Sistemas
Activo Físico	A9	Equipos de Computo	Laptop (20), PC Escritorio (300), Impresoras multifuncionales (30), scanner (09)	Jair Huarcaya, Wilson Rojas	Oficinas de la Ugel
	A10	Servidores	Servidores (30), Servidor Firewall, Laptop (7), PC Escritorio (10).	José Caro	Data Center
	A11	Equipos de Comunicación	Reuters, switch, Central Digital, Sata, Cableado de Red.	Wilson Rojas, Milagros Osores	Data Center
Servicios	A12	Servicios Eléctricos	Energía Eléctrica, Aire Acondicionado.	Luis Montoya	Luz del Sur
	A13	Servicio de Comunicación	Servicio de Datos, Servicio de Telefonía IP, Servicio RPV (Red Privada Virtual).	Jorge Távara, José Caro	Data Center
	A14	Servicios de soporte en hardware, software y redes	Mantenimiento preventivo, correctivo, helpdesk	Jair Huarcaya, Wilson Rojas	Oficina de Informática
Per son	A15	Oficina de Informática	Personal de la oficina de Informática de la Ugel01	Jorge Távara	Oficina de Informática

	A16	Personal Sede	Personal de otras áreas de la Ugel01	Yovana Mendoza	Oficinas de la Ugel
Intangibles	A17	Imagen	Imagen y Reputación Institucional	Cesar Aponte	Dirección

6.2.Tecnologías

- Herramientas Posgre para SQL Server 2008 R2.
- Herramienta de Base de Datos SQL Server
- Cristal Report 2008

7. Exclusiones del alcance

7.1.1. Planificación y Mantenimiento de HW y SW.

7.1.2. Procesamiento de Información.

7.1.3. Gestión de Proyectos

7.1.4. Operación de seguridad de información.

7.1.5. Atención de Requerimientos.

8. Validez y gestión de documentos

REGISTRO DE APROBACIÓN DE DOCUMENTOS Y FORMATOS

ÁREA SOLICITANTE: _____

DOCUMENTO (S)

CÓDIGO	NOMBRE	VERSIÓN

ETAPA 1: ELABORACIÓN Y ACTUATIZACIÓN PERSONAL A CARGO DE LA ELABORACIÓN O ACTUALIZACIÓN	**FECHA**	**FIRMA**

ETAPA 2: REVISIÓN JEFE DE GESTIÓN		

ETAPA 3: APROBACIÓN GERENTE DE ÁREA	**FECHA DE EMISIÓN**	**FIRMA**
	_____	_____

Fuente: www.iso27001standard.com .

Unidad de Gestión Educativa Local Nº1

POLÍTICA DE SEGURIDAD DEL SGSI

para la implementación del Sistema de gestión de Seguridad de la Información

Código[3]	ST-F-PDP-01
Versión:	01
Fecha de la versión:	20-05-2017
Creado por:	Enrique Llanos Guillen
Aprobado por:	Ing. Jorge Távara
Nivel de confidencialidad:	

[3] Fuente: Elaboración Propia de codificación de los documentos para la Oficina de sistemas.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
10/05/2017	0.1	Enrique Llanos Guillen	Descripción básica del plan del proyecto de sistema de gestión de seguridad de la información

INDICE

POLÍTICA DE SEGURIDAD DEL SGSI

a) La Unidad de Gestión Educativa Local Nº1, establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI) encaminados a mejorar su seguridad, a la oficina de sistemas.

b) La Unidad de Gestión Educativa Local Nº1, es una entidad pública del sector educación, cuya misión es garantizar derechos, asegurar servicios educativos de calidad a la población para que todos puedan alcanzar su potencial y contribuir al desarrollo de manera descentralizada, democrática, transparente y en función a resultados desde enfoques de equidad e interculturalidad.

c) La Unidad de Gestión Educativa Local Nº1, establece, define y revisa los objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI), entendiéndola como la conservación de la confidencialidad, disponibilidad e integridad de su información así como de los sistemas que la soportan, aumentando la confianza de nuestros usuarios.

d) El diseño, implantación y mantenimiento del SGSI, se apoyará en los resultados de un proceso continuo de análisis y gestión de riesgos del que se derivan las actuaciones a desarrollar en materia de seguridad dentro del alcance de la oficina de sistemas.

e) La Dirección de la Unidad de Gestión Educativa Local Nº1, establecerá los criterios de evaluación del riesgo como parte del SGSI, la Dirección desarrollará, implantará y mantendrá actualizado un Plan de Continuidad de Negocio acorde a los objetivos y las necesidades de la empresa y los riesgos que le afectan.

f) La Dirección de la Unidad de Gestión Educativa Local Nº1, se compromete a la implantación, mantenimiento y mejora del SGSI, necesarios concientizando a todo el personal. Para ello la UGEL Nº1 implantará las medidas requeridas para la formación y concienciación del personal con la seguridad de la información.

g) La responsabilidad general de la seguridad de la información recaerá sobre el Responsable del SGSI, siendo la responsabilidad última de la Dirección como máximo responsable del SGSI. Todo usuario tendrá la obligación de reportar los incidentes en materia de seguridad utilizando las directrices en LA Unidad de Gestión Educativa Local Nº1.

h) Todo lo definido en esta política se concretará y desarrollará en normativas y procedimientos del SGSI, las cuales se integrarán con ISO 9001, compartiendo aquellos recursos en la optimización y buscando la mejora continua de la eficiencia y eficacia de la gestión de los procesos.

COMPROMISO DE LA DIRECCION

a) La Dirección se compromete a la implementación, mantenimiento y mejorar el SGSI dotándolo de aquellos medios y recursos que sean necesarios e integrando a todo el personal para que asuma este compromiso. Para ello la Dirección implantará las medidas requeridas para la formación y concienciación del personal con la seguridad de la información. A su vez, cuando los trabajadores incumplan las políticas de seguridad la Dirección se reserva el derecho de aplicar las medidas disciplinarias acordes al convenio de los trabajadores y dentro del marco legal aplicable, y dimensionadas al impacto que tengan sobre la organización.

b) La responsabilidad general de la seguridad de la información recaerá sobre el Responsable del SGSI, siendo la responsabilidad última de la Dirección como máximo responsable del SGSI. Todo usuario tendrá la obligación de reportar los incidentes en materia de seguridad utilizando las directrices establecidas por la Ugel Nº1.

c) La presente política será de aplicación a todo el personal y recursos que se encuentran dentro del alcance del SGSI, se pone en su conocimiento y es comunicada a todas las partes interesadas.

LISTADO MAESTRO DE DOCUMENTOS

ITEM	CODIGO	DESCRIPCIÓN DEL DOCUMENTO	VERSIÓN	FECHA EMISIÓN	OBSERVACION
		AREA: SISTEMAS			
		DOCUMENTO (POLITICA)			
1	ST-DO-001	POLITICA DE ANTIVIRUS	00		
2	ST-DO-002	ACCESO FISICO AL CENTRO DE DATOS	00		
3	ST-DO-003	USO DE LOS SERVICIOS Y RECURSOS INFORMATICOS	00		
4	ST-DO-004	RESPALDO DE LA INFORMACION	00		
5	ST-DO-005	CONTRASEÑAS PARA USUARIOS DE DOMINIO	00		
6	ST-DO-006	RECURSOS COMPARTIDOS	00		
7	ST-DO-007	PRESTAMO DE EQUIPO INFORMATICO	00		
8	ST-DO-008	AUDITORIA INTERNA	00		
9	ST-DO-009	USO DE MEDIOS DE ALMACENAMIENTO REMOVIBLE	00		
10	ST-DO-010	USO DEL CORREO ELECTRONICO	00		
11	ST-DO-011	INVENTARIO DE RECURSOS INFORMATICOS	00		
12	ST-DO-012	USO DEL INTERNET	00		
13	ST-DO-013	PROPIEDAD DE LA INFORMACION	00		
14	ST-DO-014	POLITICA DE CONTRASEÑAS	00		
15	ST-DO-015	CABLEADO ESTRUCTURADO DE VOZ Y/O DATOS	00		
		PROCEDIMIENTO			
1	ST-PT-001	MANTENIMIENTO PREVENTIVO A LA INFRAESTRUCTURA INFORMATICA	00		
2	ST-PT-002	MANTENIMIENTO CORRECTIVO A LA INFRAESTRUCTURA INFORMATICA	00		
3	ST-PT-003	INVENTARIO DE RECURSOS INFORMATICOS	00		
4	ST-PT-004	CREACION, MODIFICACION O ELIMINACION DE CUENTAS DE ACTIVE DIRECTORY	00		
5	ST-PT-005	ALTA O BAJA DE CUENTAS DE CORREO ELECTRONICO	00		
6	ST-PT-006	ALTA O BAJA DE USUARIO DE TELEFONIA IP ASTERISK	00		
7	ST-PT-007	INSTALACION DE CABLEADO ESTRUCTURADO DE VOZ Y/O DATOS	00		

8	ST-PT-008	INSTALACION DE ANTIVIRUS INSTITUCIONAL			
9	ST-PT-009	ACTUALIZACION Y MONITOREO DE ANTIVIRUS INSTITUCIONAL			
10	ST-PT-010	RESPALDO DE LA INFORMACION			
		FORMATO			
1	ST-FT-001	PROGRAMA ANUAL DE MANTENIMIENTO PREVENTIVO A LA INFRAESTRUCTURA INFORMATICA	00		
2	ST-FT-002	MANTENIMIENTO PREVENTIVO A LA INFRAESTRUCTURA INFORMATICA	00		
3	ST-FT-003	MANTENIMIENTO CORRECTIVO A LA INFRAESTRUCTURA INFORMATICA	00		
4	ST-FT-004	INVENTARIO DE RECURSOS INFORMATICOS	00		
5	ST-FT-005	GESTION DE CUENTAS	00		
6	ST-FT-006	CABLEADO ESTRUCTURADO DE VOZ Y/O DATOS	00		
7	ST-FT-007	ANTIVIRUS INSTITUCIONAL	00		
8	ST-FT-008	PROGRAMA DE RESPALDO DE LA INFORMACION	00		
9	ST-FT-009	RESPALDO DE LA INFORMACION			
10	ST-FT-010	PRESTAMO DE EQUIPO INFORMATICO			
11	ST-FT-011	REGISTRO DE CONTRASEÑAS			
		MANUAL			
1	ST-MN-001	CREACION, MODIFICACION O ELIMINACION DE CUENTAS DE ACTIVE DIRECTORY	00		
2	ST-MN-002	CREACION, MODIFICACION O ELIMINACION DE CUENTAS DE CORREO ELECTRONICO	00		
3	ST-MN-003	ACCEDER AL CORREO INSTITUCIONAL VIA INTERNET	00		
4	ST-MN-004	CREACION, MODIFICACION O ELIMINACION DE ANEXO TELEFONICO EN LA CENTRAL IP	00		
5	ST-MN-005	CREACION, MODIFICACION E INACTIVACION DE USUARIOS EN EL ERP EPICOR	00		

DECLARACION DE APLICABILIDAD SOA

N°		Dominio - Control	#Ctrls	Aplica	Justificacion	Responsable
A5	**Politica de seguridad de la Información**		2	SI		
	Dirigir y dar soporte a la gestion de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.			NO		
A.5.1.1	Política de seguridad de la información	Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.		SI	Según el Documento de Politica	Comité de Seguridad de la Informacion
A.5.1.2		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.			Según el Documento de Politica	Comité de Seguridad de la Informacion
A6	**Organización de la seguridad de la información**		11			
	Gestionar la organización de la seguridad de información.					
A.6.1.1	Organización interna	La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.		SI	Según el documento del alcance	Comité de Seguridad de la Informacion
A.6.1.2		En las actividades de SI participan representantes de todas las UU.OO. Tienen roles y funciones.		SI	Esta establecido esas funciones por la Dirección	Dirección de la Ugel
A.6.1.3		Los roles y responsabilidades en SI están bien definidos.		SI	Esta establecido esas funciones por la Dirección	Dirección de la Ugel
A.6.1.4		Está establecido el proceso de autorización para nuevos activos de información (AI).		NO	La Ugel no considera eso indispensable.	Oficina de Sistemas
A.6.1.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.		NO	La Ugel no considera eso indispensable.	Oficina de Sistemas
A.6.1.6		Se mantiene los contactos apropiados con las autoridades pertinentes.		SI	Esta establecido esas funciones por la Direccion	Dirección de la Ugel
A.6.1.7		Se mantiene los contactos apropiados con entidades especializadas en SI.		SI	Los contratos son revisados por los abogados de la Ugel.	Area Juridica
A.6.1.8		El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.		NO	Contamos con solo 2 personas en el area.	Comité de Seguridad de la Informacion
A.6.2.1	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.		NO	Contamos con ninguna metodologia para gestionar los riesgos	Area de Planificación y Presupuesto
A.6.2.2		Se trata todos los requerimientos de SI antes de dar acceso a los clientes.		SI	Según lo requiera algun cliente o proveedor.	Area de Planificación y Presupuesto
A.6.2.3		Se establece acuerdos con terceros, que involucran acceder, procesar, comunicar o gestionar la información de la entidad , que abarcan los requerimientos de SI relevantes.		SI	Los acuerdos estan astablecidos en los contratos de los proveedores de servicios.	Area de Planificación y Presupuesto
A7	**Gestión de activos de información (AI)**		5			
	Lograr y mantener la protección apropiada de los activos de información					
A.7.1.1		Se mantiene un inventario de AI.		SI	Tiene un inventario General.	Oficina de Sistemas

A.7.1.2	Responsabilidad por los activos	Todo AI tiene asignado un responsable (propietario).		SI	Los usuarios de aca equipo son responsables.	Oficina de Sistemas
A.7.1.3		Se dispone de una normativa de uso de los AI		NO	cuenta con ninguna norma para hacer IA	Oficina de Sistemas
A.7.2.1	Clasificación de la información	La información esta clasificada según su valor, requisitos legales, sensibilidad y criticidad		NO	Esta clasificada de esamanera, tienes un inventario general	Oficina de Sistemas
A.7.2.2		Se dispone del procedimiento de rotulado y manejo de la información.		NO	cuenta con ninguna procedimiento para manejo de informacion	Comité de Seguridad de la Informacion
A8	**Seguridad de los recursos humanos**		**9**			
	Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y asi reducir el riesgo de robo, fraude o mal uso de los activos de información.					
A.8.1.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidadesde de SI, de todo el personal.		SI	Se tiene una norma interna que se aplica.	Dirección de la Ugel
A.8.1.2		Se verifica antecedentes de todo candidato a empleado o contratista.		SI	Esta expuesto como una norma interna	Dirección de la Ugel
A.8.1.3		Se firman contratos donde se incluye las responsabilidades de SI.		NO	Lo consideran de suma importancia.	Dirección de la Ugel
A.8.2.1	Durante el empleo	Se procura que todos los empleados apliquen la SI según la política.		NO	Toman que sea obligatorio	Dirección de la Ugel
A.8.2.2		Se sensibiliza, capacita y educa en SI pertinente a su función de trabajo.		SI	Realiza induccion a los sistemas.	Comité de Seguridad de la Informacion
A.8.2.3		Se tiene establecido un procesos disciplinario ante el incumplimiento de SI.		SI	Se tiene una norma interna que se aplica.	Comité de Seguridad de la Informacion
A.8.3.1	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.		NO	Se informa a las demas areas del personal que ya no laborara.	Recursos Humanos
A.8.3.2		Se procura la entrega de activos al término de contrato.		SI	Realizara una auditoria y revision de las informacion que no sea borrada.	Comité de Seguridad de la Informacion
A.8.3.3		Se retira los derechos de acceso al término del contrato.		SI	Procede a bloquear dicho usuario.	Oficina de Sistemas
A9	**Seguridad física y medioambiental**		**13**			
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.					
A.9.1.1	Áreas seguras	Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las areas que contienen información e instalaciones que procesan información.		SI	Por camaras de video vigilacia, personal de seguridad.	Comité de Seguridad de la Informacion
A.9.1.2		Se utiliza mecanismos de control de acceso en entradas críticas.		SI	Por sistema de llave convencional	Oficina de Sistemas
A.9.1.3		Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.		SI	Señalizaciones de Zonas seguras en las oficinas.	Area de Infraestructura
A.9.1.4		Se utiliza mecanismos de protección ante amenzas externas y ambientales.		NO	Cuenta con esos mecanismos de seguridad frente a amenazas	Comité de Seguridad de la Informacion
A.9.1.5		Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.		SI	Por el mecanismo de seguridad de Infraestructura.	Area de Infraestructura
A.9.1.6		Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).		SI	Por el mecanismo de seguridad de Infraestructura.	Area de Infraestructura
A.9.2.1		Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.		NO	Cuenta con esos mecanismos de seguridad	Oficina de Sistemas

A.9.2.2	Seguridad del equipo	Los equipos están protegidos frente a fallas de servicios públicos.		SI	Son tan frecuentes que pase	Oficina de Sistemas
A.9.2.3		El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.		NO	Tiene una adecuada proteccion frente a un daño.	Oficina de Sistemas
A.9.2.4		Los equipos son mantenidos en forma periódica.		SI	Por el mantenimiento preventivo que se realiza	Oficina de Sistemas
A.9.2.5		Se aplica seguridad a los equipos fuera del local		SI	Para prevenir la fuga de informacion o robo	Oficina de Sistemas
A.9.2.6		Antes de dar de baja un equipo se elimina la información		SI	Para verificar que no contenga informacion de la Ugel	Oficina de Sistemas
A.9.2.7		Todo equipo requiere autorización para ser retirado de la Institución		SI	Por parte de la Jefatura general	Oficina de Sistemas
A10	**Gestión de operaciones y comunicaciones**		**32**			
	Asegurar la operacion correcta y segura de los activos de información					
A.10.1.1	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados y disponible a los usuarios.		SI	Para mantener el orden en la documentacion de los usuarios	Comité de Seguridad de la Informacion
A.10.1.2		Gestión del control de cambios en los recursos de procesamiento de información.		SI	Según su Jefatura inmediata para proceder al cambio	Jefatura Inmediata de su area
A.10.1.3		Segregación de responsabilidades para reducir el mal uso de los activos.		SI	Según su Jefatura inmediata para proceder al cambio	Jefatura Inmediata de su area
A.10.1.4		Separaración de los recursos de desarrollo, prueba y producción.		NO	Se desarrolla esta operaciones en la Ugel	Oficina de Sistemas
A.10.2.1	Gestion de la entrega de servicios de terceros	Procurar que los terceros implementen, operen y mantengan los controles de seguridad.		SI	Para tener mayor seguridad y poner clausulas en los contratos con proveedores	Comité de Seguridad de la Informacion
A.10.2.2		Monitoreo y auditoria regular de los servicios e informes de terceros.				Comité de Seguridad de la Informacion
A.10.2.3		Gestionar los cambios en servicios de terceros, considerando criticidad de sistema de negocio así como procesos involucrados y la evaluacion de riesgos.		NO	Tenemos servicios con terceros que sean criticos	Comité de Seguridad de la Informacion
A.10.3.1	Planeación y aceptación del sistema	Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar buen desempeño.		SI	tener un mejor uso con el sistema y los usuarios mejoren su desempeño.	Oficina de Sistemas
A.10.3.2		Establecer los criterios de aceptación de sistemas y realizar las pruebas antes de la aceptación.		SI	Para ser obligado por la alta Jefatura a la utilizacion del sistema	Comité de Seguridad de la Informacion
A.10.4.1	Protección contra software malicioso y código móvil	Implementar controles de prevención, detección y recuperación ante software malicioso, así como controles adecuados para la toma de conciencia.		SI	Para los venderores que usan telefonos moviles para comunicarse.	Comité de Seguridad de la Informacion
A.10.4.2		Asegurar que el código móvil autorizado opere de acuerdo a las políticas de seguridad.		NO	El personal no esta capasitado para esos	
A.10.5.1	Copias de respaldo (back-up)	Se realiza copias de respaldo de información y software, y se prueba regularmente.		SI	Tenemos informacion critica que se necesita tener copias de seguridad	Oficina de Sistemas
A.10.6.1		Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.		SI	Tener claros los segmentos y direcciones IP asignadas	Oficina de Sistemas

A.10.6.2	Gestión de seguridad de redes	Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red estan identificados e incluido en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la Ugel o subcontratos.		SI	Por medio del proveedor de servicio de internet y datos	Comité de Seguridad de la Informacion
A.10.7.1	Gestión de medios (activos de almacenamiento)	Se dispone de procedimientos para la gestión de medios removibles.				
A.10.7.2		Se dispone de procedimientos formales para la eliminación de medios.		SI	Tenemos un procedimiento para la eliminacion de medios	Oficina de Sistemas
A.10.7.3		Se dispone de procedimientos para el manejo de información de manera confidencial.		NO	Tenemos prodecimientos de confidencialidad	Comité de Seguridad de la Informacion
A.10.7.4		La documentación de los sistemas es protegida del acceso no autorizado.		SI	Tenemos solo pueden utilizar como lectura los usuarios	Oficina de Sistemas
A.10.8.1	Intercambio de información (transferencia)	Se dispone de normativa para proteger la información durante su intercambio en cualquier medio de comunicación.		NO	Tenemos normas al realizamos intercambio de informacion	Comité de Seguridad de la Informacion
A.10.8.2		Se firma acuerdos para el intercambio de información y software con entidades externas		NO	Realizamos intercambio de informacion	Comité de Seguridad de la Informacion
A.10.8.3		Se protege los medios en tránsito contra acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución.		NO	Realizamos intercambio de informacion	Comité de Seguridad de la Informacion
A.10.8.4		Se protege adecuadamente la información involucrada en los mensajes electrónicos.		SI	Por medio del servidor de correo y las politicas de spam	Oficina de Sistemas
A.10.8.5		Se dispone de normativa para proteger la información asociada con la interconexión de los sistemas de información de la institución.		NO	Disponemos de normativas para el intercambio de informacion.	Oficina de Sistemas
A.10.9.1	Servicios de comercio electrónico	Se protege la información de comercio electrónico que se trasmite en redes públicas, contra actividades fraudulentas, litigios contractuales y divulgación o modificación.		NO	la Ugel no realiza ventas por internet de sus equipos.	Direccion
A.10.9.2		Se protege la información de las transacciones en línea: De transmisión incompleta, pérdida de rutas, alteración, divulgación y duplicidad.		NO	la Ugel no realiza ventas por internet de sus equipos.	Direccion
A.10.9.3		Se protege la integridad de la información disponible públicamente.		NO	la Ugel no realiza ventas por internet de sus equipos.	Direccion
A.10.10.1	Monitoreo (de actividades no autorizadas)	Se registra pistas de auditoria, excepciones y eventos de seguridad.		NO	Por el equipo de calidad de la Ugel	Area de Planificación y Presupuesto
A.10.10.2		Se dispone de procedimientos de monitoreo del uso de recursos y se revisa regularmente.		NO	Realizamos monitoreo de los recursos de monitoreo	Oficina de Sistemas
A.10.10.3		Se protege la información y los medios de registro frente a acceso manipulado o no autorizado.		SI	Por normas internas que establece la Dirección	Dirección de la Ugel
A.10.10.4		Se registra las actividades del administrador y operador del sistema.		SI	Se deben de segistrar las actividades realizadas en el dia a dia	Oficina de Sistemas
A.10.10.5		Se registran las fallas, se analizan y se toma la acción apropiada.		NO		
A.10.10.6		Los relojes de los sistemas de procesamiento de información se mantienen sincronizados.		NO	Tenemos un servidor que se sincronize con un servidor de relojes	Comité de Seguridad de la Informacion
A11	**Control de acceso (lógico)**		**25**			

A.11	Controlar el acceso lógico a los activos de información					
A.11.1.1	Requerimientos	Se dispone de una política de control de acceso con base en requerimientos del negocio y de seguridad para el acceso.		NO	Tiene una política de control para la seguridad	Comité de Seguridad de la Información
A.11.2.1	Gestión de acceso de usuarios	Se dispone de procedimiento de registro y baja de concesión de acceso a los sistemas y servicios de información.		SI	Tiene como norma pero mas no como procedimiento.	Comité de Seguridad de la Información
A.11.2.2		Se dispone de procedimiento para la gestión (restricción, control y asignación) de privilegios.		SI	Para tener una buena gestion en los privilegios	Oficina de Sistemas
A.11.2.3		Se dispone de procedimiento para la gestión de contraseñas.		SI	Para no ser vulneradas facilmente	Oficina de Sistemas
A.11.2.4		Se audita los derechos de acceso de manera regular.		NO	Tenemos personal suficienete para realizarlo	Comité de Seguridad de la Información
A.11.3.1	Responsabilidades de usuarios	Se promueve las buenas prácticas de seguridad para la selección y uso de contraseñas seguras.		SI	Para que sean contraseñas robustas ante un ataque.	Oficina de Sistemas
A.11.3.2		Se promueve que los usuarios deben asegurar la protección de los equipos desatendidos.		SI	Pero no son consientes de la proteccion de los equipos	Oficina de Sistemas
A.11.3.3		Se promueve la práctica de escritorio limpio para documentos y dispositivos de almacenamiento removibles, y una política de pantalla limpia.		SI	Para no tener algun indicio de contraseñas o informacion condifencial	Oficina de Sistemas
A.11.4.1	Control de acceso a la red	Los usuarios solo tienen acceso a los servicios que están autorizados.		SI	Para poder determinar los permisos que solo tenga a un usuario determinado	Oficina de Sistemas
A.11.4.2		Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos.		SI	Se tienes que controlar quienes iran a ingresar y que permiso tendra.	Oficina de Sistemas
A.11.4.3		La identificación del equipo forma parte de la autenticacion.		SI	Se determina si el equipo es propietario de la Ugel o no.	Oficina de Sistemas
A.11.4.4		Se controla el acceso para el diagnóstico y configuración de puertos.		NO	Se considera importante para la Ugel.	Comité de Seguridad de la Información
A.11.4.5		Se segrega en la red, los usuarios y sistemas de información.		SI	Según los indiquen que usuarios o que sistemas.	Oficina de Sistemas
A.11.4.6		Se restringe la capacidad de conexión de usuarios a redes compartidas.		SI	Para poder determinar los permisosque solo tenga el personal TI.	Oficina de Sistemas
A.11.4.7		La red se configura de modo que no se infrinja los controles de acceso.		SI	Para que no afenten es sus labores al usuario.	Oficina de Sistemas
A.11.5.1	Control de acceso al sistema operativo	Se controla el acceso al SO en las estaciones o terminales (procedimiento de conexión segura).		SI	Para poder determinar los permisos que solo tenga el personal TI.	Oficina de Sistemas
A.11.5.2		Todo usuario dispone de una cuenta de acceso única.		SI	Para poder determinar los permisos.	Oficina de Sistemas
A.11.5.3		El sistema de gestión de claves asegura su calidad.		SI	Tiener una adecuada seguridad en contraseñas	Oficina de Sistemas
A.11.5.4		Se restringe el uso de utilidades (software) no autorizadas, que podrían eludir las medidas de control del sistema.		SI	Para no permitir instalar cualquier software	Oficina de Sistemas
A.11.5.5		Las sesiones inactivas se cierran luego de un tiempo de inactividad.		SI	Para la seguridad las aplicaciones de Alto riesgo.	Oficina de Sistemas
A.11.5.6		Se restringe el horario de acceso a las aplicaciones de alto riesgo.		SI	Para la seguridad de cada usuario	Oficina de Sistemas

A.11.6.1	Control de acceso a las aplicaciones e información	Se restringe el acceso a los usuarios y al personal de TI.		SI	Tienes que tener sus respectivos permisos para ingresar a los sistemas.	Oficina de Sistemas
A.11.6.2		Los sistemas sensibles están en un ambiente aislado.		SI	Tienen que estar en un ambiente adecuado y protegido.	Oficina de Sistemas
A.11.7.1	Computación móvil y teletrabajo	Se dispone de política de protección de equipos móviles.		NO	Realizamos teletrabajo en la Ugel	Dirección de la Ugel
A.11.7.2		Se dispone de política y procedimiento para teletrabajo.		NO	Realizamos teletrabajo en la Ugel	Dirección de la Ugel
A12	**Adquisición, desarrollo y mantenimiento de sistemas de información**		**15**	NO	Desarrollamos softwares en la Ugel	Comité de Seguridad de la Informacion
	Procurar que la seguridad sea una parte integral de los sitemas de información.					
A13	**Gestión de incidentes de seguridad de información**		**5**			
	Asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción correctiva oportuna.					
A.13.1.1	Reporte de incidentes y debilidades	Los incidentes de SI se reportan por los canales apropiados tan rápido como sea posible.		SI	Por medio via Telefonico, correo, herramienta mantis.	Oficina de Sistemas
A.13.1.2		Se promueve que todo el personal reporte las debilidades de SI, que observe o sospeche.		NO	Solo se preocupan de sus tareas, al ver algo inusual no se reporta al area de sistemas	Comité de Seguridad de la Informacion
A.13.2.1	Gestión de incidentes y mejoras	Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de SI.		SI	Medio remotos o vis telefonica para solucionar los incidentes.	Oficina de Sistemas
A.13.2.2		Se dispone de mecanismos para aprender a resolver incidentes, que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de SI.		NO	Lo consideras de suma importancia.	Dirección de la Ugel
A.13.2.3		Se recolecta y mantiene evidencias (para fines de auditoría).		SI	Según la norma se tienes que tener los registros que avidencien donde se realiza.	Oficina de Sistemas
A14	**Gestión de continuidad de operaciones**		**5**			
	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos, de los efectos de fallas significativas o desastres, y asegurar su reanudación oportuna.					
A.14.1.1	Gestión de la continuidad operativa	Se dispone de un proceso de gestión de continuidad de operaciones.		NO	Tiene este proceso de gestion.	Dirección de la Ugel
A.14.1.2		Se realiza gestión de riesgos.		SI	Pero solo al nivel riesgo en seguridad de Infraestructura	Comité de seguridad de Infraestructura.
A.14.1.3		Se dispone de un Plan de Continuidad de Operaciones (PCO).		SI	Esta consideran has que ocurra dicho suceso.	Dirección de la Ugel
A.14.1.4		Se maneja un único marco referencial de PCO.		NO	Lo consideras de suma importancia.	Dirección de la Ugel
A.14.1.5		El PCO se prueba y actualiza en forma regular.		NO	Se prioriza obras obligaciones y se deja de lado.	Dirección de la Ugel
	Cumplimiento regulatorio		**11**			

A15	Evitar el incumplimiento de cualquier ley, estatuto, obligación, reglamentao o contractuales, y de cualquier requisito de seguridad.					
A.15.1.1	Con los requerimientos legales	Se ha definido, documentado y mantiene actualizado todos los requisitos legales, reglamentarios, contractuales pertinentes.		SI	tendremos que estar actualizados en al normas y leyes vigentes.	Recuros Humanos
A.15.1.2		Se dispone de procedimientos para respetar la propiedad intelectual.		NO	se aplica en la Ugel	Dirección de la Ugel
A.15.1.3		Se protege los registros importantes de la organización.		SI	Estos registros pueden desprestigiar a la Ugel	Comité de Seguridad de la Informacion
A.15.1.4		Se protege la privacidad de la información personal, según la regulaciones.		SI	según las normas de la Ugel	Comité de Seguridad de la Informacion
A.15.1.5		Se sensibiliza al personal para evitar usos no autorizados.		SI	Evitar la fuga de informacion de la Ugel	Oficina de Sistemas
		Se hace uso de cifrado, según las regulaciones.		SI	Pero solo en la VPN por el proveedor	Oficina de Sistemas
A.15.1.6		Se hace uso de cifrado, según las regulaciones.				
A.15.2.1	Con las politicas y estándares de S.I.	Se procura el cumplimiento de los procedimientos de SI.		SI	Estar mas ordendos y mantener los registros	Oficina de Sistemas
A.15.2.2		Se procura el cumplimiento de la normativa de SI en los sistemas de información.		SI	Para mantener la seguridad de los activos	Oficina de Sistemas
A.15.3.1	Auditoria de los sistemas de información	Se planifica las auditorias internas de sistemas de información.		SI	Esta establecido por el comite de Seguridad.	Comité de Seguridad de la Informacion
A.15.3.2		Se protege el acceso a las herramientas de auditoria de sistemas de información.		SI	Esta establecido por el comite de Seguridad.	Comité de Seguridad de la Informacion
			133	75		

	ID	CONTROL	ACTIVO DE INFORMACION	ACTIVIDAD / DESCRIPCION	PRIORIDAD	ESTADO	RESPONSABLE	F.TERMINO
POLITICA	A.05.1.2	Revisión de la política de seguridad de la información	Política de Seguridad de la Información / SGSI	La política de seguridad de la información se revisara periódicamente semestral mente con el comite de SGSI o cuando se presenten realizar un cambios en la organización, resultados de auditorías.	A	Iniciado	ETI / APP	
ORGANIZACION DE LA SEGURIDAD	A.06.1.1	Asegurar la actitud de compromiso frente a la Seguridad de la Información	- Comité de Seguridad de la Información o Comité de Riesgos - SOA	Se debe mantener y administrar la seguridad de la información en la organización activamente a través de la alta dirección, demostrando la actitud de compromiso frente al tema y asignando los recursos humanos necesarios que deben tener claras las responsabilidades que tienen para dar cumplimiento a la normativa de seguridad de la información. Se debe elaborar el documento con la declaración de aplicabilidad SOA (Specification Of Applicability)	A	Iniciado	ETI / APP	
	A.06.1.7	Contacto con grupos de interés especiales	-Registro en Plan de Continuidad de Negocios - Registro en Procedimiento de Gestión de Incidentes	Se debe mantener los contactos apropiados con grupos de interés especiales, foros especializados de seguridad de la información, asociaciones de profesionales en seguridad	M	Iniciado	ETI / APP	
	A.06.1.8	Revisión independiente de la seguridad de la información	Procedimiento de Auditoria Internas del SGSI	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (objetivos de control, controles, políticas, procesos, y procedmientos) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad. Se debe elaborar el documento con la declaración de aplicabilidad SOA	A	Iniciado	ETI / APP	
	A.06.2.1	Identificación de los riesgos para el acceso de terceros	- Análisis y Evaluación de Riesgos - Política de Servicios con Terceros - Acuerdos de Confidencialidad y penalidades en Contratos	Se debe identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos de negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso	A	Iniciado	APP / DU	

GESTION DE ACTIVOS	A.07.1.1	Inventario de Activos	Inventario de Activos de Información (primera entregable del Proceso de Análisis y Evaluación de Riesgos)	Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de activos críticos para la organización. Mantener inventario de activos vigente (en línea) a disposición de los usuarios autorizados	A	Iniciado	ETI / APP	
	A.07.1.3	Uso adecuado de los activos	Política de Seguridad de uso de los recursos informáticos	Se debe identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	A	Iniciado	ETI / APP	
	A.07.2.1	Directrices de Clasificación	Inventario de Activos de Información (atributos a considerar para cada activo)	La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización	A	Iniciado	ETI / APP	
	A.07.2.2	Etiquetado y tratamiento de la información	Activos de Información (formato físico o lógico)	Se debe contemplar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización	A	Iniciado	ETI / APP	
D DE RRHH	A.08.1.1	Roles y responsabilidades	Reglamento de Seguridad de la Información	Se debe definir y documentar los roles y responsabilidades de los empleados, contratistas, y usuarios de terceras partes, de acuerdo con la política de seguridad de la información de la organización	A	Iniciado	APP / DU	
	A.08.2.1	Responsabilidades de la Dirección	Reglamento de Seguridad de la Información	La dirección debe exigir que los empleados, contratistas, y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización	A	Iniciado	APP / DU	
	A.08.2.2	Concienciación y formación en seguridad de la información	Programa de Capacitación y Sensibilización en Seguridad de la Información al personal, contratistas y terceros.	Todos los empleados de la organización y cuando sea pertienente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinenete para sus funciones laborales. Se debe realizar mayor sensibilización (divulgar periódicamente las políticas de seguridad) a todos los funcionarios de BCRP.	A	Iniciado	RRHH / ETI	

SEGURIDA	A.08.2.3	Proceso disciplinario	Reglamento Interno de Trabajo (sanciones por incumplimiento de políticas de seguridad información)	Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad, que haya violado las políticas de la organización	A	Iniciado	RRHH / ETI	
	A.08.3.1	Responsabilidades en la terminación del contrato	- Contrato de Trabajo de Personal. - Contrato de Servicios con Terceros	Se debe definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral	M	Iniciado	RRHH / ETI	
	A.08.3.3	Eliminación de derechos de acceso	-Procedimiento de Altas y Bajas de Usuarios -Procedimiento de Gestión de Activos	Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato.	A	Iniciado	RRHH / ETI	
SEGURIDAD FÍSICA	A.09.2.1	Instalación y protección de equipos	Activos de información (hardware)	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado	A	Iniciado	ETI / APP	
	A.09.2.2	Suministros	Activos de información (hardware)	Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suminstro	A	Iniciado	ADM / ETI	
	A.09.2.4	Mantenimiento de equipos	Activos de información (hardware)	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. Renovación de PC´s: Establecer la configuración adecuada. Se debe definir contrato de mantenimiento para todos los equipos del BRCP	M	Iniciado	ETI / APP	
	A.09.2.5	Seguridad de los equipos fuera de las instalaciones	Activos de información (hardware)	Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. Se debe documentar las recomendaciones para el uso de equipos portátiles con la respectiva implementación de controles que se deben seguir.	M	Iniciado	ADM/ ETI	
	A.09.2.6	Seguridad en la reutilización o eliminación de equipos	Activos de información (hardware)	Se debe verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación. Se debe definir políticas y procedimientos para la eliminación o reutilización segura de medios que hayan podido contener información sensible de la Organización	M	Iniciado	ETI	

	A.13.1.2	Reporte sobre las debilidades de la seguridad	-Procedimiento de Gestión de Incidentes (reporte de eventos) - Service Desk	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sitemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sitemas o servicios. Registrar incidentes en la mesa de ayuda (ServiceDesk) y crear la base de conocimientos	A	Iniciado	ETI	
	A.13.2.1	Responsabilidades y procedimientos	- Procedimiento de Gestión de Incidentes	Se debe establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz, y ordenada a los incidentes de seguridad de la información	A	Iniciado	ETI	
	A.13.2.2	Aprendizaje de las incidencias de seguridad de la información	- Service Desk (Base de Conocimiento)	Debe existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información	A	Iniciado	ETI / APP	
	A.13.2.3	Recolección de evidencia	- Service Desk (Base de Conocimiento) - Logs,evidencias de hechos o incidentes presentados	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales, la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecida en la jurisdicción pertinente	A	Iniciado	ETI	
DE CONTINUIDAD	A.14.1.1	Inclusión de la seguridad de la información en el proceso de la gestión de continuidad del negocio	Sistema de Gestión de Continuidad de Negocios (SGCN)	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización	M	Iniciado	ETI / APP	
	A.14.1.2	Continuidad del negocio y evaluación de riesgos	Plan de Continuidad de Negocios (PCN): - Definición de Escenarios de Desastres - Análisis de Impacto al Negocio (BIA)	Se debe identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información	A	Iniciado	APP / DU	

GESTION I	A.14.1.4	Estructura para la planificación de la continuidad del negocio	Plan de Continuidad de Negocios (PCN)	Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	A	Iniciado	APP / DU	
	A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Plan de Pruebas del PCN	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia. Se debe definir un esquema de continuidad operativa y realizar las respectivas pruebas	A	Iniciado	ETI / APP	
CUMPLIMIENTO	A.15.1.3	Protección de los registros de la organización	Activos de Información (Documentos, Información Digital)	Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio	A	Iniciado	SETI	
	A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	Activos de Información (Hardware, Software, Servicios de Terceros, Red de Comunicaciones)	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados	A	Iniciado	SRTI	
	A.15.1.6	Reglamentación de los controles de cifrado	Activos de Información (Información Digital)	Se debe utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes	M	Iniciado	ETI	
	A.15.2.1	Cumplimiento con las políticas y normas de seguridad	Reglamento de Seguridad de la Información	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad	A	Iniciado	ETI / APP	
	A.15.2.2	Verificación del cumplimiento técnico	Activos de Información (Software, Sistemas de Información)	Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad	A	Iniciado	ETI / APP	

	A.15.3.1	Controles de auditoria de sistemas	Activos de Información (Software)	Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio	A	Iniciado	ETI / APP	
	A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Activos de Información (Sistemas de Información)	Se debe proteger el acceso a las herramientas de auditoria de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro	A	Iniciado	ETI / APP	