UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO 27002 EN LA ASOCIACIÓN PARA EL DESARROLLO EMPRESARIAL EN APURÍMAC – ADEA

Presentado por

KLIFFOR PALOMINO PALOMINO

TRABAJO DE SUFICIENCIA PROFESIONAL PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

ANDAHUAYLAS – APURÍMAC – PERÚ

2017

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Presentado por

KLIFFOR PALOMINO PALOMINO

BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO 27002 EN LA ASOCIACIÓN PARA EL DESARROLLO EMPRESARIAL EN APURÍMAC – ADEA

Asesor:

ING. EDWING ALCIDES MAQUERA FLORES

ANDAHUAYLAS – APURÍMAC – PERÚ

2017

DEDICATORIA

A mis padres Félix y Paulina, quienes con su amor incondicional me apoyaron en todo momento y dieron todo por mí.

A mis amigos de esta tierra querida Andahuaylas, quienes fueron fuente de inspiración y experiencia para seguir adelante y cumplir mis metas trazadas, mi completa gratitud para ellos.

AGRADECIMIENTO

A Dios por darme luz y bendición en mí día a día.

A mis padres, por ser mi fuente de vida, amor y educación.

A mis hermanos, Lucy, Olger, Jakeline, Ronny, Huberth y Daniel, siempre queridos y extrañados.

A Yaneth, por ser mi motor y motivo de superación.

TABLA DE CONTENIDOS

INDICE DE TABLAS

RESUMEN

En el presente informe de experiencia profesional se describe un proyecto de implementación de buenas prácticas en seguridad de la información basada en ISO 27002, para la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

Dicha entidad ofrece varios servicios, siendo el más importante de ellos el rubro de servicios financieros, donde hace uso de herramientas tecnológicas para la automatización de sus procesos, por lo cual actualmente tiene alta dependencia de la misma.

En dicho contexto, se procedió a realizar la identificación del estado actual de la seguridad de la información, mediante la verificación de los objetivos de control de la norma ISO 27002 en ADEA, además se tuvo que hacer uso de los niveles de madures del CMMI, haciendo un modelo que esquematice mejor el objetivo del proyecto.

Ante esta situación, el objetivo que se planteo fue de reducir la exposición al riesgo alto implícito en el proceso de salvaguarda de la información de la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros, con el uso del código de buenas prácticas en seguridad de la información de la norma ISO 27002.

Esta reducción del riesgo consistió en la implementación de soluciones tecnológicas, elaboración de políticas de seguridad de la información (documento de carácter confidencial el cual está custodiado por dicha organización), capacitación y la mejora continua de las mismas en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

ABSTRACT

This report of professional experience describes a project of implementation of good practices in information security based on ISO 27002, for the Association for the Business Development in Apurímac - Andahuaylas and Chincheros.

This entity offers several services, the most important of which is the financial services sector, where technological tools are used to automate their processes, which is why it is highly dependent on it.

In this context, the current state of information security was identified by verifying the control objectives of the ISO 27002 standard in ADEA, in addition to the use of CMMI maturity levels, making a model that better outlines the objective of the project.

Given this situation, the objective was to reduce the exposure to high risk implicit in the process of safeguarding the information of the Association for Business Development in Apurímac - Andahuaylas and Chincheros, with the use of the code of good practices in security of the information of the ISO 27002 standard.

This risk reduction consisted in the implementation of technological solutions, development of information security policies (confidential document which is guarded by said organization), training and the continuous improvement of the same in the Association for Business Development in Apurímac - Andahuaylas and Chincheros.

INTRODUCCIÓN

Actualmente los sistemas de información, los datos contenidos en ellas y la información, son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Una manera efectiva de descubrir estas vulnerabilidades y amenazas existentes es iniciando los procesos de diagnósticos que permitan establecer el estado actual de la seguridad dentro de la organización, teniendo en cuenta los procesos de análisis y evaluación de riesgos.

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información, permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación.

Para lograr una adecuada protección de los activos informáticos, los sistemas de información, los datos y la información, fue necesaria la intervención de todo el personal de la entidad, incluyendo a los directivos que deben avalar el proyecto y brindar el apoyo a todo el personal que esté involucrado en el manejo de los activos y sistemas informáticos. Estas acciones estuvieron enmarcadas en un proceso lógico, sistemático, documentado, que tuvo que ser difundido internamente para garantizar la gestión correcta de la seguridad informática y de la información, siguiendo el ciclo de mejora continua (planear, hacer, verificar y actuar - PHVA). Inicialmente se trató de comprender la norma ISO/IEC27001 en cada uno de los dominios, para determinar el alcance de su aplicabilidad. Una vez definidos los dominios y determinados los activos existentes, se aplica la metodología para realizar análisis y evaluación de riesgos respecto a los tres criterios de información que son la confidencialidad, la integridad y la disponibilidad de la información.

La siguiente tarea consistió en la verificación de la existencia de controles de seguridad existentes en la empresa y su aplicación; ya que podían estar incluidos dentro de los procesos de calidad organizacionales. Estos debían ser comparados con los controles definidos en la norma ISO/IEC 27002 como políticas y procedimientos; el resultado servirá de base para el diseño, la

implementación e implantación futura de un SGSI como respuesta a los riesgos encontrados.

En el informe se muestra un conjunto de instrumentos que posibilitaron realizar el análisis y evaluación de riesgos, las técnicas utilizadas para conocer y comprender el estado inicial y post implementación en la organización evaluada y que pueden ser aplicados para realizar procesos de auditoría a la seguridad.

Se explica también el marco metodológico que se utilizó para aplicar el proceso de análisis y evaluación de los riesgos desde la fase inicial de conocimiento del sistema, la fase de identificación de las vulnerabilidades, amenazas y riesgos de seguridad determinando el nivel de riesgo al que estaba expuesta la organización, por probabilidad e impacto en los criterios de confidencialidad, integridad y disponibilidad de la información, para luego establecer un control en el nivel de cumplimiento de los objetivos de control de la ISO 27002.

CAPITULO I: ASPECTOS GENERALES

1.1. Datos generales de la entidad

La Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA Andahuaylas, es una institución sin fines de lucro que promociona y desarrolla la micro y pequeña empresa en Apurímac y aporta al desarrollo local a través de sus servicios y programas, mediante el otorgamiento de créditos, el servicios de micro seguros y la capacitación empresarial a la MYPE y los emprendimientos de mujeres trabajadoras, favoreciendo el desarrollo económico local sostenible permanente de la región con una visión empresarial.

DATOS LA EMPRESA

RAZON SOCIAL	: ASOC.DES.EMP.APURIMAC, ANDAHYLS Y CHINCH
NOMBRE COMERCIAL	: ADEA – ANDAHUAYLAS
DIRECCION	: AV. PERÙ Nº 363 – ANDAHUAYLAS – APURIMAC
RUC Nº	: 20527005745
TELEFONOS	: 083 – 421698 – 422132
PAGINA WEB	: www.adea.org.pe

VISIÓN

“Ser líder en la provisión de servicios empresariales de calidad a los microempresarios rurales y urbanos de la región”

MISIÓN

“Brindamos innovadores servicios empresariales y de calidad a nuestros clientes, microempresarios rurales y urbanos de la región, creciendo con ellos de manera sostenida y buscando los mejores niveles de satisfacción, con el apoyo de nuestros colaboradores comprometidos y entidades vinculadas, con un enfoque de medio ambiente y de inclusión de género”.

VALORES

- ✓ Igualdad
- ✓ Solidaridad
- ✓ Respeto
- ✓ Honestidad
- ✓ Lealtad
- ✓ Compromiso Social

CONSULTA RUC

CONSULTA RUC: 20527005745 - ASOC.DES.EMP.APURIMAC, ANDAHYLS Y CHINCH		
Número de RUC:	20527005745 - ASOC.DES.EMP.APURIMAC, ANDAHYLS Y CHINCH	
Tipo Contribuyente:	ASOCIACION	
Nombre Comercial:	A.D.E.A. ANDAHUAYLAS	
Fecha de Inscripción:	10/01/2002	**Fecha Inicio de Actividades:**
Estado del Contribuyente:	ACTIVO	
Condición del Contribuyente:	HABIDO	
Dirección del Domicilio Fiscal:	AV. PERU NRO. 363 (A 1/2CDA. DEL PARQUE LAMPA DE ORO) APURIMAC - ANDAHUAYLAS - ANDAHUAYLAS	
Sistema de Emisión de Comprobante:	MANUAL/MECANIZADO/COMPUTARIZADO	**Actividad de Comercio Exterior:**
Sistema de Contabilidad:	COMPUTARIZADO	
Actividad(es) Económica(s):	Principal - 9499 - ACTIVIDADES DE OTRAS ASOCIACIONES N.C.P.	
Comprobantes de Pago c/aut. de impresión (F. 806 u 816):	FACTURA BOLETA DE VENTA NOTA DE CREDITO	
Sistema de Emisión Electrónica:	-	
Afiliado al PLE desde:	01/01/2014	
Padrones :	Incorporado al Régimen de Buenos Contribuyentes (Resolución Nº 0930050005764) a partir del 01/08/2015	

Figura 1: Consulta RUC de ADEA
Fuente: SUNAT - http://e-consultaruc.sunat.gob.pe

SERVICIOS

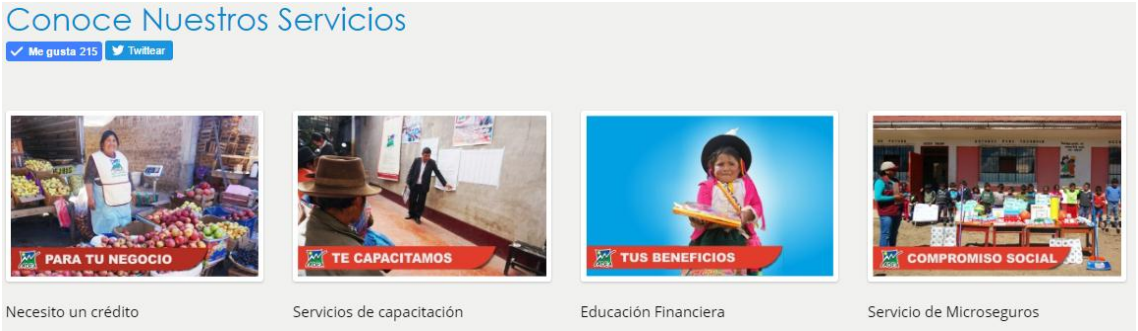


Figura 2: Servicios que brinda ADEA
Fuente: Pagina web de ADEA – http://www.adea.org.pe

- ✓ Créditos financieros

  Ofrecemos créditos a la micro y pequeña empresa y por supuesto a los emprendimientos económicos de mujeres emprendedoras.

- ✓ Capacitaciones

  Capacitación empresarial a las MYPEs y a los emprendimientos de las mujeres trabajadoras. Servicios de capacitación en gestión empresarial con enfoque de género, generando mejora económica y social en el ámbito rural y urbano.
- ✓ Beneficios

  Micros seguros para cada uno de nuestros clientes.

  Educación financiera dirigida a personas naturales con negocio propio y personas jurídicas que necesiten una cuenta para realizar sus operaciones diarias.
- ✓ Compromiso social

  Llevando apoyo a los que más necesitan en las zonas más alejadas de nuestra región. Desarrollamos procesos permanentes y sostenidos de formación y capacitación asesoría y atención a mujeres humildes.

UBICACIÓN

ADEA tiene como área de influencia parte de la región Apurímac, y está presente en 3 provincias con la presencia de 5 oficinas: La sede Central de ADEA está ubicada en Av. Perú N° 363 Provincia de Andahuaylas. La segunda oficina de atención, se encuentra en la Av. Los Incas N° 596 del distrito de Anccohuayllo, provincia de Chincheros. Su tercera oficina se encuentra en la Av. Bolívar N° 415 del distrito de Huancarama, provincia de Andahuaylas. La cuarta oficina se encuentra en el Jr. Progreso S/N del distrito de Huancaray, provincia de Andahuaylas. Por ultimo mencionar su última oficina aperturada en la Av. Perú N° 411, del distrito de Abancay, Provincia de Abancay.

Oficina principal en Andahuaylas, 2014

Figura 3: Fotografía de la fachada de la oficina Andahuaylas en 2014
Fuente: Google Maps

Oficina Andahuaylas, Julio 2017

Figura 4: Fotografía de la fachada de la oficina Andahuaylas en 2017
Fuente: Elaboración propia

Figura 5: Plano ubicación en Andahuaylas
Fuente: Google Maps

Agencias en Abancay, Uripa, Huancarama y Huancaray.

Figura 6: Distribución de Agencias de ADEA
Fuente: ADEA Andahuaylas

Oficina URIPA - ANCCOHUALLO

Figura 7: Fotografía de la fachada de la agencia Uripa
Fuente: Elaboración propia

Oficina Huancarama

Figura 8: Fotografía de la fachada de la agencia Huancarama
Fuente: ADEA Andahuaylas

Oficina Abancay

Figura 9: Fotografía de la fachada de la agencia Abancay
Fuente: ADEA Andahuaylas

Oficina Huancaray

Figura 10: Fotografía de la fachada de la agencia Huancaray
Fuente: Elaboración propia

1.2. Reseña histórica de la entidad

Desde el año 1994 hasta el año 2009 FORM/TRIAS Bélgica y APEMIPE Andahuaylas han estado firmando convenios para promover el desarrollo empresarial en Apurímac.

Los resultados logrados han permitido coadyuvar el desarrollo empresarial de la microempresa en Apurímac y también el fortalecimiento de ADEA Andahuaylas.

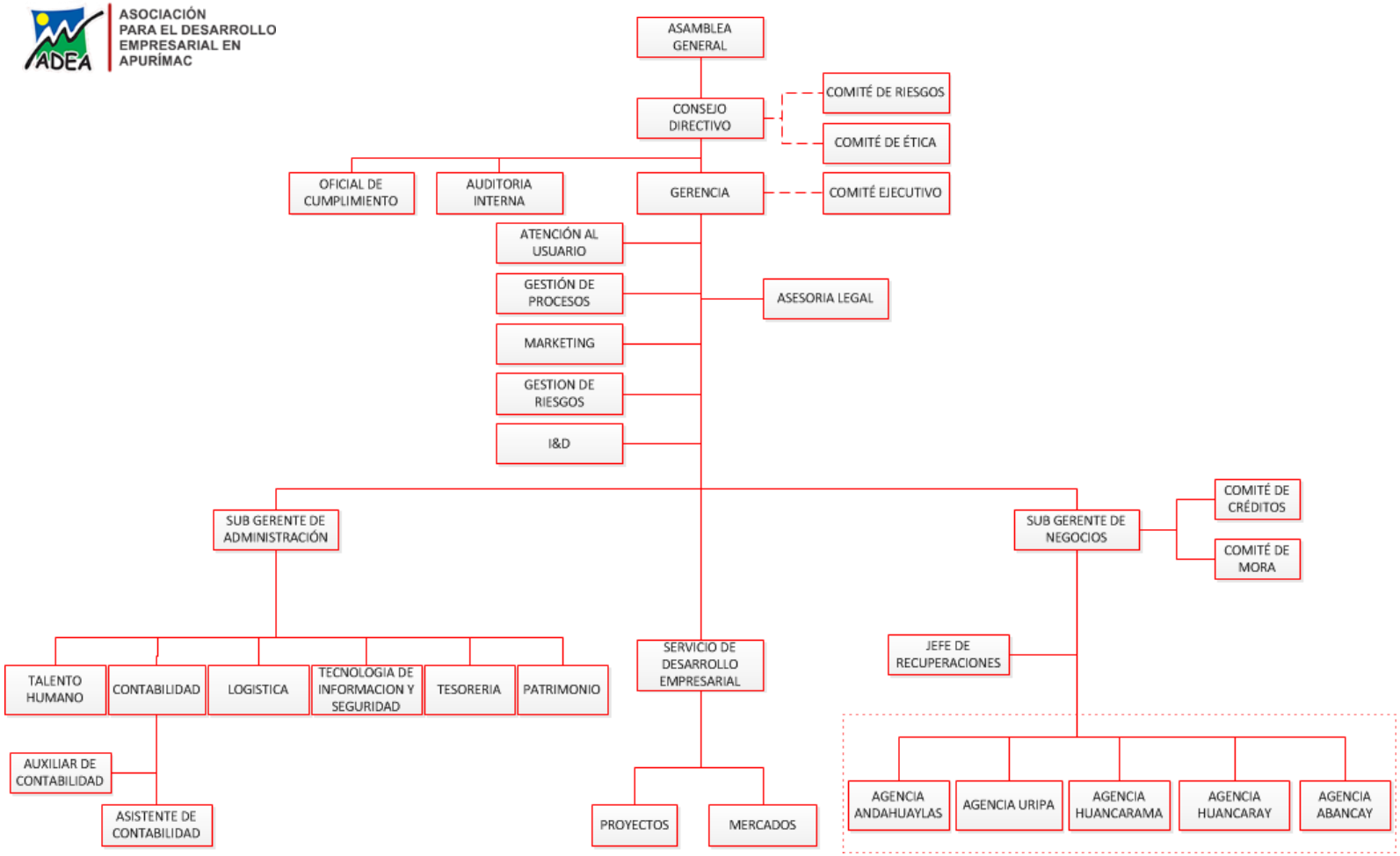
La Asociación para el Desarrollo Empresarial en Apurímac - Andahuaylas y Chincheros, fue fundada el 11 de Noviembre del 2001, en la ciudad de Andahuaylas. Actualmente cuentan con cinco oficinas en Apurímac, su oficina principal en Andahuaylas y sus agencias en Abancay, Huancarama, Uripa y Huancaray[1].

1.3. Estructura organizacional de la entidad

El presente organigrama fue aprobado en el 2017.

[1] Página web de ADEA URL: www.adea.org.pe/reseña-historica.html

ORGANIGRAMA JERARQUICO DE ADEA[2]



[2] Aprobado en sesión de consejo directivo de ADEA en fecha 20/10/2017, vigente desde el 01/11/2017.

1.4. Definición del problema

Es inevitable percibir a los 15 años transcurridos en este segundo milenio, el constante avance tecnológico que estamos viviendo, avance caracterizado por su incesante desarrollo y crecimiento en toda su amplitud. Los sistemas de información no solo están orientados a acopiar datos, procesarlos, distribuirlos y guardaros. Sino también salvaguardarlos, el sector financiero es uno de los sectores con mayor dependencia tecnológica en el mundo, a tal grado de considerarse por su alta dependencia tecnológica como crítico. Según el estándar TIA 942, que clasifica a los negocios según el riesgo de interrupción de data center o centro de procesamiento de datos, los bancos o entidades financieras configuran un riesgo elevado, en su escala de 3 niveles; escaso, medio y elevado. Es decir el más alto.

Claro está que los sistemas transaccionales que operan en dichos negocios generan grandes volúmenes y tráficos de información a diario, ya que el valor del dinero está sujeto al tiempo.

La importancia de salvaguardar la información de las organizaciones se ha hecho cultura por su altísimo valor que representa.

Cabe señalar que este riesgo depende del grado de exposición y la probabilidad de que un hecho suceda, bajo esta premisa podemos afirmar que mientras exista una fracción de posibilidad el riesgo es inevitable pero a la vez es mitigable; En enero del 2015, en el Reino Unido la ICO (Information Commissioner's Office, Oficina de Comisionados de Información) multó a un hospital del Reino Unido con 375 000 libras esterlinas por sufrir en sus mismas instalaciones el robo de discos duros con información confidencial que se pusieron finalmente a la venta a través de eBay. Del mismo modo, en los últimos años una serie de bancos minoristas han sido víctimas de robos de dispositivos de almacenamiento con información de clientes. Los datos no solo se pueden robar virtualmente, sino también físicamente. En todos los

casos, el robo no solo representó la pérdida de los activos físicos sino también de información valiosa. (Banca15, 2017)

En Junio del 2017, los analistas de Kaspersky Lab han investigado la reciente ola de ataques de ransomware; tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, estaba dirigidos a organizaciones alrededor del mundo. Se trataba de un nuevo ransomware que no se había visto anteriormente. La información de telemetría de la empresa señala que alrededor de 2,000 usuarios han sido atacados hasta el momento. Organizaciones en Rusia y Ucrania han sido las más afectadas y también hemos registrado ataques en Polonia, Italia, Reino Unido, Alemania, Francia, Estados Unidos y varios países más. (Kaspersky Lab, 2017).

Podrían citarse muchos casos más, no obstante está claro el valor que representa la información en organizaciones de alta dependencia. A través de los 15 años de existencia de ADEA, se han generado grandes volúmenes de información que en muchos casos son de naturaleza confidencial, asimismo día a día se generan alrededor de 1000 registros en promedio.

La información de ADEA está expuesta a riesgo no solo la que se encuentra en medios digitales sino también las que se encuentran en medios físicos, Las amenazas son latentes, y basta con interactuar con otros dispositivos de hardware o elementos de software para considerarse objeto de vulnerabilidad, más aún que dependemos de la red de redes, el lugar virtual donde se comente variedad de delitos informáticos. Entendiéndose que según AADAT (2017), citan que la Organización para la Cooperación Económica (OCDE) en París en 1983, definió al delito informático como “cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la trasmisión de datos”.

En el Perú los delitos informáticos se viene tratando a través de la legislación que estipula lo siguiente, el Art. 11 del código penal “son

delitos y faltas las acciones u omisiones dolosas o culposas penadas por Ley", los ilícitos se agrupan en:

- Robo bajo sus distintas modalidades
- Daño en propiedad ajena
- Terrorismo
- Privación ilegal de la libertad
- El abuso de confianza
- El Fraude
- La violación de correspondencia
- La falsificación de documentos
- La revelación de secretos

En ADEA Andahuaylas, se observó que dicha exposición al riesgo no es vista con importancia, a pesar de su alta dependencia de la información.
A continuación describo algunos sucesos en referencia a la seguridad de la información.
En Junio del 2014, por falta de control de información y actualización de la misma, conllevaron a un problema judicial de uso de datos de un personal que ya no laboraba en la entidad. El hecho de no actualizar la información, dar de baja todos los accesos a las diferentes plataformas tecnologías de ADEA, generaron un perjuicio económico para la entidad.

En Enero del 2015, la falta de equipos de contingencia en su agencia Uripa, conllevo a que la oficina se cerrara temporalmente y deje de atender.
El equipo servidor había sufrido un problema electrónico y su disco duro se quemó, haciendo difícil la recuperación de la información de las transacciones del ultimo día. Ello genero pérdidas económicas y la desconfianza de los clientes en la entidad.
Hasta Octubre del 2015, la institución trabajaba con servidores en cada agencia y no estaba centralizado, la infraestructura de red actual era inadecuada, porque no permite controlar y administrar la transmisión de información que ingresa desde el exterior de su red de área local, contando con una simple configuración de los equipos de la red y el

control en el acceso a páginas web innecesarios, que pueden provocar la propagación de amenazas de la Internet, además la deficiente administración de los servicios, tales como: Correo Electrónico, Servidor Web, Servidores de Archivos e Impresoras. El inapropiado procedimiento de compartir datos y recursos entre sus diferentes áreas, provoca que la información no esté disponible en el tiempo requerido, en general no controlan el impacto de los riesgos a los que están expuestos sus activos de información.

Si bien no han sucedido daños o perjuicios mucho más graves podemos afirmar que solo es cuestión de tiempo para que esto suceda.

1.4.1. Problema

Existencia de alto riesgo implícito en el proceso de salvaguarda de la información de la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

1.5. Definición de los objetivos

Reducir la exposición al riesgo implícito en el proceso de salvaguarda de la a información de la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros

1.5.1. Objetivos específicos

1. Diagnosticar y comprender el estado actual de la seguridad de la información en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.
2. Planificar e implementar soluciones tecnológicas con énfasis en la seguridad de la información en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.
3. Controlar y evaluar los procesos de aseguramiento y protección de los activos de información en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

1.6. Alternativas de solución

a) Implementación de las políticas de seguridad informática
    a. Implementación de políticas de seguridad de la información reactivas.

b) Implementar buenas prácticas de seguridad de la información
    a. Implementación de buenas prácticas en seguridad de la información

1.7. Planteamiento de la solución optima

Implementación de buenas prácticas en seguridad de la información basada en ISO 27002 para la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros.

Esta solución consistió de las siguientes fases de desarrollo.

4. Diagnosticar y comprender el estado actual de la seguridad de la información en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

5. Planificar e implementar soluciones tecnológicas con énfasis en la seguridad de la información basado en las buenas prácticas basadas en ISO 27002 para la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

6. Controlar y evaluar los procesos de aseguramiento y protección de los activos de información basadas en ISO 27002 para la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros.

MARCO METODOLÓGICO PARA LA IMPLEMENTACIÓN DE LA SOLUCIÓN ÓPTIMA

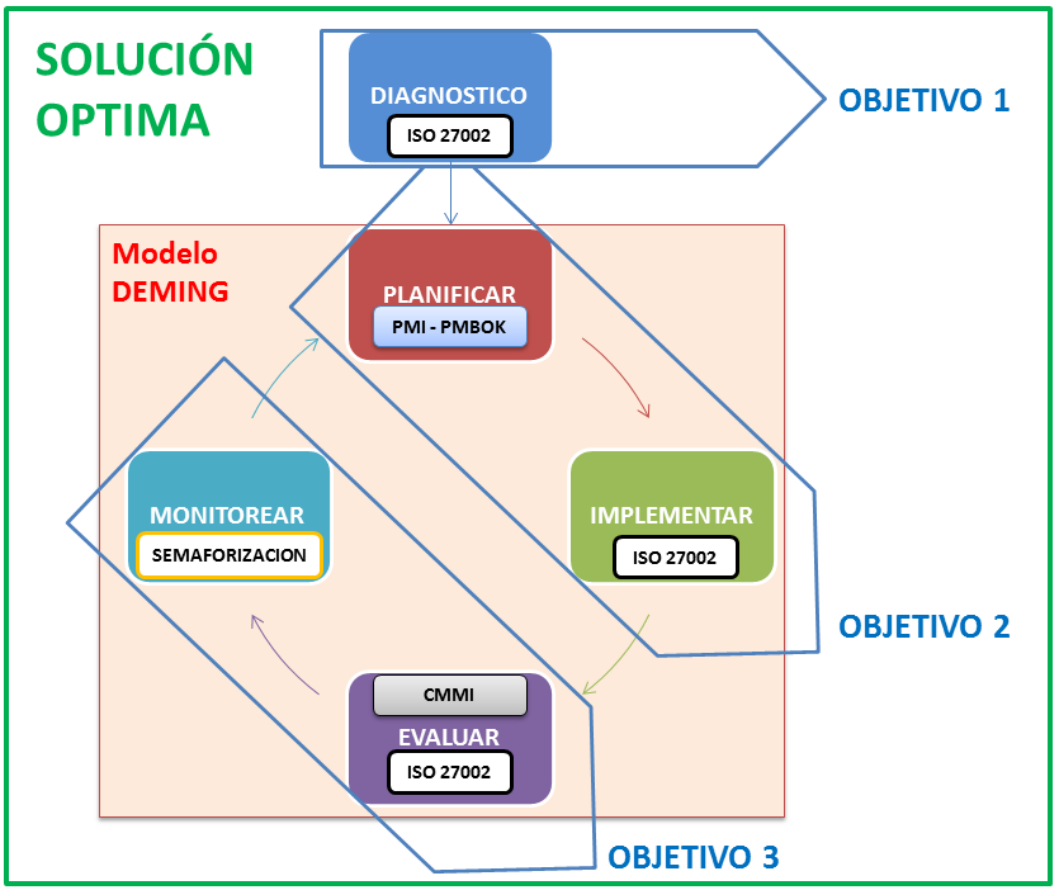


Figura 11: Marco metodológico para solución óptima
Fuente: Elaboración propia

1.8. Plan del proyecto

PLAN DEL PROYECTO “BUENAS PRACTICAS EN SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO 27002 EN LA ASOCIACIÓN PARA EL DESARROLLO EMPRESARIAL EN APURÍMAC”

	Nombre de tarea	Duraci	Comienzo	Fin	Pred
1	**DIANOSTICO**	**60 días**	**mar 01/12/15**	**lun 22/02/16**	
2	Revision de los documentos de gestión de ADEA	10 días	mar 01/12/15	lun 14/12/15	
3	Revision de la modalidad de gestión de la información de ADEA	10 días	mar 15/12/15	lun 28/12/15	2
4	Evaluación de controles basado en ISO 27002 PRIMERA ETAPA	30 días	mar 29/12/15	lun 08/02/16	3
5	Informe de estado situacional a la alta dirección de ADEA	10 días	mar 09/02/16	lun 22/02/16	4
6	**PLANIFICACION**	**60 días**	**mar 23/02/16**	**lun 16/05/16**	
7	Calendarización de Actividades	15 días	mar 23/02/16	lun 14/03/16	5
8	Determinación de recursos necesarios	5 días	mar 15/03/16	lun 21/03/16	7
9	Difusión del Plan	40 días	mar 22/03/16	lun 16/05/16	8
10	**IMPLEMENTACIÓN**	**120 días**	**mar 17/05/16**	**lun 31/10/16**	
11	Elaboración de modelo de propuesta de solucion a alta dirección de ADEA	20 días	mar 17/05/16	lun 13/06/16	9
12	Elaboración de Politicas de gestión de seguridad de la información	20 días	mar 14/06/16	lun 11/07/16	11
13	Implementación de politicas de seguridad de la Información	20 días	mar 12/07/16	lun 08/08/16	12
14	Capacitación de Usuarios e interesados	40 días	mar 09/08/16	lun 03/10/16	13
15	Puesta en marcha de políticas de seguridad de la información	20 días	mar 04/10/16	lun 31/10/16	14
16	**EVALUACIÓN**	**40 días**	**mar 01/11/16**	**lun 26/12/16**	
17	Evaluación de controles basados en ISO 27002 SEGUNDA ETAPA	40 días	mar 01/11/16	lun 26/12/16	15
18	**MONITOREO**	**40 días**	**mar 27/12/16**	**lun 20/02/17**	
19	Intervenciones de Auditoria interna	20 días	mar 27/12/16	lun 23/01/17	17
20	Políticas de Mejoras	20 días	mar 24/01/17	lun 20/02/17	19
21	**ELABORACIÓN DEL INFORME FINAL**	**70 días**	**mar 21/02/17**	**lun 29/05/17**	
22	Redacción del informe final	70 días	mar 21/02/17	lun 29/05/17	20

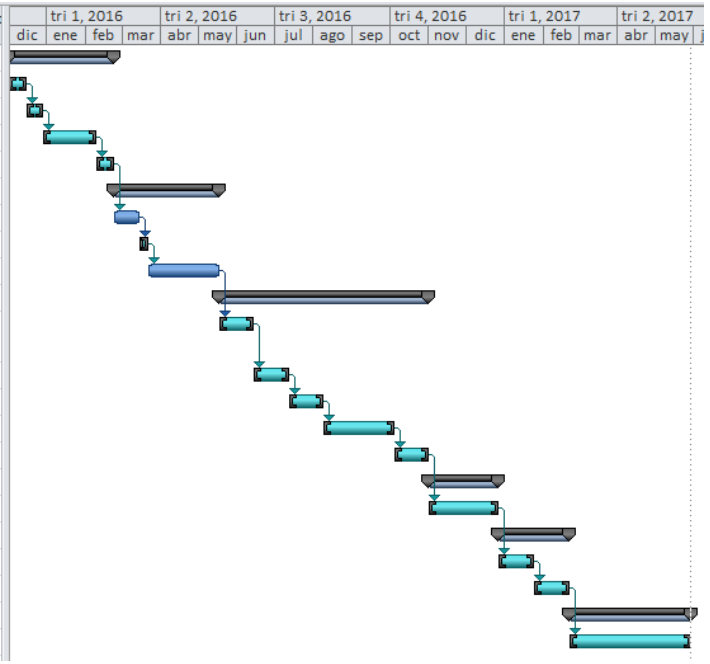


Figura 12: Cronograma de actividades del proyecto
Fuente: Elaboración propia

CAPITULO II: FUNDAMENTO TEORICO

2.1 Marco Teórico

2.1.1 Teoría de la información

Esta teoría surge inicialmente cuando se definió partir de la acelerada difusión y especialización que experimentan los medios de comunicación en el procesamiento y transmisión de información durante la primera mitad de nuestro siglo, se desarrolla el primer modelo científico del proceso de comunicación conocido como la Teoría de la Información o Teoría Matemática de la Comunicación.

Específicamente, se desarrolla en el área de la telegrafía donde surge la necesidad de determinar, con la máxima precisión, la capacidad de los diferentes sistemas de comunicación para transmitir información.

La primera formulación de las leyes matemáticas que gobiernan dicho sistema fue realizada por Hartley (1928) y sus ideas son consideradas actualmente como la génesis de la Teoría de la Información. Posteriormente, Shannon y Weaver (1949) desarrollaron los principios definitivos de esta teoría. Su trabajo se centró en algunos de los siguientes problemas que surgen en los sistemas destinados a manipular información: cómo hablar los mejores métodos para utilizar los diversos sistemas de comunicación; cómo establecer el mejor método para separar las señales del ruido y cómo determinar los límites posibles de un canal.

Según Hartley (1928), el concepto de información es definido en términos estrictamente estadísticos, bajo el supuesto que puede ser tratado de manera semejante a como son tratadas las cantidades físicas como la masa y la energía. La palabra “información” se relaciona con la libertad de elección que tenemos para seleccionar un mensaje determinado de un conjunto de posibles mensajes.

El concepto de información supone la existencia de duda o incertidumbre. La incertidumbre implica que existen diferentes alternativas que deberán ser elegidas, seleccionadas o discriminadas. Las alternativas se refieren a cualquier conjunto de signos construidos para comunicarse, sean estos letras, palabras, números, ondas, etc. En este contexto, las señales contienen información en virtud de su

potencial para hacer elecciones. Estas señales operan sobre las alternativas que conforman la incertidumbre del receptor y proporcionan el poder para seleccionar o discriminar entre algunas de estas alternativas.

Se asume que en los dos extremos del canal de comunicación – fuente y receptor – se maneja el mismo código o conjunto de signos. La función de la fuente de información será seleccionar sucesivamente aquellas señales que constituyen el mensaje y luego transmitirlas al receptor mediante un determinado canal.

Existen diversos tipos de situaciones de elección. Las más sencillas son aquellas en que la fuente escoge entre un número de mensajes concretos. Por ejemplo, elegir una entre varias postales para enviarle a un amigo. Otras situaciones más complejas son aquellas en que la fuente realiza una serie de elecciones sucesivas e un conjunto de símbolos elementales tales como letras o palabras. En este caso, el mensaje estará constituido por la sucesión de símbolos elegidos. El ejemplo más típico aquí es el del lenguaje.

Al medir cuánta información proporciona la fuente al receptor al enviar un mensaje, se parte del supuesto que cada elección está asociada a cierta probabilidad, siendo algunos mensajes más probables que otros. Uno de los objetivos de esta teoría es determinar la cantidad de información que proporciona un mensaje, la cual puede ser calculada a partir de su probabilidad de ser enviada.

El tipo de elección más simple es el que existe entre dos posibilidades, en que cada una tiene una probabilidad de ½ (0,5). Por ejemplo, al tirar una moneda al aire ambas posibilidades – cara y sello – tienen la misma probabilidad de salir. El caso del lenguaje e idioma es diferente. En éstos la elección de los símbolos que formarán el mensaje dependerá de las elecciones anteriores. Por ejemplo, si en el idioma español el ultimo símbolo elegido es “un”, la probabilidad que la siguiente palabra sea un verbo es bastante menor que la probabilidad que sea un sustantivo o un adjetivo. Asimismo, la probabilidad que a continuación de las siguientes tres palabras “el esquema siguiente” aparezca el verbo “representa” es bastante mayor que la probabilidad que aparezca “pera”. Incluso se ha comprobado que, en el caso del

lenguaje, es posible seleccionar aleatoriamente letras que luego son ordenadas según sus probabilidades de ocurrencia y éstas tienden a originar palabras dotadas de sentido.

Según afirma Correa (2008), la teoría de la información tiene sus inicios con la invención del telégrafo y con la definición del código Morse. Samuel Morse trabajo sobre dicho condigo considerando apenas tres combinaciones posibles: el punto (como resultado de una descarga eléctrica), el trazo (resultado de una corriente eléctrica aplicada continuamente durante un lapso de tiempo) y la ausencia de corriente, que daba como resultado espacios en blanco entre dos señales gráficas. Con esas posibilidades (punto, trazo y espacio), Morse desarrollo un concepto que sería la génesis de la Teoría de la Información.

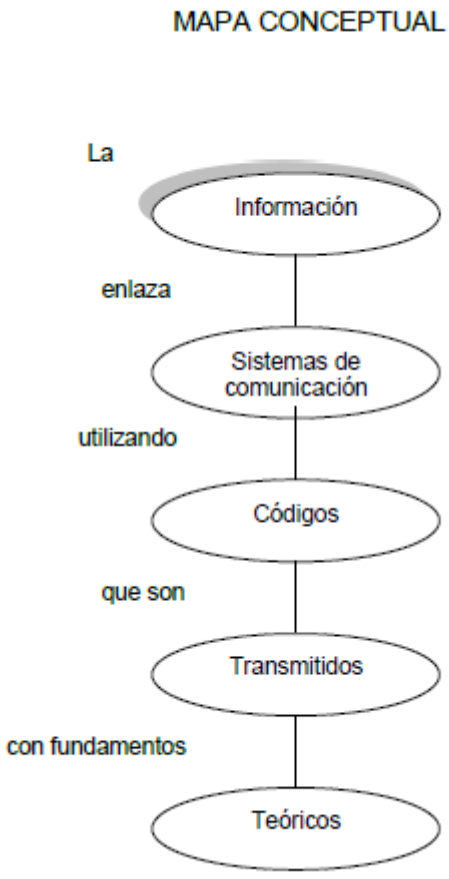


Figura 13: Mapa conceptual de la teoría de la información
Fuente: (Perea Vega, 2012)

Entonces para el mejor entendimiento, el modelo propuesto por Shannon (1948), parte de una fuente de información desde la cual, a través de una transmisión, se emite una señal, la cual viaja por un canal, pero a lo largo de su viaje puede ser interferida por algún ruido. La señal sale del canal, llega a un receptor que decodifica la información convirtiéndola posteriormente en mensaje que pasa a un destinatario.

Es entonces cuando surge y se asienta la teoría matemática de la comunicación, hoy conocida como la teoría de la información. Para desglosar este modelo, debemos entender cada uno de sus componentes.

ESQUEMA DEL PROCESO DE COMUNICACIÓN

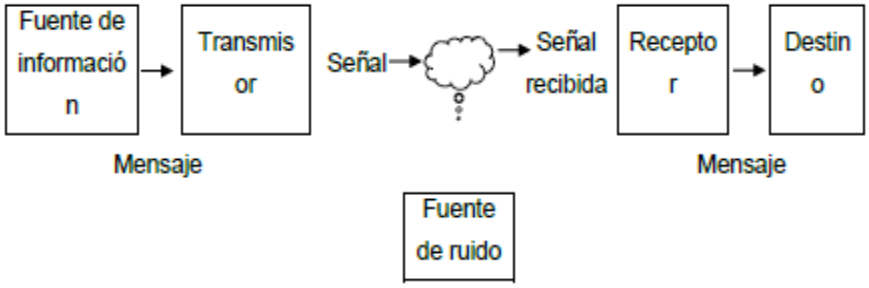


Figura 14: Esquema del proceso de comunicación

Fuente: (Perea Vega, 2012)

FUENTE

Es donde se genera el mensaje que puede ser de diferentes tipos:

- Secuencias de caracteres de un alfabeto determinado.
- Funciones matemáticas que dependan del tiempo como el caso de la radio frecuencia.
- Funciones matemáticas que dependan de diversas variables como las coordenadas de posición y algún otro parámetro, por ejemplo los puntos de color (pixeles) en la pantalla de una computadora, o ubicación y brillantez en un dispositivo monocromático.
- Funciones combinadas, fenómeno que representa cuando se envían audio y video simultáneamente.

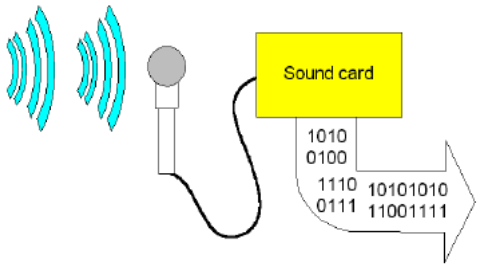


Figura 15: Mapa conceptual de la teoría de la información
Fuente: (Perea Vega, 2012)

TRANSMISOR

Codifica y transforma el mensaje de tal forma que pueda ser enviado a través de un medio. Por ejemplo: en la transmisión radial con amplitud modulada (AM), la frecuencia de audio (denominada moduladora) se convierte en frecuencia de radio cuando se mezcla con una señal adicional (conocida como portadora) que proviene de otra fuente, pasando de un rango de 300 Hz a los 3.4 kHz, a otro que va de 535 kHz hasta 1.7 MHz. Un hercio (Hz) es la unidad que representa un ciclo por segundo.

ESQUEMA DE TRANSMISIÓN

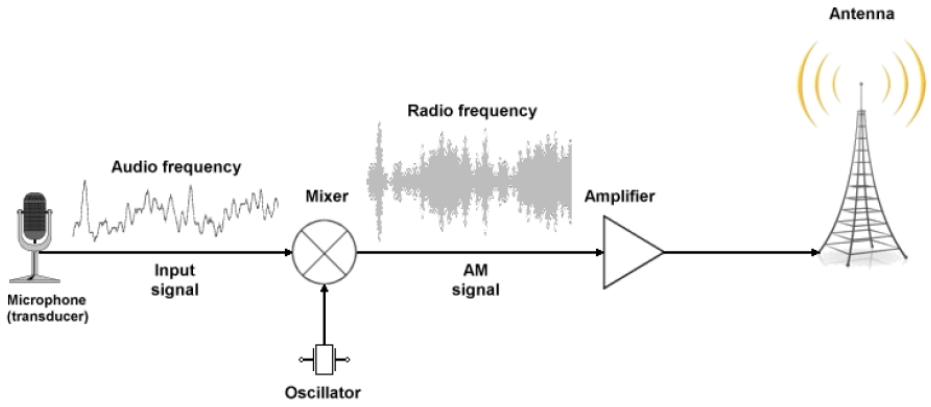


Figura 16: Esquema de transmisión
Fuente: (Perea Vega, 2012)

CANAL

Es el medio a través del cual viaja la información, puede ser cableado o inalámbrico. La capacidad del canal es la velocidad máxima de transmisión, mientras que el ancho de banda determina la tasa de transferencia (unidades/tiempo). El ingeniero sueco Nyquist (1928) estableció una expresión que relaciona las magnitudes anteriores: dado un ancho de banda B, la mayor velocidad de transmisión de la señal que se puede conseguir es 2B, suponiendo que se trata de un medio ideal (carente de ruido) y que el mensaje está compuesto por bits, involucrando solamente dos niveles de tensión.

RECEPTOR

Hace la función inversa del transmisor.

DESTINO

Es el punto final de llegada para el mensaje.

MENSAJE

Existe otro enfoque acerca de la teoría de la información, fue desarrollado por el matemático Norbert Wiener, para él resultaban importantes los mensajes que se envían por y a través de los seres vivos, dentro de su medio así como en su interior, lo que permite a un ser humano coordinar los movimientos de la mano para alcanzar un vaso, a partir de impulsos eléctricos enviados por las neuronas. Este proceso también se puede llevar a cabo usando máquinas, tal como los robots que desactivan bombas. Wiener presentó sus estudios en el libro Cibernética en 1948.

SEÑAL

La comunicación entre dos entidades se logra a través de señales, que pueden ser discretas o continuas. Las primeras toman un número limitado de valores y reciben el nombre de digitales mientras que las segundas tienen un comportamiento de onda y se conocen como analógicas. Como ejemplo se puede comparar un mensaje en código Morse contra su versión hablada.

Al proceso que selecciona un número de valores discretos a partir de una señal continua, se le conoce como muestreo. La tasa o frecuencia de muestreo, es la cantidad de mediciones que se hacen por unidad de tiempo. Después de realizar el muestreo se requiere de un procedimiento conocido como cuantificación, que se encarga de asignar a cada valor dentro de cierto rango, su equivalente en código binario, tomando en cuenta que el número de *bits* define los límites de los rangos.

ESQUEMA DE MUESTRA DE SEÑAL

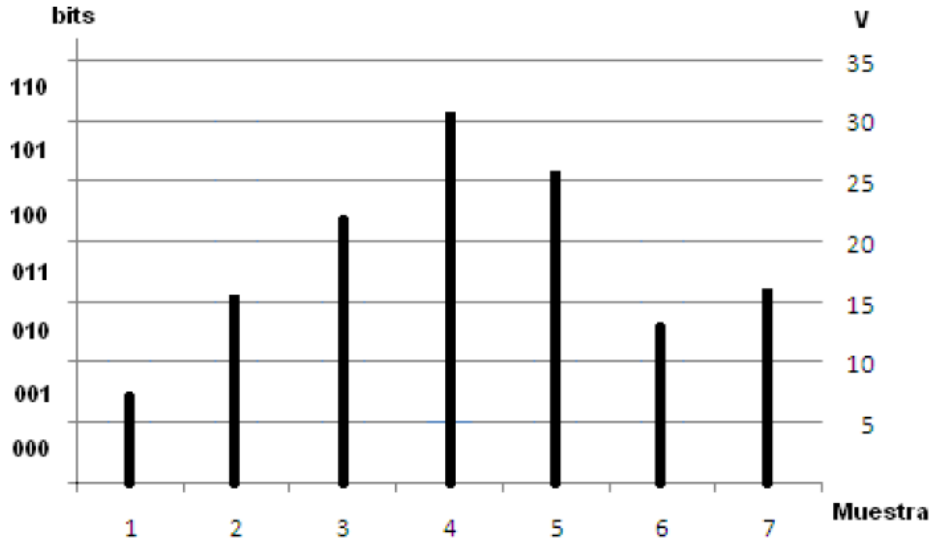


Figura 17: Esquema de muestra de señal
Fuente: (Perea Vega, 2012)

ANALÓGICA

Representan magnitudes físicas como la temperatura, luz, sonido o energía. Su representación gráfica describe una onda senoidal.

DIGITAL

Toda la información se manda como bits independientemente de su contenido, señales de audio y video deben ser preparadas para su

transmisión si provienen de fuente analógicas, tal como sucede cuando se hace una llamada a través del chat.

RUIDO

A las señales no deseadas que contaminan el mensaje, se les denomina ruido. Éste se puede clasificar en:

- Térmico. Lo genera la agitación de los electrones en función de la temperatura, a veces se le denomina ruido blanco y no se le puede suprimir.
- Intermodulación. Aparece cuando distintas frecuencias comparten un medio, combinándose mediante la suma, resta o multiplicación de las mismas, creando una nueva señal.
- Diafonía. Se produce cuando una transmisión se contamina con otra, como en el caso de escuchar otra conversación mientras se habla por teléfono.
- Impulsivo. A diferencia de los anteriores tipos, no es de magnitud constante, presenta picos de corta duración y de gran amplitud, puede originarse por condiciones meteorológicas o por fallas en los sistemas de comunicación.

ENTROPIA

La segunda ley de la termodinámica se puede expresar de diferentes formas dependiendo de su aplicación:

- ✓ El calor no fluye de forma espontánea de un cuerpo frio a uno más caliente.
- ✓ La energía no puede ser transformada por completo en el trabajo mecánico.
- ✓ El cambio de entropía entre cualquier sistema y su medio ambiente es positivo y tiende a cero si el proceso es reversible.

El término entropía fue acuñado por el físico alemán Rudolph Clausius y puede ser interpretado de distintas maneras:

- ✓ Capacidad de un sistema para hacer trabajo.
- ✓ Dirección del flujo del tiempo.

- ✓ Medida del desorden o aleatoriedad. Entre mayor sea su orden la entropía es menor.

ENTROPÍA E INFORMACIÓN

La información es tratada como magnitud física, caracterizando la información de una secuencia de símbolos utilizando la entropía. Se parte de la idea de que los canales no son ideales, aunque muchas veces se idealicen las no linealidades, para estudiar diversos métodos de envío de información o la cantidad de información útil que se pueda enviar a través de un canal.

La información necesaria para especificar un sistema físico tiene que ver con su entropía. En concreto, en ciertas áreas de la física, extraer información del estado actual de un sistema requiere reducir su entropía, de tal manera que la entropía del sistema (S) y la cantidad de la información (I) extraíble están relacionadas por:

$$S > S - I > 0$$

ENTROPIA DE UNA FUENTE

De acuerdo a la teoría de la información, el nivel de información de una fuente se puede medir según la entropía de la misma. Los estudios sobre la entropía son de suma importancia en la teoría de la información y se deben principalmente a C. E. Shannon. Existe, a su vez, un gran número de propiedades respecto a la entropía de variables aleatorias debidas a A. Kolmogorov.

NEGENTROPÍA

La negentropía es un mecanismo por el cual el sistema pretende subsistir, busca estabilizarse ante una situación caótica. Para Johannsen (1975), los sistemas vivos son capaces de conservar estados de organización improbables. Este fenómeno aparentemente contradictorio se explica porque los sistemas abiertos pueden importar energía extra para mantener sus estados estables de organización e incluso desarrollar niveles más altos de improbabilidad. La

negentropía, entonces, se refiere a la energía que el sistema importa del ambiente para mantener su organización y sobrevivir.

2.1.2 Teoría de la seguridad

SEGURIDAD

En el lenguaje común la seguridad es asumida como una cualidad de los sujetos que están libres de amenazas o de agresiones a su individualidad. Desde esta perspectiva la seguridad se puede distinguir como nombre y como adjetivo. En efecto, el diccionario de la Real Academia de la Lengua Española recoge “seguridad” como la cualidad de seguro y “de seguridad” como locución que se aplica a un ramo de la Administración pública cuyo fin es velar por la seguridad de los ciudadanos. Como adjetivo, “seguro” se define como libre y exento de todo peligro, daño o riesgo, cierto, indubitable y en cierta manera infalible; firme, constante y que no está en peligro de faltar o caerse; desprevenido, ajeno de sospecha. La seguridad es, en este uso del concepto, una alocución que designa atributos de los seres que se hallan ciertos de sí mismos, y también una cualidad de las cosas que no ven restringida su capacidad de desarrollo, su libertad.

2.2 Marco Conceptual

2.2.1 Seguridad de la información

La seguridad es proteger a algo de un riesgo o peligro, por lo tanto definiremos con ello el concepto de seguridad de la información. Según AEG (2016), “La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo a los resultados que se obtienen”. Entendiendo este concepto podemos definir que la seguridad de la información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Debemos tener en cuenta que la seguridad absoluta no es posible, no existe sistema cien por ciento seguro, de forma que el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que se debe hablar de niveles de seguridad.

Según PAREDES (2011), en su escrito denominado "Desarrollo de una metodología para la auditoria de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la dirección provincial de Pichincha del consejo de la judicatura", afirma que la información está expuesta a un mayor rango de amenazas y vulnerabilidades,. "La información que adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo de conversación, debería protegerse adecuadamente cualquiera que se la forma que tome o los medios por los que se comparta o almacene". Por lo tanto es obligación de cualquier entidad tomar en cuenta el concepto de seguridad de la información.
En el Perú, es tomado muy en cuenta como así lo refleja su norma NTP-ISO/IEC 1779 (2007), donde indica que "la seguridad de la información es importante en negocios tanto del sector público como del privado para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos".

Es necesario que exista seguridad en el activo más importante de una organización, por lo siguiente:

- Variedad de riesgos y amenazas existentes: Fraudes, espionajes, sabotaje, vandalismo, incendio, inundación, hacking, virus, denegación de servicios, etc.; Provenientes de múltiples fuentes.

- Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información interconectados.
- La mayoría de los sistemas de información no han sido diseñados para ser seguros.

2.2.2 Seguridad Informática

Entiéndase como un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros y disponibles a sus usuarios, autentificados por mecanismos de control de acceso, protegidos de diferentes amenazas y sujetos a auditoria. Para mejor entendimiento véase la figura 01.

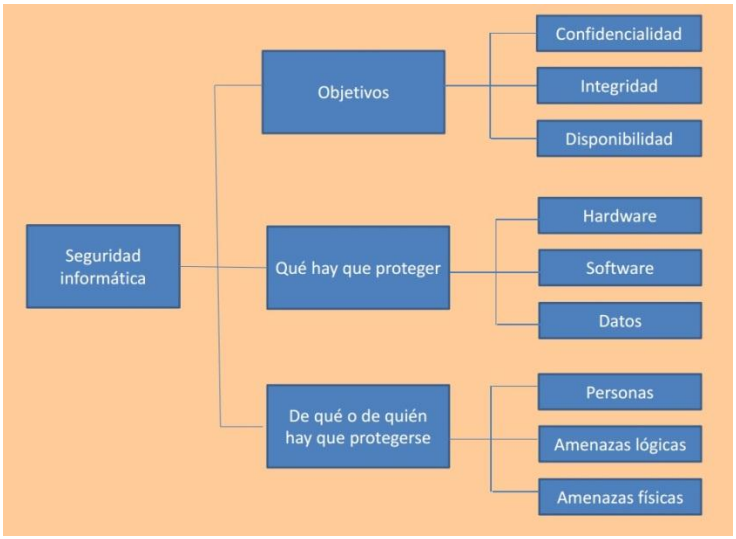


Figura 18: Esquema seguridad informática
Fuente:
https://blogcolegioelcaton.wordpress.com/2013/02/03/seguridad-informatica/

La seguridad informática debe ser administrada según los criterios establecidos por los administradores y personal capacitado, previendo que usuarios externos y no autorizados puedan acceder a ella sin autorización. Evitando que corra el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea

manipulada; llegando a obtener posteriormente datos erróneos e incompletos.

Dentro de esta variable se contempla la accesibilidad y disponibilidad funciones de la seguridad informática que permiten asegurar el acceso a la información y poder disponer de ella en el momento oportuno, incluyendo los backups para que en caso de que se presenten daños o pérdida de datos, producto de accidentes, atentados o desastres, se pueda subir una copia y evitar catástrofes organizacionales o suspensión de servicios, que en ocasiones trae como consecuencia altas perdidas económicas.

2.2.3 Aspectos importantes de la seguridad

En la seguridad se ha considerado tres aspectos importantes que son:

- **Confidencialidad.** Servicio de seguridad que asegura que la información no pueda estar disponible o ser descubierta por procesos no autorizados.

- **Disponibilidad.** Un sistema seguro debe mantener la información, hardware y software disponible para los usuarios todo el tiempo.

- **Integridad.** Condición de seguridad que garantiza que la información debe ser creada, modificada y borrada sólo por el personal autorizado.

2.2.4 Seguridad lógica

Consiste en la “aplicación de barreras y/o procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo”.

Existen muchos controles que se pueden implementar en la seguridad lógica:

- **Roles.** Se lo realiza controlando a través de la función o rol del usuario que requiere dicho acceso.

- **Controles de acceso.** Constituyen en la implementación de controles en cualquier utilitario de red para mantener la integridad de

la información y resguardar los datos confidenciales de accesos no autorizados.

 Autenticación, identificación. La identificación es el momento en que el usuario se da a conocer al sistema y autenticación se refiere a la verificación que realiza el sistema sobre esta identificación.

 Listas de control de acceso ACL's. Su objetivo es filtrar tráfico, permitiendo denegando el tráfico de red de acuerdo a diferentes condiciones establecidas en los equipos de redes.

 Limitaciones a los servicios. Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador.

2.2.5 Seguridad física

Este aspecto no es tomado muy en cuenta a la hora del diseño de un esquema de redes, sin embargo, es un punto importantísimo ya que permite "la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial", es decir la implementación de mecanismos, controles de acceso físico u otros componentes para preservar los sistemas tangibles de la organización.

Las amenazas pueden ser:

- Casos fortuitos o caso mayor (terremotos, inundaciones, tormentas, etc.).

- Intencionados por el hombre (robos, demoliciones, incendios etc.).

2.2.6 Seguridad en redes de datos

La seguridad en redes de datos viene sino a ser la seguridad informática en redes, según Álvarez (2005), "concluye que la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad", por lo tanto se recalca que la información que

se maneja en una organización es sumamente importante y tiene que estar protegida.

Del mismo modo concluye diciendo que, “la sociedad de la información y nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas en las organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan las redes y sistemas ante eventuales amenazas, ya sean presentes o futuras”.

Seguridad de datos en la red es un tema generalizado que abarca una amplia gama de sistemas de computadoras interconectados, industrias que dependen de un sistema de una red para conducir diariamente transacciones de negocios y acceso crucial a información importante, lo que quiere decir que el hecho estar interconectadas las hace tener un valor agregado. Sabiendo además que varios términos que son parte de nuestras vidas diarias como costo de membresía o calidad de servicio son los que nos ayudan a establecer una métrica de lo que cuestan estos servicios, así la industria puede estimar aspectos como integridad de los datos y la disponibilidad de estos como parte de su planeamiento y proceso de manejo de los costos. En algunas industrias, como comercio electrónico la disponibilidad y confiabilidad de la información puede ser la diferencia entre el éxito y el fracaso.

2.2.7 Esquema de seguridad

El esquema de la seguridad se divide en tres campos:

1. Física.- Se refiere a la seguridad física de los dispositivos que se utilizan para el funcionamiento de la red.

2. Personal.- Se refiere a la seguridad del usuario de la red.

3. Sistemas.- Se profundiza más en los sistemas de transmisión de datos, el cual se divide en lo siguiente:

- ✓ Privacidad. Seguridad física de los equipos (computadoras, servidores, switch, etc.) y autenticaciones.
- ✓ Integridad. Encriptación de datos para garantizar que lleguen al receptor sin problemas de robo o modificación (VPN, Certificados digitales).
- ✓ Disponibilidad. Áreas que muestra el tiempo en que los servicios están activos, la cual es más atacada por los piratas informáticos, ya que representa mayores pérdidas económicas en las redes de transmisión de datos (Sistema de Detección de Intrusos - IDS).

4. Administración.- Totalmente de dependencia humana, muestra la forma en que el administrador de la red debe manejar los archivos de acceso y las alarmas generadas por el sistema, las cuales son ignoradas en algunos casos por errores humanos o excesiva confianza.

2.2.8 Políticas de Seguridad

La política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

En el ámbito de la información, según (Benítez, 2013), Las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas.

Sin embrago para (Fischer, 1988), la política social de la seguridad de los datos establece las responsabilidades de seguridad para la generación, manipulación, servicio y uso de la información del negocio. Tal política debe ser apoyada por directrices documentadas, procedimiento y/o normas, las cuales son responsabilidad de la dirección para formularlas. Por lo tanto según lo anterior, se deben hacerse informes específicos con respecto a las responsabilidades del propietario, usuarios, custodios y director de los datos.

2.2.9 Sistema seguro

Toda organización debe entender que su activo más importante es la información, por lo tanto deben existir lineamientos que permitan su aseguramiento sin dejar de lado la seguridad física aplicada a los equipos donde se encuentra almacenada.

Dichos lineamientos o técnicas están dadas por la seguridad lógica y aspectos de la seguridad física que permite la creación de barreras y procedimientos que resguardan la información y permiten el acceso a ella única y exclusivamente a personal autorizado.

Hoy en día existe en el mercado gran variedad de dispositivos electrónicos móviles como netbooks, computadores portátiles, tabletas, smartphones etc., convirtiéndose en blanco de posibles ataques y búsquedas de debilidades entre ellas, fraude electrónico, robo de identidad, denegación de servicios entre muchos otros.

La gestión de la seguridad debe ser planteada tanto en la parte lógica como física a través de los planes de contingencia, políticas de seguridad y aplicación de normativas.

Características de un Sistema Seguro:

Confidencialidad: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

Integridad: Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen. De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella.

La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de ocurrencia de algún problema.

Otras características y conceptos que se relacionan con el proyecto y deben ser tenidos en cuenta por su composición teórica son los siguientes:

Control de acceso a los recursos: Se entiende como la regulación de quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Auditoría: Son los mecanismos para poder determinar qué es lo que está ocurriendo en el sistema, qué es lo que hace cada uno de los usuarios, los tiempos y fechas de dichas acciones.

Metodología de auditoría: Permite de una manera adecuada presentar una guía procedimental para que se efectúen tareas, actividades y tareas tendientes a realizar el proceso de revisión preliminar, revisión de controles, diagnósticos y comparación de estados actuales en materia de seguridad, finalizando con informes que presentan los resultados de la aplicación metodológica.

Papeles de trabajo: Hacen referencia al material de evidencia que el auditor maneja para recolectar datos o constancia escrita del trabajo que se está realizando, para este caso aplica la utilización de formatos.

SGSI: Un Sistema de gestión de la seguridad de la información, es como su nombre lo expresa un sistema que se encarga de proveer una cantidad de mecanismos y herramientas basados en la norma ISO 27001 y tiene por objetivo conocer al interior de la institución a los que puede estar expuesta la información, define como se deben gestionar los riesgos y debe ser un marco de referencia para la institución el cual debe ser conocido por todo el personal y debe estar sometido a una revisión y a un proceso de mejora constante.

Los anteriores aspectos deben ser tenidos en cuenta al momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto aspectos importantes para que así los usuarios y los sistemas realicen sus procedimientos de la mejor manera posible, de forma concreta y clara además se debe tener presente los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan las políticas para no generar un ambiente de tensión y/o agresión.

La seguridad informática esta creada para velar y proteger los activos informáticos, en aras de garantizar la integridad, disponibilidad y

confidencialidad de los datos propios de una organización, independiente de su tamaño, tipo o razón social.

LA INFRAESTRUCTURA COMPUTACIONAL

Parte esencial para gestionar, administrar y almacenar la información indispensable dentro del normal funcionamiento de la Institución. El papel que desempeña la seguridad informática en este punto es velar que el hardware (parte física) tengan un óptimo funcionamiento y logre evitar problemas relacionados con robo, incendios, desastres naturales, bloqueos, fallas en el suministro eléctrico, vandalismo, entre otros que lleguen a afectar directamente la infraestructura informática.

LOS USUARIOS

Son las personas que están directamente involucradas con la infraestructura tecnológica, comunicaciones y administradores de la información. La seguridad informática debe establecer normas que minimicen los riesgos tanto de información como de su infraestructura, dentro de dichas normas de debe contemplar, horarios de acceso, restricciones físicas y lógicas, permisos, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo esto debe estar regido por estándares y normas que minimicen los riesgos y el impacto en caso de llegar a presentar un siniestro.

2.2.10 Conceptos y términos

A continuación detallo algunos términos con sus respectivos conceptos.

HACKER

Persona que disfruta explorando los detalles de los sistemas programables y como extender sus capacidades. Una persona que es buena en programar rápidamente.

HACKEAR

Verbo creado para las acciones de un Hacker.

CRACKER

Persona que rompe la seguridad en un sistema. Término acuñado por la comunidad Hacker para defenderse contra el mal uso periodístico de la palabra Hacker y refleja la repulsión que hay entre los viejos Hackers por el vandalismo y destrucciones de los grupos de Crackers, Es considerado por la comunidad como una forma inferior de vida o protohacker. Algunos Hackers pasan por esta etapa, pero usualmente se espera que dure poco y que maduren para convertirse en Hackers.

CIBERPUNKS

El nombre fue tomado de una novela clásica, Neuromancer, en la comunidad Hacker se usa para referirse a los magos de la criptografía.

SNEAKER

Individuo, usualmente un Hacker, que se contrata para tratar de irrumpir en un sistema para probar su seguridad.

WIZARD

Persona que conoce a fondo como funciona una pieza compleja de equipo. Especialmente si puede reparar un sistema rápidamente en casos de emergencia, tal vez con algo de magia profunda, es decir usando instrucciones o técnicas que resultan completamente incomprensibles a los simples mortales. Mientras que un Hacker puede usar algunas técnicas avanzadas, es el Wizard el que entiende como o por que funcionan.

GURU

Es el maestro a quien recurre el Hacker y el Wizard cuando tienen algún problema, pues posee conocimientos más allá de la comprensión de un simple programador.

PROGRAMADOR VODOO

Se le llama así al programador que toma técnicas o recetas de libros sin entender cómo funcionan, por lo que no tiene manera de saber si

van a funcionar o no. Es en estos casos cuando el Hacker necesita la ayuda de un Wizard o de su Guru.

SNIFFER

Herramienta de software utilizada para el rastreo de tráfico en una red de datos.

SCANNER

Herramienta de software para la evaluación de sistemas, esta herramienta averigua que conexiones son posibles con ese sistema, comúnmente evalúa los puertos en busca de “agujeros”.

PHREAK

Una variante del hacker, el cual basa sus ataques en los sistemas telefónicos.

PUERTA TRASERA (TRAP DOOR)

Agujero de seguridad intencionalmente creado por los autores del sistema.

NEGACIÓN DE SERVICIO (DENIAL OF SERVICE, DOS)

Ataque consistente en impedir que un sistema pueda ofrecer los servicios con normalidad.

SUPLANTACIÓN (SPOOFING)

Mecanismo por el cual la máquina atacante adopta la personalidad (identificación) de una máquina amiga.

TROYANO

Código que realiza acciones ilícitas escondidas dentro de un programa útil.

GUSANO (WORM)

Programa que hace copias de sí mismo sobre distintas máquinas interconectadas por una red.

VIRUS

Fragmento de código que al ejecutarse inserta copias de sí mismo en otros ejecutables.

EXPLOIT

Programa que hace uso de una o más vulnerabilidades para romper la seguridad de un sistema.

CRIPTOGRAFÍA DE CLAVE PÚBLICA (PUBLIC KEY CRIPTOGRAPHY)

Sistema criptográfico que utiliza dos claves, una para encriptar y otra para desencriptar.

CRIPTOGRAFÍA DE CLAVE SECRETA (SECRET KEY CRIPTOGRAPHY)

Sistema criptográfico en el que la encriptación y des encriptación se realiza con una sola clave.

PALABRA CLAVE (CONTRASEÑA)

Cadena de caracteres conocida por un usuario utilizada para demostrar su identidad.

2.3 Marco Metodológico

2.3.1 Norma ISO 27002

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

1. POLÍTICAS DE SEGURIDAD.
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
3. SEGURIDAD DE LOS RECURSOS HUMANOS.
4. GESTIÓN DE LOS ACTIVOS.
5. CONTROL DE ACCESOS.
6. CRIPTOGRAFÍA.
7. SEGURIDAD FÍSICA Y AMBIENTAL.
8. SEGURIDAD DE LAS OPERACIONES.

   Procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

9. SEGURIDAD DE LAS COMUNICACIONES.

   Gestión de la seguridad de la red; gestión de las transferencias de información.

10. ADQUISICIÓN DE SISTEMAS, DESARROLLO Y MANTENIMIENTO.

Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.

11. RELACIONES CON LOS PROVEEDORES.
Seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.

12. GESTIÓN DE INCIDENCIAS QUE AFECTAN A LA SEGURIDAD DE LA INFORMACIÓN.
Gestión de las incidencias que afectan a la seguridad de la información; mejoras.

13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
Continuidad de la seguridad de la información; redundancias.

14. CONFORMIDAD.
Conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.
Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 114 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

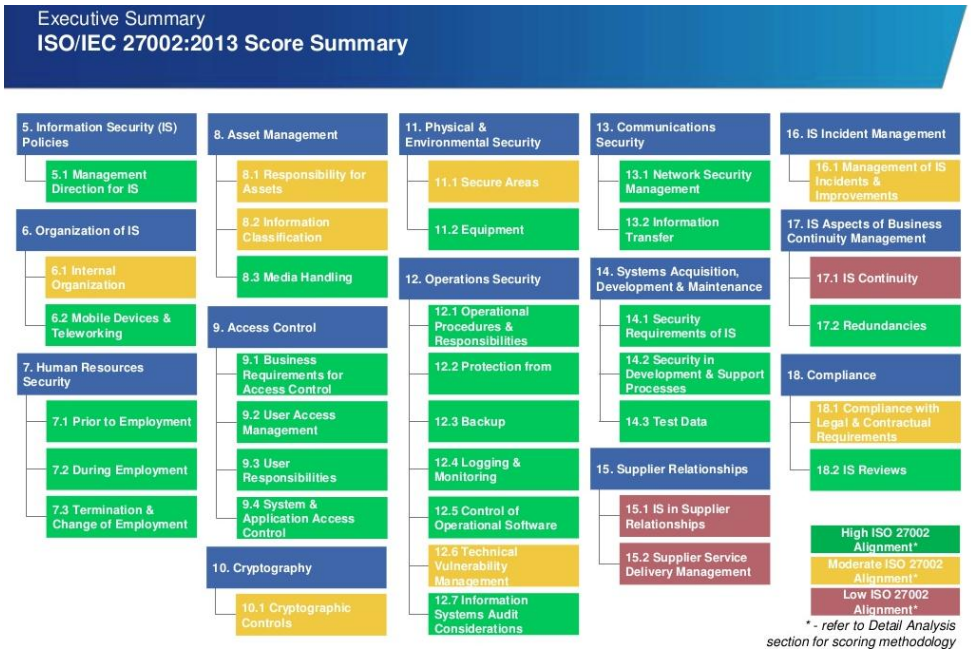


Figura 19: Esquema de ISO/IEC 27002:2013
Fuente: KPMG, Security Program Assessment

2.3.2 Modelo de mejora continua DEMING

El ciclo "Planificar-Hacer-Verificar-Actuar" fue desarrollador inicialmente en la década de 1920 por Walter Shwhart, y fue popularizado luego por W. Edwards Deming, razón por la cual es frecuentemente conocido como "Ciclo de Deming". Dentro del contexto de un sistema de gestión de calidad, el PHVA es un ciclo dinámico que puede desarrollarse dentro de cada proceso de la organización y en el sistema de procesos como un todo. Está íntimamente asociado con la planificación, implementación, control y mejora continua tanto en la realización del producto como en otros procesos del sistema de gestión de la calidad.

A partir del año 1950, y en repetidas oportunidades durante las dos décadas siguientes, Deming empleó el Ciclo PHVA como introducción a todas y cada una de las capacitaciones que brindó a la alta dirección de las empresas japonesas. De allí hasta la fecha, este ciclo (que fue desarrollado por Shewhart), ha recorrido el mundo como símbolo

indiscutido de la Mejora Continua. Las Normas NTP-ISO 9000:2001 basan en el Ciclo PHVA su esquema de la Mejora Continua del Sistema de Gestión de la Calidad. En la Figura 20 se podrá apreciar el Ciclo Deming.

Según (Pérez, 2007), describe en su libro que el círculo de Deming o Círculo de Calidad de Shwhart consiste en cuatro etapas:

1. **Planear.** Primero se define los planes y la visión de la meta que tiene la empresa; en donde quiere estar en un tiempo determinado.

   Una vez establecido el objetivo, se realiza un diagnóstico, para saber la situación actual en que nos encontramos y las áreas que es necesario mejorar, definiendo su problemática y el impacto que pueda tener en su vida.

   Después se desarrolla una teoría de posible solución, para mejorar un punto, y por último se establece un plan de trabajo en el que probaremos la teoría de solución.
2. **Hacer.** En esta etapa se lleva a cabo el plan de trabajo establecido anteriormente, junto con algún control para vigilar que el plan se esté llevando a cabo según lo acordado. Para poder realizar el control existen varios métodos, como la gráfica GANTT en la que podemos medir las tareas y tiempo.
3. **Verificar.** Aquí se comparan los resultados planeados con los que obtuvimos realmente. Antes de esto, se establece un indicador de medición, porque lo que no se puede medir, no se puede mejorar en una forma sistemática. El mejor de los ejemplos puede ser un deportista que entrena para calificar a las olimpiadas: a él se le pone a competir semanalmente con rivales de su mismo nivel, y aquí es cuando puede verificar si en verdad está logrando aumentar su rendimiento.
4. **Actuar.** Con esta etapa se concluye el ciclo de la calidad: si al verificar los resultados se logró lo que teníamos planeado entonces se sistematizan y documentan los cambios que hubo; pero si al hacer una verificación nos damos cuenta que hemos

logrado lo deseado, entonces hay que actuar rápidamente y corregir la teoría de solución y establecer un nuevo plan de trabajo.

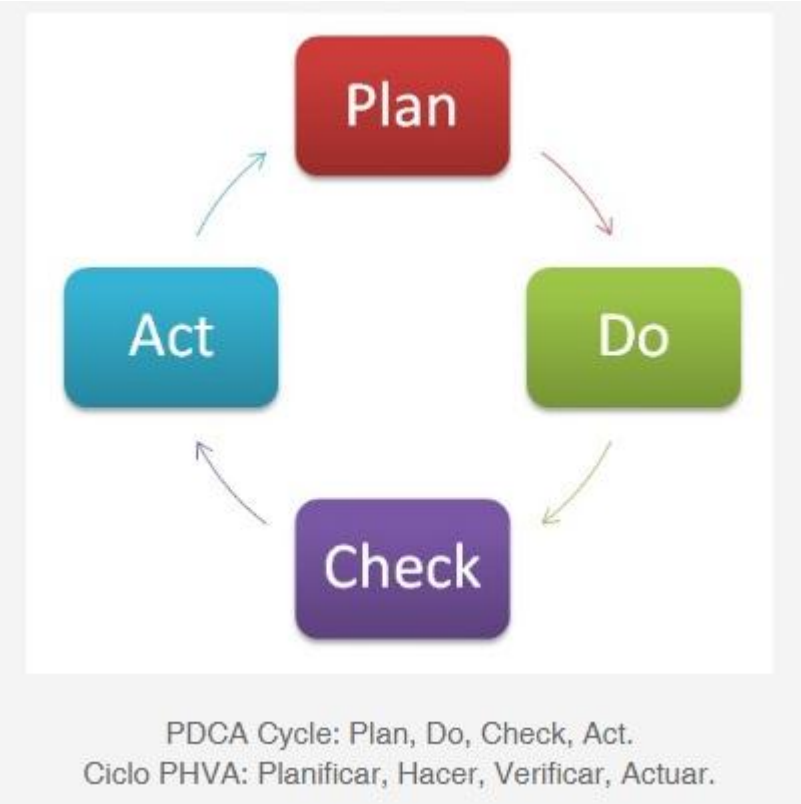


Figura 20: Esquema del Ciclo Deming
Fuente: https://www.pdcahome.com/5202/ciclo-pdca/

Entonces este proceso es cíclico y de mejora continua, una vez que se alcance el objetivo del proceso, tenemos que establecerlo y no dejar de planear, hacer, verificar y actuar hasta resolver la problemática.

Según la publicación de una nota científica de García, Quispe, Ráez (2003), “dentro del contexto de un sistema de gestión de la calidad, el ciclo PHVA es un ciclo que está en pleno movimiento. Que se puede desarrollar en cada uno de los procesos. El ciclo PHVA se explica de la siguiente forma:

Planificar:

- Involucrar a la gente correcta
- Recopilar los datos disponibles
- Comprender las necesidades de los clientes
- Estudiar exhaustivamente el/los procesos involucrados
- ¿Es el proceso capaz de cumplir las necesidades?
- Desarrollar el plan/entrenar al personal

Hacer:

- Implementar la mejora/verificar las causas de los problemas
- Recopilar los datos apropiados

Verificar:

- Analizar y desplegar los datos
- ¿Se han alcanzado los resultados deseados?
- Comprender y documentar las diferencias
- Revisar los problemas y errores
- ¿Qué se aprendió?
- ¿Qué queda aún por resolver?

Actuar:

- Incorporar la mejora al proceso
- Comunicar la mejora a todos los integrantes de la empresa
- Identificar nuevos proyectos/problemas

2.3.3 CMMI – Modelo de Integración de Capacidad y Madurez

La frase que mejor refleja la filosofía de CMMI es: “La calidad de un producto depende de la calidad de los procesos empleados en su elaboración”.

Las siglas en ingles del modelo de integración de capacidad y madurez son CMMI, y es un modelo de mejora de procesos que se ha empleado con éxito en grandes y reconocidas industrias de manufactura, aunque se ha empleado también para la mejora de

procesos de elaboración de software. El CMMI es la única metodología que tiene un enfoque sistémico para la mejora de procesos para los problemas más comunes que se presentan en toda organización.

El modelo es de capacidad cuando mide la mejora de procesos individuales dentro de una organización, y cuando se refiere a la madurez, entonces está midiendo la mejora de procesos en toda la organización.

Para un mejor entendimiento, esta metodología será utilizada para medir la mejora del proceso de salvaguarda de la información, para ello es necesario definir sus componentes. Dentro de estos componentes requeridos y esperados, define con mayor detalle las metas genéricas que se deben alcanzar con cada actividad y las metas específicas que debe lograr cada proceso. Si se efectúan como se espera, tanto las metas y las prácticas específicas como genéricas, se dice que el proceso está controlado y que mejorará con el paso del tiempo con base en ciertos niveles definidos en la metodología. Estos niveles son casi los mismos para capacidad y madurez, con la única diferencia de que para niveles de capacidad, es decir, para el análisis de procesos aislados dentro de una organización, existe un primer nivel llamado “nivel cero” o “proceso incompleto”, en tanto que en los niveles de madurez, este nivel cero no existe. Los niveles de 1 a 5, tanto en capacidad como en madurez, se llaman progresivamente: realizado o inicial, administrado, definido, administrado cuantitativamente o predecible cuantitativamente, y el quinto y último nivel es el optimizado.

El CMMI es una metodología en la cual hay certificaciones reconocidas internacionalmente, pero el problema es que no hay un organismo internacional que reconozca dichas certificaciones, excepto el propio CMMI, avalado por el Instituto de Ingeniería de Software (Software Engineering Intitute) de EUA.

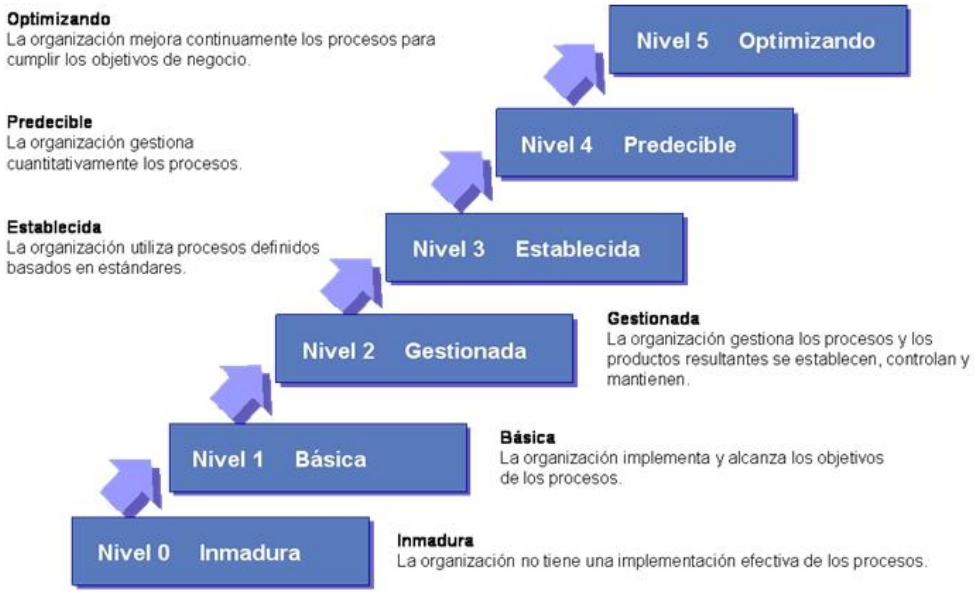


Figura 21: Esquema del CMMI
Fuente: Tecnova. Chile

ISO/IEC 15504

También conocido como Software Process Improvement Capability Determination, abreviado SPICE, en español, «Determinación de la Capacidad de Mejora del Proceso de Software» es un modelo para la mejora, evaluación de los procesos de desarrollo, mantenimiento de sistemas de información y productos de software.

La organización Internacional de Estandarización (ISO, por sus siglas en inglés), la cual es un organismo reconocido en el ámbito internacional, ha emitido la norma ISO/IEC 15504, que es un marco de trabajo para evaluar procesos, básicamente de desarrollo de software. La ISO también emitió la norma 12207, un modelo de referencia de procesos para todo el ciclo de vida de software.

La norma ISO 15504 consta de las siguientes partes:

Parte 1. Conceptos, vocabulario y normativa.

Parte 2. Realización de la evaluación.

Parte 3. Guía para la realización de la evaluación.

Parte 4. Guía sobre el uso de la mejora de procesos y determinación de la capacidad del proceso.

Parte 5. Ejemplo del modelo de evaluación del proceso.

Parte 6. Ejemplo del modelo de evaluación del ciclo de vida del sistema.

Parte 7. Evaluación de la madurez de la organización.

NIVELES DE MADUREZ DE LA NORMA ISO/IEC 15504 - SPICE

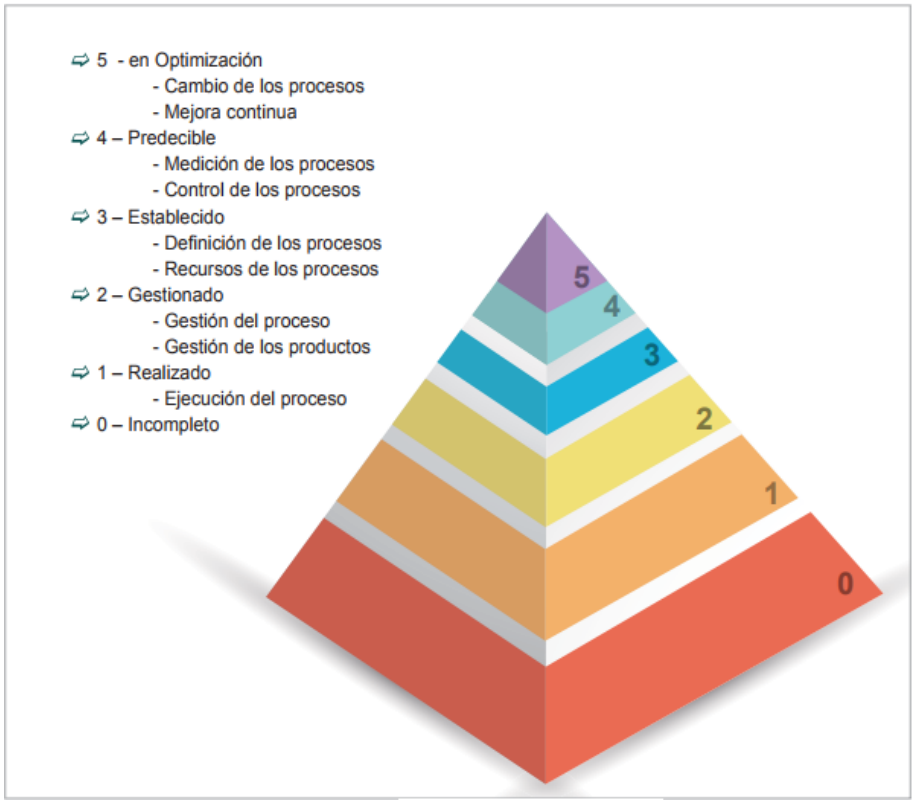


Figura 22: Niveles de madurez
Fuente: EQA – www.eqa.es - España

2.3.4 Gestión del proyecto con PMBOK

Para la elaboración del plan del proyecto de tesis se ha tomado como referencia los conocimientos, técnicas y prácticas vigentes, para la gestión exitosa de proyectos reunidas por el PMI® (Project Management Institute) en el documento llamado PMBOK (Project Management Body of Knowledge) quinta edición. El propósito principal del PMBOK es identificar el conocimiento de Gestión de Proyectos que es generalmente aceptado como buena práctica. Generalmente aceptado, significa que los conocimientos y las prácticas, son aplicables a la mayoría de proyectos la mayoría de veces y que existe

consenso sobre su valor y utilidad. Buena práctica, significa que hay un amplio acuerdo de que la aplicación correcta de las herramientas, habilidades y técnicas aumenta la posibilidad de tener éxito [PMI 2008].

A continuación se muestra las áreas de conocimiento y los procesos que se tomaran en cuenta para el presente proyecto de tesis:

- Procesos de la Dirección del proyecto: Se agrupan en 5 procesos los cuales son:

• El grupo de procesos de iniciación: Aquí se encuentran los procesos que definen el proyecto.

• El grupo de procesos de planificación: En este grupo de procesos se definen los procesos que establecen el alcance del proyecto, definir objetivos y acciones a tomar para alcanzar los objetivos.

• El grupo de procesos de ejecución: en este grupo se encuentran los procesos que se realizarán para completar el proyecto.

• El grupo de procesos de seguimiento y control: en este grupo se encuentran los procesos que se usaran para dar seguimiento, analizar y regular el progreso y el desempeño del proyecto, además que permitirá identificar áreas en las que el proyecto requiere cambios.

• El grupo de procesos de cierre: En este grupo están los procesos que permitirán finalizar todas las actividades a fin de cerrar formalmente el proyecto

- Áreas de conocimiento: En la versión actual de PMBOK (5ta. Edición), se cuenta con 10 áreas de conocimiento, con las cuales se desarrolla el presente proyecto:

• Gestión de la integración del proyecto
• Gestión del alcance del proyecto
• Gestión del tiempo del proyecto
• Gestión de los costos del proyecto
• Gestión de la calidad del proyecto
• Gestión de los recursos humanos del proyecto
• Gestión de las comunicaciones del proyecto
• Gestión de los riesgos del proyecto
• Gestión de las adquisiciones del proyecto
• Gestión de los interesados del proyecto

CAPITULO III: DESARROLLO DE LA SOLUCIÓN

3.1 Modelamiento de la solución

El modelo usado para la solución óptima, consta de 5 fases partiendo de la primera que representa la línea base del trabajo presente, la realización del diagnóstico previo.

FASE 1: DIAGNOSTICO

Esta fase inicial responde también al primer objetivo del presente trabajo. Como se muestra en la figura 23 marco metodológico de solución óptima para el presente proyecto, con la fase inicial logramos el objetivo 1 “diagnosticar y comprender el estado actual de la seguridad de la información en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros”.

FASE 2: PLANIFICACIÓN

Esta fase del proyecto comprende realizar una serie de actividades que serán precedentes de la implementación del plan de acción.

Inicialmente se elaboró la calendarización de actividades, estableciendo actividades, fechas y plazos de ejecución de todo el proyecto, para ello se tomó en consideración el uso de las buenas prácticas en gestión de proyectos de PMBok., determinando el tiempo, alcance e interesados (stakeholders).

Una segunda actividad fue determinar los recursos necesarios para la ejecución del plan de acción, seguidamente de la difusión del plan, que consistió en exponer hacia la alta dirección de la institución las intenciones y objetivos del plan del proyecto.

FASE 3: IMPLEMENTACIÓN

En esta fase se procedió con la elaboración de la propuesta de solución para la alta dirección de la institución. Posteriormente de acuerdo al estado situacional y mediante una revisión de controles del ISO 27002, se elaboró un documento de políticas de gestión de seguridad de la información de ADEA, donde se tomó en consideración los 14 dominios de control de dicha norma ISO.

En consiguiente se tuvo que realizar previa autorización la implementación de dichas políticas. Estas constaron en el requerimiento de soluciones tecnológicas, adquisición de equipos y materiales, cambios en la infraestructura, en algunos casos re-modelamiento de los ambientes de la institución, todo ello con el fin de cumplir con las políticas establecidas y así reducir el riesgo al que estaba expuesto inicialmente la información de ADEA.

Otros de los aspectos de la implementación de las políticas fueron las capacitaciones a los usuarios e interesados. En este caso fue a todo el personal que labora en ADEA, mediante reuniones, capacitaciones individuales y grupales. Finalmente en esta fase, se puso en marcha la políticas de seguridad dela información en ADEA.

FASE 4: EVALUACIÓN

En esta fase se procedió con la evaluación de los controles de la ISO 27002, la misma que se realizó al inicio del proyecto en la fase de diagnóstico. Dichas evaluaciones sirven para medir el nivel de estado en el que se encuentran por cada control que refiere dicha norma. Con el resultado de dicha segunda evaluación, se observó un avance positivo de la reducción del riesgo después de la implementación de las políticas.

FASE 5: MONITOREO

En esta fase mediante el apoyo de un profesional en auditoria, se procedió con las intervenciones en referencia a la seguridad de la información y los resultados generados sirvieron para actualizar e incluir políticas de mejora que a su vez se tienen que ejecutar constantemente. Al igual que el ciclo de Deming, el uso de políticas en una organización deben ser revisadas constantemente, repitiendo el ciclo de planear, hacer, revisar y actuar, buscando la mejora continua.

Cabe recalcar también que estas cuatro últimas fases, fueron adaptadas al modelo Deming de mejora continua, donde la fase de planificación y fase de implementación representan el logro del objetivo 2 “planificar e implementar soluciones tecnológicas con énfasis en la seguridad de la información

basado en las buenas prácticas basadas en ISO 27002 para la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros".

Las fases siguientes; fase de evaluación y fase de monitoreo, representan finalmente el logro del objetivo 3 "controlar y evaluar los procesos de aseguramiento y protección de los activos de información basadas en ISO 27002 para la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros".

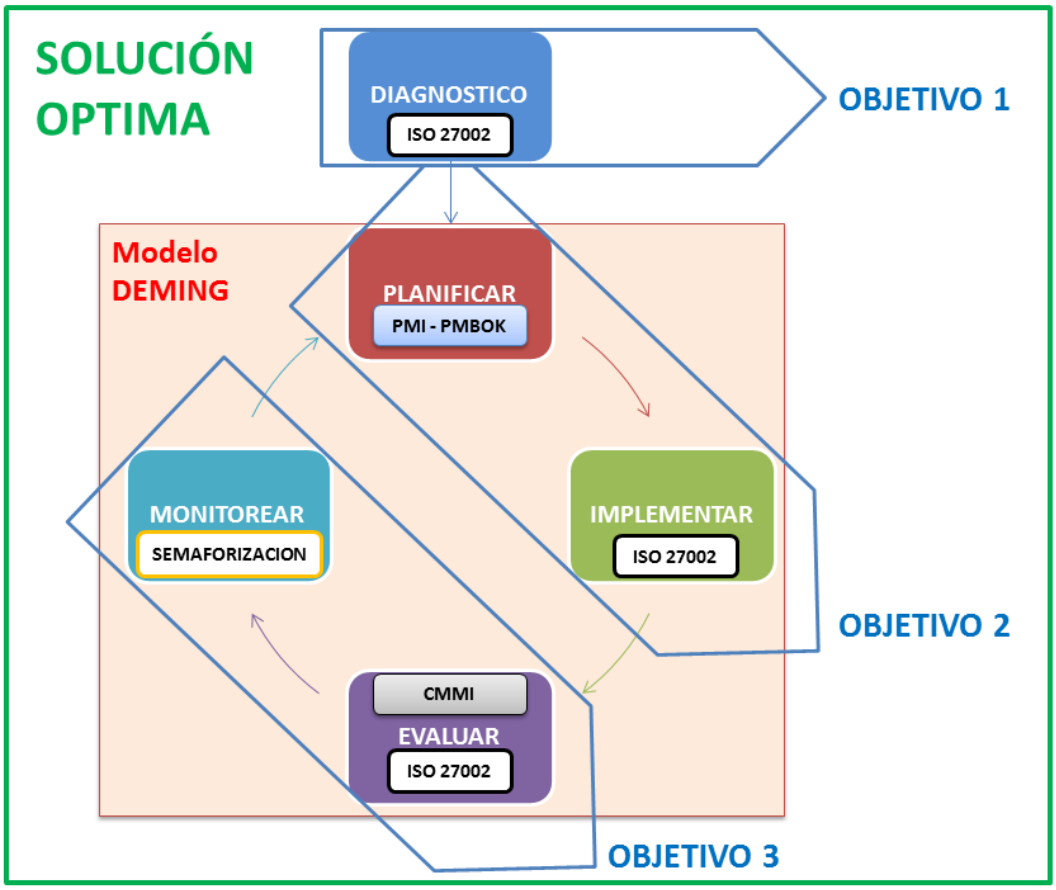


Figura 23: Marco metodológico de la solución óptima
Fuente: Elaboración propia

3.2 Marco Aplicativo

Se realiza en todas las oficinas de ADEA, para los 55 colaboradores al cierre del mes de Junio del 2017.

La implementación se realizó en el total de la institución ADEA. Tomando en consideración las funciones que tiene cada cargo en la institución, a continuación describo cada uno de los puestos implicados directamente en la ejecución del presente trabajo.

3.2.1 Identificación de los puestos y funciones del personal de ADEA

A continuación describo los puestos que comprenden el total del personal de la organización, donde se efectuó la implementación.

1. NOMBRE DEL PUESTO	**:**	**CONSEJO DIRECTIVO**
NIVEL	**:**	Representativo.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Asamblea General.
SUPERVISIÓN JERÁRQUICA	**:**	Gerencia. Oficial de Cumplimiento. Jefe de la Unidad de Riesgos.

FUNCIONES PRINCIPALES

El Consejo Directivo es el órgano colegiado elegido por la Asamblea General y tiene las facultades de gestión y representación legal suficientes para la administración de ADEA dentro de su objeto, con excepción de los asuntos que la Ley o el Estatuto atribuyan a la Asamblea General.

2. NOMBRE DEL PUESTO	**:**	**JEFE DE LA UNIDAD DE RIESGOS**
NIVEL	**:**	Gerencial.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Consejo Directivo.
SUPERVISIÓN JERÁRQUICA	**:**	No Aplica

FUNCIONES PRINCIPALES

Identificar, manejar, monitorear e informar al Consejo Directivo, Comités y a las Áreas de decisión correspondientes, sobre la exposición de ADEA a los distintos tipos de riesgos que puedan presentarse y que puedan afectar el normal desempeño de ADEA, a fin de prevenir su ocurrencia y determinar el nivel de impacto a que podría estar expuesta la institución.

Velar por una Gestión Integral de Riesgos competente, promoviendo el alineamiento de las medidas de tratamiento de los riesgos de la empresa con los niveles de tolerancia al riesgo y el desarrollo de controles apropiados.

3. NOMBRE DEL PUESTO	**:**	**GERENTE**
NIVEL	**:**	Gerencial.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Consejo Directivo.
SUPERVISIÓN JERÁRQUICA	**:**	Jefatura de Créditos. Sub Gerencia de Administración. Oficial de Atención al Usuario. Jefatura del Departamento de Asesoría Legal. Jefe de Gestión de Procesos.

A. FUNCIONES PRINCIPALES

1. Ser responsable de la gestión económico-financiera y administrativa de ADEA y ejecuta las disposiciones y acuerdos de la Asamblea General y Consejo Directivo.
2. Ejerce, conjuntamente con la presidencia del Consejo Directivo, la representación legal de la institución.

4. NOMBRE DEL PUESTO	**:**	**JEFE DE ASESORÍA LEGAL**
NIVEL	**:**	Jefatura.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Gerencia.
SUPERVISIÓN JERÁRQUICA	**:**	Asistente de Asesoría Legal.

A. FUNCIONES PRINCIPALES

1. Asesorar en la correcta aplicación de la normatividad legal vigente relacionada con la operatividad de ADEA.
2. Impulsar y coordinar el asesoramiento legal necesario para que las actuaciones de ADEA se ajusten permanentemente a derecho.

5. NOMBRE DEL PUESTO	**:**	**SUB GERENTE DE ADMINISTRACIÓN**
NIVEL	**:**	Gerencial.
SEDE	**:**	Central.

DEPENDENCIA JERÁRQUICA	:	Gerente.
SUPERVISIÓN JERÁRQUICA	:	Jefe de Tecnología de Información. Jefe de Talento Humano. Encargado de Logística. Jefe de Operaciones.

A. FUNCIONES PRINCIPALES

1. Planear, dirigir, controlar y administrar los recursos humanos, informáticos, materiales y logísticos que permitan el funcionamiento eficiente y la continuidad de las actividades de ADEA.

6. NOMBRE DEL PUESTO	**:**	**LOGISTICA**

SEDE	:	Central.
DEPENDENCIA JERÁRQUICA	:	Sub Gerente de Administración.
SUPERVISIÓN JERÁRQUICA	:	No Corresponde.

A. FUNCIONES PRINCIPALES

1. Supervisar, ejecutar, y controlar los bienes y las operaciones relacionadas al abastecimiento de ADEA así como el mantenimiento de la infraestructura de las agencias.

7. NOMBRE DEL PUESTO	**:**	**JEFE DE TECNOLOGÍA DE LA INFORMACIÓN Y SEGURIDAD**

NIVEL	:	Jefatura.
SEDE	:	Central.
DEPENDENCIA JERÁRQUICA	:	Sub Gerente de Administración.

SUPERVISIÓN JERÁRQUICA	:	Asistente de Desarrollo. Asistente de Soportes y Redes. Asistente de Gestión de Servicios.

A. FUNCIONES PRINCIPALES

1. Asegurar que el trabajo de las diferentes áreas de ADEA sea sistematizado, mediante el uso y aplicación correcta de técnicas, software y hardware, que permitan proporcionar la información necesaria y oportuna para el desarrollo de sus operaciones.
2. Controlar que todas las actividades relacionadas con el desarrollo, mantenimiento y operación de los Sistemas Informáticos de ADEA, así como la Administración de Base de Datos, plataforma de hardware y sistema de comunicaciones que los soporta.

8. NOMBRE DEL PUESTO	**:**	**JEFE DE TALENTO HUMANO**
NIVEL	:	Jefatura.
SEDE	:	Central.
DEPENDENCIA JERÁRQUICA	:	Sub Gerente de Administración.
SUPERVISIÓN JERÁRQUICA	:	No aplica

A. FUNCIONES PRINCIPALES

1. Contratar, controlar y administrar los recursos humanos de ADEA, de acuerdo a los estatutos, reglamentos y leyes laborales establecidas, ayudando a alcanzar los objetivos de la institución.
2. Dirigir las estrategias, proyectos y políticas que permitan a la institución mejorar el clima laboral y cultura institucional.

9. NOMBRE DEL PUESTO	**:**	JEFE DE OPERACIONES – CAJA GENERAL

NIVEL	**:**	Jefatura.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Sub Gerencia de Administración.
SUPERVISIÓN JERÁRQUICA	**:**	Cajera/o. Asistente de Operaciones. Auxiliar de Seguridad.

A. FUNCIONES PRINCIPALES

1. Planificar, coordinar, controlar, y supervisar las actividades relacionadas con el control y seguimiento de fondos, atención al usuario, adecuado y oportuno soporte y seguridad a las agencias, garantizando la ejecución de las operaciones y servicios que se ofrezcan en ADEA.
2. Planificar, elaborar y ejecutar las medidas de seguridad en el ámbito de su competencia.

10. NOMBRE DEL PUESTO	**:**	**JEFE DE CRÉDITOS**

NIVEL	**:**	Gerencial.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Gerente.
SUPERVISIÓN JERÁRQUICA	**:**	Jefe de Recuperaciones. Jefe de Marketing. Administradores de Agencia.

A. FUNCIONES PRINCIPALES

1. Planificar, organizar, dirigir, coordinar y controlar la actividades financieras de ADEA, garantizando una eficiente gestión y administración de los servicios financieros en sus diferentes tipos y sectores, asegurando en lo posible, el repago de los mismos, procurando obtener la máxima rentabilidad al menor riesgo posible en las colocaciones; proponiendo y controlando el cumplimiento de políticas y procedimientos que se dicte para reglamentar la actividad crediticia en ADEA y los Organismos Supervisores que reglamentan la actividad a nivel nacional.

11. NOMBRE DEL PUESTO	**:**	**ADMINISTRADOR DE AGENCIA**
NIVEL	**:**	Jefatura.
SEDE	**:**	Agencia.
DEPENDENCIA JERÁRQUICA	**:**	Jefe de Créditos
SUPERVISIÓN JERÁRQUICA	**:**	Todo personal de la Agencia a su cargo.

A. FUNCIONES PRINCIPALES

1. Responsable de planear, dirigir, organizar, ejecutar y controlar las actividades administrativas de la agencia y las relacionadas al servicio financiero que ofrece ADEA de acuerdo al Plan Operativo Anual.
2. Controlar las operaciones diarias de la Agencia de acuerdo a los dispositivos legales vigentes y a las normas internas de ADEA.
3. Velar por el cumplimiento del Sistema de Atención al Usuario.

12. NOMBRE DEL PUESTO	**:**	**ANALISTA DE CRÉDITO**
NIVEL	**:**	Asistente.
SEDE	**:**	Agencia.

DEPENDENCIA JERÁRQUICA	:	Supervisor de Créditos.
SUPERVISIÓN JERÁRQUICA	:	No Aplica.

A. FUNCIONES PRINCIPALES

1. Promocionar, evaluar y colocar los Créditos en sus diferentes tipos y modalidades que ofrece ADEA, considerando la política, procedimientos y criterios de evaluación aprobados por ADEA, asegurando en lo posible el repago, obteniendo la máxima rentabilidad al menor riesgo posible en la colocación, simultáneamente realizar la promoción de créditos.
2. Atender, analizar, calificar y evaluar todas las solicitudes presentadas por personas naturales y/o jurídicas con características crediticias y que califiquen como sujetos de crédito, y que cumplan con los requisitos mínimos exigidos para ser prestatario o beneficiario.

13. NOMBRE DEL PUESTO	**:**	**PROMOTOR DE CRÉDITOS**

NIVEL	:	Auxiliar.
SEDE	:	Agencia.
DEPENDENCIA JERÁRQUICA	:	Supervisor de Créditos.
SUPERVISIÓN JERÁRQUICA	:	No Aplica.

A. FUNCIONES PRINCIPALES

1. Promocionar los productos de créditos de ADEA.

14. NOMBRE DEL PUESTO	**:**	**ASISTENTE DE OPERACIONES**

NIVEL	**:**	Auxiliar.
SEDE	**:**	Agencia.
DEPENDENCIA JERÁRQUICA	**:**	Jefe de Operaciones.
DEPENDENCIA FUNCIONAL	**:**	Administrador de Agencia.
SUPERVISIÓN JERÁRQUICA	**:**	No Aplica.

A. FUNCIONES PRINCIPALES

1. Coordinar y organizar las actividades operativas y crediticias de la Agencia, relacionada con administración de fondos, atención al usuario, promoción, asegurando que la ejecución de las operaciones y servicios se efectúen adecuadamente.
2. Asegurar que las necesidades operativas tales como abastecimiento de formatearía, útiles de escritorio para el personal de operaciones, insumos de limpieza para la agencia sean cubiertas, canalizando sus requerimientos a las Instancias correspondientes para su atención oportuna.

15. NOMBRE DEL PUESTO	**:**	**RECIBIDOR / PAGADOR**

NIVEL	**:**	Asistente.
SEDE	**:**	Agencia.
DEPENDENCIA JERÁRQUICA	**:**	Jefe de Operaciones.
DEPENDENCIA FUNCIONAL	**:**	Administrador de Agencia.

SUPERVISIÓN JERÁRQUICA	:	No Aplica.

A. FUNCIONES PRINCIPALES

1. Responsable de la custodia del efectivo que se encuentra en su caja.
2. Brindar calidad de servicio en la atención a los clientes.

16. NOMBRE DEL PUESTO	**:**	**JEFE DE RECUPERACIONES**
NIVEL	:	Jefatura.
SEDE	:	Central.
DEPENDENCIA JERÁRQUICA	:	Jefe de Créditos.

A. FUNCIONES PRINCIPALES

1. Planificar, administrar y controlar la cobranza prejudicial, cobranza judicial y recuperación de la cartera castigada. de acuerdo a las normas, políticas y procedimientos establecidos.
2. Supervisa y aprueba las gestiones de negociación en cobranza prejudicial, cobranza judicial de la cartera vencida y recuperación de la cartera castigada.

17. NOMBRE DEL PUESTO	**:**	**GESTOR DE COBRANZAS**
NIVEL	:	Asistente.
SEDE	:	Central.
DEPENDENCIA JERÁRQUICA	:	Jefe de Agencia.
SUPERVISIÓN JERÁRQUICA	:	No aplica.

A. FUNCIONES PRINCIPALES

1. Llevar a cabo la gestión de cobranza de los créditos en situación morosa y vencida, de acuerdo a las directivas y políticas establecidas para estas operaciones.
2. Realizar lo necesario para hacer efectivo el cobro de los créditos vencidos, valiéndose de todos los medios legales para conseguir que los clientes con préstamos en mora, paguen su deuda.

18. NOMBRE DEL PUESTO	**:**	**JEFE DE CONTABILIDAD**
NIVEL	**:**	Jefatura.
SEDE	**:**	Central.
DEPENDENCIA JERÁRQUICA	**:**	Gerente de Finanzas.
SUPERVISIÓN JERÁRQUICA	**:**	Asistente de Contabilidad.

A. FUNCIONES PRINCIPALES

1. Planificar, organizar, dirigir y controlar los procesos contables, financieros y tributarios que se realizan en ADEA.
2. Velar por la realización oportuna y veraz de la información contable y financiera de la entidad, así como brindar asesoría en asuntos contables, financieros y tributarios relacionados a las actividades y servicios que realiza la institución.

19. NOMBRE DEL PUESTO	**:**	**ASISTENTE DE CONTABILIDAD**
NIVEL	**:**	Asistente.
SEDE	**:**	Central.

DEPENDENCIA JERÁRQUICA	:	Jefe de Contabilidad.
SUPERVISIÓN JERÁRQUICA	:	No Aplica.

A. FUNCIONES PRINCIPALES

1. Asistir al Jefe de Contabilidad en todas las funciones inherentes a la Contabilidad, además de apoyar en el análisis y elaboración de los Estados Financieros por Agencias y Consolidado para contar con dicha información en forma oportuna.
2. Revisar que toda la documentación entregada al Departamento de Contabilidad contenga los requisitos obligatorios para el cumplimiento de la normativa tributaria y contable.

20. NOMBRE DEL PUESTO	**:**	**JEFE DE TESORERIA**
NIVEL	:	Jefatura.
SEDE	:	Central.
DEPENDENCIA JERÁRQUICA	:	Sub Gerente de Administración.
SUPERVISIÓN JERÁRQUICA	:	Asistente de Tesorería.

A. FUNCIONES PRINCIPALES

1. Planificar, organizar, dirigir y controlar las operaciones de efectivo diarias que se realizan en las diferentes agencias de ADEA y proporcionar información diaria sobre los saldos monetarios.
2. Mantener conciliados los saldos efectivos de las cuentas diversas, en moneda nacional y extranjera.

3.2.2 Inventario general del hardware

El presente inventario describe bienes que fueron adquiridos durante y después de la implementación de la seguridad de la información. Aplicando un enfoque de abajo hacia arriba, se ha identificado los siguientes activos de TI, que dan soporte en todos los proceso de la organización.

Nº	Hardware	Cantidad
1	Equipo servidor de base de datos Oracle	6
2	Servidor de aplicaciones – Windows server	1
3	Servidor de correo y web	1
4	DVR - Sistemas de video vigilancia	5
5	Computadoras de escritorio	32
6	Laptop	7
7	Impresoras	14
8	Scanner	3
9	Access Point	1
10	Routers	1
11	Switchs	9
12	UPS	29

Figura 24: Tabla de inventario general del hardware de ADEA
Fuente: ADEA Andahuaylas

3.2.3 Identificación y clasificación de activos de tecnologías de la información

A continuación presente la tabla de activos de información con el que cuenta ADEA, clasificando el tipo de activo según la ISO 27005, puesto involucrado en su gestión y el nivel de criticidad en importancia de seguridad.

Nº	ACTIVO	TIPO DE ACTIVO - Según clasificación ISO 27005:2008	PUESTOS INVOLUCRADOS - Puestos en ADEA	NIVEL DE CRITICIDAD - Según semaforización
1	Servidor principal de base de datos	Servicios	Jefe de TI y Seguridad	MUY ALTO
2	Servidor principal de aplicaciones	Servicios	Jefe de TI y Seguridad	MUY ALTO
3	Red de comunicaciones	Comunicaciones	Jefe de TI y Seguridad	MEDIO
4	Ambiente de servidores	Instalaciones	Jefe de TI y Seguridad	MEDIO
5	Bases de datos	Informacion	Jefe de TI y Seguridad	MUY ALTO
6	Backups de base de datos	Soporte de informacion	Jefe de TI y Seguridad, Jefe de operaciones	MUY ALTO
7	Personal del area de TI	Personal	Jefe de TI y Seguridad, Jefe de operaciones	MEDIO
8	Correo corporativo	Servicios	Jefe de TI y Seguridad	ALTO
9	Equipos de computo terminales de ventanilla y analistas de negocio	Equipos informaticos	Todo el personal	MUY ALTO
10	Archivos de requerimientos informaticos	Datos o documentos	Jefe de TI y Seguridad, Jefe de operaciones	MEDIO
11	Equipos de computo del area de TI	Equipos informaticos	Jefe de TI y Seguridad	MEDIO
12	Registros de control de cambios de aplicaciones	Datos o documentos	Jefe de TI y Seguridad	ALTO
13	Backup de documentos normativos y de gestion	Informacion	Gerencia, Seb gerente de administración, Jefe de TI y Seguridad, Jefe de operaciones	MEDIO

Figura 25: Tabla de nivel de criticidad de activos de información
Fuente: ADEA Andahuaylas

3.2.4 Conectividad de las oficinas de ADEA

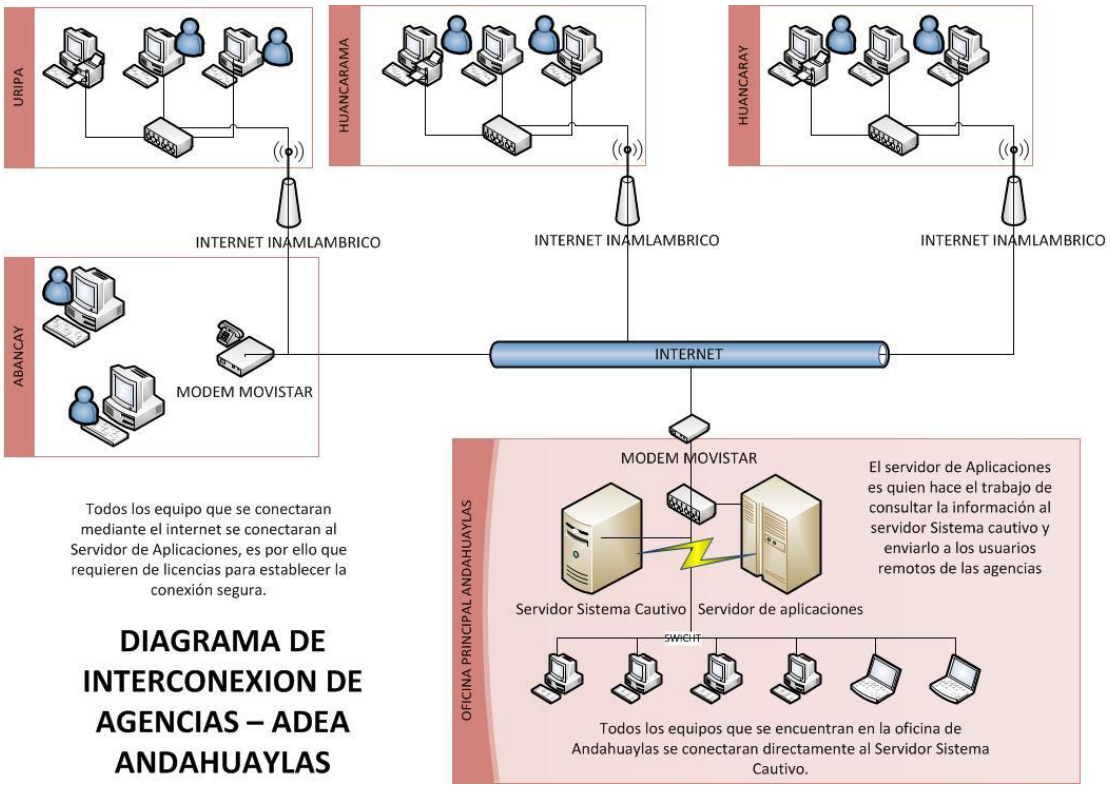


Figura 26: Esquema de conectividad entre las agencias de ADEA
Fuente: ADEA Andahuaylas

3.2.5 Plan Operativo

El plan operativo lo estableció de acuerdo al cronograma de actividades, por ello a continuación detallare las actividades realizadas de manera cronológica y secuencial del presente trabajo.

3.3 Marco Referencial

Para llevar a cabo el checklist, verificación de los controles del ISO 27002 en ADEA, se tuvo que hacer uso de los niveles de madures del CMMI, haciendo un modelo que esquematice mejor el objetivo del proyecto.

Este marco de referencia se utiliza para la calificación de los 14 dominios de la norma ISO 27002, con los cuales se elabora un tablero de mando basado en los niveles de madurez del CMMI.

3.3.1 Aplicación del marco de trabajo del ISO 27002

A continuación, detallo el marco de trabajo del ISO 27002, el cual será utilizado como herramienta básica para la el diagnostico situacional y comprender el estado actual de la seguridad de la información en la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros. El resultado del diagnóstico inicial, sirvió para la planificación y consecuentemente a su implementación mediante la elaboración de políticas, capacitaciones y soluciones tecnológicas con énfasis en la seguridad de la información.

TABLA Nº 01: LISTADO DE OBJETIVOS DE CONTROL, CLASIFICADOS POR DOMINIOS, SEGÚN LA NORMA ISO/IEC 27002:2013

Dominio	Requerimiento del objetivo de control			OBJETIVO DEL CONTROL PARA EL DESARROLLO EN ADEA
5	**POLITICAS DE SEGURIDAD**			
	5.1	**Directrices de la Direccion en seguridad de la información**		
		5.1.1	Conjunto de politicas para la seguridad de la informacion	Un documento de política de seguridad de la información debería ser aprobado por la Dirección y debería ser publicado y comunicado a todos los empleados y terceras partes.
		5.1.2	Revision de las politicas para la seguridad de la informacion	La política de seguridad de la información se debería revisar a intervalos planificados o en el caso de que se produzcan cambios significativos para asegurar la idoneidad, adecuación
6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION**			
	6.1	**Organización Interna**		
		6.1.1	Asignacion de responsabilidades para la seguridad de la informacion	Debería definirse claramente todas las responsabilidades de seguridad de la información.
		6.1.2	Segregacion de tareas	Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.
		6.1.3	Contacto con las autoridades	Se debería mantener contactos adecuados con las autoridades que corresponda.
		6.1.4	Contacto con grupos de interes especial	Se deberían mantener contactos apropiados con grupos de interés especial u otros foros especialistas en seguridad y asociaciones profesionales.
		6.1.5	Seguridad de la informacion en la gestion de proyectos	Tomar en consideracion para los futuros proyectos, la gestion de la información.
	6.2	**Dispositivos para movilidad y teletrabajo**		
		6.2.1	Politica de uso de dispositivos para movilidad	Debería implantarse una política formal y debería adoptarse las apropiadas medidas de seguridad para proteger contra los riesgos de la utilización de computadores y comunicaciones móviles.
		6.2.2	Teletrabajo	Se deberían desarrollar e implantar procedimientos, planes operacionales y una política para las actividades de teletrabajo.

7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**			
	7.1	**Antes de la contratacion**		
		7.1.1	Investigacion de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, los contratistas o los usuarios de tercera parte deberían ser llevadas a cabo de acuerdo con la legislación aplicable, las reglamentaciones y éticas de manera proporcional a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados.
		7.1.2	Terminos y condiciones de contratacion	Como parte de las obligaciones contractuales, los empleados, contratistas y usuarios de tercera parte deberían aceptar y firmar los términos y condiciones de su contrato de trabajo, que deberían establecer sus responsabilidades, así como las de la organización en lo relativo a la seguridad de la información.
	7.2	**Durante la contratacion**		
		7.2.1	Responsabilidad de gestion	La Dirección debería requerir a los empleados, contratistas y de tercera parte, el aplicar la seguridad de acuerdo a lo establecido en las políticas y procedimientos de la organización.
		7.2.2	Concienciacion, educacion y capacitacion en seguridad de la informacion	Todos los empleados de la organización y, cuando corresponda, los contratistas y los usuarios de tercera parte, deberían recibir una formación y concientización adecuadas y actualizadas de las políticas y procedimientos, según corresponda a su puesto de trabajo.
		7.2.3	Proceso disciplinario	Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna brecha de seguridad.
	7.3	**Cese o cambio de puesto de trabajo**		
		7.3.1	Cese o cambio de puesto de trabajo	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.

8	**GESTION DE ACTIVOS**			
	8.1	**Responsabilidad sobre los activos**		
		8.1.1	Inventario de activos	Todos los activos deberían ser claramente identificados y deberían prepararse y mantenerse un inventario de todos los activos importantes.
		8.1.2	Propiedad de los activos	Toda la información y los activos asociados con los recursos para el tratamiento de la información deberían ser propiedad de una parte designada de la organización.
		8.1.3	Uso aceptable de los activos	Las reglas de uso aceptable de la información y los activos asociados con el tratamiento de la información, deberían ser identificadas, documentadas e implantadas.
		8.1.4	Devolucion de activos	Todos los empleados, contratistas y usuarios de tercera parte deberían devolver los activos de la organización que tengan en posesión a la finalización de su empleo, contrato o acuerdo.
	8.2	**Clasificacion de la informacion**		
		8.2.1	Directrices de clasificacion	La información debería estar clasificada, según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.
		8.2.2	Etiquetado y manipulado de la informacion	Debería desarrollarse un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización.
		8.2.3	Manipulacion de activos	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
	8.3	**Manejo de los soportes de almacenamiento**		
		8.3.1	Gestion de soportes extraibles	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.
		8.3.2	Eliminacion de soportes	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.
		8.3.3	Soportes fisicos en transito	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización.

9	**CONTROL DE ACCESOS**			
	9.1	**Requisitos de negocio para el control de accesos**		
		9.1.1	Politica de control de accesos	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad para el acceso.
		9.1.2	Control de acceso a las redes y servicios asociados	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
	9.2	**Gestion de acceso de usuario**		
		9.2.1	Gestion de altas/bajas en el registro de usuarios	Debería haber un procedimiento de registro formal de usuarios y de retirada del registro para conceder y revocar el acceso a todos los sistemas y servicios de información.
		9.2.2	Gestion de los derechos de acceso asignados a usuarios	Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.
		9.2.3	Gestion de los derechos de acceso con privilegios especiales	La asignación y el uso de privilegios deberían estar restringidos y controlados.
		9.2.4	Gestion de informacion confidencial de autenticacion de usuarios	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.
		9.2.5	Revision de los derechos de acceso de los usuarios	La Dirección debería revisar los derechos de acceso de los usuarios a intervalos regulares y utilizando un procedimiento formal.
		9.2.6	Retirada o adaptacion de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en
	9.3	**Responsabilidad del usuario**		
		9.3.1	Uso de informacion confidencial para la autentificacion	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.
	9.4	**Control de acceso a sistemas y aplicaciones**		
		9.4.1	Restriccion del acceso a la informacion	Todos los usuarios deberían tener un identificador de usuario (ID) para su uso personal y único. Se debería elegir una técnica adecuada de autenticación para la conformación de la identidad de un usuario.
		9.4.2	Procedimientos seguros de inicio de sesion	Se debería controlar el acceso al sistema operativo mediante un procedimiento de entrada seguro.
		9.4.3	Gestion de contraseñas de usuario	Los sistemas para la administración de contraseñas deberían ser interactivos y asegurar la calidad de la contraseña.
		9.4.4	Uso de herramientas de administracion de sistemas	El uso de los programas que pueden ser capaces de invalidar los controles del sistema y de la aplicación, deberían estar restringidos y estrictamente controlados.
		9.4.5	Control de acceso al codigo fuente de los programas	Debería restringirse el acceso al código fuente de los programas.

10	**CIFRADO**			
	10.1	**Controles Criptográficos**		
		10.1.1	Politicas de uso de los controles criptograficos	Debería desarrollarse e implementarse una política acerca del uso de controles criptográficos para proteger la información.
		10.1.2	Gestion de claves	La asignación de contraseñas debería ser controlada a través de un proceso formal de gestión.
11	**SEGURIDAD FISICA Y AMBIENTAL**			
	11.1	**Areas seguras**		
		11.1.1	Perimetro de seguridad fisica	Debería usarse perímetros de seguridad (barreras tales como muros, puertas de entrada con control a través de tarjeta o mesas de recepción tripuladas) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.
		11.1.2	Controles fisicos de entrada	Las áreas seguras deberías estar protegidas por controles de entrada adecuados para asegurar que únicamente se permita el acceso al personal autorizado.
		11.1.3	Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar la seguridad física para las oficinas, despachos y recursos.
		11.1.4	Proteccion contra las amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra el daño por fuego, inundación, terremoto, explosión, malestar social y otras formas de desastres naturales o provocadas por el hombre.
		11.1.5	El trabajo en areas seguras	Se debería diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.
		11.1.6	Areas de acceso publico, carga y descarga	Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos donde pueda acceder personal no autorizado, y si es posible, dichos puntos deberías estar aislados de los recursos de tratamiento de la información para evitar accesos no autorizados.
	11.2	**Seguridad de los equipos**		
		11.2.1	Emplazamiento y proteccion de equipos	Los equipos deberías estar situados o protegidos para reducir los riesgos de las amenazas y los riesgos del entorno, así como de las oportunidades de acceso no autorizado.
		11.2.2	Instalaciones de suministro	Los equipos deberías estar protegidos de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.
		11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmiten datos a los servicios de soporte de la información debería estar protegido de interceptación o de daños.
		11.2.4	Mantenimiento de los equipos	Los equipos deberías ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.
		11.2.5	Salida de activos fuera de las dependencias de la empresa	Se debería aplicar medidas de seguridad a los equipos fuera de los locales de la organización, teniéndose en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Los equipos, la información o el software no deberían sacarse fuera de las instalaciones sin previa autorización.
		11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento	Todos los elementos del equipo que contengan medios de almacenamiento deberían ser comprobados para asegurar que todo dato sensible y software bajo licencia se ha borrado o sobrescrito, previamente a su utilización.
		11.2.8	Equipo informatico de usuario desatendido	Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada.
		11.2.9	Politica de puesto de trabajo despejado y bloqueo de pantalla	Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

12	**SEGURIDAD EN LA OPERATIVA**			
	12.1	**Responsabilidades y procedimientos de operación**		
		12.1.1	Documentacion de procedimientos de operación	Se debería implantar, mantener procedimientos operacionales y estar disponibles para todos los usuarios que lo necesiten.
		12.1.2	Gestion de cambios	Se deberían controlar los cambios en los recursos y sistemas de tratamiento de la información.
		12.1.3	Gestion de capacidades	Las tareas y áreas de responsabilidad deberían segregarse para reducir la posibilidad de modificaciones no autorizadas y no intencionadas o el mal uso de los activos de la organización.
		12.1.4	Separacion de entornos de desarrollo, prueba y produccion	Deberían separarse los recursos para el desarrollo, las pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema operativo.
	12.2	**Proteccion contra codigo malicioso**		
		12.2.1	Controles contra el codigo malicioso	Se debería implantar procedimientos de concienciación del usuario adecuados; así como controles de detección, prevención y recuperación para proteger contra código malicioso.
	12.3	**Copias de seguridad**		
		12.3.1	Copias de seguridad de la informacion	Se debería hacer copias de seguridad de la información y del software y ser comprobadas regularmente de acuerdo con la política de copias de seguridad acordadas.
	12.4	**Registro de actividad y supervision**		
		12.4.1	Registro y gestion de eventos de actividad	Se debería efectuar registros de auditoría de las actividades del usuario, excepciones e incidencias de información, y mantenerse durante un periodo acordado para ayudar en investigaciones futuras y en el seguimiento y monitorización del control de accesos.
		12.4.2	Proteccion de los registros de informacion	Los dispositivos de registro y el diario de información deberán estar protegidos contra la manipulación y los accesos no autorizados.
		12.4.3	Registros de actividad del administrador y operador del sistema	Las actividades de administrador del sistema y del operador del sistema deberán ser registradas.
		12.4.4	Sincronizacion de relojes	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o dominio de seguridad, deberían estar sincronizados con una precisión de tiempo acordada.
	12.5	**Control del software en explotacion**		
		12.5.1	Instalacion del software en sistemas en produccion	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.
	12.6	**Gestion de la vulnerabilidad tecnica**		
		12.6.1	Gestion de las vulnerabilidades tecnicas	Debería obtenerse información oportuna a cerca de las vulnerabilidades técnicas de los sistemas de información que se estén utilizando. Asimismo, deberían evaluarse la exposición de la organización a dichas vulnerabilidades y deberían adoptarse medidas adecuadas para afrontar el riesgo asociado.
		12.6.2	Restricciones en la instalacion de software	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
	12.7	**Consideraciones de las auditorias de los sistemas de informacion**		
		12.7.1	Controles de auditoría de los sistemas de información	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

13	**SEGURIDAD EN LAS TELECOMUNICACIONES**			
	13.1	**Gestion de la seguridad en las redes**		
		13.1.1	Controles de red	Las redes deberían estar adecuadamente gestionadas y controladas, para estar protegidas de amenazas y para mantener la seguridad de los sistemas y aplicaciones que usan estas redes, incluyendo la información en tránsito.
		13.1.2	Mecanismos de seguridad asociados a servicios en red	Las características de seguridad, los niveles de servicio, los requisitos de gestión para todos los servicios de red deberían estar identificadas e incluidas en todo acuerdo de servicio de red, aunque estos servicios se proporcionen desde dentro de la organización o sean subcontratados.
		13.1.3	Segregacion de redes	Los grupos de servicio de información, de usuarios y de sistema de información deberían estar segregados en redes.
	13.2	**Intercambio de informacion con partes externas**		
		13.2.1	Politicas y procedimientos de intercambio de informacion	Se debería establecer políticas de intercambio formal, procedimientos y controles para proteger el intercambio de la información mediante el uso de todos los tipos de servicios de comunicación.
		13.2.2	Acuerdos de intercambio	Se debería establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.
		13.2.3	Mensajeria electronica	La información implicada en el envío de mensajes electrónicos debería estar adecuadamente protegida.
		13.2.4	Acuerdos de confidencialidad y secreto	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION**			
	14.1	**Requisitos de seguridad de los sistemas de informacion**		
		14.1.1	Analisis y especificaciones de los requisitos de seguridad	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
		14.1.2	Seguridad de las comunicaciones en serviciso accesibles por redes publicas	La integridad de la información que se hace disponible en el sistema públicamente disponible debería estar protegida para prevenir la modificación no autorizada.
		14.1.3	Proteccion de las transacciones por redes telematicas	La información implicada en las transacciones online debería estar protegida para evitar la transmisión incompleta, las rutas erróneas, la alteración no autorizada del mensaje, la revelación no autorizada, la duplicación no autorizadas del mensaje.
	14.2	**Seguridad en los procesos de desarrollo y soporte**		
		14.2.1	Politica de desarrollo seguro de software	Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
		14.2.2	Procedimientos de control de cambios en los sistemas	En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.
		14.2.3	Revision tecnica de las aplicaciones tras efectuar cambios en el sistema operativo	Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.
		14.2.4	Restricciones a los cambios en los paquetes de software	La implementación de cambios debería estar controlada mediante el uso de procedimientos formales de control de cambios.
		14.2.5	Uso de principios de ingenieria en proteccion de sistemas	Los datos de prueba deberían seleccionarse atentamente, protegerse y controlarse.
		14.2.6	Seguridad en entornos de desarrollo	Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
		14.2.7	Externalizacion del desarrollo de software	La externalización del desarrollo del software debería ser supervisada y monitorizada por la organización.
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
		14.2.9	Pruebas de aceptacion	Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
	14.3	**Datos de prueba**		
		14.3.1	Proteccion de los datos utilizados en pruebas	Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.

15	**RELACIONES CON SUMINISTRADORES**			
	15.1	**Seguridad de la informacion en las relaciones con suministradores**		
		15.1.1	Politica de seguridad de la informacion para suministradores	Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.
		15.1.3	Cadena de suministro en tecnologias de la informacion y comunicaciones	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
	15.2	**Gestion de la prestacion del servicio por suministradores**		
		15.2.1	Supervision y revision de los servicios prestados por terceros	Se deberían gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio implicados y la revalorización de los riesgos.
		15.2.2	Gestion de cambios en los servicios prestados por terceros	Los servicios, informes y registros proporcionados por las terceras partes deberían ser controlados y revisados regularmente.
16	**GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION**			
	16.1	**Gestion de incidentes de seguridad de la informacion y mejoras**		
		16.1.1	Responsabilidades y procedimientos	Debería establecerse responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
		16.1.2	Notificacion de los eventos de seguridad de la informacion	Los eventos de seguridad de la información deberían comunicarse mediante canales adecuados de gestión lo antes posible.
		16.1.3	Notificacion de puntos debiles de la seguridad	Todos los trabajadores, contratistas y usuarios terceros de los sistemas y servicios de comunicación deberían estar obligados a anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios.
		16.1.4	Valoracion de eventos de seguridad de la informacion y toma de decisiones	Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
		16.1.5	Respuesta a los incidentes de seguridad	Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
		16.1.6	Aprendizaje de los incidentes de seguridad de la informacion	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
		16.1.7	Recopilacion de evidencias	La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO**			
	17.1	**Continuidad de la seguridad de la informacion**		
		17.1.1	Planificacion de la continuidad de la seguridad de la informacion	Debería desarrollarse e implantarse planes para mantener o restaurar las actividades y garantizar la disponibilidad de la información en el nivel y la escala temporal requeridos después de una interrupción o un fallo de los procesos críticos de un negocio.
		17.1.2	Implantacion de la continuidad de la seguridad de la informacion	Debería desarrollarse y mantenerse un proceso controlado para la continuidad del negocio en toda la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
		17.1.3	Verificacion, revision y evaluacion de la continuidad de la seguridad de la informacion	Deberían identificarse los eventos que provocan interrupciones en los procesos del negocio; así como la probabilidad y los efectos de dichas interrupciones y sus consecuencias con respecto a la seguridad de la información.
	17.2	**Redundancias**		
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la informacion	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.
18	**CUMPLIMIENTO**			
	18.1	**Cumplimiento de los requisistos legales y contractuales**		
		18.1.1	Identificacion de la legislacion aplicable	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse explícitamente, documentarse y mantenerse actualizados para cada sistema de información y la organización.
		18.1.2	Derechos de propiedad intelectual (DPI)	Deberían implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales acerca del uso de materiales con respecto a los cuales puedan existir derechos de propiedad intelectual y acerca del uso de productos de software exclusivo.
		18.1.3	Proteccion de los registros de la organización	Los registros importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios contractuales y empresariales.
		18.1.4	Proteccion de datos y privaciodad de la informacion personal	Debería garantizarse la protección de datos y la privacidad según se requiera en la legislación, las normativas y, si fuera aplicable, las cláusulas contractuales pertinentes.
		18.1.5	Regulacion de controles criptograficos	Los controles criptográficos deberían utilizarse de acuerdo con todos los contratos, leyes y normativas pertinentes.
	18.2	**Revisiones de la seguridad de la informacion**		
		18.2.1	Revision independiente de la seguridad de la informacion	Los requisitos y actividades de la auditoría que impliquen comprobaciones en los sistemas operativos, deberían planificarse cuidadosamente y acordarse, para minimizar los riesgos de interrupciones de los procesos.
		18.2.2	Cumplimiento de las politicas y normas de seguridad	Debería comprobarse periódicamente que los sistemas de información cumplan las normas de implementación de seguridad.
		18.2.3	Comprobacion del cumplimiento	Los gestores deberían asegurarse de que todos los procedimientos de seguridad, dentro de su área de responsabilidad, se realicen con el fin de cumplir las políticas y normas de seguridad.

3.3.2 Aplicación del marco de trabajo del CMMI

Para la medición de los resultados obtenidos por objetivo de control de la norma ISO 27002, es necesario utilizar un indicador de medición, es por ello que utilizo la integración de modelos de madurez de capacidades.

Este modelo de madurez para la seguridad de la información, permitió clasificar el estado situacional de cada objetivo de control revisado dentro de la organización.

Lo anterior fue para poder tener un contexto de la medida inicial y luego de la mejora de la seguridad, tener otra medición para luego constatar mejoras.

Figura 27: Niveles de Madurez CMMI
Fuente: Elaboración propia

NIVEL 0: NO EXISTENTE

Este nivel es considerado como incompleto o que no existe, por ello será considerado para el presente proyecto como control no aplicable a la organización.

NIVEL 1: REALIZADO

Para calificar cada dominio y objetivos de control de la norma ISO 27002, a continuación describo las características y/o consideraciones a tomar en cuenta para este nivel.

- Se identifican en forma general los activos de la organización.
- Se clasifican los activos de la organización como la información, la seguridad, los equipos y la sede, para así poder darle la protección adecuada a cada uno de ellos.
- Se observan eventos que atentan contra la información, los activos y la continuidad del negocio, pero no se le da la debida importancia a estos eventos.
- Los empleados no tienen conciencia de la seguridad informática (prestan sus claves, dejan sus equipos sin cerrar sesión).
- Se responde reactivamente a las amenazas de intrusión, virus, robo de equipos y de información.
- No se cuenta con un grupo interdisciplinario para tratar temas de seguridad informática dentro de la organización.
- Se cuenta con un proceso de desarrollo de software, pero este no tiene en cuenta las normas de la seguridad informática.

NIVEL 2: GESTIONADO

Para calificar cada dominio y objetivos de control de la norma ISO 27002, a continuación describo las características y/o consideraciones a tomar en cuenta para este nivel.

- Se empiezan a definir las Políticas de Seguridad de la Información de la organización basada en la Norma ISO/IEC 17799 debido a que se incrementa el interés por buscar las causas que originaron la ocurrencia de los eventos que atentaron contra la información, los activos y la continuidad del negocio. Además se cuenta con un plan de divulgación de las Políticas de Seguridad de la Información.

- Se cuenta con un grupo interdisciplinario, con el cual se busca trabajar temas de seguridad informática que sean de interés para la organización.
- De la clasificación de los activos se genera un inventario del hardware y software que hay en la organización.
- Se identifican riesgos asociados con la información, los equipos de cómputo y las sedes, así mismo se identifican vulnerabilidades de éstos por medio de las políticas.
- Se empieza a elaborar un informe de los incidentes de seguridad ocurridos.
- Se cuentan con Planes de continuidad del negocio, que contemplan solo los procesos críticos del negocio (los que garantizan la continuidad del mismo), no obstante se dejan otros procesos de la organización por fuera.
- Los roles del área de Seguridad Informática están bien definidos y se lleva un registro de las actividades que realiza cada rol. Se va incluyendo la seguridad informática dentro del proceso de desarrollo de software, pero aún en la metodología de desarrollo de software de la organización no se documenta esta inclusión.
- Se empieza a observar en los empleados una conciencia de la seguridad informática, pero aún no demuestran un compromiso con ella.

NIVEL 3: ESTABLECIDO

Para calificar cada dominio y objetivos de control de la norma ISO 27002, a continuación describo las características y/o consideraciones a tomar en cuenta para este nivel.

- Se divulgan las Políticas de Seguridad de la Información en toda la organización.
- El grupo interdisciplinario divulga a cada una de las áreas a las que representan, las medidas de seguridad que deberán ser tomadas para la conservación de la información de la organización.
- Se empieza a observar un compromiso de los empleados con la seguridad informática.

- Se incluye dentro del proceso de desarrollo de software las normas de seguridad informática.
- Se van estableciendo los controles y las medidas necesarias para disminuir los incidentes y para prevenir su ocurrencia en el futuro.
- Se cuenta con procedimientos que enseñan a los empleados a manejar la información y los equipos de cómputo en forma segura.
- Se monitorea la red de la organización, como una medida preventiva contra intrusiones, o infecciones de virus.

NIVEL 4: PREDECIBLE

Para calificar cada dominio y objetivos de control de la norma ISO 27002, a continuación describo las características y/o consideraciones a tomar en cuenta para este nivel.

- Se hacen revisiones periódicas o monitoreos a los activos de la organización.
- Se utiliza un indicador de cumplimiento para establecer si las Políticas de Seguridad de la Información y las cláusulas de seguridad establecidas por la organización en los contratos de trabajo, están siendo acatadas correctamente.
- Se realizan de manera sistemática pruebas a los controles, para determinar si están funcionando correctamente.
- Se hacen simulacros de incidentes de seguridad, para probar la efectividad de los planes de respuesta a incidentes.
- Se realizan pruebas a las aplicaciones o software desarrollados, para verificar que sí están cumpliendo con los requisitos de seguridad definidos en la metodología de desarrollo de software de la organización.
- Se hacen pruebas de intrusión a los equipos de cómputo de la organización, para detectar, claves débiles o fáciles de adivinar, y accesos a ciertos sistemas por usuarios no autorizados.

NIVEL 5: OPTIMIZADO

Para calificar cada dominio y objetivos de control de la norma ISO 27002, a continuación describo las características y/o consideraciones a tomar en cuenta para este nivel.

- Los empleados apoyan y contribuyen al mejoramiento de la seguridad informática en la organización.
- La organización aprende continuamente sobre los incidentes de seguridad presentados.
- Se deben analizar los datos arrojados por la evaluación de seguridad de la información para que se puedan definir acciones preventivas más claras.
- Se incluyen todas las áreas de la organización (críticas y no críticas), en los planes de respuesta a incidentes.

3.3.3 Aplicación del marco de trabajo del tablero de mando

Para la medición e interpretación de resultados obtenidos a partir del CMMI, utilizando la semaforización a nivel de tres colores; verde, amarillo y rojo, denotando los niveles alcanzados alto, medio y bajo respectivamente.

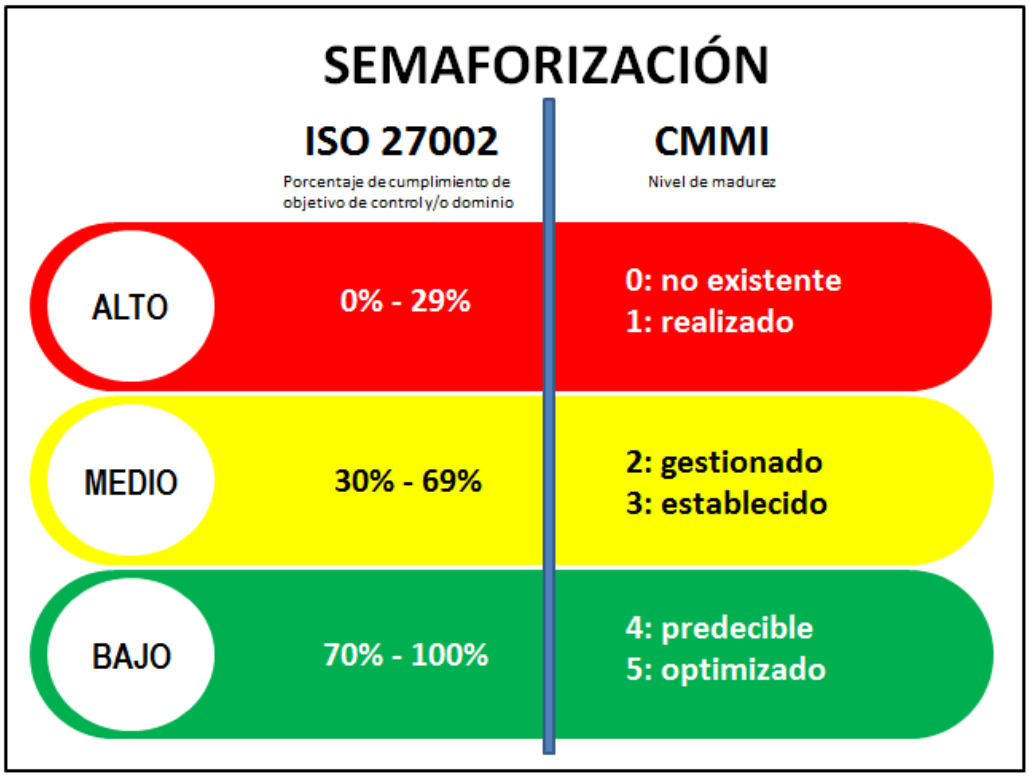


Figura 27: Cuadro de mando para la semaforización
Fuente: Elaboración propia

Para la interpretación de resultados, se homogenizo la clasificación de la medición de los controles y por ponderación los 14 dominios de la ISO 27002.

ROJO: significa riesgo alto de inseguridad de la información. En este color están clasificados los objetivos de control (los cuales son medidos de 1 – 100 %), que tienen menos del 30% de cumplimiento, por ende son clasificados en el nivel de madurez “0” o “1” del CMMI, según sea evaluado.

AMARILLO: significa riesgo medio de inseguridad de la información. En este color están clasificados los objetivos de control que su cumplimiento comprende entre el 30% al 69%. En cuanto al nivel de madurez considerados en este color, están los niveles “2” y “3” según sea evaluado.

VERDE: significa que el riesgo de inseguridad es mínimo (bajo). En este color están clasificados los objetivos de control que tengan un porcentaje de cumplimiento mayor al 70%. En cuanto al nivel de madurez, son considerados el nivel “4” y “5” del CMMI, según sea evaluado.

A continuación muestro el modelo del resultado.

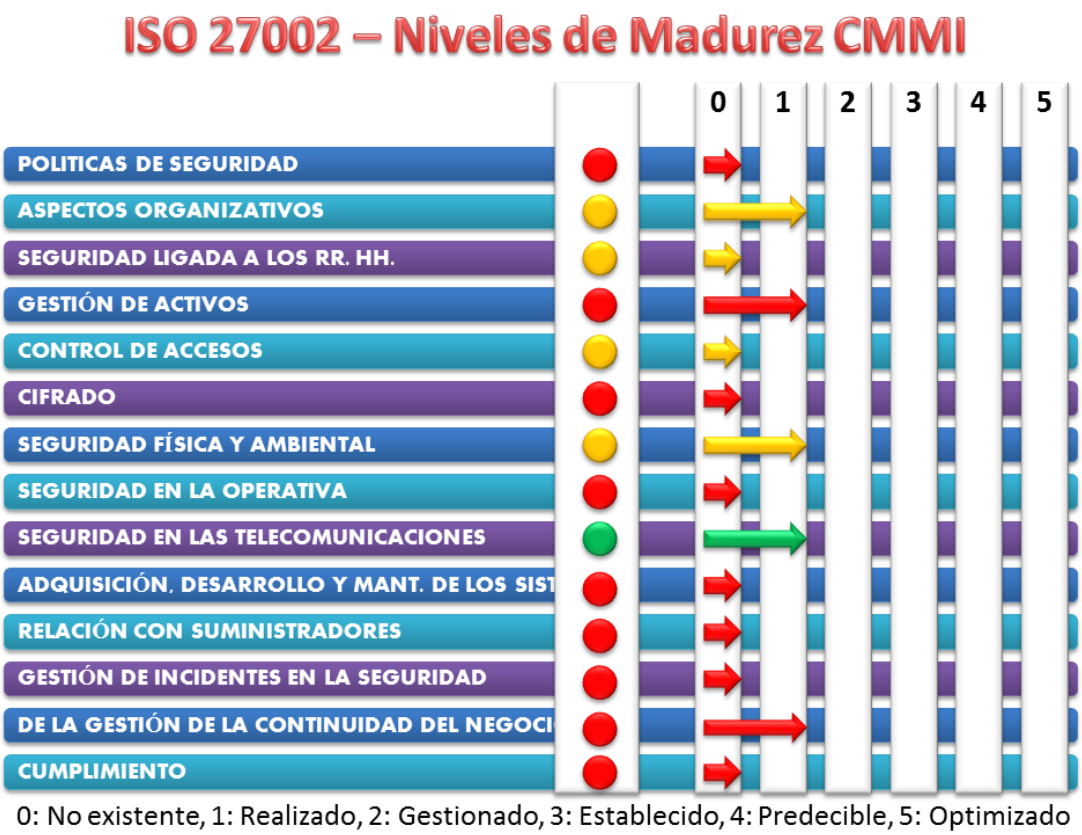


Figura 28: Modelo de resultados controles ISO27002 – Niveles de madures CMMI
Fuente: Elaboración propia

Como se puede visualizar en la figura, el resultado de la evaluación se muestra con cada dominio de la ISO 27002, donde es evaluado y determinado a un nivel de madurez del CMMI y para su mejor interpretación se hace uso de la semaforización para el cuadro de mando.

3.4 Marco Normativo

Dentro de la institución la denominación actual del puesto a mi cargo es de jefe de tecnologías de la información y seguridad, donde según el manual de organizaciones y funciones de ADEA vigente desde noviembre del 2015, estipula que una de las funciones principales de mi puesto es asegurar que el trabajo de las diferentes áreas de ADEA sea sistematizado, mediante el uso y aplicación correcta de técnicas, software y hardware, que permitan proporcionar la información necesaria y oportuna para el desarrollo de sus operaciones. Este punto justifica él porque del desarrollo del presente proyecto a cargo de mi persona en dicha institución.

En referencia a esta necesidad de establecer barreras de acceso no autorizado a la información, cabe precisar que en que Perú en el año 2007, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 17799:2007 Ed. Tecnología de la información, código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", en todas la entidades integrantes del sistema nacional de informática. (ONGEI, NTP ISO/IEC 17799:2007). En noviembre del 2014 se aprobó como norma técnica peruana la NTP-ISO/IEC 27001:2014 Tecnologías de la Información, técnicas de seguridad, sistemas de seguridad de la información, con el fin de que su uso en las entidades gubernamentales reduzca el riesgo de la seguridad de la información. (ONGEI, NTP ISO/IEC 27001:2014). Esta norma técnica hace de referencia fundamental en el uso de buenas prácticas para las entidades privadas de nuestro país y mucho más de aquellas que funcionan para el rubro financiero.

Para la implementación de controles y de las medidas reactivas, correctivas y preventivas en la gestión de la información, que aseguren conseguir las tres características básicas de la seguridad de la información, ADEA Andahuaylas rige su gestión en base a las exigencias de la SBS, el cual recomienda aplicar o utilizar un marco metodológico que esté basado en estándares como: ISO/IEC 17799 – ISO 27002 y la ISO/IEC 27001 y otras.
La SBS ha determinado algunas normas específicas para tres ámbitos diferentes:

- Gestión de seguridad de la información: Circular N° G-140-2009 sobre Gestión de Seguridad de la Información, que establece criterios para gestionar la seguridad de la información y toma como referencia estándares internacionales como el ISO 27001 e ISO 27002.
- Gestión de continuidad del negocio: Circular N° G-139-2009 sobre Gestión de Continuidad del Negocio, que establece criterios para gestionar la continuidad de negocio financiero que forma parte de la gestión de riesgo operacional que tienen que enfrentar las empresas que son supervisadas por la SBS, las cuales toman como referencia los estándares internacionales como el BS-25999.
- Riesgos operativos de TI: Circular N° G-105-2002 sobre Riesgos de Tecnología de Información, que establece criterios para identificar y gestionar los riesgos relacionados con las tecnologías de información.

CAPITULO IV: ANALISIS DE COSTO Y BENEFICIO

4.1 Viabilidad económica

COSTOS DEL PROYECTO

ITEM	DESCRIPCION	Cantidad	UNID. MEDIDA	Precio Unit	Precio parcial
1.00.00	DIAGNOSTICO				860.00
1.01.00	Revisión de los documentos de gestión de ADEA				210.00
1.01.01	Asesorías	3	Sesión	50.00	150.00
1.01.02	Servicio de internet	1	Mes	40.00	40.00
1.01.03	Impresión	0.5	Millar	40.00	20.00
1.02.00	Revisión de la modalidad de gestión de la información de ADEA				50.00
1.02.01	Impresión	0.5	Millar	100.00	50.00
1.03.00	Evaluación de controles basado en ISO 27002 PRIMERA ETAPA				300.00
1.03.01	Asesorías	3	Sesión	50.00	150.00
1.03.02	Servicio de internet	1	Mes	100.00	100.00
1.03.03	Impresión	0.5	Millar	100.00	50.00
1.04.00	Informe de estado situacional a la alta dirección de ADEA				300.00
1.04.01	Asesorías	3	Sesión	50.00	150.00
1.04.02	Servicio de internet	1	Mes	100.00	100.00
1.04.03	Impresión	0.5	Millar	100.00	50.00
2.00.00	PLANIFICACIÓN				2,675.00
2.01.00	Calendarización de Actividades				650.00
2.01.01	Asesorías	3	Sesión	50.00	150.00
2.01.02	Libros de Gestión de TIC	2	Unid	250.00	500.00
2.02.00	Determinación de Recursos Necesarios				1,650.00
2.02.01	Revisión de tesis, Papers y otros antecedentes	5	Evento	100.00	500.00
2.02.02	Libros de Auditoria de Sistemas	2	Unid	250.00	500.00
2.02.03	Libros de Gestión de TIC	2	Unid	250.00	500.00
2.02.04	Servicio de internet	1	Mes		

				100.00	100.00
2.02.05	Impresión	0.5	Millar	100.00	50.00
2.03.00	Calendarización de Actividades				375.00
2.03.01	Servicio de internet	1	Mes	250.00	250.00
2.03.02	Impresión	0.5	Millar	250.00	125.00
3.00.00	IMPLEMENTACIÓN				3,220.00
3.01.00	Elaboración de modelo de propuesta de solución a alta dirección de ADEA				480.00
3.01.01	Asesorías	3	Sesión	50.00	150.00
3.01.02	Programación de entrevistas con expertos	4	Evento	70.00	280.00
3.01.03	Impresión	0.5	Millar	100.00	50.00
3.02.00	Elaboración de políticas de gestión de seguridad de la información				780.00
3.02.01	Usuarios	60	Form	10.00	600.00
3.02.02	Auditores	4	Form	10.00	40.00
3.02.03	Administradores	4	Form	10.00	40.00
3.02.04	Impresión	1	Millar	100.00	100.00
3.03.00	Implementación de políticas de seguridad de la información				630.00
3.03.01	Asesorías	5	Sesión	50.00	250.00
3.03.02	Programación de entrevistas con expertos	4	Evento	70.00	280.00
3.03.03	Impresión	1	Millar	100.00	100.00
3.04.00	Capacitación de usuarios e interesados				780.00
3.04.01	Usuarios	60	Form	10.00	600.00
3.04.02	Auditores	3	Form	10.00	30.00
3.04.03	Administradores	5	Form	10.00	50.00
3.04.04	Impresión	1	Millar	100.00	100.00
3.05.00	Puesta en marcha de políticas de seguridad de la información				550.00
3.05.01	Asesor metodológico	5	Sesión	50.00	250.00
3.05.02	Asesor para capacitaciones	5	Sesión	50.00	250.00
3.05.03	Impresión	0.5	Millar	100.00	50.00
4.00.00	Evaluación				550.00
4.01.00	Evaluación de controles basado en ISO 27002 SEGUNDA ETAPA				550.00

4.01.01	Asesor metodológico	5	Sesión	50.00	250.00
4.01.02	Auditor	5	Sesión	50.00	250.00
4.01.03	Impresión	0.5	Millar	100.00	50.00
5.00.00	Monitoreo				**1,950.00**
5.01.00	Intervenciones de Auditoria interna				**1,250.00**
5.01.01	Asesor	5	Sesión	50.00	250.00
5.01.02	Digitador	1	Persona	750.00	750.00
5.01.03	Auditor	5	Sesión	50.00	250.00
5.02.00	Políticas de mejoras				**700.00**
5.02.01	Impresión	2	Millar	100.00	200.00
5.02.02	Anillados para presentación	10	Unid	50.00	500.00
6.00.00	Elaboración del informe final				**600.00**
6.01.00	Redacción del informe final				**600.00**
6.01.01	Pago de Derechos	1	Pago	300.00	300.00
6.01.02	Asesor	2	Sesión	50.00	100.00
6.01.03	Impresión	2	Millar	100.00	200.00
7.00.00	GASTOS GENERALES				**45,000.00**
	Personal				
	Encargado del Proyecto	18	mes	2,000.00	36,000.00
	Equipo				
	Computadora - Software de Oficina	1	Unid	3,000.00	3,000.00
	Servicios				
	Servicios de comunicación	10	Unid	30.00	300.00
	Viáticos diversos	18	mes	150.00	2,700.00
	Imprevistos – Reserva de gestión	1	Unid	3,000.00	8,800.00
	COSTO TOTAL DEL PROYECTO - SOLES				**60,655.00**

Figura 29: Presupuesto para el desarrollo del proyecto
Fuente: Elaboración propia

FLUJO DE INGRESOS Y EGRESOS

MES	0	ene-16	feb-16	mar-16	abr-16	may-16	jun-16	jul-16	ago-16	sep-16	oct-16	nov-16	dic-16
INGRESOS													
Flujo de ingresos	552,025.63	20,000.00	20,000.00	22,500.00	20,000.00	22,500.00	21,000.00	21,000.00	35,956.88	35,956.88	35,956.88	35,956.88	35,956.88
EGRESOS													
Implementación del pr	60,655.00	3,070.00	3,050.00	3,050.00	3,400.00	4,400.00	3,375.00	3,730.00	3,450.00	3,280.00	3,250.00	2,850.00	3,250.00
Costos por seguridad	51,420.00	5,000.00	5,500.00	6,500.00	5,000.00	11,500.00	8,000.00	4,000.00	2,500.00	800.00	500.00	420.00	300.00
Flujo de caja S/.	(112,075.00)	**11,930.00**	**11,450.00**	**12,950.00**	**11,600.00**	**6,600.00**	**9,625.00**	**13,270.00**	**30,006.88**	**31,876.88**	**32,206.88**	**32,686.88**	**32,406.88**

MES	ene-17	feb-17	mar-17	abr-17	may-17	jun-17
INGRESOS						
Flujo de ingresos	35,956.88	35,956.88	35,956.88	35,956.88	40,456.88	40,956.88
EGRESOS						
Implementación del pr	3,050.00	3,050.00	4,250.00	3,350.00	3,400.00	3,400.00
Costos por seguridad	250.00	250.00	200.00	250.00	250.00	200.00
Flujo de caja S/.	**32,656.88**	**32,656.88**	**31,506.88**	**32,356.88**	**36,806.88**	**37,356.88**

Tasa de descuento (costo de oportunidad)		**12%**
VAN		S/. 94,374.08
TIR		15%

TIR = 0.14709808

4.2 Análisis de Beneficios

La elaboración del presente trabajo trata de lograr para la entidad un VAN (Valor Neto Actual) positivo en este caso, mediante la utilización de recursos a través de este proyecto de buenas prácticas en seguridad de la información basada en ISO 27002 en la Asociación para el Desarrollo Empresarial en Apurímac – ADEA.

Cabe indicar que se asume que la tasa de descuento del 12%, es usualmente el porcentaje de rentabilidad que la organización considera como mínimo para los proyectos. Se aplica la fórmula del VAN para un periodo de doce meses que se considera como plazo para poder generar flujos de caja que permitan añadir valor a la empresa luego de la implementación de las buenas prácticas en seguridad de la información basada en ISO 27002.

Dado que la TIR es el retorno efectivo que entregan los flujos de caja proyectados, esa tasa de retorno puede ser comparada luego con la tasa de descuento de la empresa, que vendría a ser la tasa de retorno mínima que debe alcanzar un proyecto de inversión para una compañía, como lo indica Kremer & Berman (2009). Para este proyecto de mejora se observa que la TIR es mayor a la tasa de descuento o costo de oportunidad de ADEA, lo cual da una señal afirmativa de poder seguir adelante con el proyecto, más aun que es respaldada por la gerencia y alta dirección de la organización.

El conjunto de costos que derivaban de incidencias de seguridad de la información, equivalían a costos por un valor promedio de S/. 8,520 antes de la implementación de las buenas prácticas en seguridad de la información basada en ISO 27002. Luego de incorporadas estas buenas prácticas, ese costo promedio (egreso) decreció en un 83.6%, es decir a un valor promedio de S/. 1,400; lo cual viene a ser un ahorro equivalente a S/. 7,120, que en el flujo de caja se observa como flujo de ingresos promedio mensual a lo largo de seis meses.

Costos antes de implementación con ISO 27002	S/. 8,520.00
Costos después de la implementación	S/. 1,400.00
Ahorro promedio	S/. 7,120.00

CAPITULO V: IMPLEMENTACIÓN Y DESEMPEÑO

5.1 Metodología de la implementación de la solución

De acuerdo al modelo de la solución óptima, a continuación describo las actividades desarrolladas durante la implementación del proyecto de buenas prácticas en seguridad de la información basada en ISO 27002 en la Asociación para el Desarrollo Empresarial en Apurímac – ADEA Andahuaylas.

ETAPA DE DIAGNOSTICO

En esta etapa se usó básicamente la documentación del ISO 27002. Se procedió a elaborar un cuestionario con preguntas seleccionadas que estaban orientadas a cada dominio de control de dicha norma.

Dicho cuestionario fue llenado con el apoyo del gerente de ADEA. Como resultado del cuestionario, adjunto el mismo.

CUESTIONARIO PARA VERIFICACIÓN DE CONTROLES BASADO EN LA NORMA ISO 27002:2013

PRIMERA ETAPA - DIAGNOSTICO

5 POLITICAS DE SEGURIDAD

Cuenta con politicas de seguridad de la informacion

SI		NO	X	PARCIALMENTE	

Tiene implementados controles de cumplimiento de las politicas de seguridad de la informacion

SI		NO	X	PARCIALMENTE	

Las politicas de seguridad de la informacion son de conocimiento de todo el personal de la institucion

SI		NO	X	PARCIALMENTE	

6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION

Cuentan con un area de labores exlusivas de seguridad de la informacion

SI		NO		PARCIALMENTE	X

Han contratado un asesoramiento en materia de seguridad de la informacion

SI		NO	X	PARCIALMENTE	

Los incidentes de seguridad de los sistemas de informacion son reportados por los usuarios

SI		NO		PARCIALMENTE	X

Cuenta con convenios o clausulas de contratos de confidencialidad de la informacion

SI	X	NO		PARCIALMENTE	

7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Cuando realizan contratos con empresas externas exigen clausulas de seguridad de la informacion

SI		NO	X	PARCIALMENTE	

8 GESTION DE ACTIVOS

Cuentan con un inventario de activos de informacion actualizado asignado a responsables

SI		NO		PARCIALMENTE	X

El inventario esta automatizado

SI		NO		PARCIALMENTE	X

El inventario de activos informaticos hardware y software es actualizado periodicamente

SI	X	NO		PARCIALMENTE	

Los inventarios tienen clasificacion de riesgo

SI		NO	X	PARCIALMENTE	

9 CONTROL DE ACCESOS

Cuentan con una politica de control de accesos

SI		NO	X	PARCIALMENTE	

Las aplicaciones con las que cuenta la institucion cuenta con una contraseña para permitir el acceso al usuario

SI	X	NO		PARCIALMENTE	

Para el acceso remoto a aplicaciones de la institucion, tienen establecidos mecanismos de autenticacion

SI	X	NO		PARCIALMENTE	

Revisan los perfiles de acceso de los usuarios

SI		NO		PARCIALMENTE	X

Cuentan con un control de acceso al codigo fuente del software utilizado en la empresa

SI		NO	X	PARCIALMENTE	

10 CIFRADO

Cuentan con controles criptograficos, por ejemplo el uso de certificados digitales o programas de encriptacion de datos

SI		NO	X	PARCIALMENTE	

Tienen controles que impidan el acceso no autorizado a los programas fuente de las aplicaciones de la institucion

SI		NO	X	PARCIALMENTE	

11 SEGURIDAD FISICA Y AMBIENTAL

Todas las areas de trabajo estan debidamente identificadas

SI		NO		PARCIALMENTE	X

Para las areas seguras, cuentan con controles de ingreso del personal

SI		NO		PARCIALMENTE	X

En el caso de alguna falla en el cableado de datos, estan preparados para su pronta correccion

SI		NO		PARCIALMENTE	X

Se realiza mantenimiento periodico del hardware y software en la institucion

SI	X	NO		PARCIALMENTE	

Cuentan con criterios de seguridad las instalaciones desuministros y red de datos

SI		NO	X	PARCIALMENTE	

Controlan la salida de equipos y activos fuera de la empresa

SI		NO		PARCIALMENTE	X

Gestionan el uso correcto de los equipos de computo y dispositivos de almacenamiento

SI		NO	X	PARCIALMENTE	

12 SEGURIDAD EN LA OPERATIVA

Cuentan con un manual de procedimientos en la Oficina de Tecnologias de la Informaciòn

SI		NO		PARCIALMENTE	X

Cuentan con controles de seguridad de los medios de almacenamiento

SI		NO	X	PARCIALMENTE	

Gestionan las vulnerabilidades del software que utiliza la institucion

SI		NO	X	PARCIALMENTE	

Restringen la instalacion de software

SI		NO	X	PARCIALMENTE	

13 SEGURIDAD EN LAS TELECOMUNICACIONES

Cuentan con software de control de redes

SI		NO	X	PARCIALMENTE	

Cuentan con mecanismos de gestion de seguridad de la red de la institucion

SI		NO	X	PARCIALMENTE	

Cuentan con politicas y procedimientos de intercambio de informacion con partes externas

SI		NO	X	PARCIALMENTE	

14 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION

Cuentan con procedimientos de control de los cambios para aplicaciones, software y S.O.

SI		NO	X	PARCIALMENTE	

Cuentan con acceso completo al codigo fuente del sistema financiero utilizado por la institucion

SI		NO	X	PARCIALMENTE	

Se validan codigos fuentes desarrollados por el externo antes de la puesta en marcha

SI		NO	X	PARCIALMENTE	

15 RELACIONES CON SUMINISTRADORES

Cuentan con politicas de seguridad de informacion para suministradores

SI		NO	X	PARCIALMENTE	

Gestionan el riesgo dentro de acuerdos con suministradores

SI		NO	X	PARCIALMENTE	

Supervisan y revisan los servicios prestados por terceros

SI		NO	X	PARCIALMENTE	

16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION

Cuentan con un procedimiento formal para reportes de incidentes

SI		NO	X	PARCIALMENTE	

Cuentan con herramientas de registro de incidentes o Help Desk

SI		NO	X	PARCIALMENTE	

Al presentarse un incidente de seguridad, cuentan con un plan de respuesta

SI		NO	X	PARCIALMENTE	

Se investiga y recolecta evidencias sobre el incidente de seguridad

SI		NO	X	PARCIALMENTE	

17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO

Cuentan con planes o reglamentos de continuidad del negocio aprobado y vigente

SI		NO		PARCIALMENTE	X

Cuentan con un plan de mantenimiento y pruebas aprobado y vigente

SI		NO	X	PARCIALMENTE	

Cuentan con equipos de redundancia

SI		NO		PARCIALMENTE	X

18 CUMPLIMIENTO

Tienen identificada la normativa legal que aplican a las aplicaciones de la institucion

SI		NO	X	PARCIALMENTE	

Cuentan con politicas de proteccion de datos y privacidad de la informacion de los colaboradores

SI		NO	X	PARCIALMENTE	

Cuentan con controles del uso adecuado de los recursos de la institucion

SI		NO	X	PARCIALMENTE	

Cuentan con controles de cumplimiento de las politicas de seguridad de la informacion

SI		NO	X	PARCIALMENTE	

Realizan auditoria a los sistemas informaticos de la institucion

SI		NO		PARCIALMENTE	X

Figura 30: Cuestionario para el checklist de controles de la ISO 27002
Fuente: Elaboración propia

A continuación muestro el resultado del checklist realizado en febrero del 2016. La calificación de los controles se realizó de acuerdo a la escala de valoración de control recomendado por la norma ISO 27002:2013. Se toma en cuenta

también la escala de nivel de madurez de dicho control con la escala normativa de CMMI.

RESULTADO DE CHECKLIST DE CONTROLES DE LA NORMA ISO 27002:2013 DE LA ASOCIACION PARA EL DESARROLLO EMPRESARIAL EN APURIMAC, ANDAHUAYLAS Y CHINCHEROS

PRIMERA ETAPA

DIAGNOSTICO SITUACIONAL DE SEGURIDAD DE LA INFORMACIÓN EN LA ASOCIACION PARA EL DESARROLLO EMPRESARIAL EN APURIMAC, ANDAHUAYLAS Y CHINCHERO - ADEA ANDAHUAYLAS

Responsal Bach. Ing. Sis. Kliffor Palomino Palomino

DESCRIPCION DE LA PLANTILLA ISO 27002

Dominio	Número del dominio
Obj. de control	Cantidad y número del objetivo de control
Controles	Cantidad y número de controles por cada objetivo
Orientacion	Proporciona información sobre la obligatoriedad de implementar o no el control
Descripcion	Breve descripción de cada objetivo de control agrupandolos por dominio
PD	Peso del dominio
NC.D	Nivel de cumplimineto del dominio
PO	Peso del objetivo
NC.O	Nivel de cumplimineto del dominio
PC	Peso del control
NC.C	Nivel de cumplimiento del control
Escala	Escala del cumplimiento del control

Escala visual de la valoración del control para ADEA Andahuaylas

Alto	Mas del 70% de cumplimiento
Medio	Entre el 30 y 69 % de cumplimiento
Bajo	Por debajo del 30%

Indicaciones para el uso de la plantilla correctamente:

Ingrese valores entre 0 y 100 SOLO en los cuadros azules, los cuales corresponderán al valor asignado al nivel de cumplimiento de cada control "NC.C" de la norma; tenga en cuenta que en esta escala de valoración, el "0" indica que no cumple el control y "100" que lo cumple satisfactoriamente, recuerde que también se puede asignar valores intermedios cuando se cumple parcialmente cualquiera de los controles.

DOMINIOS DE TI A EVALUAR

14	**Dominios**
35	**Objetivos Control**
114	**Actividades de Control**

Dominios	Objetivos de Control	Controles	Descripción	Orientación	% de cumplimiento de la norma							NIVEL CMMI
					PD	NC. D	PO	NC. O	PC	NC. C	ESTADO	
5	POLITICAS DE SEGURIDAD				1.75	10		100				
	5.1		Directrices de la Direccion en seguridad de la información				100	10				
		5.1.1	Conjunto de politicas para la seguridad de la informacion						50	10		REALIZADO
		5.1.2	Revision de las politicas para la seguridad de la informacion						50	10		REALIZADO
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION				7.02	11.43		100				
	6.1		Organización Interna				71.43	10				
		6.1.1	Asignacion de responsabilidades para la seguridad de la informacion						14.28	10		REALIZADO
		6.1.2	Segregacion de tareas						14.28	30		GESTIONADO
		6.1.3	Contacto con las autoridades						14.28	10		REALIZADO
		6.1.4	Contacto con grupos de interes especial						14.28	10		REALIZADO
		6.1.5	Seguridad de la informacion en la gestion de proyectos						14.28	10		REALIZADO
	6.2		Dispositivos para movilidad y teletrabajo				28.57	1.43				
		6.2.1	Politica de uso de dispositivos para movilidad						14.28	10		REALIZADO
		6.2.2	Teletrabajo	NO APLICA					14.28	0		NO EXISTENTE
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				5.26	35		100				
	7.1		Antes de la contratacion				33.33	8.33				
		7.1.1	Investigacion de antecedentes	NO APLICA					16.66	0		NO EXISTENTE
		7.1.2	Terminos y condiciones de contratacion						16.66	50		ESTABLECIDO
	7.2		Durante la contratacion				50	18.33				
		7.2.1	Responsabilidad de gestion						16.66	50		ESTABLECIDO
		7.2.2	Concienciacion, educacion y capacitacion en seguridad de la informacion						16.66	10		REALIZADO
		7.2.3	Proceso disciplinario						16.66	50		ESTABLECIDO
	7.3		Cese o cambio de puesto de trabajo				16.67	8.34				
		7.3.1	Cese o cambio de puesto de trabajo						16.66	50		ESTABLECIDO

8	**GESTION DE ACTIVOS**				**8.77**	**21**		**100**					
	8.1	Responsabilidad sobre los activos					**40**	**15**					
		8.1.1	Inventario de activos						**10**	50		**ESTABLECIDO**
		8.1.2	Propiedad de los activos						**10**	50		**ESTABLECIDO**
		8.1.3	Uso aceptable de los activos						**10**	50		**ESTABLECIDO**
		8.1.4	Devolucion de activos	**NO APLICA**					**10**	0		**NO EXISTENTE**
	8.2	Clasificacion de la informacion					**30**	**3**					
		8.2.1	Directrices de clasificacion						**10**	10		**REALIZADO**
		8.2.2	Etiquetado y manipulado de la informacion						**10**	10		**REALIZADO**
		8.2.3	Manipulacion de activos						**10**	10		**REALIZADO**
	8.3	Manejo de los soportes de almacenamiento					**30**	**3**					
		8.3.1	Gestion de soportes extraibles						**10**	10		**REALIZADO**
		8.3.2	Eliminacion de soportes						**10**	10		**REALIZADO**
		8.3.3	Soportes fisicos en transito						**10**	10		**REALIZADO**
9	**CONTROL DE ACCESOS**				**12.28**	**17.93**		**100**					
	9.1	Requisitos de negocio para el controlde accesos					**14.29**	**0.79**					
		9.1.1	Politica de control de accesos						**7.14**	1		**REALIZADO**
		9.1.2	Control de acceso a las redes y servicios asociados						**7.14**	10		**REALIZADO**
	9.2	Gestion de acceso de usuario					**42.86**	**8.57**					
		9.2.1	Gestion de altas/bajas en el registro de usuarios						**7.14**	10		**REALIZADO**
		9.2.2	Gestion de los derechos de acceso asignados a usuarios						**7.14**	30		**GESTIONADO**
		9.2.3	Gestion de los derechos de acceso con privilegios especiales						**7.14**	30		**GESTIONADO**
		9.2.4	Gestion de informacion confidencial de autenticacion de usuarios						**7.14**	30		**GESTIONADO**
		9.2.5	Revision de los derechos de acceso de los usuarios						**7.14**	10		**REALIZADO**
		9.2.6	Retirada o adaptacion de los derechos de acceso						**7.14**	10		**REALIZADO**
	9.3	Responsabilidad del usuario					**7.14**	**0.71**					
		9.3.1	Uso de informacion confidencial para la autentificacion						**7.14**	10		**REALIZADO**
	9.4	Control de acceso a sistmas y aplicaciones					**35.71**	**7.86**					
		9.4.1	Restriccion del acceso a la informacion						**7.14**	30		**GESTIONADO**
		9.4.2	Procedimientos seguros de inicio de sesion						**7.14**	30		**GESTIONADO**
		9.4.3	Gestion de contraseñas de usuario						**7.14**	10		**REALIZADO**
		9.4.4	Uso de herramientas de administracion de sistemas						**7.14**	30		**GESTIONADO**
		9.4.5	Control de acceso al codigo fuente de los programas						**7.14**	10		**REALIZADO**

10	**CIFRADO**				1.75	5		100					
	10.1	Controles Criptográficos					100	5					
		10.1.1	Politicas de uso de los controles criptograficos	NO APLICA					50	0			NO EXISTENTE
		10.1.2	Gestion de claves						50	10			REALIZADO
11	**SEGURIDAD FISICA Y AMBIENTAL**				13.16	21.07		100					
	11.1	Areas seguras					40	7.4					
		11.1.1	Perimetro de seguridad fisica						6.66	40			GESTIONADO
		11.1.2	Controles fisicos de entrada						6.66	10			REALIZADO
		11.1.3	Seguridad de oficinas, despachos y recursos						6.66	10			REALIZADO
		11.1.4	Proteccion contra las amenazas externas y ambientales						6.66	1			REALIZADO
		11.1.5	El trabajo en areas seguras						6.66	10			REALIZADO
		11.1.6	Areas de acceso publico, carga y descarga						6.66	40			GESTIONADO
	11.2	Seguridad de los equipos					60	13.67					
		11.2.1	Emplazamiento y proteccion de equipos						6.66	10			REALIZADO
		11.2.2	Instalaciones de suministro						6.66	10			REALIZADO
		11.2.3	Seguridad del cableado						6.66	50			ESTABLECIDO
		11.2.4	Mantenimiento de los equipos						6.66	50			ESTABLECIDO
		11.2.5	Salida de activos fuera de las dependencias de la empresa						6.66	50			ESTABLECIDO
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones						6.66	5			REALIZADO
		11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento						6.66	10			REALIZADO
		11.2.8	Equipo informatico de usuario desatendido						6.66	10			REALIZADO
		11.2.9	Politica de puesto de trabajo despejado y bloqueo de pantalla						6.66	10			REALIZADO
12	**SEGURIDAD EN LA OPERATIVA**				12.28	9.63		100					
	12.1	Responsabilidades y procedimientos de operación					28.57	1.43					
		12.1.1	Documentacion de procedimientos de operación						7.14	10			REALIZADO
		12.1.2	Gestion de cambios						7.14	10			REALIZADO
		12.1.3	Gestion de capacidades	NO APLICA					7.14	0			NO EXISTENTE
		12.1.4	Separacion de entornos de desarrollo, prueba y produccion	NO APLICA					7.14	0			NO EXISTENTE
	12.2	Proteccion contra codigo malicioso					7.14	2.14					
		12.2.1	Controles contra el codigo malicioso						7.14	30			GESTIONADO
	12.3	Copias de seguridad					7.14	2.14					
		12.3.1	Copias de seguridad de la informacion						7.14	30			GESTIONADO
	12.4	Registro de actividad y supervision					28.57	1.43					
		12.4.1	Registro y gestion de eventos de actividad						7.14	5			REALIZADO
		12.4.2	Proteccion de los registros de informacion						7.14	5			REALIZADO
		12.4.3	Registros de actividad del administrador y operador del sistema						7.14	10			REALIZADO
		12.4.4	Sincronizacion de relojes	NO APLICA					7.14	0			NO EXISTENTE
	12.5	Control del software en explotacion					7.14	0.71					
		12.5.1	Instalacion del software en sistemas en produccion						7.14	10			REALIZADO
	12.6	Gestion de la vulnerabilidad tecnica					14.29	1.07					
		12.6.1	Gestion de las vulnerabilidades tecnicas						7.14	5			REALIZADO
		12.6.2	Restricciones en la instalacion de software						7.14	10			REALIZADO
	12.7	Consideraciones de las auditorias de los sistemas de informacion					7.14	0.71					
		12.7.1	Controles de auditoría de los sistemas de información						7.14	10			REALIZADO

13	SEGURIDAD EN LAS TELECOMUNICACIONES				6.14	17.29		100				
	13.1	Gestion de la seguridad en las redes					42.86	10				
		13.1.1	Controles de red						14.28	30		GESTIONADO
		13.1.2	Mecanismos de seguridad asociados a servicios en red						14.28	30		GESTIONADO
		13.1.3	Segregacion de redes						14.28	10		REALIZADO
	13.2	Intercambio de informacion con partes externas					57.14	7.29				
		13.2.1	Politicas y procedimientos de intercambio de informacion						14.28	1		REALIZADO
		13.2.2	Acuerdos de intercambio	NO APLICA					14.28	0		NO EXISTENTE
		13.2.3	Mensajeria electronica						14.28	40		GESTIONADO
		13.2.4	Acuerdos de confidencialidad y secreto						14.28	10		REALIZADO
14	ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION				11.4	2.31		100				
	14.1	Requisitos de seguridad de los sistemas de informacion					23.08	1.54				
		14.1.1	Analisis y especificaciones de los requisitos de seguridad						7.69	10		REALIZADO
		14.1.2	Seguridad de las comunicaciones en serviciso accesibles por redes public						7.69	10		REALIZADO
		14.1.3	Proteccion de las transacciones por redes telematicas	NO APLICA					7.69	0		NO EXISTENTE
	14.2	Seguridad en los procesos de desarrollo y soporte					69.23	0.77				
		14.2.1	Politica de desarrollo seguro de software	NO APLICA					7.69	0		NO EXISTENTE
		14.2.2	Procedimientos de control de cambios en los sistemas						7.69	10		REALIZADO
		14.2.3	Revision tecnica de las aplicaciones tras efectuar cambios en el sistema o	NO APLICA					7.69	0		NO EXISTENTE
		14.2.4	Restricciones a los cambios en los paquetes de software	NO APLICA					7.69	0		NO EXISTENTE
		14.2.5	Uso de principios de ingenieria en proteccion de sistemas	NO APLICA					7.69	0		NO EXISTENTE
		14.2.6	Seguridad en entornos de desarrollo	NO APLICA					7.69	0		NO EXISTENTE
		14.2.7	Externalizacion del desarrollo de software	NO APLICA					7.69	0		NO EXISTENTE
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	NO APLICA					7.69	0		NO EXISTENTE
		14.2.9	Pruebas de aceptacion	NO APLICA					7.69	0		NO EXISTENTE
	14.3	Datos de prueba					7.69	0				
		14.3.1	Proteccion de los datos utilizados en pruebas	NO APLICA					7.69	0		NO EXISTENTE

15	RELACIONES CON SUMINISTRADORES				4.39	16		100					
	15.1	Seguridad de la informacion en las relaciones con suministradores					60	4					
		15.1.1	Politica de seguridad de la informacion para suministradores						20	10		REALIZADO	
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores						20	10		REALIZADO	
		15.1.3	Cadena de suministro en tecnologias de la informacion y comunicaciones	NO APLICA					20	0		NO EXISTENTE	
	15.2	Gestion de la prestacion del servicio por suministradores					40	12					
		15.2.1	Supervision y revision de los servicios prestados por terceros						20	30		GESTIONADO	
		15.2.2	Gestion de cambios en los servicios prestados por terceros						20	30		GESTIONADO	
16	GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION				6.14	13.57		100					
	16.1	Gestion de incidentes de seguridad de la informacion y mejoras					100	13.57					
		16.1.1	Responsabilidades y procedimientos						14.28	50		ESTABLECIDO	
		16.1.2	Notificacion de los eventos de seguridad de la informacion						14.28	5		REALIZADO	
		16.1.3	Notificacion de puntos debiles de la seguridad						14.28	10		REALIZADO	
		16.1.4	Valoracion de eventos de seguridad de la informacion y toma de decisione						14.28	5		REALIZADO	
		16.1.5	Respuesta a los incidentes de seguridad						14.28	10		REALIZADO	
		16.1.6	Aprendizaje de los incidentes de seguridad de la informacion						14.28	10		REALIZADO	
		16.1.7	Recopilacion de evidencias						14.28	5		REALIZADO	
17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NI				3.51	7.5		100					
	17.1	Continuidad de la seguridad de la informacion					75	5					
		17.1.1	Planificacion de la continuidad de la seguridad de la informacion						25	5		REALIZADO	
		17.1.2	Implantacion de la continuidad de la seguridad de la informacion						25	5		REALIZADO	
		17.1.3	Verificacion, revision y evaluacion de la continuidad de la seguridad de la ir						25	10		REALIZADO	
	17.2	Redundancias					25	2.5					
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la informacion						25	10		REALIZADO	
18	CUMPLIMIENTO				7.02	7.5		100					
	18.1	Cumplimiento de los requisistos legales y contractuales					62.5	3.75					
		18.1.1	Identificacion de la legislacion aplicable						12.5	10		REALIZADO	
		18.1.2	Derechos de propiedad intelectual (DPI)	NO APLICA					12.5	0		NO EXISTENTE	
		18.1.3	Proteccion de los registros de la organización						12.5	10		REALIZADO	
		18.1.4	Proteccion de datos y privaciodad de la informacion personal						12.5	10		REALIZADO	
		18.1.5	Regulacion de controles criptograficos	NO APLICA					12.5	0		NO EXISTENTE	
	18.2	Revisiones de la seguridad de la informacion					37.5	3.75					
		18.2.1	Revision independiente de la seguridad de la informacion						12.5	10		REALIZADO	
		18.2.2	Cumplimiento de las politicas y normas de seguridad						12.5	10		REALIZADO	
		18.2.3	Comprobacion del cumplimiento						12.5	10		REALIZADO	

El resultado de la revisión es que nos muestra una situación crítica de riesgo elevado de la gestión de la seguridad de la información de ADEA.

RESUMEN DEL PLAN DE ACCIÓN DESARROLLADO EN LA ASOCIACIÓN PARA EL DESARROLLO EMPRESARIAL EN APURÍMAC, ANDAHUAYLAS Y CHINCHEROS.

FASE	TAREA	INTERESADOS	ACTIVIDADES DE DESARROLLO	PLAZO	RESULTADOS	OBJETIVO DE CONTROL ISO 27002 ABARCADO
DIAGNOSTICO	REVISION DE DOCUMENTOS DE GESTIÓN DE ADEA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Gerencia - Sub Gerente de Administración - Asistente de Operaciones	*Se realizó una reunión con la gerencia para exponer la idea del proyecto de "buenas practicas en seguridad de la información basado en la ISO 27002 para ADEA"	10 días	Visto bueno a idea y apoyo en su ejecución de parte de la gerencia	6.1.3
			*Solicitar a gerencia acceso a todos los documentos de gestión de ADEA		Tener acceso a documentos de gestion de carácter privado de ADEA.	
			*Revisar la documentación del proporcionada por la gerencia de ADEA		Tener un diagnostico inicial	5.1.2
	REVISION DE LA MODALIDAD DE GESTION DE LA INFORMACIÓN DE ADEA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Gerencia	*Determinar como gestionan la información de ADEA, en sus diferentes estados	10 días	Tener un diagnostico inicial	5.1.2
	EVALUACIÓN DE CONTROLES BASADO EN ISO 27002 PRIMERA ETAPA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Con el uso del Check List del ISO 27002:2013, se realizo la verificacion del nivel de cumplimiento de cada objetivo de control en ADEA - PRIMERA ETAPA	30 días	Archivo Check list con los resultados de la evaluación de objetivos de control del ISO 27002, antes de implementar mejoras	18.2.1
			*El check list fue modificado para poder manejar una ponderación por dominio de control, ya que algunos de los objetivos de control del ISO, no son aplicables a ADEA, tomandose en consideración los mas urgente y necesarios		Archivo Check list con ponderaciones en la medición de resultados.	18.2.2
	INFORME DE ESTADO SITUACIONAL A LA ALTA DIRECCIÓN DE ADEA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Gerencia	*Se determino el estado situacional de acuerdo al resultado del Check List del ISO 27002: 2013 realizado en su PRIMERA ETAPA	10 días		18.2.3
			*Se elevo un informe a gerencia, describiendo el estado situacional de la gestión de la seguridad de la información de ADEA		Informe de estado situacional de la gestión de la seguridad de la información en ADEA.	
			*Gerencia solicitó al gestor del presente proyecto, evaluar un plan de acción a informe situacional			

FASE	TAREA	INTERESADOS	ACTIVIDADES DE DESARROLLO	PLAZO	RESULTADOS	OBJETIVO DE CONTROL ISO 27002 ABARCADO
PLANIFICACIÓN	CALENDARIZACIÓN DE ACTIVIDADES	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Se planificó la calendarización de actividades a realizar para implementar una posible solución	15 días	Se cuenta con el plan incial de acción.	
			*En reunión con el gerente y el Sub gerente de Administración, se procedio a definir un calendario de actividades en busca de definir una propuesta de solución		Se cuenta con el plan incial de acción.	6.1.4
	DETERMINACIÓN DE RECURSOS NECESARIOS	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Gerencia - Sub Gerencia de Administración	*Se elaboró un cuadro de recursos necesarios	5 días	Se cuenta con el cuador de recursos necesarios y presupuesto inicial.	
			*Se solicito a Sub Gerencia de Administración, recursos materiales para la implementación del proyecto		Se cuenta con el cuador de recursos necesarios y presupuesto inicial.	
			*Gerencia y Sub Gerencia de Administración aprobaron solicitud de adquisición de recursos para proyecto		Se cuenta con el cuador de recursos necesarios y presupuesto inicial.	
	DIFUSIÓN DEL PLAN	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Consejo Directivo - Gerencia - Sub Gerencia de Negocios y Administradores de Agencias	*Se presento a alta dirección la calendarización y recursos necesarios para desarrollar el proyecto buenas practicas en seguridad de la información basado en ISO 27002 en ADEA	40 días	Informe con el plan de acción propuesto a gerencia.	
			*En reunión con gerencia, Sub Gerencia de Administración, Sub Gerencia de Negocios y Administradores de Agencias, se presento el plan del proyecto, informando el proposito e importancia del mismo		Informe con el plan de acción propuesto a gerencia.	

FASE	TAREA	INTERESADOS	ACTIVIDADES DE DESARROLLO	PLAZO	RESULTADOS	OBJETIVO DE CONTROL ISO 27002 ABARCADO
	ELABORACIÓN DE MODELO DE PROPUESTA DE SOLUCION A ALTA DIRECCIÓN DE ADEA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Gerencia - Sub Gerencia de Administración	*Se determinó el modelo de propuesta de la solución mas optimo	20 días	Selección de entre varias alternativas, la solución mas optima para el proyecto.	
			*Se presento el Project Charter a gerencia, quien a su vez lo presento al consejo directivo de ADEA		Informe con el Project Charter a gerencia.	
			*Se dio el visto bueno y aprobación al proyecto a desarrollarse, mediante memorando para ejecución		Memorando de aprobacion a desarrollo de proyecto.	
			*Se elaboró documento de politicas de gestión de seguridad de la información para ADEA, de acuerdo a resultado de check list poniendo enfasis en controles de riesgo muy alto		ADEA cuenta con un documento de politicas de gestión de seguridad de la información	5.1.1
			*Se redacto el documento de politicas de uso del correo institucional de ADEA		ADEA cuenta con un documento politicas de uso del correo institucional vigente para todos los colaboradores	5.1.2
			*Se aprobo un nuevo y actualizado MOF, donde se establece claramente las funciones y responsabilidades de cada puesto de trabajo en ADEA. Tambien se actualizo el organigrama estructural y se definio el organigrama por agencias.		MOF, modificado vigente de ADEA.	6.1.1
			*Se redacto el documento de politica de uso de equipos moviles, los cuales son asignados normalmente a los analistas de negocios de ADEA.		Gerencia emitio un memorando de normativa de uso de equipos moviles asignados a los colaboradores de ADEA	6.2.1
			*Gerencia remitió la orden de tomar en consideración la investigación de antecedentes y revisión de los terminos y condiciones de contratación de futuros nuevos colaboradores. En este caso la jefe de Talento Humano y Asesoria legal tendrian esta responsabilidad.		ADEA cuenta con nuevos procedimientos de gestión del talento humano	7.1.1 - 7.1.2

IMPLEMENTACIÓN	ELABORACIÓN DE POLITICAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Consejo Directivo - Gerencia - Sub Gerencia de Negocios y Administradores de Agencias, Consejo directivo y cada uno de los colaboradores de ADEA Andahuaylas	*Se diseño documentos y formatos para llevar el control de: Actualizaciones de aplicativos del sistema financiero, revisión de derechos de acceso de los usuarios, bitacora de uso de los generadores, control de mantenimiento preventivo de equipos de computo, servidores y sistemas de seguridad, documento para llevar el control de contraseñas de superusuario y usuarios.	20 días	La unidad de Tecnologias de la información y seguridad cuenta con formatos para el control de actualizaciones de aplicativos del sistema financiero, revisión de derechos de acceso de los usuarios, bitacora de uso de los generadores, control de mantenimiento preventivo de equipos de computo, servidores y sistemas de seguridad, documento para llevar el control de contraseñas de superusuario y usuarios.	8.2.3 - 9.2.1 - 9.2.5 - 9.4.3 - 10.1.2
			*Se elaboró un plan de mantenimiento de equipos tecnológicos en general para ADEA.		La unidad de Tecnologias de la información y seguridad cuenta y actualiza su POA, plan operativo anual en la cual planifica el plan de adquisiciones, mantenimientos y proyectos.	11.2.4
			*Se esatablecio un plan de generación de copias de seguridad: Data en general, correos, base de datos en medios fisicos y respaldos resguardados de menara segura.		TIyS, tiene procedimientos establecidos y documentados de generación y resguardo de backups de datos.	12.3.1
			*Se procedio con la revisión de los contratos con suministradores de servicios que brindan para ADEA, añadiendo a ellos adendas de confidencialidad de la información.			15.1.1 - 15.1.2
IMPLEMENTACIÓN			*Se redacto el Plan de continuidad del negocio de ADEA.		ADEA cuenta con un documento de Plan de continuidad del negocio.	17.1.1 - 17.1.2 - 17.1.3
			*Se estableció un plan de evaluaciones periodicas de funciones.		Encargado de riesgo, tiene como función las evaluaciones periódicas de funciones	18.2.1 - 18.2.3
			*Se reviso y redacto un documento de sanciones a faltas cometidas por el personal, incumplimiento de normas, politicas, codigo de ética.		ADEA cuenta con un documento de codigo de ética, el cual fue entregado a cada colaborador.	18.2.2
			*Se solicito que mediante la ayuda de un especialista actualizar los manuales de procedimientos y funciones de los puestos de trabajo y procesos de ADEA.		ADEA tiene elaborado un nuevo MOF.	6.1.1 - 6.1.2

IMPLEMENTACIÓN			*Se reviso las debilidades de ADEA, entre los mas importantes: Infraestructura tecnológica, física y logica, red de datos, configuración de equipos de computo, seguridad en accesos, telecomunicación entre agencias, red de datos, sala de servidores, suministradores, equipos de respaldo, copias de seguridad, zonas seguras, equipos para continuidad de negocio.	Contar con un analisis FODA.	5.1.2
			*Para el responsable de patrimonio, se diseño un aplicativo basico, para la mejore gestión de activos de ADEA.	Patrimonio controla mediante un aplicativo los activos de ADEA	8.1.1 - 8.1.2
			*Se solicitó que el responsable de patrimonio fuese a capacitarse en temas de gestión de activos.	Colaborador capacitado en temas de gestion de activos.	8.1.3 - 8.1.4
			*Para la manipulación de medios informaticos removibles, se estableció como norma el uso de equipos designados para ese proposito. Se procedio a deshabilitar puertos USB, quitar lectoras de DVD.	Cada equipo PC de ADEA esta maquetado, con las configuraciones y medidas necesarias.	8.3.1 - 8.3.2 - 8.3.3
			*Se adquirio proveedores de internet ISP, redundantes 2 proveedores por oficina, para la conexión.	ADEA cuenta con lineas de internet independientes de proveedores; Movistar y Bitel	17.1.1 - 17.1.2 - 17.2.1
IMPLEMENTACIÓN			*Se realizo la implementación de un servidor de aplicaciones para poder centralizar la data del sistema financiero: Para ello se adquirio una linea dedicada de internet con router cisco para la configuración de enlaces con las agencias. Se adquirió licencias Microsoft para el acceso remoto de cada equipo de computo de agencias a la central.	ADEA cuenta con un servidor Windows Server 2012, el cual centraliza la aplicación del sistema financiero utilizado. El servidor y los equipos remotos de usuarios, cuentan con sus respectivas licencias corporativas.	9.1.2 - 9.2.1 - 9.2.4 - 9.4.1 - 12.4.1
			*Se crearon perfiles de acceso: Se establecieron niveles de acceso a los diferentes sistemas. Perfil de equipo de computo y perfil de permisos en el sistema financiero.	ADEA tiene establecido perfiles de acceso para cada grupo de colaboradores, de acuerdo a sus necesidades: Analistas de negocios, Administradores de Oficina, Area administrativa.	9.2.2 - 9.2.3 - 9.2.5 - 9.2.6 - 9.4.1 - 9.4.5
			*Se realizo configuración de servicios denegados, filtros de acceso a la internet.	ADEA cuenta con filtros de acceso a internet en las instalaciones de sus equipos PC, Laptop y SmartPhone.	9.4.1 - 9.4.4

IMPLEMENTACIÓN	IMPLEMENTACIÓN DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Consejo Directivo - Gerencia - Sub Gerencia de Negocios y Administradores de Agencias, Consejo directivo y cada uno de los colaboradores de ADEA Andahuaylas	*Implemente un servidor de correo corporativo propio, el cual funciona con sistema operativo Linux, distribución Ubuntu Server 14.0 LST: El servidor permite la gestión total de los correos institucionales de ADEA, ademas de tener las funciones de Firewalls de red, servidor de archivos y servidor web.	20 días	Servidor de correo correctamente funcionando en ADEA, que es gestionado por la unidad de TIyS.	10.1.2 - 9.2.1 - 13.1.1 - 13.1.2 - 13.1.3 - 13.2.3
			*Se procedieron a señalizar la señalización de todos los ambientes de las agencias de ADEA, en algunos casos se modificaron su infraestructura. Señalizaciones de acceso no autorizado a algunos ambientes.		Con el apoyo de un especialista defensa civil, se procedio a realizar la señalización de todos los ambientes de ADEA.	11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5
			*Se realizo la instalación de sistemas de circuito cerrado de televisión - Camaras de vigilancia en cada una de las agencias de ADEA.		Cada agencia de ADEA cuenta con un sistema de video vigilancia funcionando.	11.1.3
			*Se realizo la instalación de sistemas de alarma en cada una de las agencias de ADEA.		Cada agencia de ADEA cuenta con un sistema de alarma	11.1.1
			*Se realizó la adquisición e instalación de luces de emergencia en el total de las agencias de ADEA.		Cada agencia de ADEA cuenta con instalaciones de luces de emergencia.	11.2.1 - 11.2.2
			*Se procedio a maquetar cada equipo de computo asignado, con los servicios y recursos necesarios para cada puesto de trabajo.		Equipos de computo maquetados.	11.2.1 - 11.2.5 - 11.2.9
			*Se realizo la adquisicion de Antivirus Empresarial, en este caso, según el informe de requerimientos de acuerdo a la funcionalidad. Optandose por licencias de Kaspersky Internet Security 2015-2016, para 42 equipos de computo.		ADEA cuenta con 42 licencias de antivirus KIS 2017	12.2.1 - 14.1.2 - 14.1.3
			*Se realizo la reconfiguración de la red de datos de las 5 agencias con enfasis en la mejor gestión.		TIyS, controla la configuración de la red de datos de todas las agencias de ADEA.	13.1.1 - 13.1.2 - 13.1.3
			*Adquisición de dispositivos SAI para el total de equipos informaticos de las 5 agencias de ADEA.		ADEA cuenta con UPS instalados en cada equipo de computo que cuenta.	11.2.2
NTACIÓN			*Se realizo la adquisicioón de generadores electricos para 3 de las agencias principales, las cuales fueron instaladas por especialistas en el tema.		Las agencias Andahuaylas, Uripa y Huancarama cuentan con generadores electricos.	11.2.2

IMPLEMEI			*Se instalo servidores proxy/firewall para la gestión del tráfico de internet en cada agencia.		ADEA cuenta con servidores Proxy debidamente gestionados por la unidad de TIyS.	13.1.2 - 13.2.1 - 14.1.2
			*Se implemento un servidor alterno para el sistema financiero el cual tiene un proposito de realizar pruebas de las aplicaciones, cambios y parches al sistema financiero.		ADEA cuenta con servidores alternos de respaldo.	14.2.3 - 14.2.4 - 14.2.8 -14.2.8 - 14.3.1
			*Se solicitó la inclusión de un personal para la Unidad de riesgos, quien tendria la función de revisar, auditar, puntos debiles de riesgo de seguridad.		ADEA cuenta con un personal encargado de la unidad de riegos.	16.1.1 - 16.1.2 - 16.1.3 - 16.1.5 - 16.1.6 - 18.2.1 - 18.2.2 - 18.2.3
			*Se implemento el servidor de datos de contingencia.		ADEA cuenta con servidores alternos de respaldo.	17.1.2 - 17.1.3 - 17.2.1
			*Se solicitó la instalación de un sistema de pozo a tierra, en su primera fase en la oficina principal de ADEA, donde se encuentra la sala de servidores.		La oficina Andahuaylas cuenta con la instalacion de pozo a tierra en su ambiente.	17.1.2
	CAPACITACIÓN DE USUARIOS E INTERESADOS	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad - Consejo Directivo - Gerencia - Sub Gerencia de Negocios y Administradores de Agencias, Consejo directivo y cada uno de los colaboradores de ADEA Andahuaylas	*Se programo reuniones con gerencia para cordinaciones	40 días	Planificar un plan de capacitaciones para todos los colaboradores.	6.1.3 - 6.1.4
			*Se realizo reuniones de comité ejecutivo con gerencia, Sub Gerente de Administración, Sub Gerente de Negocios, Jefe de Talento Humano, Jefe de Tecnologias de la Informacion y Seguridad, Jefe de Unidad de Riesgos y Administradores de Agencias, para ver temas de seguridad.		Se informo de las medidas que se debe tomar para mejorar la seguridad en general.	6.1.3 - 6.1.4
			*Viaje a cada agencia para capacitar a cada uno de los colaboradores en temas concernientes a seguridad de la información		Colaboradores capacitados, quienes conocen sus funciones y responsabilidades.	
			*Se realizo la capacitación a los colaboradores sobre la responsabilidad del correcto resguardo de documentos, bienes e información en su puesto de trabajo frente a los clientes de ADEA.		Colaboradores capacitados, quienes conocen sus funciones y responsabilidades.	

			trabajo frente a los clientes de ADEA.			
	PUESTA EN MARCHA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Gerencia y alta dirección dispusieron el cumplimiento de las politicas de seguridad de la información y el cumplimiento de las mismas debia ser de manera obligatoria por todos los colaboradores de ADEA.	20 días	Se da el cumplimiento de las politicas de seguridad en ADEA	18.2.2
EVALUACIÓN	EVALUACIÓN DE CONTROLES BASADOS EN ISO 27002 SEGUNDA ETAPA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Con el uso del Check List del ISO 27002:2013, se realizo la verificacion del nivel de cumplimiento de cada objetivo de control en ADEA - SEGUNDA ETAPA	40 días	Archivo Check list con los resultados de la evaluación de objetivos de control del ISO 27002, luego de implementar mejoras	18.2.1 - 18.2.2 - 18.2.3
MONITOREO	INTERVENCIONES DE AUDITORIA INTERNA	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Auditoria externa evaluó la modalidad de gestión de la seguridad de la información en entrevista al Jefe de Tecnologias de la Información y Seguridad.	20 días	Con el apoyo de un auditor externo se evaluo las mejoras realizadas en cuanto a la gestión de la seguridad en ADEA.	18.2.1 - 18.2.2 - 18.2.3
			*Auditoria externa se reunió con cada uno de las unidades de alta y mediana dirección de ADEA, para evaluar la modalidad de gestión de la información		Con el apoyo de un auditor externo se evaluo las mejoras realizadas en cuanto a la gestión de la seguridad en ADEA.	18.2.1 - 18.2.2 - 18.2.3
	POLÍTICAS DE MEJORAS	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Auditoria externa presento informe de auditoria realizada a ADEA, dirigida a gerencia con los resultados obtenidos.	20 días	Informe de resultados de auditoria externa.	18.2.1 - 18.2.2 - 18.2.3
			*Gerencia dispuso a los responsables, el levantamiento de las observaciones encontradas por auditoria y el cumplimento de las mismas hacia futuro.		Cada colaborador procede con el levantamiento de las observaciones encontradas por auditoria externa.	18.2.1 - 18.2.2 - 18.2.3
	REDACCIÓN DEL INFORME FINAL	Gestor del proyecto; Jefe de Tecnologías de la Información y Seguridad	*Proceder con la redacción del informe final para la posterior presentación y sustentación de la misma en la UNAJMA.	70 días		

Figura 30: Cuadro de resumen del plan de acción realizado
Fuente: Elaboración propia

A continuación se presentan algunas fotografías de la implementación de BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO 27002 EN LA ASOCIACIÓN PARA EL DESARROLLO EMPRESARIAL EN APURÍMAC - ADEA para que se observe la importancia de la selección del equipamiento y medidas que se tomaron para iniciar con dicha ejecución.

Se tomó en consideración principalmente la implementación de puntos básicos de seguridad.

Figura 31: Cámaras Tuvo - Implementación de sistema de video vigilancia
Fuente: Elaboración propia

Figura 32: Cámaras Domo - Implementación de sistema de video vigilancia
Fuente: Elaboración propia

Figura 33: Generador eléctrico para respaldo de energía
Fuente: Elaboración propia

Figura 34: Dispositivos SAI (UPS)
Fuente: Elaboración propia

Figura 35: Dispositivos SAI (UPS)
Fuente: Elaboración propia

Figura 36: Instalación de sistemas de video vigilancia
Fuente: Elaboración propia

Figura 37: Señalización e instalación de luces de emergencia
Fuente: Elaboración propia

Figura 38: Equipos de comunicación en la sede central
Fuente: Elaboración propia

Figura 39: Señalización e instalación de extintores de gas carbónico
Fuente: Elaboración propia

Figura 40: Equipos de seguridad – sistema de video vigilancia
Fuente: Elaboración propia

DIFUSIÓN Y CAPACITACIÓN

Figura 41: Reunión con Administradores de Agencias para difusión
Fuente: Elaboración propia

Figura 42: Reunión con Administradores de Agencias, Sub Gerente de Administración y Gerencia para difusión
Fuente: Elaboración propia

Figura 43: Reunión con Administradores de Agencias, Sub Gerente de Administración y Gerencia para difusión
Fuente: Elaboración propia

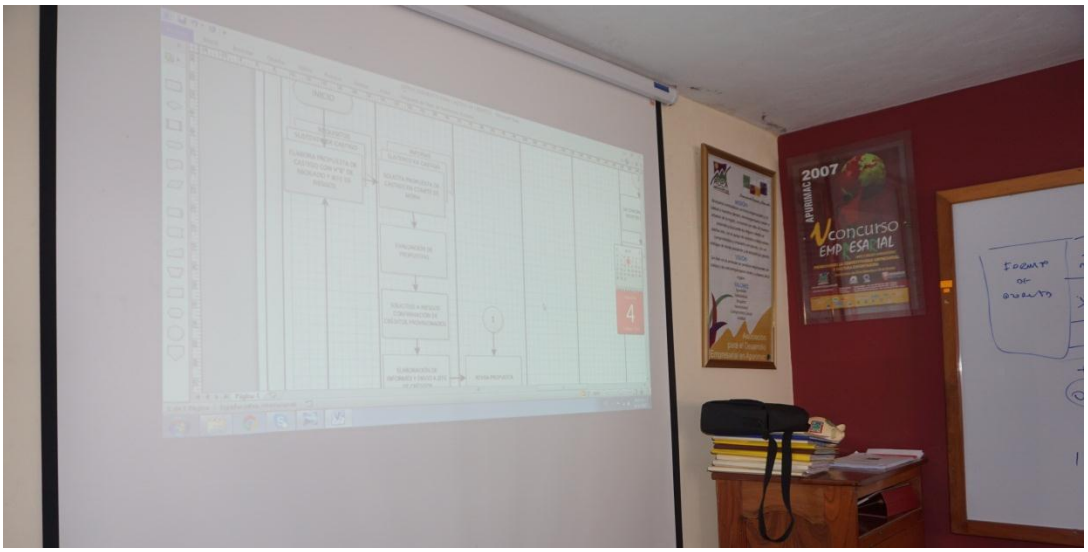


Figura 44: Reunión con Administradores de Agencias, Sub Gerente de Administración y Gerencia para difusión
Fuente: Elaboración propia

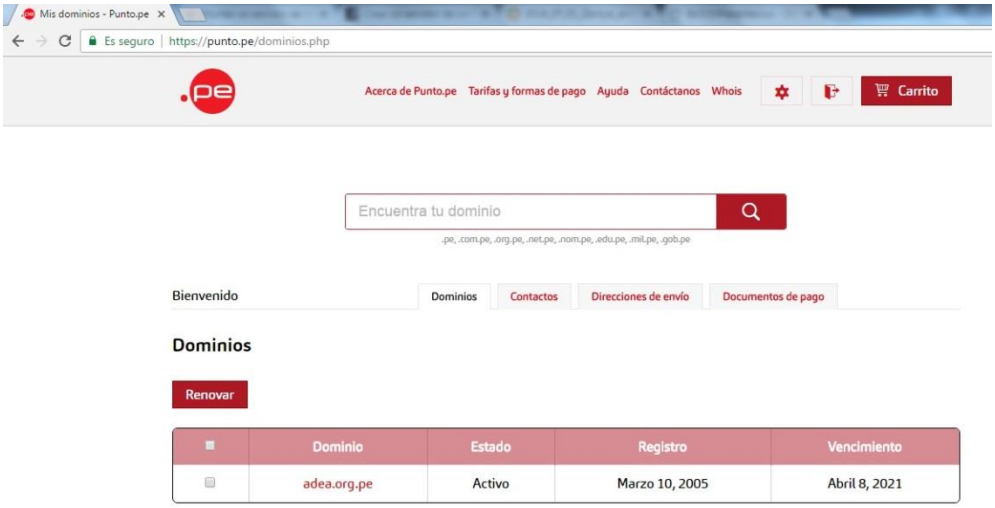
Difusión y capacitación

Figura 45: Capacitación y difusión del proyecto con directorio y colaboradores de ADEA Andahuaylas
Fuente: Elaboración propia

IMPLEMENTACIÓN DE UN SERVIDOR DE CORREO CORPORATIVO PARA ADEA ANDAHUAYLAS

En la presente implementación se detalla la forma, manera y mecanismo para configurar un servidor corporativo, que contara con los servicios de correo, web, directorio activo, DNS, PROXY y FIREWALL, entre los más importantes. Dicha implementación estará alineada a las buenas prácticas y reglas desarrolladas y aceptadas por organismos internacionales, con los cuales se pueda brindar confianza y aceptabilidad a la presente solución.

Cabe señalar que ADEA Andahuaylas, actualmente no cuenta con un servidor propio que brinde las soluciones que pretende la presente implementación. Estas soluciones las tienen parcialmente y con servicio de terceros con soluciones simples y domesticas no propias para una entidad que se dedica al rubro de las finanzas.



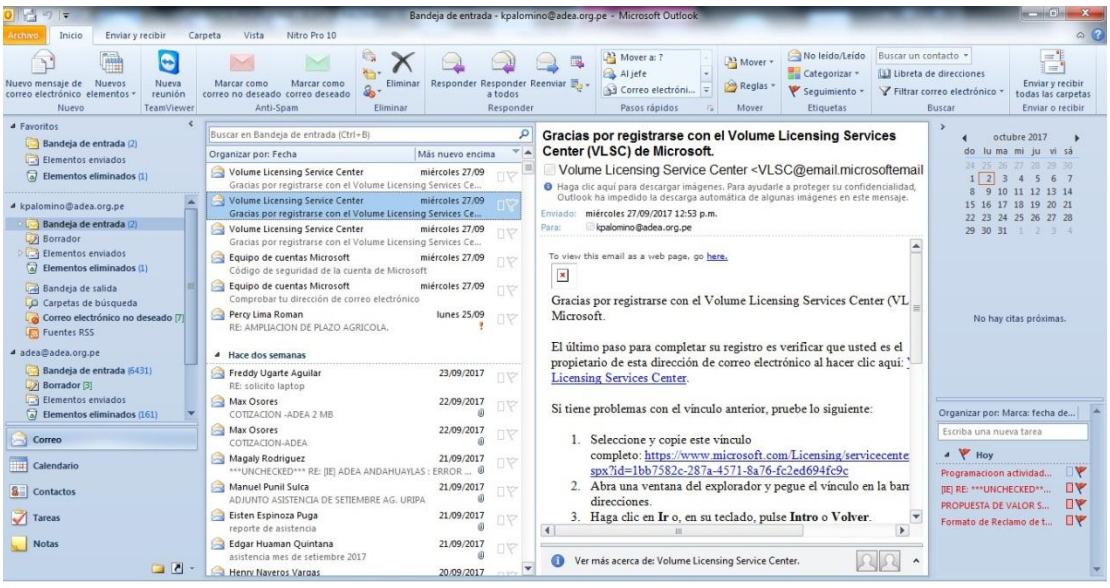


Figura 46: Configuración de DNS para servidor de correo corporativo
Fuente: Elaboración propia

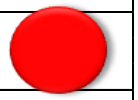
Adicionalmente se tiene que registrar la dirección de los servidores DNS que utilizara el servidor a implementar. En el presente caso, el proveedor del servicio de internet para el servidor es la empresa Movistar.

5.2 Evaluación de desempeño de la solución

Para la evaluación del desempeño de la solución, se elaboró un cuadro de resultados que, mediante un proceso de ponderación se obtuvo el nivel de cumplimiento por cada uno de los dominios de control de la norma ISO 27002.

En consecuencia, se tuvo que comparar resultados entre el resultado del check list inicial; primera etapa, versus el resultado de la segunda etapa, una vez desarrollado el plan de acción de buenas prácticas en ADEA.

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
5	POLITICAS DE SEGURIDAD							10	
	5.1	Directrices de la Direccion en seguridad de la información							
		5.1.1	Conjunto de politicas para la seguridad de la informacion	ALTO	60	10	REALIZADO		
		5.1.2	Revision de las politicas para la seguridad de la informacion	MEDIO	40	10	REALIZADO		
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION							13	
	6.1	Organización Interna							
		6.1.1	Asignacion de responsabilidades para la seguridad de la informacion	ALTO	20	10	REALIZADO		
		6.1.2	Segregacion de tareas	MEDIO	15	30	GESTIONADO		
		6.1.3	Contacto con las autoridades	MEDIO	15	10	REALIZADO		
		6.1.4	Contacto con grupos de interes especial	MEDIO	15	10	REALIZADO		
		6.1.5	Seguridad de la informacion en la gestion de proyectos	ALTO	20	10	REALIZADO		
	6.2	Dispositivos para movilidad y teletrabajo							
		6.2.1	Politica de uso de dispositivos para movilidad	MEDIO	15	10	REALIZADO		
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS							43.2	
	7.1	Antes de la contratacion							
		7.1.2	Terminos y condiciones de contratacion	ALTO	25	50	ESTABLECIDO		
	7.2	Durante la contratacion							
		7.2.1	Responsabilidad de gestion	ALTO	25	50	ESTABLECIDO		
		7.2.2	Concienciacion, educacion y capacitacion en seguridad de la informacion	MEDIO	17	10	REALIZADO		
		7.2.3	Proceso disciplinario	MEDIO	17	50	ESTABLECIDO		
	7.3	Cese o cambio de puesto de trabajo							
		7.3.1	Cese o cambio de puesto de trabajo	MEDIO	16	50	ESTABLECIDO		
8	GESTION DE ACTIVOS							33.8	
	8.1	Responsabilidad sobre los activos							
		8.1.1	Inventario de activos	ALTO	20	50	ESTABLECIDO		
		8.1.2	Propiedad de los activos	MEDIO	16	50	ESTABLECIDO		
		8.1.3	Uso aceptable de los activos	MEDIO	16	50	ESTABLECIDO		
	8.2	Clasificacion de la informacion							
		8.2.1	Directrices de clasificacion	MEDIO	16	10	REALIZADO		
		8.2.2	Etiquetado y manipulado de la informacion	MEDIO	16	10	REALIZADO		
		8.2.3	Manipulacion de activos	MEDIO	16	10	REALIZADO		
	8.3	Manejo de los soportes de almacenamiento							
		8.3.1	Gestion de soportes extraibles	MEDIO	10	10	REALIZADO		
		8.3.2	Eliminacion de soportes	MEDIO	10	10	REALIZADO		
		8.3.3	Soportes fisicos en transito	MEDIO	10	10	REALIZADO		

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
9	CONTROL DE ACCESOS							17.1	
	9.1	Requisitos de negocio para el controlde accesos							
		9.1.1	Politica de control de accesos	ALTO	10	1	REALIZADO		
		9.1.2	Control de acceso a las redes y servicios asociados	ALTO	10	10	REALIZADO		
	9.2	Gestion de acceso de usuario							
		9.2.1	Gestion de altas/bajas en el registro de usuarios	MEDIO	6	10	REALIZADO		
		9.2.2	Gestion de los derechos de acceso asignados a usuarios	MEDIO	6	30	GESTIONADO		
		9.2.3	Gestion de los derechos de acceso con privilegios especiales	MEDIO	6	30	GESTIONADO		
		9.2.4	Gestion de informacion confidencial de autenticacion de usuarios	MEDIO	6	30	GESTIONADO		
		9.2.5	Revision de los derechos de acceso de los usuarios	MEDIO	6	10	REALIZADO		
		9.2.6	Retirada o adaptacion de los derechos de acceso	MEDIO	6	10	REALIZADO		
	9.3	Responsabilidad del usuario							
		9.3.1	Uso de informacion confidencial para la autentificacion	MEDIO	6	10	REALIZADO		
	9.4	Control de acceso a sistmas y aplicaciones							
		9.4.1	Restriccion del acceso a la informacion	ALTO	10	30	GESTIONADO		
		9.4.2	Procedimientos seguros de inicio de sesion	MEDIO	6	30	GESTIONADO		
		9.4.3	Gestion de contraseñas de usuario	MEDIO	6	10	REALIZADO		
		9.4.4	Uso de herramientas de administracion de sistemas	MEDIO	6	30	GESTIONADO		
		9.4.5	Control de acceso al codigo fuente de los programas	ALTO	10	10	REALIZADO		
10	CIFRADO							10	
	10.1	Controles Criptográficos							
		10.1.2	Gestion de claves	MUY ALTO	100	10	REALIZADO		
11	SEGURIDAD FISICA Y AMBIENTAL							21.6	
	11.1	Areas seguras							
		11.1.1	Perimetro de seguridad fisica	ALTO	8	40	GESTIONADO		
		11.1.2	Controles fisicos de entrada	ALTO	8	10	REALIZADO		
		11.1.3	Seguridad de oficinas, despachos y recursos	ALTO	8	10	REALIZADO		
		11.1.4	Proteccion contra las amenazas externas y ambientales	MEDIO	5	1	REALIZADO		
		11.1.5	El trabajo en areas seguras	MEDIO	5	10	REALIZADO		
		11.1.6	Areas de acceso publico, carga y descarga	MEDIO	5	40	GESTIONADO		
	11.2	Seguridad de los equipos							
		11.2.1	Emplazamiento y proteccion de equipos	MUY ALTO	10	10	REALIZADO		
		11.2.2	Instalaciones de suministro	MUY ALTO	10	10	REALIZADO		
		11.2.3	Seguridad del cableado	ALTO	8	50	ESTABLECIDO		
		11.2.4	Mantenimiento de los equipos	ALTO	8	50	ESTABLECIDO		
		11.2.5	Salida de activos fuera de las dependencias de la empresa	MEDIO	5	50	ESTABLECIDO		
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	MEDIO	5	5	REALIZADO		
		11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento	MEDIO	5	10	REALIZADO		
		11.2.8	Equipo informatico de usuario desatendido	MEDIO	5	10	REALIZADO		
		11.2.9	Politica de puesto de trabajo despejado y bloqueo de pantalla	MEDIO	5	10	REALIZADO		

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
12	SEGURIDAD EN LA OPERATIVA							14.25	
	12.1	Responsabilidades y procedimientos de operación							
		12.1.1	Documentacion de procedimientos de operación	MEDIO	7	10	REALIZADO		
		12.1.2	Gestion de cambios	MEDIO	7	10			
	12.2	Proteccion contra codigo malicioso							
		12.2.1	Controles contra el codigo malicioso	ALTO	10	30	GESTIONADO		
	12.3	Copias de seguridad							
		12.3.1	Copias de seguridad de la informacion	MUY ALTO	18	30	GESTIONADO		
	12.4	Registro de actividad y supervision							
		12.4.1	Registro y gestion de eventos de actividad	ALTO	10	5	REALIZADO		
		12.4.2	Proteccion de los registros de informacion	MEDIO	7	5	REALIZADO		
		12.4.3	Registros de actividad del administrador y operador del sistema	MEDIO	7	10	REALIZADO		
	12.5	Control del software en explotacion							
		12.5.1	Instalacion del software en sistemas en produccion	MEDIO	7	10	REALIZADO		
	12.6	Gestion de la vulnerabilidad tecnica							
		12.6.1	Gestion de las vulnerabilidades tecnicas	ALTO	10	5	REALIZADO		
		12.6.2	Restricciones en la instalacion de software	MEDIO	7	10	REALIZADO		
	12.7	Consideraciones de las auditorias de los sistemas de informacion							
		12.7.1	Controles de auditoría de los sistemas de información	ALTO	10	10	REALIZADO		
13	SEGURIDAD EN LAS TELECOMUNICACIONES							24.2	
	13.1	Gestion de la seguridad en las redes							
		13.1.1	Controles de red	MUY ALTO	30	30	GESTIONADO		
		13.1.2	Mecanismos de seguridad asociados a servicios en red	ALTO	20	30	GESTIONADO		
		13.1.3	Segregacion de redes	MEDIO	5	10	REALIZADO		
	13.2	Intercambio de informacion con partes externas							
		13.2.1	Politicas y procedimientos de intercambio de informacion	ALTO	20	1	REALIZADO		
		13.2.3	Mensajeria electronica	ALTO	20	40	GESTIONADO		
		13.2.4	Acuerdos de confidencialidad y secreto	MEDIO	5	10	REALIZADO		
14	ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION							10	
	14.1	Requisitos de seguridad de los sistemas de informacion							
		14.1.1	Analisis y especificaciones de los requisitos de seguridad	ALTO	40	10	REALIZADO		
		14.1.2	Seguridad de las comunicaciones en serviciso accesibles por redes public	ALTO	40	10	REALIZADO		
	14.2	Seguridad en los procesos de desarrollo y soporte							
		14.2.2	Procedimientos de control de cambios en los sistemas	MEDIO	20	10	REALIZADO		

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
15	RELACIONES CON SUMINISTRADORES							18	
	15.1	Seguridad de la informacion en las relaciones con suministradores							
		15.1.1	Politica de seguridad de la informacion para suministradores	ALTO	40	10	REALIZADO		
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	MEDIO	20	10	REALIZADO		
	15.2	Gestion de la prestacion del servicio por suministradores							
		15.2.1	Supervision y revision de los servicios prestados por terceros	MEDIO	20	30	GESTIONADO		
		15.2.2	Gestion de cambios en los servicios prestados por terceros	MEDIO	20	30	GESTIONADO		
16	GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION							16.2	
	16.1	Gestion de incidentes de seguridad de la informacion y mejoras							
		16.1.1	Responsabilidades y procedimientos	ALTO	20	50	ESTABLECIDO		
		16.1.2	Notificacion de los eventos de seguridad de la informacion	MEDIO	12	5	REALIZADO		
		16.1.3	Notificacion de puntos debiles de la seguridad	MEDIO	12	10	REALIZADO		
		16.1.4	Valoracion de eventos de seguridad de la informacion y toma de decisiones	MEDIO	12	5	REALIZADO		
		16.1.5	Respuesta a los incidentes de seguridad	ALTO	20	10	REALIZADO		
		16.1.6	Aprendizaje de los incidentes de seguridad de la informacion	MEDIO	12	10	REALIZADO		
		16.1.7	Recopilacion de evidencias	MEDIO	12	5	REALIZADO		
17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NI							7.25	
	17.1	Continuidad de la seguridad de la informacion							
		17.1.1	Planificacion de la continuidad de la seguridad de la informacion	ALTO	25	5	REALIZADO		
		17.1.2	Implantacion de la continuidad de la seguridad de la informacion	MUY ALTO	30	5	REALIZADO		
		17.1.3	Verificacion, revision y evaluacion de la continuidad de la seguridad de la in	MEDIO	20	10	REALIZADO		
	17.2	Redundancias							
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la informacion	ALTO	25	10	REALIZADO		
18	CUMPLIMIENTO							10	
	18.1	Cumplimiento de los requisistos legales y contractuales							
		18.1.1	Identificacion de la legislacion aplicable	MEDIO	10	10	REALIZADO		
		18.1.3	Proteccion de los registros de la organización	ALTO	20	10	REALIZADO		
		18.1.4	Proteccion de datos y privaciodad de la informacion personal	MUY ALTO	30	10	REALIZADO		
	18.2	Revisiones de la seguridad de la informacion							
		18.2.1	Revision independiente de la seguridad de la informacion	MEDIO	10	10	REALIZADO		
		18.2.2	Cumplimiento de las politicas y normas de seguridad	ALTO	20	10	REALIZADO		
		18.2.3	Comprobacion del cumplimiento	MEDIO	10	10	REALIZADO		

Figura 47: Resultado de evaluación de controles con semaforización – Primera Etapa
Fuente: Elaboración propia

Según el trabajo realizado en la primera etapa, los resultados muestran una alta deficiencia en el proceso de salvaguardar la información de la entidad.

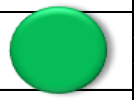
Para el trabajo de la segunda etapa, el procedimiento de la evaluación fue realizado después de realizar lo siguiente:

1. Elaboración de políticas de seguridad para ADEA
2. Implementación de políticas de seguridad de la información para ADEA. Usando recursos tecnológicos, humanos, materiales.
3. Capacitación de los usuarios e interesados.
4. Puesta en marcha de las políticas de seguridad de la información en ADEA.

Para su aplicación se consideró las siguientes características:

- Anonimato: durante la aplicación, ninguno de los colaboradores a los que se les entrevisto, sabían que se les estaba entrevistando a los otros también.
- Respuestas del grupo: LA información que se presenta, no es solo el punto de vista de uno solo, sino de todas las opiniones de los involucrados directamente del proyecto.

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
5	POLITICAS DE SEGURIDAD							56	
	5.1	Directrices de la Direccion en seguridad de la información							
		5.1.1	Conjunto de politicas para la seguridad de la informacion	ALTO	60	60	ESTABLECIDO		
		5.1.2	Revision de las politicas para la seguridad de la informacion	MEDIO	40	50	ESTABLECIDO		
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION							54.5	
	6.1	Organización Interna							
		6.1.1	Asignacion de responsabilidades para la seguridad de la informacion	ALTO	20	50	ESTABLECIDO		
		6.1.2	Segregacion de tareas	MEDIO	15	40	GESTIONADO		
		6.1.3	Contacto con las autoridades	MEDIO	15	70	PREDECIBLE		
		6.1.4	Contacto con grupos de interes especial	MEDIO	15	50	ESTABLECIDO		
		6.1.5	Seguridad de la informacion en la gestion de proyectos	ALTO	20	50	ESTABLECIDO		
	6.2	Dispositivos para movilidad y teletrabajo							
		6.2.1	Politica de uso de dispositivos para movilidad	MEDIO	15	70	PREDECIBLE		
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS							73.4	
	7.1	Antes de la contratacion							
		7.1.2	Terminos y condiciones de contratacion	ALTO	25	80	PREDECIBLE		
	7.2	Durante la contratacion							
		7.2.1	Responsabilidad de gestion	ALTO	25	80	PREDECIBLE		
		7.2.2	Concienciacion, educacion y capacitacion en seguridad de la informacion	MEDIO	17	70	PREDECIBLE		
		7.2.3	Proceso disciplinario	MEDIO	17	70	PREDECIBLE		
	7.3	Cese o cambio de puesto de trabajo							
		7.3.1	Cese o cambio de puesto de trabajo	MEDIO	16	60	ESTABLECIDO		
8	GESTION DE ACTIVOS							61.8	
	8.1	Responsabilidad sobre los activos							
		8.1.1	Inventario de activos	ALTO	20	70	PREDECIBLE		
		8.1.2	Propiedad de los activos	MEDIO	16	70	PREDECIBLE		
		8.1.3	Uso aceptable de los activos	MEDIO	16	50	ESTABLECIDO		
	8.2	Clasificacion de la informacion							
		8.2.1	Directrices de clasificacion	MEDIO	16	30	GESTIONADO		
		8.2.2	Etiquetado y manipulado de la informacion	MEDIO	16	30	GESTIONADO		
		8.2.3	Manipulacion de activos	MEDIO	16	50	ESTABLECIDO		
	8.3	Manejo de los soportes de almacenamiento							
		8.3.1	Gestion de soportes extraibles	MEDIO	10	50	ESTABLECIDO		
		8.3.2	Eliminacion de soportes	MEDIO	10	30	GESTIONADO		
		8.3.3	Soportes fisicos en transito	MEDIO	10	30	GESTIONADO		

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
9	CONTROL DE ACCESOS							65.8	
	9.1	Requisitos de negocio para el controlde accesos							
		9.1.1	Politica de control de accesos	ALTO	10	50	ESTABLECIDO		
		9.1.2	Control de acceso a las redes y servicios asociados	ALTO	10	70	PREDECIBLE		
	9.2	Gestion de acceso de usuario							
		9.2.1	Gestion de altas/bajas en el registro de usuarios	MEDIO	6	70	PREDECIBLE		
		9.2.2	Gestion de los derechos de acceso asignados a usuarios	MEDIO	6	70	PREDECIBLE		
		9.2.3	Gestion de los derechos de acceso con privilegios especiales	MEDIO	6	70	PREDECIBLE		
		9.2.4	Gestion de informacion confidencial de autenticacion de usuarios	MEDIO	6	70	PREDECIBLE		
		9.2.5	Revision de los derechos de acceso de los usuarios	MEDIO	6	70	PREDECIBLE		
		9.2.6	Retirada o adaptacion de los derechos de acceso	MEDIO	6	60	ESTABLECIDO		
	9.3	Responsabilidad del usuario							
		9.3.1	Uso de informacion confidencial para la autentificacion	MEDIO	6	50	ESTABLECIDO		
	9.4	Control de acceso a sistmas y aplicaciones							
		9.4.1	Restriccion del acceso a la informacion	ALTO	10	60	ESTABLECIDO		
		9.4.2	Procedimientos seguros de inicio de sesion	MEDIO	6	70	PREDECIBLE		
		9.4.3	Gestion de contraseñas de usuario	MEDIO	6	80	PREDECIBLE		
		9.4.4	Uso de herramientas de administracion de sistemas	MEDIO	6	70	PREDECIBLE		
		9.4.5	Control de acceso al codigo fuente de los programas	ALTO	10	70	PREDECIBLE		
10	CIFRADO							80	
	10.1	Controles Criptográficos							
		10.1.2	Gestion de claves	MUY ALTO	100	80	PREDECIBLE		
11	SEGURIDAD FISICA Y AMBIENTAL							57	
	11.1	Areas seguras							
		11.1.1	Perimetro de seguridad fisica	ALTO	8	60	ESTABLECIDO		
		11.1.2	Controles fisicos de entrada	ALTO	8	50	ESTABLECIDO		
		11.1.3	Seguridad de oficinas, despachos y recursos	ALTO	8	50	ESTABLECIDO		
		11.1.4	Proteccion contra las amenazas externas y ambientales	MEDIO	5	70	PREDECIBLE		
		11.1.5	El trabajo en areas seguras	MEDIO	5	60	ESTABLECIDO		
		11.1.6	Areas de acceso publico, carga y descarga	MEDIO	5	60	ESTABLECIDO		
	11.2	Seguridad de los equipos							
		11.2.1	Emplazamiento y proteccion de equipos	MUY ALTO	10	60	ESTABLECIDO		
		11.2.2	Instalaciones de suministro	MUY ALTO	10	70	PREDECIBLE		
		11.2.3	Seguridad del cableado	ALTO	8	70	PREDECIBLE		
		11.2.4	Mantenimiento de los equipos	ALTO	8	70	PREDECIBLE		
		11.2.5	Salida de activos fuera de las dependencias de la empresa	MEDIO	5	50	ESTABLECIDO		
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	MEDIO	5	30	GESTIONADO		
		11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento	MEDIO	5	50	ESTABLECIDO		
		11.2.8	Equipo informatico de usuario desatendido	MEDIO	5	30	GESTIONADO		
		11.2.9	Politica de puesto de trabajo despejado y bloqueo de pantalla	MEDIO	5	50	ESTABLECIDO		

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
12	SEGURIDAD EN LA OPERATIVA							56.8	
	12.1	Responsabilidades y procedimientos de operación							
		12.1.1	Documentacion de procedimientos de operación	MEDIO	7	80	PREDECIBLE		
		12.1.2	Gestion de cambios	MEDIO	7	50			
	12.2	Proteccion contra codigo malicioso							
		12.2.1	Controles contra el codigo malicioso	ALTO	10	60	ESTABLECIDO		
	12.3	Copias de seguridad							
		12.3.1	Copias de seguridad de la informacion	MUY ALTO	18	70	PREDECIBLE		
	12.4	Registro de actividad y supervision							
		12.4.1	Registro y gestion de eventos de actividad	ALTO	10	50	ESTABLECIDO		
		12.4.2	Proteccion de los registros de informacion	MEDIO	7	70	PREDECIBLE		
		12.4.3	Registros de actividad del administrador y operador del sistema	MEDIO	7	70	PREDECIBLE		
	12.5	Control del software en explotacion							
		12.5.1	Instalacion del software en sistemas en produccion	MEDIO	7	60	ESTABLECIDO		
	12.6	Gestion de la vulnerabilidad tecnica							
		12.6.1	Gestion de las vulnerabilidades tecnicas	ALTO	10	30	GESTIONADO		
		12.6.2	Restricciones en la instalacion de software	MEDIO	7	30	GESTIONADO		
	12.7	Consideraciones de las auditorias de los sistemas de informacion							
		12.7.1	Controles de auditoría de los sistemas de información	ALTO	10	50	ESTABLECIDO		
13	SEGURIDAD EN LAS TELECOMUNICACIONES							72	
	13.1	Gestion de la seguridad en las redes							
		13.1.1	Controles de red	MUY ALTO	30	70	PREDECIBLE		
		13.1.2	Mecanismos de seguridad asociados a servicios en red	ALTO	20	70	PREDECIBLE		
		13.1.3	Segregacion de redes	MEDIO	5	70	PREDECIBLE		
	13.2	Intercambio de informacion con partes externas							
		13.2.1	Politicas y procedimientos de intercambio de informacion	ALTO	20	70	PREDECIBLE		
		13.2.3	Mensajeria electronica	ALTO	20	80	PREDECIBLE		
		13.2.4	Acuerdos de confidencialidad y secreto	MEDIO	5	70	PREDECIBLE		
14	ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION							58	
	14.1	Requisitos de seguridad de los sistemas de informacion							
		14.1.1	Analisis y especificaciones de los requisitos de seguridad	ALTO	40	50	ESTABLECIDO		
		14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes public	ALTO	40	70	PREDECIBLE		
	14.2	Seguridad en los procesos de desarrollo y soporte							
		14.2.2	Procedimientos de control de cambios en los sistemas	MEDIO	20	50	ESTABLECIDO		

Dominios	Objetivos de Control	Controles	Descripción	NIVELDE CRITICIDAD	cumplimiento por criticidad %C	cumplimiento por criticidad NC. C	NIVEL CMMI	PONDERACION DOMINIO %	SEMAFORO DOMINIO
15	RELACIONES CON SUMINISTRADORES							70	
	15.1	Seguridad de la informacion en las relaciones con suministradores							
		15.1.1	Politica de seguridad de la informacion para suministradores	ALTO	40	70	PREDECIBLE		
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	MEDIO	20	70	PREDECIBLE		
	15.2	Gestion de la prestacion del servicio por suministradores							
		15.2.1	Supervision y revision de los servicios prestados por terceros	MEDIO	20	70	PREDECIBLE		
		15.2.2	Gestion de cambios en los servicios prestados por terceros	MEDIO	20	70	PREDECIBLE		
16	GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION							65.2	
	16.1	Gestion de incidentes de seguridad de la informacion y mejoras							
		16.1.1	Responsabilidades y procedimientos	ALTO	20	70	PREDECIBLE		
		16.1.2	Notificacion de los eventos de seguridad de la informacion	MEDIO	12	70	PREDECIBLE		
		16.1.3	Notificacion de puntos debiles de la seguridad	MEDIO	12	50	ESTABLECIDO		
		16.1.4	Valoracion de eventos de seguridad de la informacion y toma de decisiones	MEDIO	12	70	PREDECIBLE		
		16.1.5	Respuesta a los incidentes de seguridad	ALTO	20	70	PREDECIBLE		
		16.1.6	Aprendizaje de los incidentes de seguridad de la informacion	MEDIO	12	70	PREDECIBLE		
		16.1.7	Recopilacion de evidencias	MEDIO	12	50	ESTABLECIDO		
17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NE							72.5	
	17.1	Continuidad de la seguridad de la informacion							
		17.1.1	Planificacion de la continuidad de la seguridad de la informacion	ALTO	25	80	PREDECIBLE		
		17.1.2	Implantacion de la continuidad de la seguridad de la informacion	MUY ALTO	30	70	PREDECIBLE		
		17.1.3	Verificacion, revision y evaluacion de la continuidad de la seguridad de la in	MEDIO	20	70	PREDECIBLE		
	17.2	Redundancias							
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la informacion	ALTO	25	70	PREDECIBLE		
18	CUMPLIMIENTO							73	
	18.1	Cumplimiento de los requisistos legales y contractuales							
		18.1.1	Identificacion de la legislacion aplicable	MEDIO	10	70	PREDECIBLE		
		18.1.3	Proteccion de los registros de la organización	ALTO	20	80	PREDECIBLE		
		18.1.4	Proteccion de datos y privaciodad de la informacion personal	MUY ALTO	30	80	PREDECIBLE		
	18.2	Revisiones de la seguridad de la informacion							
		18.2.1	Revision independiente de la seguridad de la informacion	MEDIO	10	50	ESTABLECIDO		
		18.2.2	Cumplimiento de las politicas y normas de seguridad	ALTO	20	70	PREDECIBLE		
		18.2.3	Comprobacion del cumplimiento	MEDIO	10	70	PREDECIBLE		

Figura 48: Resultado de evaluación de controles con semaforización – Segunda Etapa
Fuente: Elaboración propia

COMPARACIÓN DE RESULTADOS DE EVALUACION DE CONTROLES PRIMERA ETAPA VS SEGUNDA ETAPA

Para poder tener una interpretación de los resultados, a continuación muestro los resultados obtenidos en la evaluación de la PRIMERA ETAPA y un segundo momento SEGUNDA ETAPA, luego de haber realizado la implementación de buenas prácticas. Cabe indicar que los resultados fueron ponderados por dominios de control, los cuales muestran en su mayoría mejoras positivas de cumplimiento de dichos controles en ADEA.

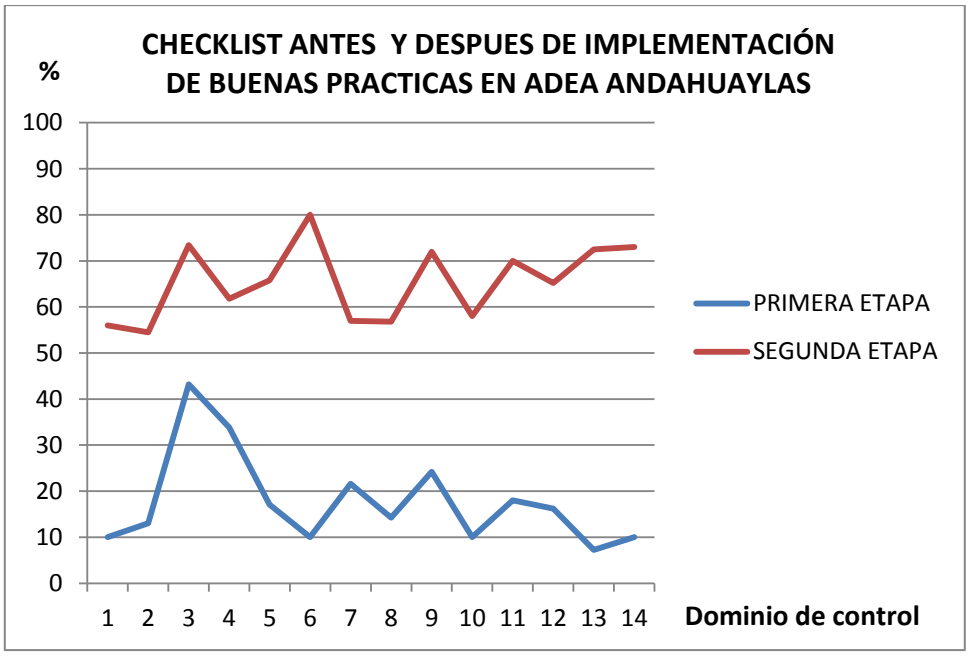


Figura 49: Resultados de checklist primera etapa vs segunda etapa
Fuente: Elaboración propia

De acuerdo a la figura 38, podemos apreciar que en el eje X, se encuentran los 14 dominios de la norma ISO 27002:2013 y en el eje Y, el porcentaje del nivel de cumplimiento que va del 0 al 100 %.

Muestra la imagen, diferencias que hay en entre el momento de la primera etapa (color azul), donde se realiza la verificación del cumplimiento de los controles de la ISO 27002 en ADEA Andahuaylas tal cual se gestionaba normalmente la organización. El segundo momento (color rojo), muestra los resultados la misma

verificación del cumplimiento de los controles, pero luego de haber realizado las mejoras en seguridad de la información con buenas prácticas; el cual fue el objetivo de este proyecto, teniendo esta resultados positivos, los cuales se muestran el dicho gráfico.

Según el dominio 5. Políticas de seguridad, desarrollar políticas de seguridad de la información en ADEA Andahuaylas, la cual proviene de la recopilación de información, hallazgos y análisis de la situación inicial en la que se encontraban, generó una mejora significativa del cumplimiento de dicho dominio.

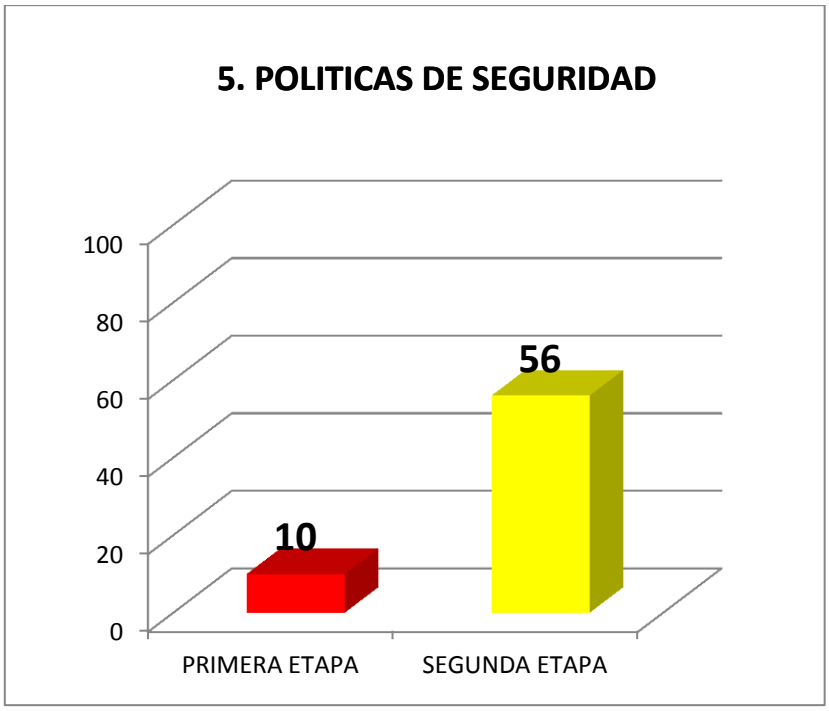


Figura 50: Políticas de seguridad – primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 6. Aspectos organizativos de la seguridad de la información, actualmente se está recibiendo apoyo desde el directorio y gerencia con la iniciativa de implementación del sistema de gestión de seguridad de la información en ADEA Andahuaylas. Lo anterior, generó una mejora significativa del cumplimiento de dicho dominio.

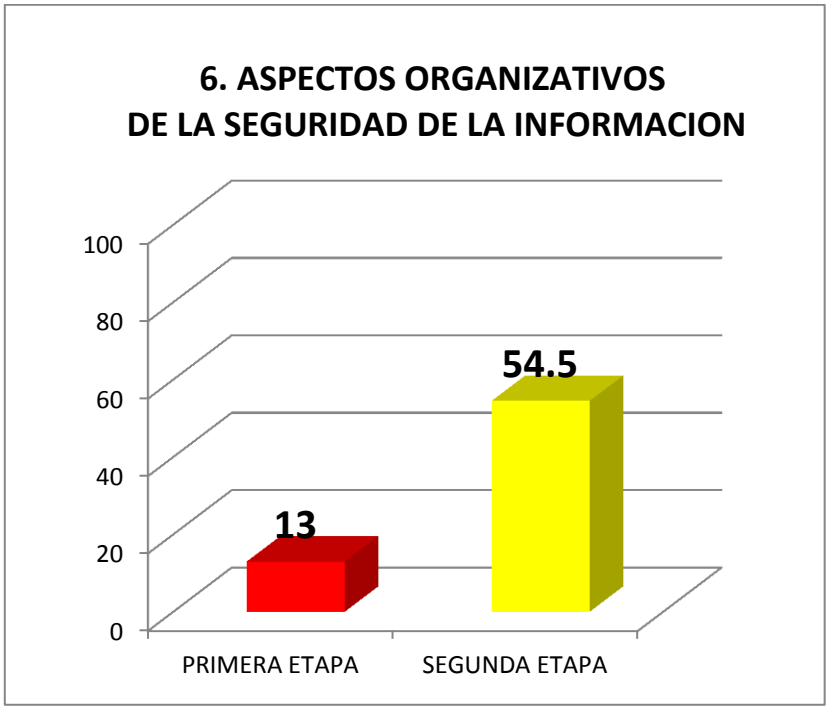


Figura 51: Aspectos organizativos de la seguridad de la información - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 7. Seguridad ligada a los recursos humanos, actualmente ADEA Andahuaylas gestiona antes y durante el empleo de sus colaboradores. También cuando hay cese del empleado o cambio de funciones de los mismos, es por ello que generó una mejora en el cumplimiento de dicho dominio.

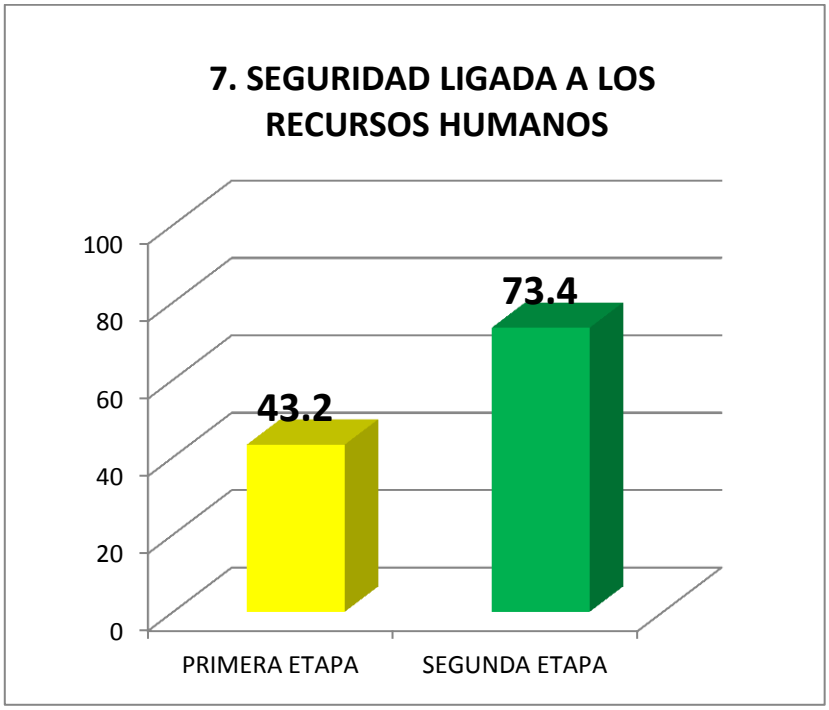


Figura 52: Seguridad ligada a los recursos humanos - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 8. Gestión de activos, actualmente ya cuentan con manual de gestión de activos, clasifican mejor la información, controlan mejor la salida y entrada de bienes de la organización, además de que cuentan con un colaborador capacitado en dicho tema gestión de seguridad de la información en ADEA Andahuaylas. En consecuencia generó una mejora del cumplimiento de dicho dominio.

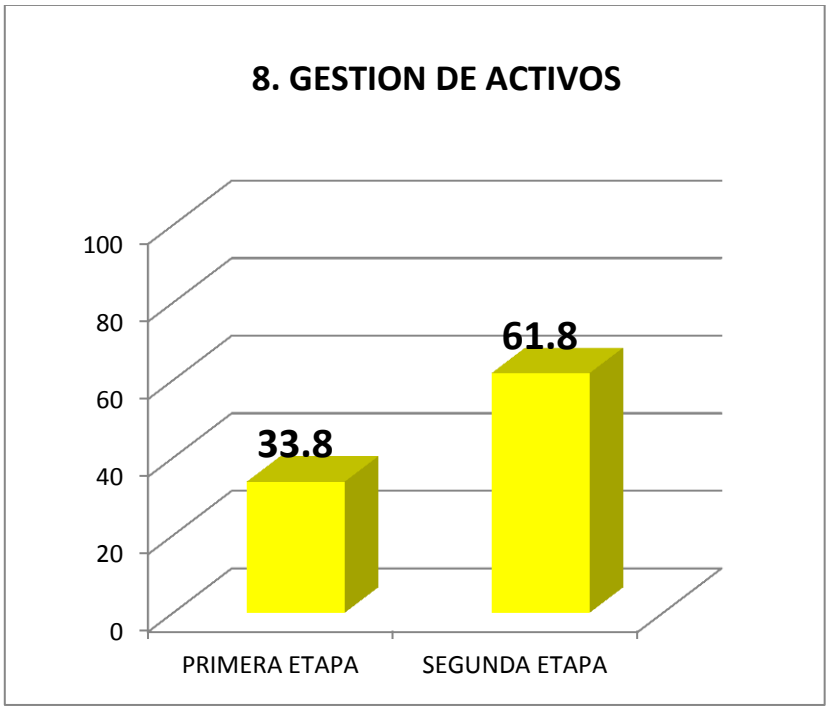


Figura 53: Gestión de activos - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 9. Control de accesos, actualmente se ha realizado capacitaciones de concientización a los colaboradores sobre las responsabilidades y/o condiciones de otorgarles accesos, ya sea lógica; accesos a la red, aplicativos y sistemas en general y físicamente; a los ambientes a cada uno de ellos en ADEA Andahuaylas. Cuentan con una política de accesos en general para la organización, y en consecuencia generó una mejora del cumplimiento de dicho dominio.

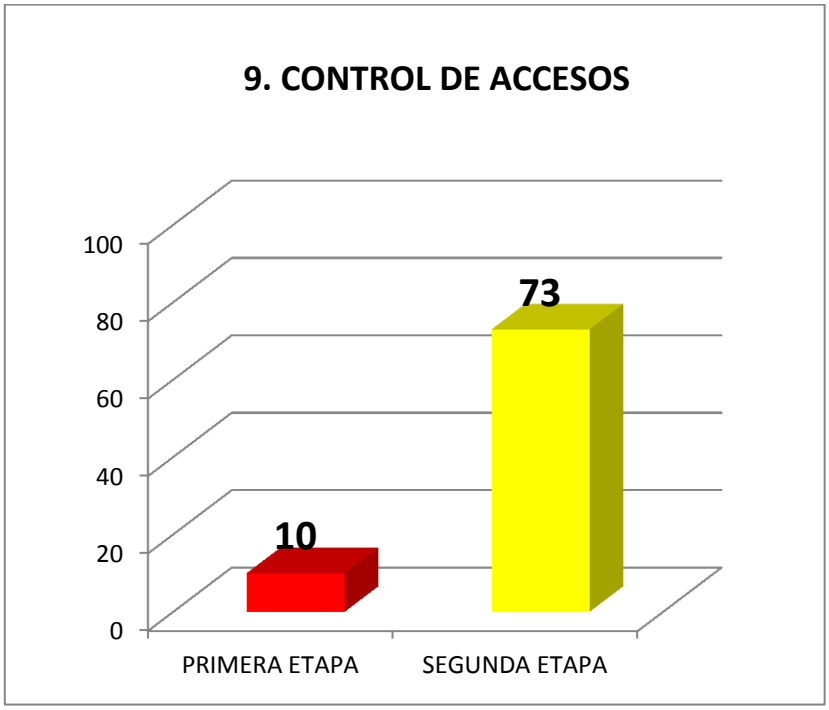


Figura 54: Control de accesos - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 10. Cifrado, se ha realizado trabajos de seguridad al implementar un servidor de aplicaciones para el uso de equipos remotos e interconectar todas sus oficinas. Ahora se utiliza tecnologías de cifrado para sus conexiones de aplicaciones y correo. En consecuencia generó una mejora significativa en el cumplimiento de dicho dominio.

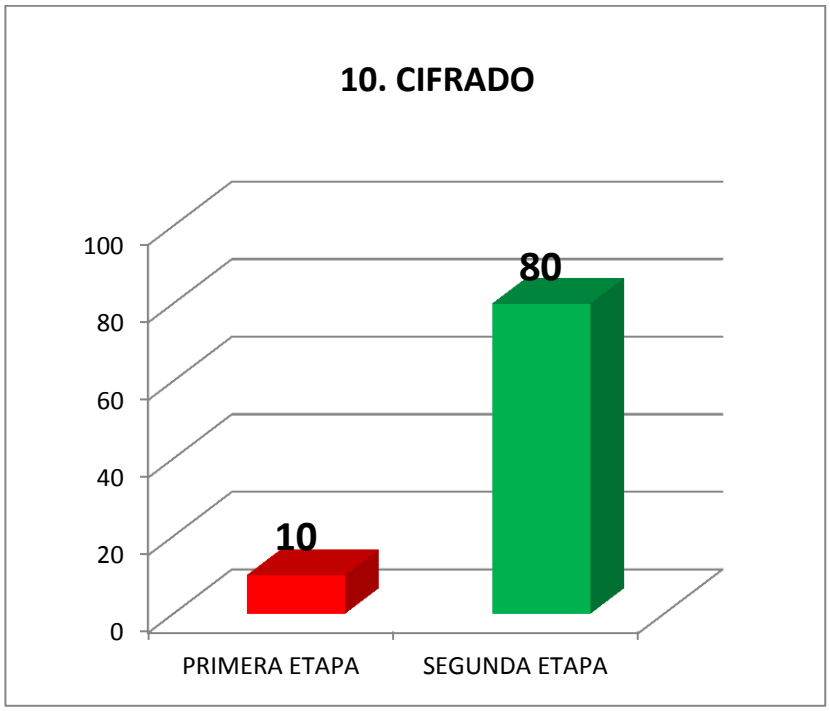


Figura 55: Cifrado - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 11. Seguridad física y ambiental, se ha realizado algunos cambios en lo que respecta a la seguridad física, ya que la organización ya venía realizando procedimientos y prácticas de seguridad física en sus infraestructuras. Se generó una ligera mejora del cumplimiento de dicho dominio.

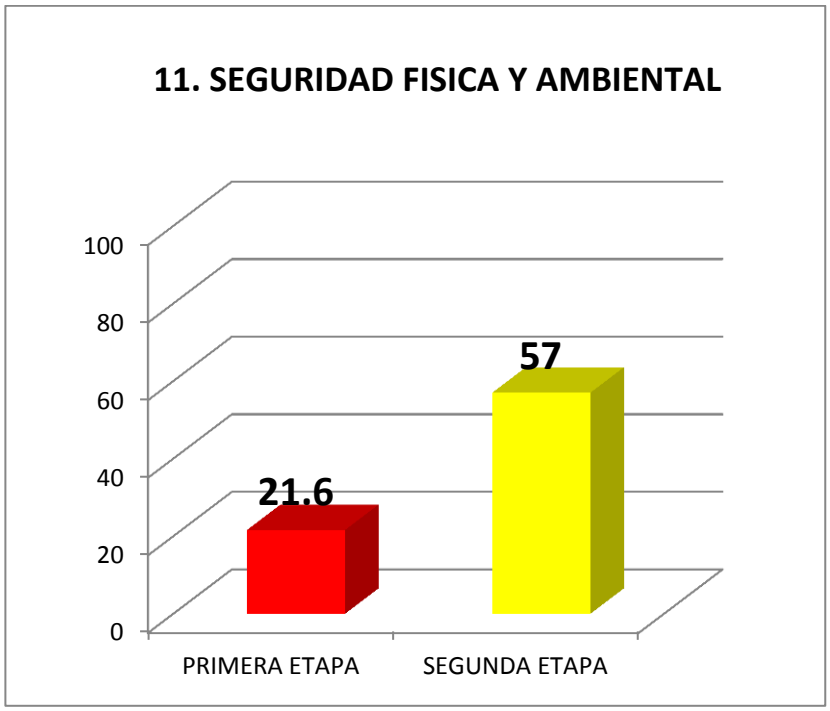


Figura 56: Seguridad Física y Ambiental - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 12. Seguridad en la operativa, actualmente la unidad de tecnologías de la información y seguridad, cuenta con procedimientos de seguridad documentados, en la cual lleva el control de procedimientos de operación, gestión de cambios, copias de seguridad, protección de sistemas y registros para auditoria en ADEA Andahuaylas. En consecuencia generó una mejora del cumplimiento de dicho dominio.

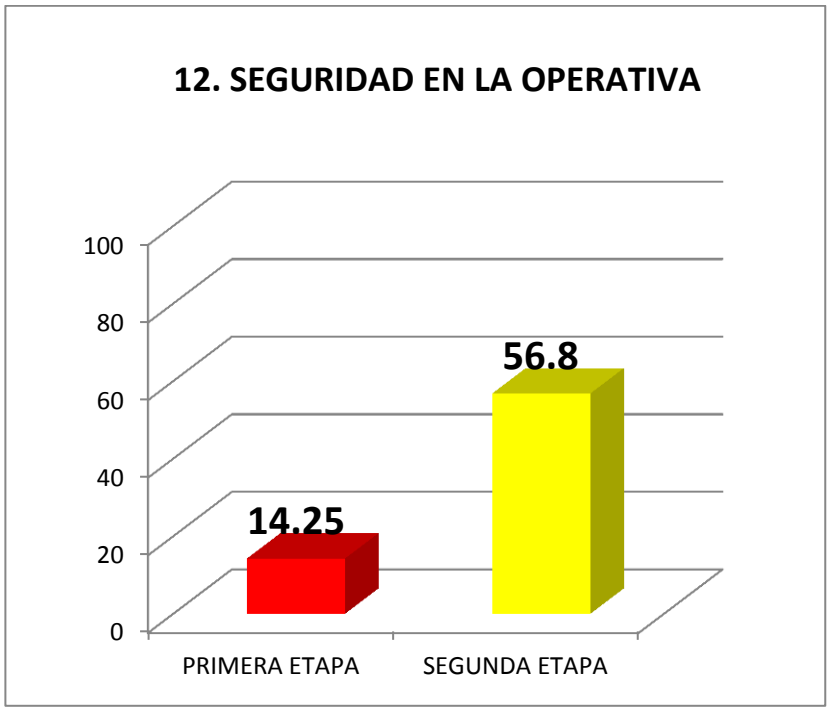


Figura 57: Seguridad en la operativa - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 13. Seguridad en las telecomunicaciones, actualmente cuentan con software de control de redes implementados para la interconexión de sus agencias en la organización, un servidor de correo institucional propio administrable y políticas de uso y procedimientos en la red de ADEA. En consecuencia generó una mejora del cumplimiento de dicho dominio.

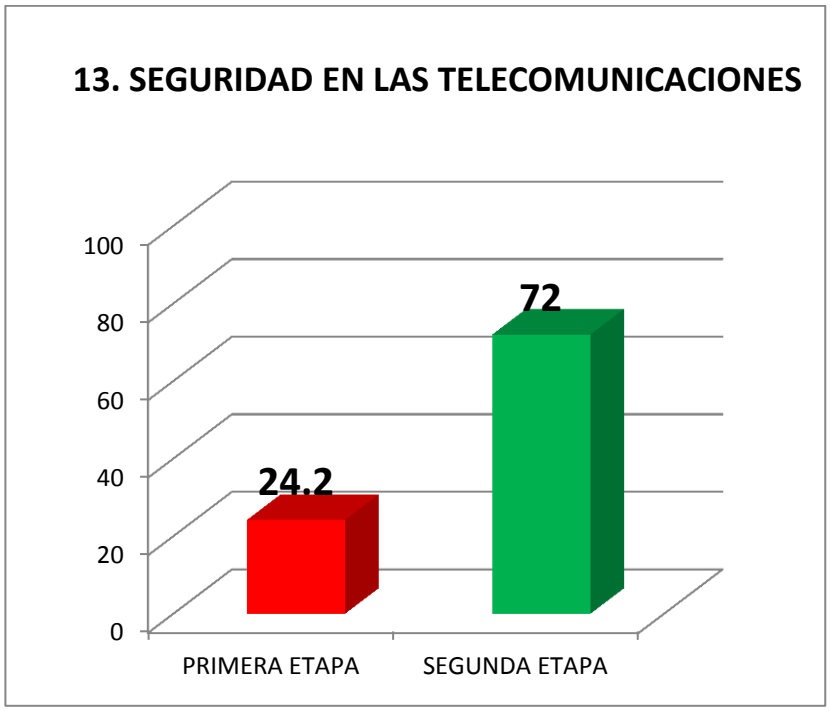


Figura 58: Seguridad en las telecomunicaciones - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 14. Adquisición, desarrollo y mantenimiento de los sistemas de información, la unidad de tecnologías de la información y seguridad cuenta con un manual de procedimientos específicamente para la gestión de sistemas de información, esto generó una mejora del cumplimiento de dicho dominio.

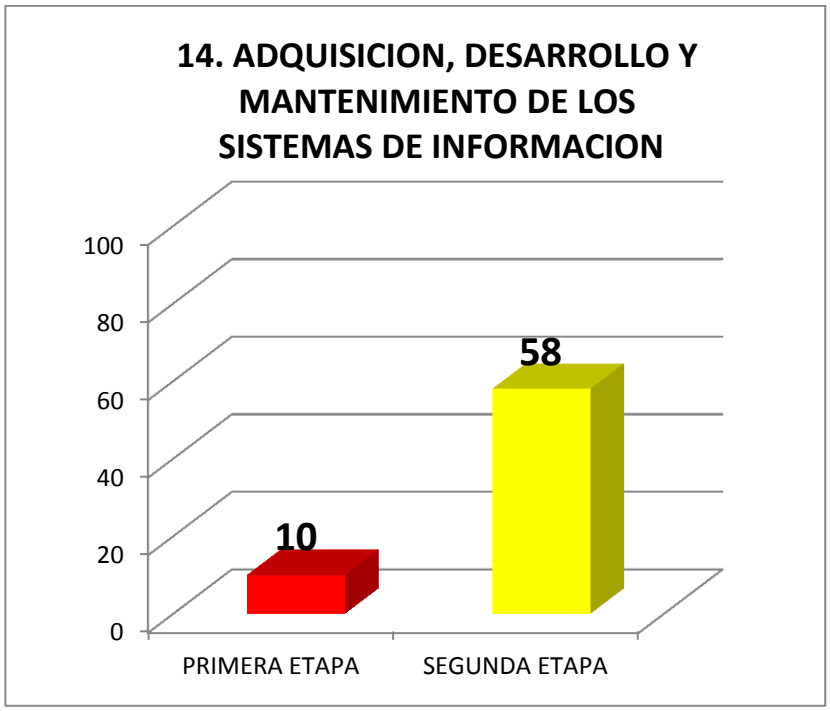


Figura 59: Adquisición, desarrollo y mantenimiento de los sistemas de información - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 15. Relaciones con suministradores, actualmente ya cuentan con políticas de seguridad de la información para suministradores, donde se describe los riesgos dentro de acuerdos con suministradores, la supervisión y revisión de servicios prestados por terceros y la gestión de cambios en los servicios prestados por terceros en ADEA Andahuaylas. En consecuencia generó una mejora del cumplimiento de dicho dominio.

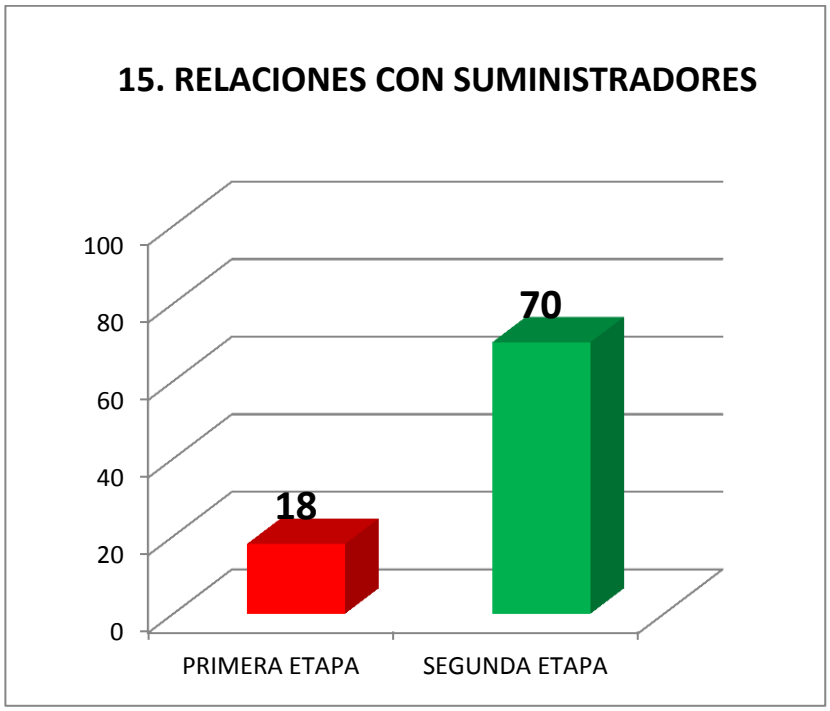


Figura 60: Relaciones con suministradores - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 16. Gestión de incidentes en la seguridad de la información, actualmente ya cuentan con documentos para gestión de incidentes de seguridad, donde describen las responsabilidades y procedimientos a seguir, puntos débiles de la seguridad y registro de incidencias de seguridad para el aprendizaje de los mismos ADEA Andahuaylas. En consecuencia generó una mejora del cumplimiento de dicho dominio.

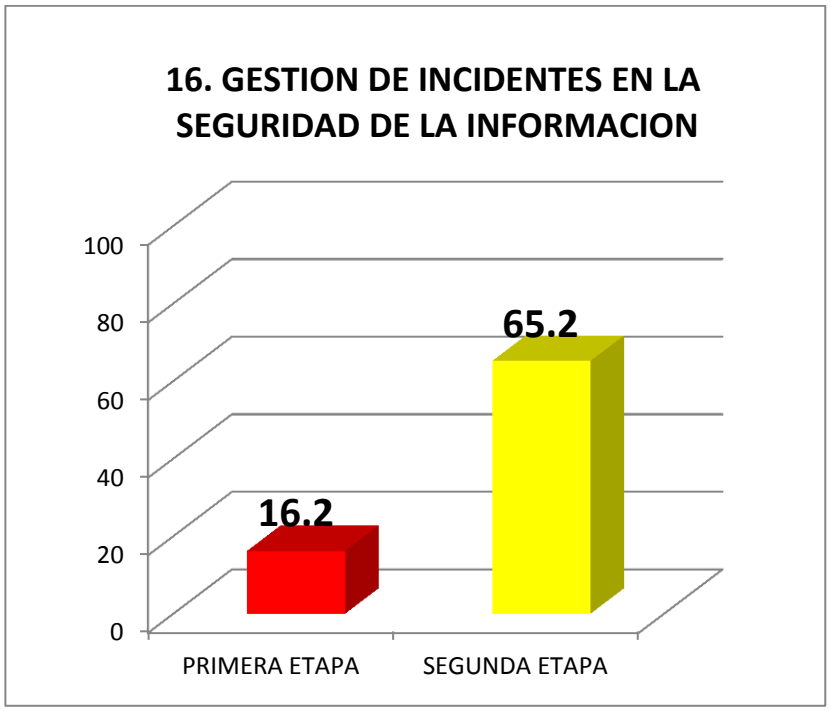


Figura 61: Gestión de incidentes en la seguridad de la información - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio, actualmente ya cuentan con un plan de continuidad de negocio aprobado por el directorio y vigente, el cual viene complementándose en su implementación en ADEA Andahuaylas. En consecuencia generó una mejora muy significativa del cumplimiento de dicho dominio.

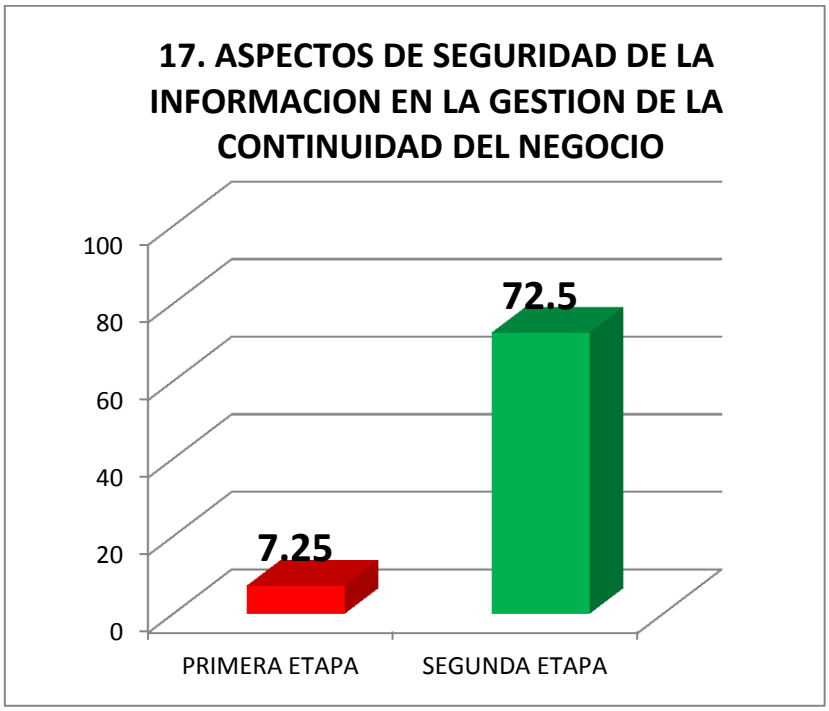


Figura 62: Aspectos de seguridad de la información en la gestión de la continuidad del negocio - primera etapa vs segunda etapa
Fuente: Elaboración propia

Según el dominio 18. Cumplimiento, actualmente ya cuentan con un colaborador de la unidad de riesgos, el cual viene realizando la función de auditor interno quien verifica el cumplimiento de las políticas de seguridad de la información de ADEA Andahuaylas. También se planifican auditorías externas que tengan prioridad en seguridad de la información. En consecuencia generó una mejora muy significativa del cumplimiento de dicho dominio.

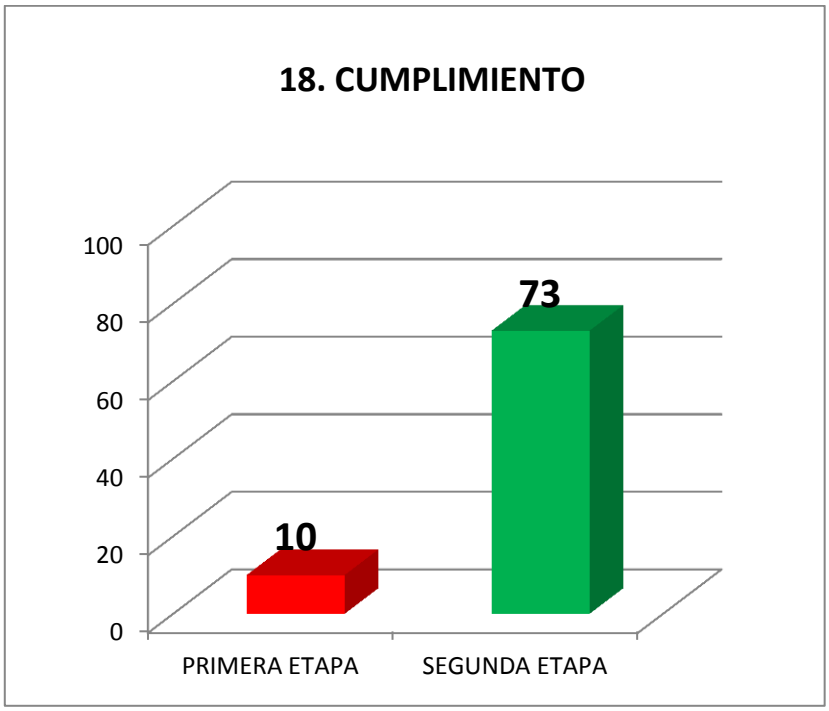


Figura 63: Cumplimiento - primera etapa vs segunda etapa
Fuente: Elaboración propia

De las actividades desarrolladas en el presente proyecto, puedo concluir resaltando lo siguiente:

- Con la definición de políticas de seguridad de la información, las cuales deben ser tangibilizados en procedimientos, reglamentos y controles debidamente formalizados, se ha logrado establecer un nivel de conocimiento, concientización y cultura en el personal de ADEA orientado hacia el control y la seguridad de la información, que se expresa en la disminución de incidencias relacionados con las caídas de las TI que dan soporte a los principales procesos: créditos, captaciones de inversiones y capacitaciones.
- Con la correcta identificación de los procesos críticos de ADEA, con su correspondiente priorización de nivel de riesgo de pérdida de la información, se ha logrado identificar la infraestructura de TI más crítica y

aplicar las estrategias para su recuperación y continuidad, lo que ha conllevado a disminuir el número de caídas o problemas.

- Se ha logrado implementar un modelo inicial de gestión de la seguridad de la información para ADEA, que identifica, evalúa y trata nítidamente los activos de TI, sus amenazas, debilidades y niveles de riesgo relacionadas con las categorías: disponibilidad, integridad y confidencialidad de la información, que exige la SBS para este tipo de organizaciones en sus planes de seguridad (Circular G-139-2009 – SBS (Gestión de la continuidad del negocio), Circular G-140-2009 – SBS (Gestión de la seguridad de la información) y Resolución S.B.S.N° 2116 - 2009). Esto ha permitido lograr establecer pautas para evaluar la magnitud de los riesgos de modo coherente y contar con indicadores clave para monitorizar periódicamente la eficacia de las actividades de gestión de la seguridad de la información en ADEA, mediante la evaluación de los controles de seguridad de la información de la norma ISO 27002.
- Queda demostrado que la norma ISO 27002, código de buenas prácticas es aplicable a cualquier tipo de organización y en los niveles que lo requiera. Esta herramienta es indispensable para poder realizar una certificación en ISO 27001; Sistema de gestión de la seguridad de la Información.
- Es importante recalcar que si se cumpliera al cien por ciento con las políticas desarrolladas en la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA, no se garantiza que no tengan problemas de seguridad ya que no existe la seguridad al cien por ciento; con el manual de políticas de seguridad de la información, con el cumplimiento de las mismas y con la implementación de soluciones tecnológicas a los controles de seguridad, se conllevo a la minimización de los riesgos asociados a los activos de información, reduciendo así el impacto, fuga de información y perdidas económicas originados por la carencia de las normas y políticas de seguridad de la información.

CONCLUSIONES

1. Es de vital importancia la evaluación temprana de la seguridad de la información, a través de un diagnostico que permita comprender las debilidades y amenazas en las que la organización se somete, ya que el diagnostico sirve como línea base para la estructuraciones de la solución.
2. La planificación permitió abordar la problemática a través de acciones, tiempo y recursos debidamente asignado a las tareas cuyo objetivo tiene llevar a cabo una implementación exitosa de la solución elegida para el aseguramiento de la información.
3. Los mecanismos de control son necesarios durante todo el proceso de implementación ya que permiten la realimentación en los procesos mediante la verificación del cumplimiento de los dominios de la norma ISO 27002, con la finalidad de evitar riesgos, demoras y gastos innecesarios dentro del proyecto.
4. Con la utilización de buenas prácticas en seguridad de la información, se ha logrado reducir significativamente la exposición al riego de los diferentes activos de las tecnologías de la información, en promedio un 47 %. También se ha incorporado procedimientos de mantenimiento y mejora continua de los controles de seguridad de la información.
5. Los dominios que tuvieron mayor impacto fueron los aspectos de seguridad de la información en la gestión de la continuidad del negocio, relaciones con suministradores y gestión de incidentes en la seguridad de la información, con una mejora en el nivel de cumplimiento de 65%, 52% y 49% respectivamente.
6. Identificar los riesgos en los activos de las tecnologías de la información oportunamente, también permiten reducir costos asociados a dichos activos que en un futuro cercano o lejano puede ser valorado.
7. Luego de la implementación de las buenas prácticas en seguridad de la información con la norma ISO 27002 para la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA, inicialmente se pudo detectar muchas deficiencias en la parte de seguridad de la información, en todas sus formas y estados.

8. Con el manual de políticas de seguridad de la información diseñada para la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA, proporcionara una guía a seguir para trabajar en los aspectos de seguridad.

RECOMENDACIONES

1. La aplicación de este instrumento como es la norma ISO 27002, debe ser utilizado permanentemente de manera progresiva para así incorporar nuevas metas a medida que estas sean alcanzadas dentro de un proceso de mejora continua.
2. Es necesario que la Alta Dirección y consecuentemente el total de colaboradores de ADEA se mantengan comprometidos en aplicar un enfoque a procesos y en su mejora continua, determinen las mejoras maneras de realizar sus actividades.
3. Se recomienda realizar la constante sensibilización sobre la importancia de la seguridad de la información, esta campaña será dirigida a la totalidad de colaboradores de la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA.
4. Seguir implementando mediante soluciones tecnológicas más objetivos de control de la norma ISO 27002 adecuados al crecimiento de la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA.
5. La unidad de Tecnologías de la Información y Seguridad de la Asociación para el Desarrollo Empresarial en Apurímac, Andahuaylas y Chincheros – ADEA, debe afrontar con las deficiencias de seguridad de la información, para lo cual debe tomar seriedad sobre lo documentado y realizar proyectos de enmendadura basados en las políticas de seguridad y por ultimo debe realizar campañas de concientización sobre los temas abordados.

BIBLIOGRAFIA

AADAT (2017) DELITOS INFORMÁTICOS, Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos por Nora Paterlini, Carolina Vega, Gabriela Guerriero y Mercedes Velázquez. Recuperado el 20 de 07 del 2017. http://www.aadat.org/delitos_informaticos20.htm

AEG (2016), ASOCIACION ESPAÑOLA PARA LA CALIDAD, Seguridad de la Información. Recuperado el 21 de 07 del 2017. https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Alvarez Basaldua, L. (2005). Seguridad en Informatica (Auditoria de Sistemas). Mexico DF.

Banca15 (2017), La importancia de la seguridad en los bancos y en el sector financiero, MARTA MARCHINI, HONEYWELL SECURITY GROUP. Recuperado el 20 de 07 del 2017. http://www.banca15.com/secciones/tribunas/2012/marta-marchini-honeywell.htm

Benitez, M. (2013). Politicas de Seguridad Informatica. Gestion Integlar, Recuperado el 22 de 08 del 2017, de: http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

Correa Villa, Mauricio. (2008). Fundamentos de la teoría de la información. Instituto Tecnologico Metropolitano.

Fischer, Royal P. (1988). Seguridad en los sistemas informáticos. Ediciones Díaz de Santos, S.A. Pág. 33.

Garcia, Quispe, Ráez (2003), Mejora continua de la calidad en los procesos, Recuperado el 20 de 07 del 2017, de : http://www.redalyc.org/html/816/81606112/

Hartley R. V. (1928). Transmission of Information. Bell system Tech. Journal, vol. 7, págs. 535-563.

ISO.org , Gestion de la Seguridad de la Informacion – 27001 ISO/IEC. Recuperado el 22 de 08 del 2015, de http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO27000.ES, ISO 27001 en español Recuperado el 22 de 08 del 2017, de http://iso27000.es/iso27000.html

ISO/IEC 27002, Recuperado el 22 de 08 del 2017, de Wikipedia https://es.wikipedia.org/wiki/ISO/IEC_27002

ISO/IEC 1779 (2007), Norma Tecnica Peruana. EDI, Tecnologia de la informacion. Codigo de buenas practicas para la gestion de la seguridad de la informacion, 2007, P. 8.

Johannsen O. (1975). Introducción a la teoria general de sistemas. Facultad de Economía y Administración. Universidad de Chile.

Kaspersky LAb (2017), Como protegerse de la nueva epidemia global de Ransonware, Recuperado el 24 de 07 del 2017 de Kaspersky Lab Daily. https://latam.kaspersky.com/blog/como-protegerse-de-la-nueva-epidemia-global-de-rnasomware/10741/

Kremer, C. & Berman, K. (2009), Entendiendo las Finanzas – Soluciones prácticas para los desaficos del día a día. Boston – Massachusetts. Harvard Business Press.

Nyquist, Harry (1928). Certain Topics in Telegraph Transmission Theory.

ONGEI, NTP ISO/IEC 17799:2007 Recuperado el 22 de 08 del 2017, de ONGEI http://www.ongei.gob.pe/bancos/banco_normas/archivos/P01-PCM-ISO17799-001-V2.pdf

ONGEI, NTP ISO/IEC 27001:2014 Recuperado el 22 de 08 del 2017, de ONGEI http://www.ongei.gob.pe/docs/Aprobacion%20NTP%20ISO%20IEC%207001%202014.pdf

Paredes F. Geomayra y Vega N. Mayra (2011), Desarrollo de una metodologia para la auditoria de riesgos informaticos (fisicos y logicos) y su aplicación al departamente de informatica de la direccion provincial de pichincha del consejo de la judicatura. Provincia de Chimborazo, Ecuador, escuela superior Politecnica de Chimborazo.

Pérez Pastor, Múnera Francisco (2007), Reflexiones para implementar un sistema de gestión de la calidad (ISO 9001:2000), en coperativas y empresas de economía solidaria. Editorial Educc, Primera edición, Bogotá, 2007.

Pilla Yanzapanta, J. (2013). Implementacion de seguridad en la red interna de datos para el manejo adecuado de usuarios y acceso remoto en el Intituto Tecnologico Pelileo. Recuperado el 16 de 08 del 2017, de http://repo.uta.edu.ec/handle/123456789/4936

Shannon, Claude Elwood (1948), Teoria matemática de la información. Bell Labs Advances Intelligent Networks.

ANEXOS

BUENAS PRÀCTICAS EN SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO 27002 EN LA ASOCIACIÓN PARA EL DESARROLLO EMPRESARIAL EN APURÍMAC - ADEA