



FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

**AUDITORÍA DE SEGURIDAD DE INFORMACIÓN Y
RIESGOS DE TECNOLOGÍA DE INFORMACIÓN EN UNA
COOPERATIVA DE AHORRO Y CRÉDITO**

**PRESENTADO POR
GUILLERMO JULIO CHERRES JIMÉNEZ**

**TRABAJO DE SUFICIENCIA PROFESIONAL
PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE
COMPUTACIÓN Y SISTEMAS**

LIMA – PERÚ

2020



**Reconocimiento - Compartir igual
CC BY-SA**

El autor permite a otros transformar (traducir, adaptar o compilar) esta obra incluso para propósitos comerciales, siempre que se reconozca la autoría y licencien las nuevas obras bajo idénticos términos.

<http://creativecommons.org/licenses/by-sa/4.0/>



USMP
UNIVERSIDAD DE
SAN MARTÍN DE PORRES

**FACULTAD DE
INGENIERÍA Y ARQUITECTURA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y
SISTEMAS**

**AUDITORÍA DE SEGURIDAD DE INFORMACIÓN Y RIESGOS
DE TECNOLOGÍA DE INFORMACIÓN EN UNA COOPERATIVA
DE AHORRO Y CREDITO**

TRABAJO DE SUFICIENCIA PROFESIONAL

**PARA OPTAR EL TÍTULO DE INGENIERO DE
COMPUTACIÓN Y SISTEMAS**

PRESENTADO POR

CHERRES JIMÉNEZ, GUILLERMO JULIO

LIMA – PERÚ

2020

Agradezco a mi querida esposa María Elena, quien es la persona que me ha motivado constantemente en seguir mejorando, a mi querida hija Vannia motores y alegrías de mi vida diaria. Agradezco también a nuestros profesores por su empeño y dedicación al logro de los objetivos de este informe y porque sabemos que ellos junto con nuestros padres y hermanos nos seguirán ayudando y apoyando siempre que los necesitemos.

RESUMEN

En el presente informe, se desarrolla una auditoría de seguridad de información y un análisis de riesgos de tecnología de información en la Cooperativa de Ahorros y Créditos San Pedro de Andahuaylas, con el fin de evaluar la solidez de los sistemas de control e información, la efectividad y eficiencia de los programas y operaciones y el cumplimiento de los reglamentos y normas ordenadas a la orientación de la seguridad de información. Como resultado se detallan las debilidades encontradas y se proponen recomendaciones que contribuyan a realizar mejoras en la organización de T.I. de la institución.

Para el desarrollo de este informe, se propone un diagnóstico de la seguridad de información y los riesgos de tecnología de información, documentación que es requerida mediante Circular N° G-140-2009-SBS, Circular de Gestión de la Seguridad de la Información- Superintendencia de Banca y Seguros, a las entidades públicas y financieras, las mismas que toman como referencia estándares internacionales como son: ISO 17799 e ISO 27001. Asimismo, cabe resaltar que esta auditoría de la Seguridad de Información y Riesgos, permite la identificación de las debilidades en el manejo de los riesgos y los controles requeridos para reducirlos.

El propósito de identificar las debilidades o deficiencias es poder proponer los controles y mitigaciones necesarias para fortalecer la seguridad da información como resguardar los activos y la información de la institución, tratando de obtener integridad disponibilidad y confidencialidad de los datos, y las responsabilidades que debe arrogarse cada uno de los colaboradores de la institución

ABSTRACT

In this report, an information security audit and an information technology risk analysis are developed in the Cooperativa de Ahorros y Creditos San Pedro de Andahuaylas, in order to evaluate the soundness of the control and information systems, the effectiveness and efficiency of programs and operations and compliance with the regulations and standards ordered to guide information security. As a result, the weaknesses found are detailed and recommendations are proposed that contribute to making improvements in the IT organization. of the institution.

For the development of this report, a diagnosis of information security and information technology risks is proposed, documentation that is required by Circular N ° G-140-2009-SBS, by the Superintendencia de Banca y Seguros, to public and financial entities, the same that take as reference international standards such as: ISO 17799 and ISO 27001. Likewise, it should be noted that this audit of Information Security and Risks, allows the identification of the weaknesses in risk management and the controls required to reduce them.

The purpose of identifying weaknesses or deficiencies is to be able to propose the controls and mitigations necessary to strengthen information security such as safeguarding the assets and information of the institution, trying to obtain integrity, availability and confidentiality of the data, and the responsibilities that must arrogate each one of the institution's collaborators

INTRODUCCION

La Seguridad de la Información como los riesgos de tecnología de información ha cobrado en la actualidad, una importancia en las empresas sobre todo en las financieras; los riesgos y la Seguridad de Información han obtenido gran auge, dadas las actuales nuevas plataformas y condiciones cambiantes computacionales disponibles, situación que nos lleva en la aparición de nuevas amenazas en las estructuras de los sistemas informáticos.

Esto ha llevado a que muchas instituciones hayan podido desarrollar documentos y normas que orientan en el uso correcto de estas tecnologías para obtener el mayor provecho de las ventajas que ofrecen. De esta manera las políticas de Seguridad de Información y Riesgos surgen como un instrumento para concientizar a los miembros de una institución sobre la importancia de la información y servicios críticos que permiten a la organización desarrollarse y mantenerse en su sector de negocio.

En este informe, desarrollo una auditoría de seguridad de información y un análisis de riesgos de tecnología de información en la C.A.C. San Pedro de Andahuaylas, una de las más grandes del país, con el fin de absolver la consistencia de los sistemas de información y de control, la efectividad y eficiencia de los programas y operaciones y el cumplimiento de los

reglamentos y normas prescritas a la orientación de la seguridad de información.

Este informe contiene los siguientes capítulos:

El capítulo I, describe la mi trayectoria profesional, donde enumero y detallo la fecha, el cargo y las actividades realizadas en las empresas donde he aportado mi experiencia hasta la actualidad., siendo la última mi Alma Mater.

El capítulo II, presenta el contexto donde se desarrolló el trabajo de suficiencia profesional motivo de este informe y se describen aspectos principales de la institución como: su organización, organigrama funciones, y puestos ocupados.

El capítulo III, refiere la situación problemática y el plan de solución propuesto, así como la metodología empleada y las actividades propuestas a realizarse, como resultado se puntualizan las debilidades encontradas y se enumeran recomendaciones que puedan servir para realizar mejoras en la organización de T.I. de la institución

El capítulo IV, trata sobre la reflexión crítica de la experiencia profesional, como aportes, el diagnóstico de la administración de riesgos de TI. Finalmente, se enumeran las conclusiones, las recomendaciones y los anexos a este informe

Las políticas de Seguridad de Información y Riesgos establecen los procedimientos y mecanismos que deben acoger las organizaciones para proteger la información y sus sistemas que estos contienen. Estas políticas deben diseñarse para así recoger las características propias de cada organización. Este informe, no pretende detallar los mecanismos de seguridad de la Cooperativa, ni ser un documento legal que sirva para imponer sanciones a malos procedimientos de los colaboradores, es más bien una presentación detallada de lo que como profesionales de sistemas, debemos

asegurar o proteger y en base a estos estándares definir el fundamento del que hacer, es decir; que se puede definir como un documento de referencia o forma de comunicación entre la alta gerencia y los usuarios.

Por lo tanto, el implementar políticas de seguridad en la C.A.C. San Pedro de Andahuaylas, demanda una alta responsabilidad con la institución, experiencia técnica, destreza e ingenio para ubicar defectos y debilidades, y empeño para modernizar y actualizar dichas políticas en función del cambiante ambiente que comprende las instituciones modernas.

INDICE GENERAL

	Pag
RESUMEN	iii
INTRODUCCIÓN	v
CAPÍTULO I. TRAYECTORIA PROFESIONAL	
1.1 Experiencia laboral	1
CAPÍTULO II. CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA	
2.1 Presentación	6
2.2 Misión	
2.3 Visión	7
2.4 Valores	
2.5 Historia	
2.5 Puesto y funciones del cargo	10
CAPÍTULO III. APLICACIÓN PROFESIONAL	
3.1 Auditoria de seguridad de información	12
3.1.1 Situación Problemática	
3.1.2 Proyecto de solución:	14
3.1.2.1 Objetivo General	
3.1.2.2 Objetivos Específicos	
3.1.3 Alcance	
3.1.4 Etapas del Proyecto	15
3.1.5 Normativa	16
3.1.6 Informe de Relevamiento	17
3.1.6.1 Organigrama Institucional	
3.1.6.2 Plan Estratégico de Sistemas	22
3.1.6.3 Controles de Datos Fuentes, de Operación y de Salida	23
3.1.6.4 Mantenimiento de Equipos de Computación	24
3.1.6.5 Seguridad de Programas, de Datos y Equipos de Cómputo	25
3.1.6.6 Plan de Contingencia	27
3.1.6.7 Aplicación de Técnicas Intranet	29

3.1.6.8	Gestión de recursos Humanos: Selección, Evaluación del desempeño, Formación, Promoción y Finalización.	
3.1.6.9	Evaluación de Costos	31
3.1.6.10	Punto de equilibrio	34
3.1.7	Informe de Debilidades y Recomendaciones	35
3.1.7.1	Carencia de Plan de Seguridad de Información (PSI) y de un Plan de Continuidad de Negocio (PCN), dispuesto en la Circular G-140-2009-SBS	
	Recomendación	37
	Formulación del Plan de Seguridad de la Información	38
	Formulación de un Plan de Continuidad de Negocio (PCN)	39
3.1.7.2	Carencia de una metodología de administración de proyectos definidos	41
	Recomendación	42
3.1.7.3	Carencia de un Plan de mantenimiento de equipos a los servidores y equipos de cómputo de la CAC San Pedro de Andahuaylas	43
	Recomendación	44
3.1.7.4	Carencia de aplicativos en áreas específicas que ayuden a la gestión de la Cooperativa de Ahorro y Crédito San Pedro de Andahuaylas	
	Recomendación	46
3.1.7.5	El cableado estructurado deficiente en la CAC San Pedro de Andahuaylas	
	Recomendación	47
3.1.7.6	Falta de formalización e inobservancia de la metodología del ciclo de vida de vida de desarrollo de sistema	48
	Recomendación	49
3.1.7.7	Carencia de una arquitectura tecnológica que interconecte la sede principal con las agencias	50
	Recomendación	51
3.1.7.8	Carencia de procedimientos formales para la verificación de la información respaldada; así como, el estado	

de los dispositivos de seguridad de la sala de servidores	
Recomendación	53
3.1.7.9 Carencia de procedimientos formales para las pruebas y pase a producción de los sistemas de información	
Recomendación	54
3.1.7.10 Deficiente control de las licencias del software instalado	
Recomendación	55
3.2 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN	56
3.2.1 Introducción	
3.2.2 Objetivo y alcance del trabajo	
3.2.3 Procedimientos	58
3.2.4 Diagnóstico	59
CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA	
4.1 Experiencia durante el periodo laboral en la CAC San Pedro de Andahuaylas.	77
4.2 Herramientas utilizadas	78
4.3 Importancia de habilidades adicionales a formación profesional	79
4.4 Importancia del conocimiento y capacitación	80
CONCLUSIONES	81
RECOMENDACIONES	91
ANEXOS	97
FUENTES DE CONSULTA	264

INDICE DE GRAFICOS

FIGURAS

	Pag.
Figura N° 1 Organigrama de la C:A:C: San Pedro de Andahuaylas	18
Figura N° 2 Punto de Equilibrio: Costo/Seguridad/Riesgo	34
Figura N° 3 Estructura Organizacional Para la Administración de Riesgos de Tecnología De Información	59
Figura N° 4 PLAN DE SEGURIDAD DE LA INFORMACIÓN	60
Figura N° 5 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD	60
Figura N° 6 SEGURIDAD LÓGICA	61
Figura N° 7 SEGURIDAD DE PERSONAL	61
Figura N° 8 SEGURIDAD FÍSICA Y AMBIENTAL	62
Figura N° 9 CLASIFICACIÓN DE SEGURIDAD	63
Figura N° 10 ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES	64
Figura N° 11 DESARROLLO Y MANTENIMIENTO	67
Figura N° 12 PROCEDIMIENTOS DE RESPALDO	69
Figura N° 13 PLANEAMIENTO PARA LA CONTINUIDAD DEL NEGOCIO	70
Figura N° 14 CRITERIOS PARA EL DISEÑO E IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIOS	72
Figura N° 15 PRUEBA DEL PLAN DE CONTINUIDAD DE NEGOCIO	73
Figura N° 16 SUBCONTRATACIÓN	74
Figura N° 17 CUMPLIMIENTO NORMATIVO	75
Figura N° 18 PRIVACIDAD DE LA INFORMACIÓN	75
Figura N° 19 AUDITORÍA INTERNA Y EXTERNA	76

TABLAS

Tabla N° 1: Servidores CAC San Pedro	26
Tabla N° 2: Desktops CAC San Pedro	26
Tabla N° 3: Impresoras CAC San Pedro	27
Tabla N° 4: Sub Plan de adecuación para la administración de riesgos de tecnología de información	35
Tabla N° 5: Descripción de los gráficos de la evaluación y análisis	60
Tabla N° 6: Nivel mínimo de riesgos posibles	83

CAPÍTULO I

TRAYECTORIA PROFESIONAL

EXPERIENCIA LABORAL

USMP

Marzo 2017-Mayo 2019

Facultad de Ciencias de la Comunicación Turismo y Psicología

Encargado de la Medición de la Calidad Educativa - Unidad de Acreditación y Calidad

- Responsable de la Planificación de la medición de la calidad (satisfacción alumnos, docentes y administrativos de las Escuelas profesionales de Ciencias de la Comunicación, Turismo y Hotelería y Psicología)
- Responsable de la ejecución de la evaluación docente. (Escuelas profesionales de Ciencias de la Comunicación, Turismo y Hotelería y Psicología)
- Diseñe e implemente el Aula Virtual de Acreditación, para la capacitación docente de la Facultad de Ciencias de la Comunicación, Turismo y Psicología.
- Diseñe, implemente y Presentación ante las autoridades de la Facultad de Ciencias de la Comunicación Turismo y Psicología la Plataforma de Seguimiento y Avance del proceso de autoevaluación, como complemento al Sistema de Gestión de la Calidad.
- Implementé los requerimientos institucionales de desarrollo y mantenimiento de sistemas de información, (Plataforma de Plan de Desarrollo Docente 2018-2021 y Curriculum Vitae docente 2018-2019).

- Diseño e implementación de plataformas para consolidar la información (evidencias) para las diversas acreditadoras. (ACSUG, TECQUAL)

Logros:

- Cree el Aula virtual lo que permitió pasar del 40% a 70% de docentes capacitados en la facultad.
- Cree la Plataforma de Seguimiento del Sistema de Gestión de la Calidad, donde se puede obtener las evidencias, informes, estadísticas para las diversas acreditaciones de la facultad.
- Innove el desarrollo de nuevos informes con indicadores del sistema de gestión de calidad.

USMP

Marzo 2015-Noviembre 2015

Facultad de Ciencias de la Comunicación Turismo y Psicología

Docente del curso de Estadística – Escuela de Ciencias de la Comunicación

- Docente del curso de Estadística

Logros:

- Capacite al 75% los docentes de la Escuela en Estadística para la obtención de sus grados de magister.
- Obtención de calificación Muy Bueno en la evaluación docente 2015-II

CORPORACION SYMTECH SAC

Enero 2012 -Mayo 2015

- Colaboración con las municipalidades en definir los objetivos del proyecto.
- Asesoramiento estadísticamente a Municipios de las provincias de Andahuaylas y Chincheros, Región Apurímac.
- Orientación y coordinación de todos los recursos empleados en el proyecto
- Planificación del proyecto en todos sus aspectos, los recursos a poner en juego, identificando las actividades a realizar, costos previstos y los plazos de ejecución
- Mantenimiento intacto de las relaciones con los pobladores.

Logros:

- Desarrolle Proyectos de inversión en el tema de Plantas de tratamiento de aguas (servida y potable), en la provincia de Andahuaylas, Región Apurímac.

**Escuela Europea de Negocios
Febrero 2009 – Diciembre 2011**

Administrador de la Sede Latinoamérica.

- Encargado de representar a la Sede Principal de España ante las actividades a llevarse a cabo en las sedes de Latinoamérica: Bolivia, Colombia, Argentina y Perú. Adicionalmente, con las sedes de Latinoamérica tuve el encargo de desarrollar y mantener un fluido contacto con todas ellas.

Logros:

- Elaboración y aplicación del Plan de Mercadeo 2010-2011. La Paz, Bolivia 2009
- Entrada al mercado Peruano.

**Cooperativa de Ahorro y Crédito San Pedro
Enero 1995 - Agosto 2008**

Administrador de la Agencia Lima

Marzo 2006 - Agosto 2008

- Representante legal y Administrador de la Agencia y oficinas en el departamento de Lima

Logros:

- Cumplí con el objetivo de llegar al punto de equilibrio en el tiempo propuesto.
- Implementé y aperturé 4 oficinas en Lima y selección de 35 colaboradores para las mismas.
- Participé en la elaboración del Plan Estratégico institucional 2007-2011.
- Elaboré y ejecute los planes operativos de la Agencia Lima los años 2007 y 2008 de la Agencia Lima.
- Diseñe los planes de publicidad para la agencia Lima y sus oficinas.

Jefe de Sistemas

Enero 1995 - Marzo 2006

- Encargado de toda el área de sistemas de la sede principal y agencias (Lima, Cusco, Apurímac) y oficinas.

Logros:

- Implemente (Sistemas, seguridad y otros) de todas las agencias y oficinas de la C.A.C. San Pedro de Andahuaylas en este periodo.
- Implemente nuevas tecnologías y sistemas de información durante mi periodo.
- Implementación de las redes informáticas en la agencia principal, agencias y oficinas(Apurímac, Cusco y Lima)

CONGRESO DE LA REPUBLICA

Octubre 1994 – Junio 2000

Asesor Técnico.

- Encargado de coordinaciones informáticas con el departamento de Cerro de Pasco.
- Representante del congreso ante más de 300 personas capacitaciones diversas.
- Coordinaciones con diversas oficinas gubernamentales: Equipamiento, Infraestructura, comunicaciones, etc.
- Aspectos de Auditoria y Seguridad de Sistemas de Cómputo.
- Verificaciones de Planes de Pruebas, Contingencia.

Logros:

- Auditoria de los sistemas informático del Jurado Electoral en Cerro de Pasco
- Coordinación con las diversas autoridades de la Sub Región Pasco del Desarrollo de las elecciones presidenciales 1995

IDIOMAS

Inglés: Nivel Intermedio

MANEJO DE SOFTWARE

- SPSS
- Moodle
- Office Nivel Avanzado
- Programas de diseño
- Programas de base de datos
- Lenguajes de programación

ORGANIZACIONES, ASOCIACIONES Y SOCIEDADES

2010 Presidente de la Asociación de Tiro Santiago de Surco 266.

2011 Presidente de la Asociación Nacional de Tiro Defensivo - IDPA del Perú.

2017 Presidente de la Dirección Nacional de sociedades de Tiro.

ULTIMAS CAPACITACIONES

- Seminario de capacitación calidad educativa. ACSUG. Abril 2019
- Programa de formación formativa. USMP. Noviembre 2019
- Seminario taller didáctica y evaluación basados en el enfoque por competencias. USMP. Marzo 2018
- Curso: Gestión de Procesos Administrativos. Telefónica USMP. Octubre 2017

MENCIONES

1995 Huésped Ilustre del Departamento de Cerro de Pasco

2007 Mención de felicitación por superar el punto de quiebre, Dic 2006.

2006 Premio Empresa Peruana del Año 2006
2006 Medalla de Oro Empresa Peruana del Año
2006 Master en Liderazgo Empresarial. Premio otorgado a la
capacidad profesional y gestión de excelencia

CAPÍTULO II

CONTEXTO EN EL QUE SE DESARROLLO LA EXPERIENCIA

2.1 PRESENTACIÓN

Fundada un 20 de noviembre de 1960, por un grupo de ilustres ciudadanos de la Provincia de Andahuaylas, la misma que buscó aliviar las necesidades de la una población dispuesta a orientarse a un crecimiento, inicialmente fue conformada con 123 socios y desde un inicio su estructura fue basada en los principios cooperativos que nos rigen.

Durante la crisis financiera que sufrió el país durante la década de los ochenta y posteriormente a la de los noventas estuvo a punto de ser cerrada y gracias a la intervención de sus funcionarios, logro recuperar e iniciar una política de crecimiento que en la actualidad cuenta con mas de 60 mil asociados, ser la institución financiera líder en el mercado regional y contar con presencia en la Región de Cusco y en la ciudad capital Lima.

Dentro del Departamento de Apurimac, la Cooperativa San Pedro es la institución financiera con mayor participación del mercado tanto en sus productos pasivos como activos, cuenta con recursos humanos de diferentes especialidades que contribuyen al desarrollo sostenido de la organización.

Desde Julio del año 1998 se viene otorgando créditos a los sectores rurales mas necesitados por medio de un producto financiero denominado Grupos Solidarios, el cual a la fecha representa más del 70% de las colocaciones de la organización.

2.2 MISIÓN

“Somos una cooperativa de ahorro y crédito de espíritu solidario, que brinda servicios financieros y no financieros de calidad, contribuyendo a mejorar el nivel de vida de cada uno de sus socios y la comunidad”.

2.3 VISIÓN

“Ser una cooperativa de ahorro y crédito sólida y líder del sector cooperativo a mediano plazo, brindando productos y servicios diferenciados, mediante tecnología y el conocimiento extensivo de las necesidades de sus socios, basados en la excelencia y los valores cooperativos”.

2.4 VALORES

1. Solidaridad.
2. Respeto.
3. Honestidad.
4. Responsabilidad.
5. Confianza.
6. Democracia.

2.5 HISTORIA

A inicios de 1960, la provincia de Andahuaylas, en el departamento de Apurímac, era una ciudad pequeña, de mucha pobreza que se dedicaba principalmente a la agricultura y a la ganadería que era promovida en ese

momento por los hacendados de la zona. Es también en ese año que surge la idea de formar una Cooperativa de Ahorro y Crédito, con la finalidad de llenar un vacío muy sentido: satisfacer las necesidades y aspiraciones económicas, sociales y culturales de la población, mediante una empresa de propiedad conjunta y de gestión democrática sin fines de lucro.

En esos días acababa de llegar de los Estados Unidos el Padre Joseph Martin Cummins, para encargarse de la parroquia San Pedro de Andahuaylas, quien conocía al economista Aquiles Lanao Flores que había fundado otras cooperativas en el interior del Perú y quien fue invitado a la provincia de Andahuaylas, para apoyarlos en fundar una Cooperativa.

Fue a los 20 días del mes de noviembre de 1960 que se reunieron 72 notables ciudadanos del distrito de Andahuaylas, provincia de Andahuaylas, departamento de Apurímac, en una asamblea en donde el Economista Lanao Flores, dio a conocer la finalidad de contar con una cooperativa de Ahorro y Crédito, los beneficios que tendría para los asociados y la ayuda que el Gobierno brinda a ese tipo de asociaciones.

Acto seguido, se nombró un secretario para esta asamblea quien dio lectura al que sería el estatuto de la Cooperativa, que después de ser debatido, artículo por artículo, finalmente, fueron aceptados por unanimidad.

A continuación, se procedió en votación secreta, de acuerdo con los Estatutos, a la elección de los miembros de los órganos de gobierno, como son: Consejo de Administración, Consejo de Vigilancia y Comité de Crédito. A continuación, se procedió con la elección de los suplentes de los consejos, con el siguiente resultado:

Para el Consejo de Administración:

Miembros titulares:

Sr. Lázaro Carrillo Meneses.
R.P. Jhosep Martín Cummins.
Sra. Nataniel Hermoza Guzmán.
Sra. Amelia Munares Tapia.
Sr. Javier Urquizo Vargas.
Sr. Luis Cueto Aragón.
Sra. Carmen León de Ligarda.

Para el Consejo de Vigilancia:
Miembros titulares:

Sra. Dora de Colunge.
Sr. Milciades Montoya Obregón.
Sr. Efraín Zevallos Ipenza.
Sra. Ceida Ligarda de Carrasco.

Para el Comité de Crédito.
Miembros titulares:

Sra. Noemí Zúñiga Trelles.
Sr. Enrique Alarcón Sosa.
Sra. Emma Ipenza de Barrios.

Uno de los principales acuerdos fue el contar con un aporte mínimo, la cantidad de S/.20.00 (Veinte Soles Oro). Iniciando la cooperativa con un capital social de S/. 42,810.00 (Cuarenta y dos mil ochocientos diez Soles Oro).

Ya como asamblea general de socios, esta procedió a autorizar al, Sacerdote Joseph Martín Cummins, para que proceda a realizar la inscripción de los aportes de los socios fundadores, suma que ascendía a S/. 40,490.00

(Cuarenta mil cuatrocientos noventa Soles Oro). Monto que se tomaría como referencia para iniciar sus actividades la CAC. San Pedro de Andahuaylas.

Ya, con los Estatutos aceptados, los socios fundadores acordaron en desembolsar el valor de las Letras de Aportaciones que les correspondió reconocer y cumplir.

Finalmente, la asamblea general de socios aprobó el afiliarse FENACREP (Federación Nacional de Cooperativas de Crédito del Perú) y firmar el contrato de seguro, con fecha 1 de diciembre de 1960.

2.5 PUESTO Y FUNCIONES DEL CARGO

Mi experiencia en la Cooperativa San Pedro de Andahuaylas fue por decir lo menos, fructífera, cuando llegue a ella la Cooperativa ocupaba solo un piso de un edificio de tres pisos y solo tenía 4 trabajadores y recién se implementaban el sistema de información financiero contable. Al finalizar mi periodo teníamos 4 edificios propios (Andahuaylas, Abancay, Uripa y Cusco) otras 7 oficinas más en estos mismos departamentos, además de una agencia en Lima y contábamos ya con más de 250 colaboradores, estando yo a cargo de 40 de ello como administrador de la Agencia Lima con 4 oficinas adicionales. El puesto que desempeñé para este informe en particular para fue el de asesor externo del Gerente General para realizar una auditoría seguridad de información y un análisis de riesgos de tecnología de información, con el fin de evaluar la solidez de los sistemas de información y de control, la efectividad y eficiencia de los programas y operaciones y el cumplimiento de los reglamentos y normas ordenadas a la orientación de la seguridad de información. Mis funciones fueron las siguientes:

1. Identificar, desarrollar, documentar y sugerir políticas, normas y procesos escritos sobre:
 - a. La protección y conservación de la Seguridad lógica
 - b. La protección y conservación de la Seguridad de personal
 - c. La protección y conservación de la Seguridad física y ambiental
 - d. Descripción de activos y clasificación de la información.

- e. Administración de las operaciones y comunicaciones.
 - f. Adquisición, desarrollo y mantenimiento de plataformas informáticas.
 - g. Administrar los procedimientos de respaldo.
 - h. Administrar la gestión de incidentes de seguridad de información.
 - i. Verificar el cumplimiento normativo.
 - j. Verificar la privacidad de la información.
2. Detallar las debilidades encontradas.
 3. Emitir recomendaciones que contribuyan a una oportunidad de mejoras en la organización de T.I. de la institución.
 4. En base al marco legal de la Cooperativa, presentar al Gerente propuesta de Manuales de Procesos conteniendo normas, políticas y procedimientos escritos para asegurar la seguridad de la información.
 5. Elaborar informes y asistir a reuniones de trabajo.
 6. Realizar otras funciones afines al cargo que el Gerente General asignara.

CAPÍTULO III

APLICACIÓN PROFESIONAL

3.1 AUDITORIA SEGURIDAD DE INFORMACION

3.1.1 SITUACION PROBLEMÁTICA

La Cooperativa de Aorro y Crédito San Pedro de Andahuaylas (C.A.C. San Pedro de Andahuaylas), es una entidad financiera, inaugurada en 1960, con su sede principal en Andahuaylas la cual establece las políticas de la institución y lineamientos generales en la estructura organizacional, cultura, gobierno, operaciones, reportes, entre las más importantes, y con oficinas en Abancay, Uripa, Curahuasi Cusco, Ayacucho y Lima, a lo largo de estos años se ha tenido cambios en el sector y el marco regulatorio de la misma a través de la Federación Nacional de Cooperativas de Ahorro y Crédito del Perú (FENACREP). El considerable crecimiento de la C.A.C. San Pedro de Andahuaylas, hecho ocurrido principalmente a partir del año 1993 en que se reduce drásticamente la actividad terrorista en la zona sur del Perú, en especial de Apurímac, y ante la falta de entidades financieras –bancos Principalmente- que apoyen con financiamiento a los pobladores de la zona representada en un primer momento por comerciantes, agricultores y ganaderos en su mayoría, ayudó en el incremento de las actividades de ahorro y crédito, convirtiéndola por muchos años en la principal institución crediticia en Apurímac, pero que, denota -incluso en la actualidad- un incremento en la complejidad de su organización administrativa, tanto desde las áreas directivas, gerenciales, así como en las áreas operativas.

Esta complejidad recae en gran medida en el área de sistemas en el que los controles han venido a menos, principalmente por los cambios de personal con poca experiencia en el área, políticas de seguridad desactualizadas y un incremento de los riesgos están aumentando en las organizaciones. Adicionalmente, en estos 20 años de crecimiento, nunca se ha hecho una auditoría de Seguridad de Información y Riesgos de Tecnología de Información, se trabaja bajo normas dictadas hace años. Es por eso que se hace necesario realizar una auditoría de seguridad de información y un análisis de riesgos de tecnología de información, con el fin de evaluar la solidez de los sistemas de información y de control, la efectividad y eficiencia de los programas y operaciones y el cumplimiento de los reglamentos y normas ordenadas a la orientación de la seguridad de información. Como resultado se detallarán las debilidades encontradas y se formularán recomendaciones que contribuyan a una oportunidad de mejoras en la organización de T.I. de la institución.

A través de este informe, deseamos Identificar, desarrollar, documentar y sugerir políticas, normas y procesos escritos sobre:

La protección y conservación de la Seguridad lógica

- a. La protección y conservación de la Seguridad de personal
- b. La protección y conservación de la Seguridad física y ambiental
- c. Inventario de activos y clasificación de la información.
- d. Administración de las operaciones y comunicaciones.
- e. Adquisición, desarrollo y mantenimiento de plataformas informáticas.
- f. Administrar los procedimientos de respaldo.
- g. Administrar la gestión de incidentes de seguridad de información.
- h. Verificar el cumplimiento normativo.
- i. Verificar la privacidad de la información.

Con el fin de:

1. Detallar las debilidades encontradas.
2. Emitir recomendaciones que contribuyan a una oportunidad de mejoras en la organización de T.I. de la institución.
3. En base al marco legal de la Cooperativa, someter al Gerente propuesta de Manuales de Procesos conteniendo políticas, normas y procedimientos escritos para asegurar la seguridad de la información.

3.1.2 PROYECTO DE SOLUCION

3.1.2.1 OBJETIVO GENERAL

Elaborar un diagnóstico de la seguridad de información y los riesgos de tecnología de información, implementados mediante Circular N° G-140-2009-SBS, Circular de Gestión de la Seguridad de la Información- Superintendencia de Banca y Seguros, basados en los estándares internacionales ISO 27001 e ISO 17799

3.1.2.2 OBJETIVOS ESPECÍFICOS

1. Identificar las debilidades o deficiencias de la información y los activos de la organización en base a la Circular N° G-140-2009-SBS.
2. Establecer en las principales operaciones, el grado de seguridad, en base a la Circular N° G-140-2009-SBS.
3. Determinar el nivel de cumplimiento de las Normas Técnicas de Control Interno para los Sistemas Informáticos, en base a la Circular N° G-140-2009-SBS.
4. Proponer los controles y mitigaciones necesarias para fortalecer la seguridad da información para asegurar la información y los activos de la institución.

3.1.3 ALCANCE

Nuestro examen se realizó en cumplimiento a las Normas de Auditoría Gubernamental y comprendió la evaluación de la Unidad de Sistemas, en el período comprendido entre el 12-01-2015 al 18-04-2016.

Para tal efecto, se verificó el grado de servicio por parte de la Unidad de Sistemas que reciben los principales usuarios de la institución; se examinó el funcionamiento y operación del software SICAC PLUS en la atención al público; se realizaron pruebas a las bases de datos mediante software de auditoría y se examinó la organización y funcionamiento de la Unidad de Sistemas.

3.1.4 ETAPAS DEL PROYECTO

Las etapas o metodología utilizada para la ejecución de la presente Auditoría de Seguridad de Información se basan en la identificación y desarrollo de las siguientes tareas:

- a. Definir los objetivos de la auditoría y demarcación del alcance **(ver Anexo 1)**.
- b. Análisis del origen de la información (datos) y recopilación de información **(ver Anexo 2)**.
- c. Creación y difusión del plan de trabajo, definición de recursos y plantear tiempos de ejecución **(ver Anexo 3)**.
- d. Creación y puesta en marcha de cuestionarios y sus adecuaciones a ser desarrolladas por el área de TI y Gerencias basándose en los perfiles de los entrevistados **(ver Anexo 4)**.
- e. Proceso de Relevamiento:
 - e.i. Entrevistas:
 - Alta dirección: Gerentes de órgano de línea
 - Responsable de la Unidad de Sistemas: Jefe
 - Personal de sistemas: Asistente, programadores, administradores de red

- Usuarios del sistema: colaboradores del área administrativa y operativa.
- e.ii. Reunir documentación de la organización
 - e.iii. Reconocimiento del entorno y ámbito del desarrollo del trabajo
 - f. Análisis de los datos encontrados, hallazgos de debilidades y planteamiento de recomendaciones.
 - g. Plantear el desarrollo de un análisis de riesgos (**ver Anexo 5**).
 - h. Discusión de resultados
 - i. Elaboración de conclusiones
 - j. Presentación del informe definitivo a los directivos y alta gerencia de la institución.

3.1.5 NORMATIVA

Para la elaboración de la presente auditoría de seguridad de información se utilizarán las siguientes normas:

1. Normas de Auditoría Gubernamental, aceptadas por la Contraloría General de la Republica, mediante Resolución N° 162-95 del 22.Set.95 y
2. Normas Sustitutorias contenidas en la Resolución N° 141-99 CG del 25.Nov.99; así como,
 - a) Normas Técnicas de Control Interno para el Sector Público;
 - b) Directivas, Circulares y Memos Múltiples emitidos por las áreas involucradas internas y externas.
3. Circular N° G-139-2009-SBS, sobre Gestión de la continuidad del Negocio de la Superintendencia de Banca y Seguros (**Ver Anexo 6**).
4. Circular N° G-140-2009-SBS, sobre Gestión de la seguridad de la Información de la Superintendencia de Banca y Seguros (**Ver Anexo 6**).
5. Compendio de Normas Técnicas Informáticas del INEI (Instituto Nacional de Estadística e Informática):

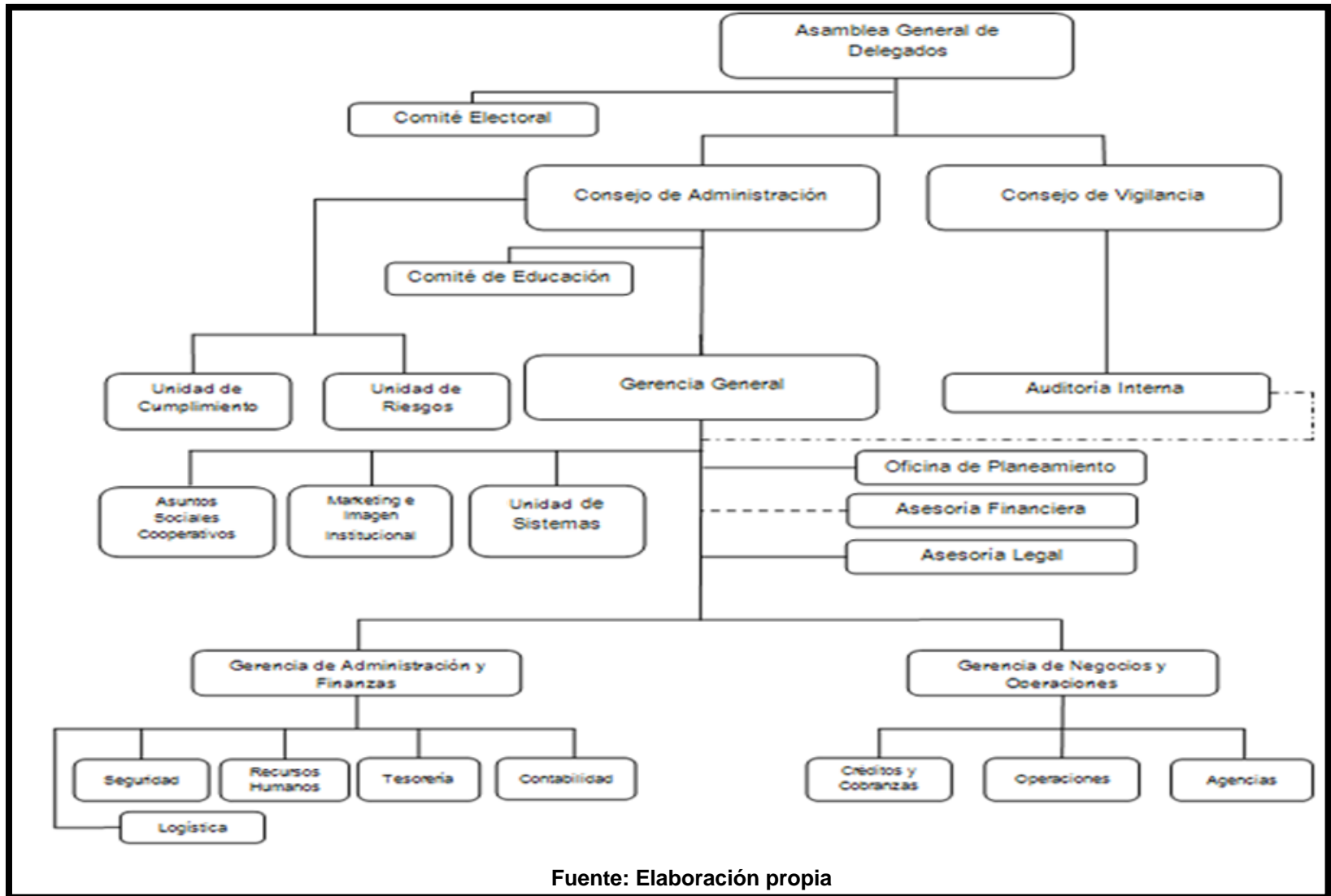
- a. Normas técnicas para el almacenamiento y respaldo de la información que se procesa en las entidades del Estado. Resolución Jefatural N° 340-94-INEI
- b. Normas para la prevención, detección y eliminación de Virus Informáticos en los equipos de cómputo de la Administración Pública. Resolución Jefatural N° 362-94-INEI
- c. Recomendaciones técnicas para la seguridad e integridad de la información que se procesa en la Administración Pública. Resolución Jefatural N° 076-95-INEI.
- d. Recomendaciones técnicas para la protección física de los equipos y medios de procesamiento de la información en la Administración Pública. Resolución Jefatural N° 090-95-INEI.
- e. Recomendaciones técnicas para la organización y gestión de los servicios informáticos en la Administración Pública. Resolución Jefatural N° 140-95-INEI.
- f. Recomendaciones técnicas para la elaboración de planes de sistemas información en la Administración Pública. Resolución Jefatural N° 229-95-INEI.

3.1.6 INFORME DE RELEVAMIENTO

A continuación, se describe la información recogida durante el relevamiento realizado a la C.A.C. San Pedro de Andahuaylas, detallando a su vez cada uno de los exámenes que se implementan en la actualidad.

3.1.6.1 ORGANIGRAMA INSTITUCIONAL

Figura N° 1: Organigrama C:A:C: San Pedro de Andahuaylas



Fuente: Elaboración propia

UNIDAD DE SISTEMAS

Órgano de Apoyo responsable de administrar el flujo de información, el procesamiento de datos, el mantenimiento de software y hardware y las copias de seguridad de la información financiera, esta unidad orgánica cuenta con los siguientes cargos:

Cuadro de Distribución de Recursos Humanos

Número Orden	Código de Cargo	Cargo Estructural	Cargo Funcional
007	US-1F3	Jefe de Unidad de Sistemas	Jefe de Sistemas
008	US-2E2	Operador de Sistemas	Operador

Descripción de Cargo

Código de Cargo : US-1F3
Cargo Estructural : **Jefe de Unidad de Sistemas**
Cargo Funcional : Jefe de Sistemas
Número de cargos : 01

Dependencia Funcional

Depende de : Gerente General
Ejerce Autoridad sobre : Operador de Sistemas

Condiciones del Cargo : Funcionario Nivel 3

Requisitos Mínimos del Cargo

- Título profesional de Ingeniero de Sistemas e Informática y/o carreras afines.
- Experiencia en cargos similares no menor a tres años.
- No contar con referencias crediticias negativas en el sistema financiero.
- No contar con antecedentes penales, judiciales ni policiales.
- Buenas reseñas personales y profesionales.

Descripción del Cargo

El Jefe de la Unidad de Sistemas es el funcionario responsable del correcto funcionamiento del Hardware y el Software de la Cooperativa y tiene como principales funciones:

- a) Administración de los Servidores de Datos, Comunicaciones, Web, Correo, FTP y HTTP.
- b) Administrar y controlar las actividades diarias de procesamiento de información.
- c) Administrar el servicio de interconexión entre oficinas.
- d) Dar mantenimiento a la Página Web de la Cooperativa.
- e) Brindar soporte informático de software y hardware.
- f) Brindar asesoramiento en el proceso de innovación de nuevas tecnologías con el propósito de mejorar la calidad de atención a los socios de la Cooperativa.
- g) Capacitar al personal operativo de la Cooperativa en asuntos concernientes al manejo de los Aplicativos Informáticos.
- h) Velar por el correcto funcionamiento de los equipos informáticos propiedad de la Cooperativa.
- i) Velar por el correcto cuidado y almacenamiento de las copias de seguridad del Aplicativo Informático Financiero de la Cooperativa.

- j) Formular el Plan Anual de mantenimiento preventivo y correctivo de equipos de Procesamiento Automatizado de Datos.
- k) Formular el Plan Anual de Adquisiciones de Equipos de Informática acorde a la necesidad de la institución.
- l) Implementar planes integrales de seguridad y contingencia a nivel de los sistemas informáticos.
- m) Elaborar y Desarrollar Sistemas Complementarios al Aplicativo Informático Financiero.
- n) Otras funciones que le asigne el Gerente General.

Descripción de Cargo

Código de Cargo : US-2E2
 Cargo Estructural : **Operador de Sistemas**
 Cargo Funcional : Operador
 Número de cargos : 01

Dependencia Funcional

Depende de : Gerente General
 Jefe de la Unidad de Sistemas

Condiciones del Cargo : Empleado Nivel 2

Requisitos Mínimos del Cargo

- Egresado de Instituto Superior de Prestigio
- No contar con referencias crediticias negativas en el sistema financiero.
- No contar con antecedentes penales, judiciales ni policiales.
- Buenas reseñas personales y profesionales.

Descripción del Cargo

El operador de Sistemas es el soporte de Hardware y el Software con el que cuenta el Jefe de la Unidad de Sistemas y tiene como principales funciones:

- a) Realizar el Backup diario de las operaciones en la Oficina principal y coordinar dicha actividad con las diferentes Agencias u Oficinas de Enlace e Información que tuviere la Cooperativa.
- b) Es Responsable del cableado estructurado de la Oficina Principal y de las Agencias u Oficinas de Enlace e Información que tuviere la Cooperativa.
- c) Brindar el Soporte Técnico – Administrativo al Jefe de la Unidad de Sistemas en labores de trámites técnico – administrativos para acciones dentro y fuera de la Cooperativa.
- d) Apoyo en el mantenimiento y operación de la Página Web que cuenta la Cooperativa.
- e) Brindar soporte general en Hardware y Software a los clientes internos de la Cooperativa.
- f) Velar por el adecuado almacenamiento y conservación de los backups del aplicativo informático de la Cooperativa.
- g) Otras funciones que le asigne el Gerente y General y/o el Jefe de la Unidad de Sistemas.

3.1.6.2 PLAN ESTRATÉGICO DE SISTEMAS

Actualmente no se evidencia la existencia de un Plan de TI / SI, existiendo sí esfuerzos aislados, expresados a modo de “proyectos” aunque sin llegar a constituirse en tales por falta de aplicación de una metodología de desarrollo de proyectos, y por falta de una visión que permita integrar todos estos esfuerzos a un objetivo común, con estrategias a su vez integradas.

Es así que un Plan de Tecnologías de Información o de Sistemas debe contener como mínimo lo siguiente:

- Análisis del escenario actual informático con el fin de saber las capacidades actuales de la empresa.
- Elaboración de objetivos y estrategias del sistema informático que sirva para definir la misión y los objetivos de la empresa
- Desarrollo del modelamiento de datos para determinar qué información es necesaria para la empresa.
- Concepción, ordenamiento y priorización (según importancia e inversión) sistemática de los planes informáticos.
- Programación de fechas para la puesta en marcha de los proyectos o planes designados, considerando el periodo de vida de cada proyecto.

Se debe dar prioridad a la elaboración de un Plan Estratégico de Sistemas que ayude a lograr los objetivos de la institución, por lo que se pudo comprobar que la carencia de ese documento no ha permitido un crecimiento planificado y ordenado de la arquitectura informática que apoya los diferentes procesos de esta organización.

3.1.6.3 CONTROLES DE DATOS FUENTE, DE OPERACIÓN Y DE SALIDA (FUNCIÓN APLICATIVOS)

En la revisión de la funcionalidad de los sistemas se pudo observar que existe un solo aplicativo llamado SICAC PLUS, pero que con la necesidad del servicio se le han desarrollado diversos módulos, situación que no mejora el servicio informático prestado por esta área.

Asimismo, para ejecutar la implementación de los controles de datos fuente, es necesario que la cooperativa defina, quienes serán los responsables o encargados de salvaguardar los datos. Sin embargo no cuentan con políticas que definan claves de acceso. Cabe resaltar que para la creación de usuarios, el Área de RR. HH. toma sus datos, dando de alta su usuario o ID, sin embargo, no existe un procedimiento específico realizar estas acciones. Si este usuario necesita hacer uso de otro recurso del sistema de información, el área de RR. HH. hace el

requerimiento a la Unidad de Sistemas, donde se genera la aceptación o alta del usuario al sistema.

En el caso de dar de baja a la cuenta del usuario, esta es deshabilita, de esta forma los datos de las cuentas deshabilitadas quedan almacenadas en los backups y en el disco, no siendo posible repetir los ID's de usuarios anteriores para nuevos colaboradores.

No hay ninguna regla formal para dar de baja un usuario del sistema de información. El área de RR. HH. informará a la Unidad de Sistemas, del corte de al acceso, siendo allí donde se procede a dar de baja al colaborador una vez que se ha desligado de la institución.

La Unidad de Sistemas cuenta con los programas fuentes del SICAC PLUS pero dicho aplicativo trabaja en un ambiente Visual, el mismo que trabaja con DBF, situación que no garantiza la integridad de la información haciéndola débil y vulnerable.

En la transferencia de la información del SICAC PLUS, desde la sede central y las agencias esta se efectúa mediante un traslado físico de medios magnéticos (discos flexibles) también utilizan el correo electrónico (público), en ese caso dicha información no está encriptada lo que genera una debilidad en la seguridad, ya que podría ser vulnerable.

Para los controles de salida, se cuenta con la política de generación de backups por medio de cd's pero no cuentan con controles internos y externos que garanticen el resguardo adecuado para estos medios de almacenamiento.

3.1.6.4 MANTENIMIENTO DE EQUIPOS DE COMPUTO

En la revisión de las políticas de mantenimiento de equipos de cómputo y comunicaciones de la entidad se pudo apreciar que no

cuentan con políticas definidas de mantenimiento preventivo ni correctivo, solo se encontró un documento que menciona la realización de dichos mantenimientos, estableciendo dos fechas: a inicios del año y a mediados del año 2013, las cuales solo se cumplió la primera en las agencias que se muestran mediante informe, de fecha 14 de Febrero del 2014, dirigido al Jefe de la Unidad de Sistemas por el Auxiliar de sistemas, donde indica la realización de este mantenimiento solo en algunas agencias, pero no se encontró evidencia de hacerse realizado dicho mantenimiento en la Sede Principal.

Dicha situación pone en riesgo no solo la inversión en la adquisición de estos equipos, sino que pone en riesgo a la institución a un colapso de los servicios informáticos y sus consecuentes repercusiones.

3.1.6.5 SEGURIDAD EN LOS PROGRAMAS, EN LA DATA Y EN LOS EQUIPOS DE CÓMPUTO

En las visitas de inspección realizadas al ambiente de trabajo de la Unidad de Sistemas se pudo observar que no cuenta con una infraestructura adecuada, debido a que todas las funciones de esta área se realizan en un mismo ambiente, el mismo que cuenta con un espacio bastante reducido.

No hay restricciones para entrar a dicha área, es decir no está prohibido el acceso a personal no autorizado, por lo que se expone la seguridad de los equipos y de la información. Asimismo se visualizan los cables de conexión de las estaciones. En consecuencia, es un ambiente en condiciones no adecuadas para albergar equipos de cómputo y personal. Asimismo no posee puertas de escape, ni extintores y existen materiales altamente combustibles.

En relación con los backups, cuentan con políticas de backups diarios realizados por medio de cd's. Estos son realizados diariamente pero no se lleva un control externo ni interno de la información procesada, ocasionando un desorden en la ubicación de la información.

En las agencias el procedimiento para la obtención de backups es el mismo al de la sede principal, pero asimismo tiene las mismas

inexistencias de controles. Para el almacenamiento y resguardo de los backups, estos se realizan en la misma institución, pero se ha observado que estos se encuentran en un lugar no adecuado para su manutención, lo que no garantiza la seguridad de la información, ya que está propenso a cualquier tipo de desastres.

Servidores:

TABLA N° 1 Servidores

Modelo de PC	Procesador	N° de PC's
HP PROLIANT ML110 GEN9	Intel® Xeon® E5-2600 v3	05
DELL POWER EDGE T20	Intel Xeon E3-1225 v3, 3.2 GHz	02

Fuente: Elaboración propia

Desktops:

TABLA N° 2 : Desktops

Modelo de PC	Procesador	N° de PC's
HP 8200 Elite	Core i5 2400M 3.1Ghz	12
HP 6200pro	Intel Core i3 -2100 (3.1Ghz)	37
DELL OPTIPLEX 790	Intel Core i3 - 2100 de 3.1Ghz	28

Fuente: Elaboración propia

Impresoras:

TABLA N° 3 : Impresoras

Modelo de PC	Tecnología	Impresión en color	Nº de Unidades
Epson TM-T88V	Térmica	NO	38
Epson FX-890	Matricial	NO	5
HP Laserjet P1006	Laser	NO	6
Hp Laserjet Pro P1102w	Laser	NO	12

Fuente: Elaboración propia

El inventario de equipos informáticos presentado corresponde a la sede principal y las agencias, dicho inventario es realizado en forma manual, debido a que no existe un sistema de inventario de equipos informáticos que proporcione una información veraz y actualizada de dichos equipos.

3.1.6.6 PLAN DE CONTINGENCIAS

Según lo indicado por la Unidad de Sistemas se cuenta con un plan de contingencia que esta propuesto pero no está aprobado por la alta dirección, asimismo se puede observar la falta de argumentos técnicos en metodología, en varios puntos expuestos, como sigue a continuación:

- **Análisis de riesgos.**- No se especifica el nivel (alto, bajo y medio) de riesgos, al cual está expuesto la C.A.C. San Pedro de Andahuaylas, como incendios, sismo, robo, etc.
- **Prioridad de información.**- No se especifica cómo llegaron a la conclusión que Operaciones es el sistema o información más crítico, sin tomar en cuenta los demás sistemas o información que se maneja en archivos de textos (para las áreas que poseen un sistema de información crítica, como la unidad de Personal), así

como la identificación del servidor que posee esta aplicación o información.

- **Acciones actuales y futuras referentes a los posibles riesgos.**- No especifican qué acciones se van a tomar en caso de algún desastre y las recomendaciones respectivas, solo se mencionan tipos de extintores, sin mencionar el que posee y que además no se encuentran, debido a que venció la fecha de vencimiento.
- **Carencia de plan de actividades.**- No posee un plan de actividades específicas, en donde se indiquen los procedimientos necesarios para las contingencias referidas a los servidores (el más importante que contiene la prioridad de información), en caso de falla de S.O., disco duro, etc., así como lo referente a la restauración de información, en este caso CDROM, sin especificar el tiempo que tomaría, debido a que no poseen pruebas de estas posibles actividades, así como la carencia de números de teléfonos críticos en caso de emergencia (bomberos, defensa civil, etc.).
- **No hay formación de equipos de trabajo.**- No se mencionan, ni se especifican equipos de trabajo, que deberían encargarse de las posibles acciones posteriores a posibles desastres, siendo lideradas por el jefe de Sistemas.
- **Ausencia de actas de pruebas.**- No existen actas de pruebas firmadas por el Comité formado para estas actividades.
- **No posee recomendaciones de uso de los equipos.**- No se indican recomendaciones que eviten el deterioro de estos.

El objetivo de este plan es definir y programar los procedimientos para la adopción de las medidas de contingencia que garanticen el funcionamiento continuo de los sistemas y servicios informáticos de la C.A.C. San Pedro de Andahuaylas.

Se requiere que este plan sea revisado, evaluado y aprobado a la brevedad posible para salvaguardar la integridad de los recursos informáticos de la institución.

3.1.6.7 APLICACIÓN DE TÉCNICAS INTRANET

La C.A.C. San Pedro de Andahuaylas, no cuenta con una Intranet, situación que no permite una comunicación de la institución hacia sus áreas operativas y administrativas, que permita conocer reglamentos, estructura e información importante de la institución.

Se ha establecido un esquema de seguridad con un equipo FIREWALL / PROXY basado en Windows 2008 server.

Cabe mencionar que poseen políticas de Internet, su acceso es libre de restricciones sólo para los jefes, asimismo brindan servicio de Internet de uso restringido (es decir visualización de páginas web de entidades del gobierno) a determinados usuarios de acuerdo a su gestión, pero aún su conocimiento y manejo es limitado por lo que no existe un adecuado uso de la tecnología.

No poseen un Portal Web Institucional, por lo que no permite mantener una sólida permanencia e imagen que permita fortalecer la institución y mejorar los servicios a los usuarios.

3.1.6.8 ADMINISTRACION DE LOS RECURSOS HUMANOS: SELECCIÓN, ADIESTRAMIENTO, EVALUACIÓN DEL DESEMPEÑO, ASCENSOS (PROMOCIÓN) Y CONCLUSION DE LABORES.

La administración de los RR. HH. es uno de los puntos críticos en la estructura organizacional del entorno informático. La buena selección de los RR. HH., influye directamente en la eficacia de los sistemas de TI originados, mantenidos y operados por la Unidad de

Sistemas. Además, parte del personal humano necesario en un área informática son técnicos especializados en alguna función específica. Seleccionarlos, formarlos, mantenerlos y motivarlos convenientemente puede ser vital para la buena marcha del área de sistemas y su papel en la institución.

En ese sentido, se deberá considerar algunos aspectos, para que:

1. La selección de personal se base en criterios objetivos y tenga como prioridad la formación, experiencia y niveles de responsabilidad anteriores.
2. La producción de cada colaborador, se evalúe cada cierto periodo de tiempo en base a responsabilidades específicas del puesto de trabajo y a estándares establecidos.
3. Existan diversos métodos para la promoción de los colaboradores que tengan en cuenta su desempeño y logros profesionales en la institución.
4. Existan controles que nos puedan asegurar que cualquier cambio o rotación de los colaboradores, así como la conclusión de los contratos laborales no influyan en la seguridad informática ni en los controles internos.
5. Evaluar las necesidades de capacitación de los colaboradores en base a su experiencia, responsabilidad, desarrollo, cargo en la empresa, futuro personal y expectativa tecnológica en la unidad. Se analiza la cobertura de estas necesidades y se lleva a la ejecución.
6. Finalmente, se deberá considerar que los puntos antes descritos, estén en concordancia con los procedimientos y políticas de la institución.

Entre las tareas a realizar, vamos a nombrar:

1. Conocimiento y evaluación de las tecnologías utilizados en la institución, para cubrir los puestos en la Unidad de Sistemas, sea por ascenso interno, búsqueda directa de trabajadores externos, recomendaciones de empresas de elección de personal o de trabajo temporal.

2. Estudio de las cifras de niveles de ausentismo laboral, rotación de personal y número de proyectos terminados, proyectos fuera del presupuesto y proyectos fuera de plazo. Si las estadísticas son muy altas, podrían darnos una señal de falta de liderazgo por parte del encargado o de toda la Unidad de Sistemas y/o de estimulación por parte de los colaboradores.
3. Llevar a cabo entrevistas al personal de la unidad de sistemas, para establecer su conocimiento de las responsabilidades relacionadas a su área de trabajo y de los modelos de rendimiento, y verificar si los resultados de sus evaluaciones de desempeño les han sido notificadas de una manera coherente con los procedimientos establecidos por la institución.
4. Revisar el cronograma de capacitaciones, explicación de los mismos, métodos y técnicas de enseñanza, para establecer que las capacitaciones son congruentes con la experiencia, conocimientos, responsabilidades, etc. asignadas al colaborador y con la estrategia tecnológica marcada para las TICS de la institución.
5. Revisar los pasos a seguir para la culminación de los contratos. Verificar si dicha metodología prevé que los IDs de usuario, claves, passwords y otros elementos para tener acceso a la institución, oficinas o unidad de sistemas sean cancelados, reintegrados, etc., con seguridad inmediata tras la culminación del contrato de un colaborador.

3.1.6.9 EVALUACION DE COSTOS

Definir el costo de los datos es algo totalmente referente, pues la información establece un recurso que, en muchos casos, no se valora apropiadamente debido a su imperceptibilidad, algo que no ocurre con los servidores, equipos de cómputo, las aplicaciones o la documentación.

Desde un punto de la C.A.C. San Pedro de Andahuaylas, el reto de responder la interrogante del costo de la información es considerado siempre difícil, y más difícil, es considerar que estos costos sean prudentes, siguiendo el principio que “si desea evidenciarlo, debe tener un valor”.

Además, la decisión de adoptar normas de seguridad no interviene positivamente en la productividad del sistema por lo que las instituciones son evasivas a brindar recursos a esta tarea. Por lo tanto, es necesario comprender que los esfuerzos invertidos en la seguridad son costos que incurrida en un mayor valor a nuestro proyecto.

La estimación de costos más aceptada consiste en medir los daños que cada potencial vulnerabilidad puede producir teniendo en consideración las posibilidades. Para considerar el desarrollo de estos procedimientos o políticas es necesario el estudio de lo siguiente:

- ¿Qué medidas se pueden implementar para proteger estos recursos de una manera asequible y adecuada?
- ¿Qué tan ciertas son estas amenazas?
- ¿Qué elementos se quieren proteger?
- ¿Qué tan trascendente son estos recursos?
- ¿De qué individuos necesita proteger los recursos?

Con estas simples preguntas, deberíamos saber que recursos valen más y a cuales proteger, entendiendo que algunos recursos son más importantes que otros.

La finalidad que se pretende conseguir, es lograr que un ataque a los recursos sea más costoso que su valor, invirtiendo menos de lo que es su valor.

Para esto se define tres costos fundamentales:

1. **CP:** Precio de los recursos y bienes protegidos.
2. **CR:** Precio de los medios necesarios para fraccionar las medidas de seguridad instituidas.
3. **CS:** Precio de las medidas de seguridad.

Para que las normas de seguridad sean lógicas y sólidas se debe verificar que cumplan:

1. $CR > CP$: Esto es que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos.
Las ganancias obtenidas de quebrar las medidas de seguridad no deben compensar el costo de desarrollar el ataque.
2. $CP > CS$: o sea que el precio de los recursos a proteger debe ser mayor que el costo de proteger estos recursos.

Luego, **$CR > CP > CS$** y lo que se busca es:

1. “Minimizar los costos de proteger los recursos manteniendo estos, por debajo de los recursos a proteger”. Si protegiendo los recursos resulta más caro de lo que valen, entonces resultaría conveniente adquirirlos nuevamente en vez de protegerlos.
2. “Maximizar el costo de los ataques, manteniendo este costo, por encima de los recursos a proteger”. Si atacar nuestros recursos le resulta más caro de su valor, entonces al agresor le resultaría mejor obtenerlo por otros medios que le sea menos costoso.

En conclusión, debemos tratar de apreciar los costos en que se puede incidir en el peor de los casos comparando con el coste de las políticas de seguridad adoptadas.

Valor Intrínseco

Se fundamenta en darle un valor a la información respondiendo preguntas como las citadas y examinando cuidadosamente todos los elementos a proteger. Es el más fácil de calcular.

Costos Derivados de la Pérdida

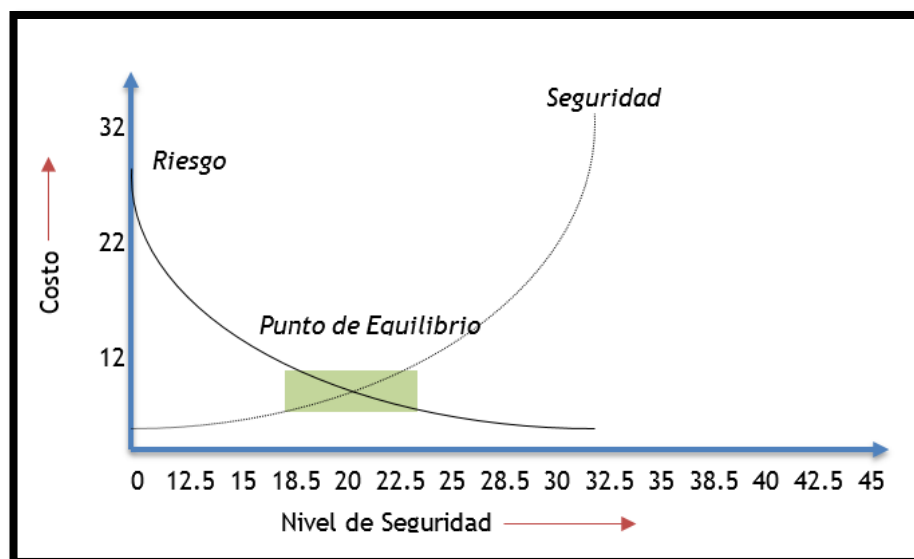
Nuevamente, deben incluirse todas las posibilidades, pretendiendo revelar todos los valores procedentes de la pérdida de algún elemento del sistema. Mucha de estas veces se trata del valor añadido que obtiene un agresor y la consecuencia de este valor para el entorno, además del coste del componente perdido. Debe considerarse elementos tales como:

1. Información supuestamente inofensiva como datos personales, que pudieran permitir reemplazar identidades.
2. Datos confidenciales de convenios y contratos que un agresor podría usar para su favor.
3. Tiempos necesarios para conseguir ciertos recursos. Un agresor o atacante podría acceder a ellos para librarse de los costos (y tiempos) que son necesarios para su desarrollo.

3.1.6.10 PUNTO DE EQUILIBRIO

Una vez estimados los riesgos y los costos en los que se está preparado a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entre estas magnitudes:

Figura N° 2: Punto de Equilibrio: Costo/Seguridad/Riesgo



Fuente: Elaboración propia

Como puede verse; los al aumentar la seguridad, los riesgos disminuyen, pero como sabemos este costes tenderán al infinito sin poder alcanzar el 100% de seguridad y lógicamente, siempre correremos algún tipo de riesgo. Lo transcendental es poder conocer que tan seguro se estará si conocemos los costes y los riesgos en los que se incurren (Punto de Equilibrio)

3.1.7 INFORME DE DEBILIDADES Y RECOMENDACIONES

En el presente documento se muestran las debilidades encontradas y las sugerencias que pueden implementarse ante la carencia o la falta en los controles para el procesamiento de la información.

3.1.7.1 CARENCIA DE UN PLAN DE SEGURIDAD DE INFORMACIÓN Y DE UN PLAN DE CONTINUIDAD DE NEGOCIO, DISPUESTO EN LA CIRCULAR G-140-2009-SBS.

El Sub Plan de Adecuación para la Administración de Riesgos de Tecnología de Información, remitido por la SBS (Superintendencia de Banca y Seguros), establece tres (03) proyectos globales:

TABLA N° 4: Sub plan de adecuación para la administración de riesgos de tecnología de información

Proyectos	Responsable
Plan de Seguridad de la Información - PSI	Riesgos
Plan de Continuidad de Negocio – PCN	Riesgos
Proyecto de Implementación de los planes	Riesgos

Fuente: Elaboración propia

En ese sentido, de acuerdo a la información proporcionada por la Unidad de Sistemas, se comprobó que la institución carece de un **Plan de Seguridad de la Información (PSI)** y de un **Plan de Continuidad de**

Negocios (PCN), situación que genera que la institución no cuente con normas mínimas para el reconocimiento y administración de los peligros asociados a la tecnología de información.

Lo expuesto trasgrede la **Circular N° G-139-2009** (véase anexo 6), Ref. Seguridad de Información, en los siguientes numerales:

Artículo 3, (véase anexo 8, "CIRCULAR N° G-105-2002") – Responsabilidad de la empresa.

Artículo 5, (véase anexo 8, "CIRCULAR N° G-105-2002") – Administración de la seguridad de información,

Artículo 7.1, (véase anexo 8, "CIRCULAR N° G-105-2002") – Seguridad lógica.

Artículo 7.2, (véase anexo 8, "CIRCULAR N° G-105-2002") – Seguridad de personal.

Artículo 7.3, (véase anexo 8, "CIRCULAR N° G-105-2002") – Seguridad física y ambiental.

Artículo 8, (véase anexo 8, "CIRCULAR N° G-105-2002") – Administración de las operaciones y comunicaciones.

Artículo 9, (véase anexo 8, "CIRCULAR N° G-105-2002") – Desarrollo y mantenimiento de sistemas informáticos – Requerimientos de seguridad.

Artículo 10, (véase anexo 8, "CIRCULAR N° G-105-2002") – Procedimiento de respaldo.

Artículo 11, (véase anexo 8, "CIRCULAR N° G-105-2002") – Planeamiento para la continuidad de negocios.

Artículo 12, (véase anexo 8, "CIRCULAR N° G-105-2002")– Criterios mínimos para el diseño e implementación del Plan de Continuidad de Negocios.

Artículo 13, (véase anexo 8, "CIRCULAR N° G-105-2002") – Prueba del Plan de Continuidad de Negocios.

Dicha situación, tiene como efecto inmediato:

- ✓ La institución no estaría cumpliendo con lo establecido en la circular emitida por la SBS, donde recomiendan a las instituciones financieras la ejecución e Implementación del PSI, siendo dichos documentos las líneas matrices para las acciones referidas a la Seguridad de la Información y los riesgos de tecnología asociados a los principales procesos de la Institución. Además la no existencia del PSI en la Institución, conllevaría a que no se contara con una identificación de los riesgos a los que se expone la información, clasificados como físicos o lógicos.
- ✓ No contar con un Plan de Continuidad de Negocios efectivo, con criterios mínimos en su desarrollo, podría generar que ante cualquier incidencia en la institución referido a tecnología, esta no se encuentre preparada para asumir una continuidad del servicio en el procesamiento de la información.

La situación descrita, se debe al desconocimiento de los actuales responsables de las Unidades de Riesgos y de Sistemas de la envergadura de dichos documentos.

RECOMENDACIÓN

Que la Gerencia General disponga que los responsables de la Gestión Informática y de la Unidad de Riesgos, establezcan las acciones respectivas para elaborar el Plan de Seguridad de Información (PSI) y Plan de Continuidad de Negocio (PCN), dispuesto en la Circular G-140-2009-SBS y G139-2009 - SBS, es así que recomendamos la siguiente

metodología para la reestructuración de la documentación mencionada. Es por ello que damos unos alcances:

FORMULACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

ETAPA 1 – Definición de la Organización de seguridad

El objetivo de esta etapa es la definición de la organización de seguridad de la C.A.C. San Pedro de Andahuaylas, basada en los cuatro pilares que son: Visión y Estrategia de Seguridad, Programa de entrenamiento y concientización, Estructura de administración de la seguridad y el Compromiso de la alta dirección con la seguridad. Durante esta etapa se definirán dichos pilares con el objetivo de brindar el apoyo necesario al desarrollo del resto del PSI.

ETAPA 2 – Identificación de riesgos asociados a factores estratégicos

Esta etapa permitirá obtener un entendimiento de los factores estratégicos del negocio, que permitirá una definición más ajustada a la realidad de los requerimientos de seguridad necesarios para la C.A.C. San Pedro de Andahuaylas, incluye el análisis de la estrategia de tecnología y los procesos de negocio. Basándose en el entendimiento resultante de esta etapa, será posible priorizar los requerimientos de seguridad.

ETAPA 3 – Desarrollo / Completar políticas y arquitectura de seguridad

El objetivo de esta etapa es validar y formalizar las políticas de seguridad por la Unidad de Sistemas para proveerlas de sustento formal y de un enfoque orientado a la de seguridad de la información de toda la C.A.C. San Pedro de Andahuaylas.

Esta etapa se permitirá plasmar la estrategia de seguridad de la organización en una etapa de desarrollo de políticas, arquitectura de seguridad y estándares guías para la implementación de la misma. Asimismo, se cubrirá las deficiencias de documentación existentes al nivel de estándares y procedimientos administrativos y de usuario final, encontradas en la etapa de diagnóstico.

ETAPA 4 – Implementación – Validación

Es objetivo de esta etapa la validación e implementación de los controles existentes y faltantes acordes con las etapas previas de diseño del PSI, así como la ejecución y mantenimiento de los controles designados para mitigar los riesgos de la información en la cooperativa.

FORMULACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO (PCN)

ETAPA I - Análisis de Impacto

El proyecto comienza con un análisis de impacto de la cooperativa (negocio), donde se identifican los procesos de negocio críticos para la continuidad y supervivencia de las operaciones de la C.A.C. San Pedro de Andahuaylas.

El trabajo realizado en esta etapa incluye una evaluación detallada de los efectos financieros y operacionales que puedan presentarse para la organización, dada una pérdida parcial o total de las instalaciones de cómputo.

ETAPA 2 - Selección de Estrategia

La selección de la estrategia se encuentra enfocada en la elección de la más apropiada opción de respaldo y recuperación de desastre considerando las opciones disponibles.

La selección de la estrategia involucra la recolección de información relacionada a la recuperación de procesos de negocio críticos y necesarios identificados en la etapa de análisis de impacto. Esta información será usada para documentar detalles de las operaciones existentes, revisar objetivos definidos durante la etapa de análisis de impacto y finalmente seleccionar una estrategia de recuperación de desastres integrada y comprensiva.

ETAPA 3 - Desarrollo del PCN

La preparación del PCN requiere de la participación substancial del propio personal de la C.A.C. San Pedro de Andahuaylas, para asegurar la confianza que este funcionará cuando se presente la necesidad.

El plan deberá contener como mínimo:

- Introducción que documente el propósito y criterio para determinar cuándo se utilizará el plan.
- Sección que documente los pasos a seguir inmediatamente luego de ocurrido el desastre.
- Procedimientos forzosos para rescatar las operaciones de los procesos críticos.
- Responsabilidades, composición y tareas para todos los equipos de recuperación de desastre.
- Responsabilidades, staff crítico y tareas para todos los equipos críticos de departamentos (aquí se puede incluir referencias a manuales de procedimientos existentes).
- Información sobre las medidas implementadas de prevención de desastre y su uso.
- Información sobre arreglos coordinados previamente a la ocurrencia del desastre.
- Apéndices para listas de inventario, contactos, mapas, diagramas y otra información detallada.

A esta documentación, deberá anexarse el Plan de contingencia de la institución.

ETAPA 4 - Prueba y Mantenimiento del PCN

Esta etapa estará orientada a verificar que el PCN pueda ser usado para recuperar las funciones críticas y necesarias del negocio luego que estas sean interrumpidas.

Al término de la ejecución de todas las fases del proyecto se obtendrá el gran entregable que es la versión final del PCN. Las pruebas a realizar deben incluir las pruebas programadas por la Unidad de Sistemas para el plan de continuidad informático.

3.1.7.2 CARENCIA DE UNA METODOLOGÍA DE ADMINISTRACIÓN DE PROYECTOS DEFINIDOS

De la evaluación a la gestión de informática y de la documentación proporcionada por la Unidad de Sistemas, se pudo apreciar la carencia de un plan de trabajo y una metodología para la administración de proyectos en tecnología, definidos por el responsable de la gestión en informática. Dicha deficiencia es evidenciada por la información que ha sido proporcionado al equipo de auditoría y los cuestionarios respectivos.

Esta situación no se alinea con el objetivos de control para la implementación y tecnologías afines, definidos en el **COBIT**, modelo generalmente aceptado y también aplicado, para el uso correcto de seguridad y control en tecnología de información (TI), donde el control sobre el proceso de Tecnología de la Información en la dirección de proyectos debe satisfacer los requerimientos de la institución, requiriendo establecer los puntos críticos, para posteriormente entregar servicios en el momento oportuno y de acuerdo a los presupuestos

fijados. En ese sentido, la C.A.C. San Pedro de Andahuaylas deberá aplicar y adoptar fuertes técnicas de gerencia de proyectos, para cada proyecto a ser iniciado.

El efecto respectivo es que puede generar retrasos en la culminación de los proyectos de tecnología aumentando costos y tiempo, además en el orden administrativo generaría penalidades respectivas a la empresa proveedora.

La situación descrita, se debe a que los encargados de la gestión de informática no han adoptado acciones encaminadas a la formalización, actualización, difusión y uso obligatorio de la Metodología del ciclo de vida del desarrollo de Sistemas, hecho que incide a incrementar la complejidad y el tiempo a emplear en el mantenimiento e integración de los sistemas de información.

RECOMENDACIÓN

Que la Gerencia General disponga al responsable de la Unidad de Sistemas, la revisión, actualización e implementación de un modelo adaptado a la realidad de la C.A.C. San Pedro de Andahuaylas, referente a los sistemas de información; también, adoptar un estándar para el periodo de vida de desarrollo de sistemas que defina todo el proceso de desarrollo, adquisición, implementación y mantenimiento de las tecnologías de información de la C.A.C. San Pedro de Andahuaylas. Esta metodología del ciclo de vida de los sistemas seleccionada, deberá ser adaptada para este entorno para el/los futuro(s) sistema(s) a ser desarrollado(s), adquirido(s) e implementado(s). Igualmente, se deben realizar cada cierto tiempo revisiones de estas metodologías a utilizar, para aseverar que incluya técnicas y procedimientos aceptados, en la actualidad.

3.1.7.3 CARENCIA DE UN PLAN EFECTIVO DE MANTENIMIENTO A LOS SERVIDORES Y EQUIPOS DE CÓMPUTO DE LA C.A.C. SAN PEDRO DE ANDAHUAYLAS.

De la información proporcionada por la Unidad de Sistemas al equipo de auditoría y de las inspecciones de verificación, se aprecia que no cuentan con un plan de trabajo y cronogramas respectivos donde especifique las acciones para realizar un mantenimiento de equipos en la sede principal. En ese mismo sentido, existen reportes que muestran que han realizado un mantenimiento preventivo a algunos equipos de agencias, pero no se ha considerado en detalle cuáles fueron.

Lo expuesto transgrede la norma técnica de control interno para el sector público N° 500, (*véase anexo 9*), **Normas de control interno para sistemas computarizados**", aceptada a partir de la Resolución de Contraloría N° 072-98-CG, del 26 de junio de 1998, en su punto **500-04 "Mantenimiento De Equipos de Computación"** que establece:

"La dirección de cada entidad debe establecer políticas respecto al mantenimiento de los equipos de computación que permitan optimizar su rendimiento". El mantenimiento de equipos tiene por finalidad optimizar el funcionamiento de los dispositivos informáticos y proteger la información que está en ellos. Existen dos clases de mantenimiento que deben considerarse: el mantenimiento correctivo y el mantenimiento preventivo (Superintendencia de Banca, Seguros y AFP, 1998).

El efecto respectivo es un riesgo muy alto, ya que los servidores y equipos computarizados, son la base para la operatividad de la institución.

La situación expuesta, obedece a la falta de comunicación oportuna del Jefe de la Unidad de Sistemas, en lo referente a diseñar un verdadero plan de mantenimiento de los equipos informáticos.

RECOMENDACIÓN

Que la Gerencia General, realice las acciones que correspondan para que la Unidad de Sistemas diseñe en detalle un plan de mantenimiento de los servidores y los equipos de cómputo, el cual especifique los equipos involucrados, los tiempos requeridos y el personal necesario para cumplir con dicho plan. Para ello deberá contar con el consentimiento de la gerencia general para su ejecución.

3.1.7.4 CARENCIA DE APLICATIVOS EN ÁREAS ESPECÍFICAS QUE AYUDEN A LA GESTIÓN DE LA C.A.C. SAN PEDRO DE ANDAHUAYLAS.

De la evaluación a la gestión de informática y de la documentación proporcionada por la Unidad de Sistemas, se pudo observar que las áreas de Personal, Logística y Planeamiento no cuentan con aplicativos para el desarrollo de sus funciones, que ayuden a su gestión y por ende a la institución. Por otro lado para cumplir sus funciones dichas áreas, se valen de herramientas ofimáticas, por la que dichas áreas no pueden cumplir con la eficiencia que se requiere.

Dicha deficiencia es evidenciada por la información proporcionada por la Unidad de Sistemas y por las entrevistas con los responsables de dichas áreas.

Lo expuesto inobserva lo normado por el INEI (Instituto Nacional de Estadística e Informática), según la **Directiva N° 007-95-INEI/SJI “Recomendaciones técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública”** que tiene como fin el de establecer los pasos y procedimientos para el óptimo uso, protección y conservación de la información que se deberá procesar en los equipos de cómputo.

Además, lo expuesto transgrede la norma técnica de control interno para el sector público N°. 500 “**Normas de control interno para sistemas computarizados**” (véase *anexo 9*), aceptada a partir de la Resolución de Contraloría N° 072-98-CG, con fecha 26Jun98, en su **punto 500-03 “Controles de datos fuente, de Operación y de Salida”** que establece: “Toda entidad debe proteger la información procesada con el propósito de garantizar su integridad y exactitud, así como respecto de los equipos de cómputo” (Superintendencia de Banca, Seguros y AFP, 1998)

Del mismo modo, como una práctica sana de control interno todo Sistema de Información, debe responder a reales necesidades de las diferentes áreas usuarias, las cuales conlleven al cumplimiento de objetivos y metas institucionales

Se puede observar que el efecto de esta debilidad es el excesivo trabajo manual y el riesgo de alteración de la información al trabajar con archivos compartidos aumentando el nivel de descontrol en la manipulación de datos. Asimismo, si se mantiene dicha deficiencia generaría:

- Información no oportuna.
- Redundancia de información
- Información errónea
- Incremento de los gastos de operación de los recursos

La situación expuesta, obedece a lo siguiente:

- Carencia de coordinación y planificación, con respecto al desarrollo de los sistemas que darán soporte a la institución.
- Carencia al asignar el presupuesto para la compra o realización de proyectos orientados al mejoramiento de los sistemas de información.

RECOMENDACIÓN

Que la Gerencia General disponga a los responsables de la gestión informática la evaluación y desarrollo de sistemas para las Áreas de Personal, Logística y Planeamiento, que por lo comprobado requieren sistemas automatizados, lo que reduciría considerablemente el proceso actual, ya que en la actualidad se lleva manualmente, lo que genera mayores costos y tiempos.

3.1.7.5 EL CABLEADO ESTRUCTURADO QUE UTILIZA LA C.A.C. SAN PEDRO DE ANDAHUAYLAS NO PERMITE UNA COMUNICACIÓN EFICIENTE ENTRE LAS DIVERSAS ÁREAS.

De las visitas realizadas a los ambientes de la C.A.C. San Pedro de Andahuaylas y de la documentación proporcionada por la Unidad de Sistemas, se ha podido verificar que no existe un cableado estructurado adecuado para la sede principal, ya que cada piso del local se ha instalado de manera diferente, es decir se ha ido incrementando los puntos de red de acuerdo a las necesidades diarias, situación que no garantiza una comunicación confiable y segura entre los equipos. Dicha debilidad es mencionada en la Hoja de Coordinación de noviembre del 2015 dirigido al Jefe de Sistemas, por el encargado de la Jefatura de Operaciones, donde informa que frecuentemente los diferentes módulos de atención se cuelgan, originando congestión en el área de atención al público y molestias en los clientes.

Lo expuesto transgrede la norma técnica de control interno para el sector público N°. 500 **“Normas de control interno para sistemas computarizados”** (véase anexo 9), aceptada a partir de la Resolución de Contraloría N° 072-98-CG, del 26 de junio de 1998, en su **punto 500-05 “Seguridad de programas, de datos y equipos de cómputo”** que

señala: “Deben establecerse mecanismos de seguridad en los programas y datos del sistema para proteger la información procesada por la entidad, garantizando su integridad y exactitud así como respecto de los equipos de computación” (Superintendencia de Banca, Seguros y AFP, 1998).

Asimismo, se transgrede lo dispuesto por el INEI (Instituto Nacional de Estadística e Informática) según la **Directiva N° 007-95-INEI/SJI “Recomendaciones técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública”** que tiene como fin el de establecer los pasos y procedimientos para el óptimo uso, protección y conservación de la información que se deberá procesar en los equipos de cómputo.

Dicha deficiencia está generando:

- Un servicio informático débil y deficiente.
- Procesos y tareas que demoran por contar con un cableado inadecuado.
- Congestión de información, originando deficiente comunicación entre las estaciones de trabajo.

Esta situación es causada por la carencia de una planificación orientada a las reales capacidades de crecimiento en la red de la institución. Además por no haber considerado supervisiones oportunas bajo un enfoque técnico, que garantice dicha instalación.

RECOMENDACIÓN

Que la Gerencia General disponga a los responsables de la gestión informática, establecer un análisis en detalle de las instalaciones de la red que está instalada en toda la institución, con la finalidad de corregir las deficiencias en las instalaciones y comunicaciones; del mismo modo,

diseñar una infraestructura modelo para tener en cuenta en posibles instalaciones de agencias o locales que adquiriera la institución.

3.1.7.6 CARENCIA DE FORMALIZACIÓN E INOBSERVANCIA DE LA METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SISTEMAS

Habiéndosele solicitado a la Unidad de Sistemas, la Metodología del Ciclo de Vida de Desarrollo de Sistema; el Equipo de Auditoría recibió un documento denominado "Proceso interno para el Desarrollo de Sistemas"; el cual entre otros aspectos, se refiere a lo siguiente:

Básicamente, resume en dicho Documento, las actividades para cualquier requerimiento y/o modificación sobre las aplicaciones, además establece formatos de requerimientos, formato de atención de desarrollo de aplicaciones.

También existe un documento de procedimientos para cambios de programas, donde establece las actividades y formatos de actualización de programas y base de datos, etc.

Aspectos que resultan insuficientes para una adecuada administración, control y monitoreo de proyectos de Desarrollo de Sistemas; más aún, cuando en la práctica no es de total aplicación, tal como se pudo constatar al solicitar los manuales de usuario, operación y documentación técnica de algunos aplicativos; de los cuales, lo definido como metodología solo se aplicó parcialmente como muestra y ha evidenciado en este caso el cuestionario y la documentación que han proporcionado (únicamente el manual de usuario desactualizado y de operación).

Al respecto, como uso y costumbre universalmente aplicable y aceptada de control y administración en Tecnologías de Información, el área

correspondiente deberá definir e implementar un estándar de sistema de información y adoptar un modelo de una metodología para el ciclo de vida de desarrollo de sistemas que con la finalidad de puntualizar los procesos de: Desarrollo, Adquisición, Implementación y Mantenimiento de los sistemas de información de la institución.

El efecto respectivo, generaría una dependencia absoluta con los programadores que desarrollaron los sistemas de la institución, además una carencia de acciones que deben estar encaminadas a la formalización, actualización, difusión y uso obligatorio de un modelo para nuestro Ciclo de vida del desarrollo de sistemas, hecho que incide al incrementar la complejidad y el tiempo a emplear en el mantenimiento e integración de los sistemas de información.

La situación descrita, se debe a que el responsable de la gestión informática no ha adoptado acciones destinadas a llevar un correcto orden en el desarrollo de los sistemas.

RECOMENDACIÓN:

Que la Gerencia General disponga al responsable de la Unidad de Sistemas, la revisión, actualización e implementación de un modelo adaptado a la realidad de la C.A.C. San Pedro de Andahuaylas, referente a los sistemas de información; también, adoptar un estándar para el ciclo de vida del desarrollo de sistemas (CVDS), con la finalidad de puntualizar los procesos de: Desarrollo, Adquisición, Implementación y Mantenimiento de los sistemas de información de la institución.

Esta metodología del CVDS elegida, deberá ser adaptada para este entorno para los futuros sistemas a ser desarrollados, adquiridos e implementados en nuestra área de sistemas. Igualmente, se deberán efectuar revisiones periódicas de la referida metodología, para certificar que se incluya técnicas y procedimientos actualmente acreditados.

3.1.7.7 CARENCIA DE UNA ARQUITECTURA TECNOLÓGICA QUE INTERCONECTE LA SEDE PRINCIPAL CON LAS AGENCIAS.

De la evaluación efectuada por el equipo de auditores se ha podido detectar que la sede principal no se encuentra interconectada con sus agencias respectivas. Para ello, realizan procesos en lotes o Batch, para la actualización de la información.

También, existe un proyecto de interconexión presentado por un proveedor donde especifica a nivel técnico la forma que ellos brindarían el servicio para una posible interconexión.

Dicha situación, no contempla lo dispuesto en el M.O.F. sobre el particular de la Unidad de Sistemas, tiene como función canalizar la atención de las necesidades de información, no solo de las áreas de la sede central sino, de las diferentes unidades operativas que conforman el eje principal de las actividades de la C.A.C. San Pedro de Andahuaylas.

En tal sentido, es su responsabilidad velar por la continua integración de los sistemas y, por otro lado, la evaluación permanentemente de los requerimientos existentes, así como de las facilidades que el uso de nuevas tecnologías de información brinda, para lo cual debe, a su vez, proponer y/o efectuar los estudios de viabilidad técnico económico correspondiente.

Dicha deficiencia perjudica el desenvolvimiento de las operaciones de la institución, ya que no permite anticiparse a las necesidades de las áreas operativas; por lo que, dificulta la planificación al tener que recurrir a acciones de corto plazo, sin evaluar las proyecciones de crecimiento de los servicios brindados y no considera los criterios de integración que permiten un ahorro de costos importante en comunicaciones y la

obtención de información oportuna, tanto para seguimiento de acciones como para toma de decisiones.

La situación expuesta obedece a la falta de un estudio de costo/beneficio, que el responsable de la gestión informática debió presentar a la alta dirección, indicando cómo crecería la institución en sus servicios, con la adquisición de una arquitectura de comunicaciones.

RECOMENDACIÓN:

Que la Gerencia General disponga a los responsables de la gestión informática, efectuar un análisis de los riesgos en ese sentido, además realicen una propuesta al directorio que considere entre otros puntos lo siguiente:

- Definición de proyectos específicos, que permitan la expansión e integración de los servicios brindados, a través de la interconexión de las redes de sus agencias con la oficina principal (WAN).
- El desarrollo de sistemas debe orientarse a la integración de los sistemas principales, con una sola base de datos centralizada. Aspecto que resultará más evidente cuando las aplicaciones se encuentren trabajando en ambiente WAN.
- El proyecto de interconexión de redes, debe incluir la interconexión de voz y datos, evaluando la posibilidad de instalar anexos extendidos, lo cual redundaría en la eliminación de los costos por llamadas de larga distancia nacional.

3.1.7.8 CARENCIA DE PROCEDIMIENTOS FORMALES PARA LA VERIFICACIÓN DE LA INFORMACIÓN RESPALDADA; ASÍ COMO, EL ESTADO DE LOS DISPOSITIVOS DE SEGURIDAD DE LA SALA DE SERVIDORES.

La Unidad de Sistemas, encargada del respaldo de la información de los servidores y de los sistemas de información, no cuenta con procedimientos de pruebas selectivas, que permitan validar la integridad de la información respaldada, recurriendo únicamente al restablecimiento de los referidos "Backups" o copias de respaldo, en casos de reales necesidades de esa información. Situación que presenta riesgos al desconocer el resultado de los procesos de respaldo, estado de los medios y otros aspectos que puedan afectar la integridad de esa información.

Asimismo, no hay evidencia escrita (Actas), sobre las ensayos de funcionamiento de los Sistemas de Seguridad del área del Centro de Cómputo, uso de equipos, alarmas audibles, extintores portátiles, sistemas contra incendio y aniegos; así como identificación adecuada de las salidas de emergencia.

Por otro lado, también inobserva la **Directiva N° 008-95-INEI/SJI "Normas Técnicas para Almacenamiento y Respaldo de la Información que se Procesa en las entidades del Estado"**.

Directiva que precisa los procedimientos que realizan los colaboradores de las instituciones del estado, que utilizan equipos de cómputo, para el óptimo uso y constante observación de cómo realizar el almacenamiento y como proceder al respaldo de la información que se plasman en los medios de almacenamiento.

Del mismo modo, inobserva la **Directiva N° 007-95-INEI/SJI "Recomendaciones técnicas para la seguridad e integridad de la información que se procesa en la administración pública"** que tiene como finalidad establecer recomendaciones técnicas para la elaboración de Planes de Sistemas de Información.

Lo anterior podría generar, por un lado que la información respaldada no se encuentre completa lo que afectaría a su integridad y por otro lado, la seguridad de los servidores y equipos de computación y las personas,

que en dicha área laboran corren un alto riesgo por no contar con mecanismos de seguridad pertinentes.

Dicha situación es originada por la falta de conocimiento de los gestores informáticos, ya que se evidencia que no se han establecido las instrucciones adecuadas para el correcto almacenamiento o resguardo de nuestra información.

RECOMENDACIÓN:

Que la Gerencia General disponga que los responsables de la gestión informática, establezcan procedimientos para afirmar que los Backups de información sean realizados adecuadamente y que su utilidad y/o estado sea verificada regularmente. Asimismo, evaluar de manera regular el óptimo funcionamiento de los medios y/o dispositivos de seguridad; así como, la capacitación en su uso por parte del personal responsable. Debiendo disponer una preparación cuidadosa de la documentación, el informe de resultados de los exámenes y diseñar un procedimiento de acción de acuerdo con los resultados.

3.1.7.9 CARENCIA DE PROCEDIMIENTOS FORMALES PARA LAS PRUEBAS Y PASE A PRODUCCIÓN DE LOS SISTEMAS DE INFORMACIÓN.

De acuerdo a la información proporcionada por el responsable de la gestión informática, se evidenció que no existe documentación que norme los mencionados procedimientos. Asimismo, el encargado de la Unidad de Sistemas manifestó que no cuentan con ello, sin embargo todo cambio es respaldado con un requerimiento del usuario, pero muchas veces carecen de documentación sobre todo cuando la unidad interviene en el arreglo de datos que han sido generados erróneamente.

La Unidad de Sistemas deberá especificar e implementar procesos estándares para verificar la entrega (pase del sistema de un ambiente de pruebas al ambiente de producción) del sistema en fase de desarrollo a la fase de prueba y posteriormente a operación. Los ambientes de la unidad de sistemas, deberá separarse y protegerse adecuadamente.

La deficiencia descrita, no permite un control adecuado, por lo tanto; no podemos asegurar la calidad de los Sistemas de Información, hecho que conlleva a riesgos de posibles situaciones anómalas en la ejecución de los programas informáticos, los cuales no son fueron identificados en su fase previa; asimismo, no permite un adecuado control de versiones de los Sistemas de Información.

Dicha situación generará que las diferentes personas de la Unidad de Sistemas que intervienen en los procesos de pruebas y pase a producción de los Sistemas de Información, no cuenten con procedimientos formales que guíen la ejecución de esas actividades, así como la falta de un ambiente adecuado para la realización de las pruebas con los usuarios y así dar el pase a producción de los sistemas.

RECOMENDACIÓN:

Que la Gerencia General disponga a los encargados de la gestión informática, cumplan con definir e implementar procedimientos formales para controlar el pase de los sistemas de información del ambiente de Desarrollo al de Producción. Debiendo asegurar que las pruebas sean realizadas por un equipo independiente; en concordancia con la evaluación de los recursos e impacto y llevadas a cabo en un lugar de prueba adecuado, antes de iniciar su uso en producción.

3.1.7.10 DEFICIENTE CONTROL DE LAS LICENCIAS DEL SOFTWARE INSTALADO.

En la recopilación, revisión y análisis de la información obtenida por la Unidad de Sistemas, se pudo evidenciar lo siguiente:

- El servidor de desarrollo carece de un software instalado contra virus.
- Supuestamente en los documentos proporcionados, establece que tienen 92 computadoras, con sus respectivas licencias, sin embargo no lo han podido demostrar.
- Hasta la emisión del presente informe, los responsables de la gestión estaban inventariando y generando el número de licencias que tenían, siendo un punto de riesgo, pues se está utilizando software sin licencias de respaldo

Lo expuesto, contraviene lo normado en el **Decreto Legislativo D.L. 822** del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (**INDECOPI**), **aprobado mediante la Resolución Nº 0121-1998/ODA-INDECOPI**, que establece que uso de software sin tener la debida licencia autorizada por el titular del derecho de autor o su representante, es ilícita lo cual nos puede conllevar a sanciones administrativas y/o judiciales en perjuicio de la C.A.C. San Pedro de Andahuaylas.

El efecto respectivo podría originar reparos y/o multas determinadas por los organismos reguladores competentes.

La situación descrita, se debe a que no hubo una planificación en la distribución de las licencias del antivirus, lo que indica que no ha existido un control en el manejo de este software por parte de los responsables de la gestión informática.

RECOMENDACIÓN:

Que la Gerencia General disponga a los encargados de la gestión informática, realicen el inventario de todas las licencias correspondiente, efectuando los pedidos respectivos coordinando previamente con el área

de logística, a efectos de regularizar en el más corto plazo, las licencias de uso del software que no se encuentren sustentadas. Asimismo, se deberá a la brevedad posible, instalar un software antivirus en el servidor de desarrollo.

3.2 DIAGNOSTICO DE LA SITUACIÓN EXISTENTE, RELACIONADA CON LA GESTIÓN DE RIESGOS DE INFORMACION Y DE TECNOLOGÍA DE LA INFORMACIÓN

3.2.1 INTRODUCCIÓN

Es necesario indicar que el diagnóstico preliminar, está dirigido a revisar en forma independiente y objetiva la situación existente relacionada con la gestión de los riesgos de información y de la tecnología de información. Asimismo, la documentación requerida para una adecuada administración del riesgo, tales como políticas, procedimientos y planes de continuidad del negocio, entre otros definidos en la Circular N° G-140-2009. (Véase Anexo N° 7), “Gestión de la Seguridad de Información de la Superintendencia de Banca y Seguros y AFP y compararla con lo requerido por la circular.

La revisión no tiene como objetivo la detección de errores, fraudes, desfalcos u otras irregularidades que pudieran existir.

3.2.2 OBJETIVO Y ALCANCE DEL TRABAJO

El objetivo del trabajo estará dirigido a proponer a la C.A.C. San Pedro de Andahuaylas, el desarrollo de un Plan de Acción que les permita identificar los riesgos de tecnología de información de acuerdo con las mejores prácticas y cumplir con la normatividad del organismo regulador.

Es necesario indicar que el diagnóstico preliminar deberá ser revisado y evaluado por la C.A.C. San Pedro de Andahuaylas, así como los esfuerzos

que deberá desplegar para la ejecución de las actividades detalladas en el mismo.

Este trabajo implica fundamentalmente una investigación en la gestión de los riesgos de las tecnologías de información y está dirigido a revisar en forma independiente y objetiva la situación existente relacionada con la gestión de los riesgos de las tecnología de información, así como; la documentación requerida para una adecuada administración del riesgo, tales como políticas, procedimientos y planes de continuidad del negocio, entre otros, definidos en la Circular N° G-140-2009 de la SBS, compararla con lo requerido por la circular y desarrollar el plan para adecuarse a la norma del organismo regulador.

El alcance de esta fase de este trabajo comprende:

- Entendimiento de la situación actual de las siguientes funciones al interior de la Unidad de Sistemas, en adelante TI:
 - Organización de la empresa
 - Gerencia del área de sistemas
 - Políticas y procedimientos para gestionar los riesgos del área de sistemas
 - Subcontratación de diversos recursos (ambiental, lógica, personal, y física)
 - Las acciones de desarrollo y mantenimiento de servidores y sistemas informáticos.
 - Gerenciar la Seguridad de la Información.
 - Aspectos de la seguridad de la información (lógica, personal, física y ambiental)
 - Seguridad de la Información
 - Descripción constante de activos asociados a Tecnologías de Información
 - Operaciones sistémicas
 - Gerencia de las operaciones y comunicaciones
 - Rutinas backups

- Planeamiento y prueba del plan para la continuidad de negocios
- Comprensión del momento actual analizando los siguientes puntos:
 - Aplicación y cumplimiento de normas
 - Mantener la privacidad de todo tipo de información
 - Auditoría de sistemas
 - Identificación de las brechas entre la situación actual y lo normado.
 - Definir de las actividades principales, u cronograma y las personas responsables para hacer cumplir la Circular N° G-140-2009-SBS.


3.2.3 PROCEDIMIENTOS





Los pormenores de la evaluación y análisis de brechas se mostrarán en un cuadro, cuyo contenido damos a continuación:

- **Situación actual:** Muestra una síntesis de la situación actual encontrada en la C.A.C. San Pedro de Andahuaylas, emanada de la información obtenida de los testimonios, entrevistas y de la documentación levantada, obtenida y entregada a nuestro equipo.
- **Mejores prácticas:** Expone una síntesis de nuestras mejores prácticas y de los requerimientos normados en la Circular N° G140-2009-SBS de la Superintendencia de Banca y Seguros y AFP.
- **Análisis de brecha:** Expone de modo gráfico la diferencia que existe entre la situación actual y nuestras mejores prácticas y los requerimientos normados en la Circular N° G140-2009-SBS de la Superintendencia de Banca y Seguros y AFP.

En el siguiente cuadro se detalla la descripción de los gráficos:

TABLA N° 5: Descripción de los gráficos

	Razonable- mente cubierto	Las exigencias de la Circular N° G140-2009-SBS de la Superintendencia de Banca, Seguros y AFP, están razonablemente cubiertos.
---	---------------------------------	--


	Sustancialmente cubierto	Faltan ejecutar algunas actividades para cubrir prudentemente las exigencias de la Circular N° G140-2009-SBS de la Superintendencia de Banca, Seguros y AFP
	Parcialmente cubierto	Se han ejecutado actividades que cubren parcialmente las exigencias de la Circular N° G140-2009-SBS de la Superintendencia de Banca, Seguros y AFP
	Limitadamente Cubierto	Se han ejecutado algunas actividades para cubrir las exigencias de la Circular N° G140-2009-SBS de la Superintendencia de Banca, Seguros y AFP.
	No cubierto	No se ha ejecutado ninguna actividad relacionada con las exigencias de la Circular N° G140-2009-SBS de la Superintendencia de Banca, Seguros y AFP.

Fuente: Elaboración propia

3.2.4 Diagnóstico


A continuación, se muestra de modo gráfico una síntesis de la situación actual encontrada en la C.A.C. San Pedro de Andahuaylas y los aspectos a contemplar como: mejores prácticas

Figura N° 3: estructura Organizacional Para la Administración de Riesgos de Tecnología De Información

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
1.	ESTRUCTURA ORGANIZACIONAL PARA LA ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN		
	<p>la C.A.C. San Pedro de Andahuaylas:</p> <ul style="list-style-type: none"> - Cuenta con una Unidad de Riesgos como responsable de la administración de riesgos, la misma que si bien cuenta con un M.O.F. aprobado, aún se encuentra en proceso de implementación. - En el MOF no está explícitamente definido el responsable de la administración de riesgos de TI. - No existen, o no se encuentran debidamente documentados, los procedimientos y acciones que permitan administrar adecuadamente los riesgos. - No se dispone de indicadores definidos que permitan evaluar y monitorear los riesgos de tecnología. 	<p>Se debería contemplar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Definición y mantenimiento de una estructura organizacional que permita administrar adecuadamente los riesgos asociados a la tecnología de información. - La Unidad de Riesgos deberá contar con un responsable de la administración del riesgo de TI. - La responsabilidad de la Seguridad de la Información debería ser ejercida de forma exclusiva. - El Área de Riesgos Operativos y Tecnológicos debería contar con una estructura acorde con los riesgos de tecnología evaluados para la C.A.C. San Pedro de Andahuaylas y definir indicadores que ayuden a monitorear los mismos. 	


Fuente: Elaboración propia

Figura N° 4: PLAN DE SEGURIDAD DE LA INFORMACIÓN

Nº	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
2. PLAN DE SEGURIDAD DE LA INFORMACIÓN			
	<p>la C.A.C. San Pedro de Andahuaylas:</p> <ul style="list-style-type: none"> - Carece de una política de seguridad. - No dispone de una evaluación de riesgos ni inventario asociado a riesgos de seguridad de la información. - Existen criterios, procedimientos y acciones específicas no integradas para evitar los riesgos de información. - No cuenta con una selección de controles y objetivos de control destinados a mitigar dichos riesgos. - No cuentan con un plan de implementación de los controles y procedimientos de revisión periódica. 	<p>Se deberían contemplar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Definición de una política de seguridad. - Evaluación de riesgos de seguridad a los que está expuesta la información. - Inventario de riesgos de seguridad de la información. - Selección de controles y objetivos de control para reducir, eliminar y evitar los riesgos identificados, indicando las razones de su inclusión o exclusión - Plan de implementación de los controles y procedimientos de revisión periódicos. - Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas de auditoría. 	


Fuente: Elaboración propia

Figura N° 5: POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD

Nº	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
2.1 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD			
	<p>La C.A.C. San Pedro de Andahuaylas, no cuenta con políticas de seguridad formales que indiquen los procedimientos de seguridad a ser adoptados para salvaguardar la información de posibles pérdidas en la integridad, disponibilidad y confidencialidad.</p> <p>Sin embargo, se ha observado la existencia de algunas políticas y controles específicos en distintos aspectos de la seguridad de la información.</p>	<p>La definición de una política de seguridad debería contemplar:</p> <ul style="list-style-type: none"> - Declaración escrita de la política. - Definición de la propiedad de la Política. - Políticas debidamente comunicadas. - Autoridad definida para realizar cambios en la Política. - Aprobación por el área legal. - Alineamiento de la política con la organización. - Definición de responsabilidades de la seguridad. - Confirmación de usuarios de conocimiento de la política. 	


Fuente: Elaboración propia

Figura N° 6: SEGURIDAD LÓGICA

Nº	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
2.1.1 SEGURIDAD LÓGICA			
	<p>La C.A.C. San Pedro de Andahuaylas presenta lo siguiente:</p> <ul style="list-style-type: none"> - Carece de procedimientos formales para la administración de perfiles, pero tiene implementado formatos y estándares para la creación de cuentas de nuevos usuarios. - Cuenta con seguridad de acceso a nivel de los Sistemas Operativos (Windows 8) y aplicaciones - Carece de herramientas de auditoría y control de accesos a nivel de plataforma, base de datos. - La Unidad de Sistemas solo puede acceder con clave personal que labora en ella. - Existen conexiones remotas los cuales son registrados en la red a través de código y clave. 	<p>La Seguridad Lógica debería contemplar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Definición de procedimientos formales para la administración de perfiles y usuarios, así como la revocación de usuarios y procedimientos de revisiones periódicas sobre los concedidos. - Identificación única de usuarios. - Controles sobre el uso de herramientas de auditoría y utilidades sensibles del sistema. - Controles sobre el acceso y uso de los sistemas y otras instalaciones físicas. - Controles sobre usuarios remotos y computación móvil. - Administración restringida de los equipos de acceso remoto y configuración de seguridad del mismo. 	


Fuente: Elaboración propia

Figura N° 7: SEGURIDAD DE PERSONAL

Nº	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
2.1.2 SEGURIDAD DE PERSONAL			
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Toda selección de personal se realiza por concurso, el proceso incluye consulta Infocorp, examen psicológico y solicitud escrita de antecedentes a anteriores empleadores. No incluye verificación de diplomas. - Se hace entrega al nuevo empleado del RIT, MOF, Manual de Prevención de lavado de dinero, Código de conducta y 10 reglas de oro. - Carece de documentación formal al respecto. - En opinión del Área de Personal no existe un plan de monitoreo, paralelo a ello los accesos a la red se dan sin cruce de horarios autorizados. 	<p>Se debería considerar:</p> <ul style="list-style-type: none"> - Procedimientos de revisión de datos en el proceso de selección de personal previo a su contratación (Ex. Referencias de carácter, verificación de estudios, revisión de crédito –si aplica- y revisión independiente de identidad) - Entrega formal de las políticas de manejo de información confidencial a los nuevos integrantes de la C.A.C. San Pedro de Andahuaylas. - Definición apropiada de responsabilidad sobre la seguridad es parte de los términos y condiciones de la aceptación del empleo (Términos en el contrato). - Difusión de las políticas con respecto al monitoreo de actividades en la red y sistemas de información, antes entregar <u>IDs</u> a usuarios. 	


Fuente: Elaboración propia

Figura N° 8: SEGURIDAD FÍSICA Y AMBIENTAL

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
2.1.3 SEGURIDAD FÍSICA Y AMBIENTAL			
	<p>Adicionalmente se puede mencionar:</p> <p>Áreas seguras</p> <ul style="list-style-type: none"> - Cuenta con controles de acceso a activos físicos e instalaciones - Tienen instalado monitoreo del Área de Plataforma. - El movimiento de activos es primero autorizado, luego se comunica al área de logística y contabilidad. <p>Seguridad de equipos</p> <ul style="list-style-type: none"> - No existe un cronograma de prueba de alarmas y equipos de control ambiental. - Se deshabilita puerto Ethernet y cableado cuando está vacante. <p>Protección de equipos</p> <ul style="list-style-type: none"> - No cuentan con controles ambientales así como medidas preventivas y correctivas ante incendios. - Existen conocimientos de las precauciones a tomar del personal que trabaja con laptops, pero no está formalizado. <p>Controles generales</p> <ul style="list-style-type: none"> - Implantación de protectores de pantalla con contraseña manual. No está estandarizado. 	<p>Se debería considerar los siguientes aspectos:</p> <p>Áreas seguras</p> <ul style="list-style-type: none"> - Procedimientos de reubicación de empleados - Controles de áreas de carga y descarga. - Controles físicos de entrada. - Seguridad del perímetro físico de las instalaciones. - Procedimientos de Remoción o reubicación de activos. - Aseguramiento de oficinas, áreas de trabajo y facilidades. <p>Seguridad de Equipos</p> <ul style="list-style-type: none"> - Aseguramiento de Cableado - Acciones y planes de mantenimiento de equipos <p>Protección de equipos</p> <ul style="list-style-type: none"> - Normas de seguridad para laptops. - Fuentes de poder redundantes. - Procedimientos de eliminación o uso reiterado seguro de equipos de manera segura <p>Controles generales</p> <ul style="list-style-type: none"> - Política de “mesa limpia” - Política de “pantallas limpias” 	


Fuente: Elaboración propia


Figura N° 9: CLASIFICACIÓN DE SEGURIDAD


N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
2.1.4 CLASIFICACIÓN DE SEGURIDAD			
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Cuenta con un catálogo de activos físicos de la organización, se puede mejorar. - Cuenta con un inventario de aplicaciones usadas por la Institución, se puede mejorar. - Tiene un listado de servicios por el departamento de Logística, se puede mejorar. - Falta definir la clasificación de los Sistemas de Información asignando roles y procedimientos de mantenimiento. - Los listados presentados deben mejorarse. 	<p>Se debería considerar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Un catálogo de todos los activos físicos de la organización, indicando tipo de activo, ubicación física, responsable y nivel de criticidad. - Un catálogo de todos los activos de software tales como herramientas de desarrollo, aplicaciones, etc. Debe indicar entre otros, vendedor, ubicación lógica y física, responsable, nivel de criticidad, clasificación de la información, etc. - Un catálogo o descripción de alto nivel de todos los activos de información más importantes de la organización. Debe indicar información como tipo de data, ubicación lógica o física, responsable o dueño de la información, clasificación de la información y nivel de criticidad. - Un listado de todos los servicios tales como comunicaciones, cómputo, servicios generales, etc. y documentar la información relativa a los proveedores del servicio. Debería incluir entre otros, persona de contacto con el proveedor, procedimientos de servicios de emergencia, criticidad y unidades de negocio afectadas por el servicio. - Clasificación de los sistemas de información y/o grupos de data según su criticidad y sus características de confidencialidad, integridad y disponibilidad. - Asignación de la responsabilidad de clasificación - Procedimientos de mantenimiento de la clasificación 	

Fuente: Elaboración propia

Figura N° 10: ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES


N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
3 ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
	<p>La C.A.C. San Pedro de Andahuaylas, cuenta con:</p> <p>Procedimientos y responsabilidades de operación.</p> <ul style="list-style-type: none"> - No existen Procedimientos definidos. - Formalmente no definido sin embargo existe la función de desarrollo o creación de sistemas. que es la única que tiene acceso a las fuentes de los programas. <p>Control en cambios operacionales</p> <ul style="list-style-type: none"> - Los cambios de los equipos de comunicación son realizados en coordinación con las áreas involucradas. Estos cambios de infraestructura lo realizan sólo la Unidad de Sistemas o en su defecto la empresa proveedora. - Los roles y responsabilidades no están formalizados. - Todos los cambios y requerimientos provienen de las áreas solicitadas mediante documento y luego de una respectiva evaluación se define su implementación. Para estos requerimientos existen formatos. - La función de producción y desarrollo se encuentran en un solo ambiente. - Los estándares de administración de cambios, así como los cambios de emergencia, no están definidos. - El control de acceso es exclusivo para el personal de desarrollo. 	<p>Se deberían considerar los siguientes aspectos:</p> <p>Procedimientos y responsabilidades de operación.</p> <ul style="list-style-type: none"> - Documentación formal de todos los procedimientos de operación, así como procedimientos y niveles de autorización definidos para su mantenimiento. - Programación de trabajos o procesos debe ser correctamente documentada, así como el resultado de dichas ejecuciones. <p>Control en cambios operacionales</p> <ul style="list-style-type: none"> - Todo cambio en la red de datos, incluyendo software, dispositivos, cableado o equipos de comunicación deben seguir procedimientos formales definidos y adecuadamente registrados. - Roles y responsabilidades deben ser claramente definidos y las funciones adecuadamente segregadas. - Los cambios deben ser adecuadamente aprobados. - Los resultados de todo cambio deben ser correctamente documentados. Roles y responsabilidades en las actividades de pase a producción correctamente definidos y segregados. - Adecuada separación de ambientes de producción y desarrollo. - Estándar de administración de cambios definido, incluyendo cambios de emergencia. - Control de accesos a escritura sobre sistemas en producción. 	


N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
3 ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
	<p>Administración de incidentes de seguridad.</p> <ul style="list-style-type: none"> - No indican si cuentan con una administración de incidentes de seguridad. <p>Segregación de funciones</p> <ul style="list-style-type: none"> - Falta ampliar el área de desarrollo adicionalmente realiza labores de soporte. <p>Planeamiento de sistemas</p> <ul style="list-style-type: none"> - No existen herramientas para el planeamiento de los sistemas. <p>Protección contra software malicioso</p> <ul style="list-style-type: none"> - No tienen instalados antivirus en todas las estaciones de trabajo. <p>Operaciones de verificación</p> <ul style="list-style-type: none"> - No cuentan con estándares para el registro de fallas - Tienen procedimientos de copias de respaldo, pero deben mejorarlos. - Falta formalizar registros adecuados de todas las actividades de operación. 	<p>Administración de incidentes de seguridad.</p> <ul style="list-style-type: none"> - Definición de procedimientos y equipos de respuesta ante incidentes de seguridad. <p>Segregación de funciones.</p> <ul style="list-style-type: none"> - Las actividades de desarrollo, migración y operación de sistemas, así como las de administración de aplicaciones, helpdesk, administración de red y de IT deben ser correctamente segregadas. <p>Planeamiento de sistemas.</p> <ul style="list-style-type: none"> - Procedimientos formales definidos de planeamiento de recursos. <p>Protección contra software malicioso.</p> <ul style="list-style-type: none"> - Controles preventivos y detección sobre el uso de software de procedencia dudosa, virus, etc.). <p>Operaciones de verificación</p> <ul style="list-style-type: none"> - Adecuado registro de fallas. - Adecuados procedimientos de generación de copias de respaldo. - Registros adecuados de todas las actividades de operación. 	

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
3 ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
	<p>Administración de Red</p> <ul style="list-style-type: none"> - No cuentan con herramientas de monitoreo, ni controles de operaciones automáticas. <p>Manipulación y seguridad de dispositivos de almacenamiento de información.</p> <ul style="list-style-type: none"> - No existen políticas con respecto al manejo de otros dispositivos de almacenamiento de información en la Unidad de Sistemas. (discos, CDs, etc.) <p>Intercambio de información y seguridad</p> <ul style="list-style-type: none"> - No cuenta con un reglamento sobre el uso de los seguros de comunicaciones, correspondencia, Infraestructura y su (correspondencia general, fax, correo electrónico, Internet, software aplicativo y operativo). 	<p>Administración de Red</p> <ul style="list-style-type: none"> - Adecuados controles de operación de red implementados. - Protección de la red y comunicaciones usando dispositivos de control de accesos, procedimientos y sistemas de monitoreo de red (Detección de intrusos) y procedimientos de reporte. <p>Manipulación y seguridad de dispositivos de almacenamiento de información.</p> <ul style="list-style-type: none"> - Aseguramiento sobre medios de almacenamiento y documentación de sistemas. <p>Intercambio de información (Correo electrónico y otros) y seguridad</p> <ul style="list-style-type: none"> - Controles de seguridad en el Correo electrónico y cualquier otro medio de transferencia de información (Ex. Normas, filtros, sistemas de protección contra virus, etc.). 	

Fuente: Elaboración propia


Figura N° 11: DESARROLLO Y MANTENIMIENTO

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
4 DESARROLLO Y MANTENIMIENTO	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Un análisis de requerimiento, participa un equipo conformado por sistemas, usuarios y O y M para definir el alcance del requerimiento y la mejor solución posible. - Un plan de escalamiento que contempla el control de acceso, autorización, criticidad del sistema, clasificación de la información, disponibilidad del sistema, integridad y confidencialidad de la información, pero falta mejorarlo. - Rutinas de validación de data en los módulos o aplicaciones, pero falta mejorarlas. - Cambios que se registran en la misma data y los accesos limitados posibilitan modificaciones no autorizadas. - En los controles de procesamiento, se realizan procesos en batch que están definidos y ordenados de manera que estos no alteren la data por malos procesos. - En los controles de salida de información, la mayoría de los reportes están definidos de manera tal que solo contienen la información que se necesita. - No cuenta con técnicas de encriptación. 	<p>Se debería considerar lo siguiente:</p> <ul style="list-style-type: none"> - Contar con metodologías y estándares formales de desarrollo y mantenimiento de sistemas. - Los requerimientos deben ser definidos antes de la fase de diseño y se debe determinar un apropiado ambiente de control para la aplicación, estos requerimientos deben incluir: <ul style="list-style-type: none"> ▪ Control de acceso ▪ Autorización ▪ Criticidad del sistema ▪ Clasificación de la información ▪ Disponibilidad del sistema ▪ Integridad y confidencialidad de la información. - Todas las aplicaciones deberán tener rutinas de validación de data. - Toda la data debe ser revisada periódicamente, a fin de detectar inexactitud, cambios no autorizados e integridad de la información. - Se deben definir controles para prevenir que la data se vea afectada por un mal procesamiento. - Se deben definir controles que permitan revisar toda información obtenida por un sistema de información, asegurando que sea completa, correcta y solo disponible para personal autorizado. 	

Nº	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
4 DESARROLLO Y MANTENIMIENTO			
	<ul style="list-style-type: none"> - Antes del ingreso a producción se realizan los cambios y las implementaciones son probadas y aprobadas. - El código fuente se encuentra en un servidor de acceso restringido. - Cada responsable de cada una de las aplicaciones del módulo lleva el control del código fuente con el que trabaja. - No se menciona si cuentan con control de acceso para que el personal IT tenga acceso al código fuente. - Se tiene procedimientos para la realización de cambios, pero falta mejorarlos. - No hay separación de ambientes entre desarrollo y producción. - Los cambios en los programas fuentes se realizan con autorización de la jefatura. - Falta mejorar políticas en la administración de versiones. 	<ul style="list-style-type: none"> - Uso de técnicas de encriptación estándar. - Controles para el acceso a las librerías de programa fuentes. - Mantener un estricto y formal control de cambios, que sea debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios. - Procedimientos formales y adecuados para las pruebas y reportes de las mismas. 	


Fuente: Elaboración propia


Figura N° 12: PROCEDIMIENTOS DE RESPALDO

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
5	PROCEDIMIENTOS DE RESPALDO		
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Los Procedimientos de Respaldo se desarrollan mediante lineamientos aislados y no están articulados en un modelo general. - El medio de almacenamiento de la Copia de Respaldo se realiza en discos compactos CD y con frecuencia diaria. - La herramienta Zip Backus v.2 utilizada para crear las copias de respaldo genera un Log que es revisado al final de cada proceso de respaldo y se toman las acciones correspondientes. - No existe un control externo ni interno de la información respaldada. - Los medios que conforman las Copias de Respaldo se almacenan en la Unidad de Sistemas, hasta cada fin de semana se baja a la bóveda principal, en el caso de los cd's de provincia, cada fin de semana se remitirá a la Unidad de Sistemas 2 cd's, los cuales se almacenaran 1 en la bóveda principal y el otro en la Unidad de Sistemas, además cada agencia guardará una copia en su respectiva bóveda. 	<p>Los procedimientos de generación de copias de respaldo deberían contar con los siguientes controles clave:</p> <ul style="list-style-type: none"> - Aseguramiento de que el proceso de generación de copias de respaldo haya culminado exitosamente. - Procedimientos que contemplen pruebas periódicas de las copias de respaldo. - El tiempo de almacenamiento de las copias de respaldo debe estar en concordancia con los requisitos legales y normativos vigentes. 	

Fuente: Elaboración propia


Figura N° 13: PLANEAMIENTO PARA LA CONTINUIDAD DEL NEGOCIO

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
6 PLAN DE CONTINUIDAD DE NEGOCIOS			
6.1 PLANEAMIENTO PARA LA CONTINUIDAD DEL NEGOCIO			
	<p>La C.A.C. San Pedro de Andahuaylas, no ha desarrollado un plan de continuidad de negocios. Existen, sin embargo, criterios aislados para basar este trabajo en:</p> <ul style="list-style-type: none"> - Necesidad de asegurar la continuidad para los servidores principales. - Lineamientos de continuidad para la infraestructura de comunicaciones LAN/MAN. <p>No existe un Plan de Emergencias, para respuesta centralizada ante una interrupción de los procesos críticos de negocio de la C.A.C. San Pedro de Andahuaylas. Sin embargo, algunos documentos informáticos incluyen la identificación de eventos en recursos informáticos críticos y procedimientos mitigantes de riesgo actual y propuesto para mejora de los mismos.</p> <p>No existe una evaluación de procesos críticos de negocio y de los recursos críticos que los soportan, por lo que no existe un Plan de Continuidad de Negocio que garantice la marcha de todos los procesos críticos de la C.A.C. San Pedro de Andahuaylas, ante el evento de una interrupción de los mismos.</p> <p>En cuanto a estrategias de respaldo de información, se cuenta con algunos procedimientos aislados para el resguardo de información crítica, que no constituyen un Plan de Recuperación.</p>	<p>Se debería considerar la formulación de lo siguiente:</p> <ul style="list-style-type: none"> - Generación de Plan de Contingencias que abarque todos los procesos críticos de la C.A.C. San Pedro de Andahuaylas, y que se desarrolle siguiendo una metodología formal. Este plan debería contar con tres documentos mínimos: <ul style="list-style-type: none"> - Plan de Emergencias, Un mecanismo de respuesta centralizada que asegura la ejecución de las instrucciones y el control durante una interrupción operacional. Este plan incluye: identificación de incidentes, evaluación, escalamiento, declaración, plan de activación y desactivación y procedimientos de restauración. - Plan de Continuidad del Negocio, un plan que dirija la continuidad y recuperación de todos los procesos del negocio requeridos para mantener un nivel aceptable de operación en el evento de una interrupción de los mismos y/o de los recursos que los soportan. - Plan de Recuperación, un plan que dirija la restauración de las aplicaciones de sistemas, software, datos e infraestructura de las mismas (por ejemplo, hardware, comunicaciones, redes, etc.) después que el desastre ha ocurrido. 	

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
6 PLAN DE CONTINUIDAD DE NEGOCIOS			
6.1 PLANEAMIENTO PARA LA CONTINUIDAD DEL NEGOCIO			
		<ul style="list-style-type: none"> - Creación de un equipo para implementar el plan en el que todos los miembros conocen sus responsabilidades y cómo deben cumplir con las tareas asignadas. - Existencia de preparativos adecuados para asegurarse de la continuidad del procesamiento computadorizado (existe centro de procesamiento alterno). - Una copia del plan de contingencias se almacena en una sede remota y será de fácil acceso en caso de que ocurriera cualquier forma de desastre. - Preparativos de contingencia para el hardware y software de comunicaciones y redes. - Realización periódica un back-up de los archivos de datos críticos, los sistemas y bibliotecas de programas almacenándolo en una sede remota cuyo tiempo de acceso sea adecuado. 	

Fuente: Elaboración propia

Figura N° 14: CRITERIOS PARA EL DISEÑO E IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIOS

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
6.2 CRITERIOS PARA EL DISEÑO E IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIOS			
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Los actuales lineamientos y acciones desarrollados por la C.A.C. San Pedro de Andahuaylas, se centran en un análisis limitado de recursos informáticos críticos; no se ha realizado un análisis de procesos críticos de negocio, ni de recursos que soportan a dichos procesos. - No existen procedimientos para realizar la revisión del impacto en el negocio. - Existe un Plan de Contingencias, pero no está bien formulado. Existen procedimientos aislados para atender situaciones específicas. 	<p>Se debería considerar lo siguiente:</p> <ul style="list-style-type: none"> - Revisión del impacto sobre el negocio, previo al diseño del Plan de continuidad de negocios, identificando las partes más expuestas a riesgo. - Realizar revisión del impacto en el negocio, estableciendo los procedimientos a seguirse en el caso de que ocurriera un desastre (por Ej. explosión, incendio, daño por tormenta, pérdida de personal clave) en cualquiera de las dependencias operativas de la organización. - Deberían existir planes de contingencia para cada recurso computarizado. - El plan de contingencias debería contemplar las necesidades de los departamentos usuarios en términos de traslados, ubicación y operación. - El plan de contingencias debería asegurar que se observen normas de seguridad de información en caso de que ocurriera un desastre. - El cronograma para la recuperación de cada función debería ser revisado asegurando que sea adecuado. 	


Fuente: Elaboración propia

Figura N° 15: PRUEBA DEL PLAN DE CONTINUIDAD DE NEGOCIO

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
6.3 PRUEBA DEL PLAN DE CONTINUIDAD DE NEGOCIO			
	De acuerdo a la información proporcionada no existen procedimientos formales para la prueba y mantenimiento de los planes de continuidad de los recursos informáticos definidos por la C.A.C. San Pedro de Andahuaylas.	El plan de contingencias debería probarse periódicamente para asegurarse de que aún es viable y efectivo.	○


Fuente: Elaboración propia

Figura N° 16: SUBCONTRATACIÓN

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
7	SUBCONTRATACIÓN		
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - No se han identificado contratos por servicios de terceros vigentes. - No se han identificado servicios de terceros que procesen información de la C.A.C. San Pedro de Andahuaylas. - No se han identificado normas establecidas sobre cláusulas de seguridad en contratos con terceros, de darse el caso. - No cuentan con mantenimiento de equipos por empresas externas. - No existe un procedimiento formal para establecer un servicio de subcontratación. 	<p>El plan de contingencias debe incluir la eventualidad de la pérdida del servicio prestado por terceros.</p> <p>Los contratos de servicios con terceros deberían incluir entre otros aspectos, los siguientes:</p> <ul style="list-style-type: none"> - Requerimientos de seguridad y las acciones que se tomarán de no cumplirse el contrato. - Acuerdos de controles de seguridad y políticas a aplicarse para garantizar el cumplimiento de los requerimientos. - Determinación de los niveles de servicio requeridos (Service Level Agreement - SLA). - El derecho de la entidad, y la Superintendencia de Banca y Seguros, o las personas que ellos designen, de auditar el ambiente de la empresa que brinda el servicio, para verificar los controles de seguridad aplicados a la data y los sistemas. - Documentación sobre los controles físicos y lógicos, empleados por la empresa que brinda el servicio, para proteger la confidencialidad, integridad y disponibilidad de la información y equipos de la C.A.C. San Pedro de Andahuaylas. - Determinación de los requerimientos legales, incluyendo privacidad y protección de la data. - Procedimiento que asegure que la empresa que brinda el servicio realizará pruebas periódicas para mantener la seguridad de la data y los sistemas. - Cláusula sobre exclusividad de utilización de los equipos que procesan información de la C.A.C. San Pedro de Andahuaylas. 	


Fuente: Elaboración propia

Figura N° 17: CUMPLIMIENTO NORMATIVO

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
8 CUMPLIMIENTO NORMATIVO			
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Una Unidad de Organización y Métodos, que se encarga de actualizar los reglamentos y procedimientos, define los nuevos para que la operatividad se cumpla dentro del marco regulatorio establecido por las normas. - Existen controles, por ejemplo, en el caso de las estaciones no tienen acceso al uso de disquete o cd para evitar así la copia de software sin autorización, pero falta mejorar. - Las áreas de Asesoría Legal, Planeamiento, Gerencia, Contabilidad mantienen archivos actualizados de normas legales para consulta y revisión. 	<p>Se debería contar con:</p> <ul style="list-style-type: none"> - Definición de responsable del cumplimiento de las normas emitidas por la Superintendencia. - Procedimientos de control establecidos para el cumplimiento de las normas emitidas por la Superintendencia. - Control de cumplimiento de normas sobre la propiedad intelectual (licenciamiento de software). 	


Fuente: Elaboración propia

Figura N° 18: PRIVACIDAD DE LA INFORMACIÓN

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
9 PRIVACIDAD DE LA INFORMACIÓN			
	<p>La C.A.C. San Pedro de Andahuaylas, no cuenta con un responsable asignado para la salvaguarda de la privacidad de la información.</p> <p>Existen algunos procedimientos dispersos y se han implementado determinados controles en los sistemas, con el fin de restringir el acceso a información confidencial. Una sola persona es depositaria de las llaves y claves principales de la C.A.C. San Pedro de Andahuaylas.</p> <p>No se han definido políticas referentes a la privacidad de la información.</p>	<p>Se debería contar con:</p> <ul style="list-style-type: none"> - Definición de responsabilidades con respecto a la aplicación del secreto bancario y de la privacidad de la Información. - Restricciones de acceso a información en salvaguarda de su privacidad y del secreto bancario. - Existencia de autorizaciones internas para la entrega y transferencia de información. 	

Fuente: Elaboración propia

Figura N° 19: AUDITORÍA INTERNA Y EXTERNA

N°	Situación Actual	SBS, Mejores Prácticas	Análisis de Brecha
10 AUDITORÍA INTERNA Y EXTERNA			
	<p>La C.A.C. San Pedro de Andahuaylas, presenta lo siguiente:</p> <ul style="list-style-type: none"> - Un área de auditoría interna que está incluyendo en su plan de auditoría el cumplimiento de lo dispuesto en la norma G-140-2009 de la Superintendencia. - En la auditoría externa correspondiente al período 2014, un punto de la evaluación estuvo referido al Avance del informe sobre los riesgos de Tecnología de Información. - No se dispone de un auditor de sistemas que forme parte de la estructura organizacional del área de Auditoría Interna. 	<p>Se debería considerar:</p> <ul style="list-style-type: none"> - La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la norma G-105-2002 de la Superintendencia. - Las sociedades de Auditoría Externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de tecnología de información. - La C.A.C. San Pedro de Andahuaylas, deberá contar con un servicio permanente de auditoría de sistemas. 	

Fuente: Elaboración propia

CAPÍTULO IV

REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

4.1 Experiencia durante el periodo laboral en la C.A.C. San Pedro de Andahuaylas.

El periodo de trabajo en la C.A.C. San Pedro de Andahuaylas comprendidas entre los años 1994 al 2009, fue un tiempo dedicado al aprendizaje. Cuando llegue a la C.A.C. San Pedro de Andahuaylas, solo había 4 trabajadores a parte del Gerente General, la Cooperativa ocupaba únicamente el tercer piso de un edificio propio en el que el primer piso estaba alquilado al Banco de Crédito, se tenía 4 estaciones PC Intel 80386 y 80486, algunas impresoras como la LX-810, una red en arquitectura Bus con una red Novell Netware. Al finalizar mi periodo en la Cooperativa éramos 250 colaboradores, con locales propios en Andahuaylas, Abancay, Chincheros, Cusco y Lima, otras oficinas más en otras provincias, principalmente en Apurímac y la Cooperativa, pasó ocupar en el ranking de la FENACREP, el 8avo. lugar entre las 164 Cooperativas de Ahorro y Crédito del país. Empecé desempeñando una nueva faceta como soporte técnico, principalmente en lo concerniente a las funciones técnicas de la red y de los equipos de cómputo, la configuración de Switches, la llegada de los módems, el internet, la instalación y gestión de los servidores, la instalación de PC's los drivers ZIPS Backup, los dispositivos ópticos, fueron pasos posteriores.

Todas estas peculiaridades de un entorno empresarial grande debían ser absorbidas y asimiladas rápidamente, a fin de atender a los socios sin que estos perciban cambios significativos, se manejaban diariamente millones de soles y no debía haber fallas. Empezamos a trabajar con un software en Cobol (SIFC) Sistema Integrado Financiero y Contable. Empezamos a utilizar el sistema operativo Novell Netware, una topología de red en anillo, las Tarjetas de red ISA de 10 Mbit/s. y los Conectores BNC (Coaxial), poco tiempo después se cambió a una red Ethernet, otra tipología, el cableado UTP o par trenzado, los conectores RJ45 y los concentradores o Hubs fueron la novedad ya que tuvimos más distancias que cubrir, se mejoró notablemente la interconexión de los equipos en red estableciendo lo que se conoce como una red de área local (LAN), y cuyos detalles técnicos siguen el patrón conocido como Ethernet, al cambiar el cableado, nos expandimos más en la oficina principal, ocupamos ya el segundo piso y antes de empezar el año 2000 utilizamos los 3 pisos de nuestro edificio.

Posteriormente, llego el despegue de la Cooperativa, empezamos a abrir oficinas en diversas provincias, al ser conecedor del manejo y los procesos me ocupo instalar, servidores, las redes, capacitar al nuevo personal de planta, a los nuevos encargados de sistemas de las nuevas oficinas, etc. Las actividades de soporte técnico, conllevaron a instalaciones de nuevas oficinas en otras ciudades, se adoptó posteriormente los servidores Windows NT, lo que supuso una mejor comunicación e interface lo que nos permitió en un primer momento intercambiar información con las otras oficinas y posteriormente la ansiada interconexión entre oficinas, también se adoptó los sistemas operativos de Windows en los equipos de cómputo de la cooperativa, se desarrollaron también algunas soluciones para la oficina mediante el uso de aplicaciones o programas específicos en base a los conocimientos obtenidos anteriormente. Se empezó mi capacitación ya en otras labores más directivas, preparándome para otras actividades.

4.2 Herramientas utilizadas

Para el desarrollo de este trabajo, se pusieron en valor los conocimientos ganados a lo largo de la formación profesional en la Escuela de Ingeniería de Computación y Sistemas y en otras capacitaciones que lleve dentro de mi época de estudiante, esto tuvo como prueba el año de 1994 en el que ingrese a trabajar al Congreso de la Republica, en donde se me nombro como técnico en las elecciones de 1995, después de un periodo de capacitación en redes, seguridad, soporte, etc. Fui designado a la Región de Cerro de Pasco para llevar una (en ese tiempo) auditoria de sistemas, con formatos y especificaciones ya pres establecidos, pero en la que fue en su momento información a través de módems.

4.3 Importancia de habilidades adicionales a formación profesional

En el tiempo en el que se desarrolló de mi experiencia laboral en la C.A.C. San Pedro de Andahuaylas, se hizo inevitable aplicar destrezas desarrolladas adicionales a la formación brindada en la universidad, después de haber pasado por diversas capacitaciones en el ámbito de sistemas y financiero, tuve la oportunidad de ser designado como Administrador de la Oficina en Lima, estaba encargado de 5 oficinas en diversos distritos de Lima (Gamarra, San Juan de Lurigancho, Los Olivos, etc.) donde se desarrollaba trabajos de captación de ahorros y otorgamiento de créditos, hipotecarios, a sola firma, solidarios, etc. y con 40 colaboradores bajo mi mando, en una etapa un poco difícil para esta oficina logrando llegar en un año al punto de equilibrio, en base a trabajo en equipo y lineamiento de los objetivos de la empresa, siendo por esta situación reconocido en diferentes oportunidades. En ese contexto, desarrollar un trabajo con compañeros de diversas actividades profesionales, puntos de vista, etc., ha ayudado favorablemente para el perfeccionamiento de actividades dentro de la institución.

Producto de estas habilidades, me he acoplado bien en mi trabajo actual en la Unidad de Acreditación y Calidad de la Facultad de Ciencias de la Comunicación Turismo y Psicología de la Universidad de San Martín de Porres, he logrado ganar día a día el respeto y consideración, de mis superiores, habiendo sido cada vez más, considerado para proponer, diseñar,

integrar y ejecutar proyectos, además de mis responsabilidades estipuladas dentro de la unidad.

4.4 Importancia del conocimiento y capacitación

En base a mi experiencia a lo largo también de mi vida profesional he podido comprobar la importancia de la capacitación para después poner en práctica los conocimientos adquiridos en este trabajo, mucho me valió en un principio las capacitaciones en redes en los primeros años después de terminar la universidad, paso que me llevo al primer trabajo de auditoria, trabajo que realicé para el Jurado Nacional de Elecciones en su momento, pero que fue decisivo en el manejo de información para posteriores trabajos

Igualmente, fue importante el conocimiento sobre el manejo que fui adquiriendo de la empresa en sus diversas áreas, lo que me permitió ocupar los diversos cargos en la C.A.C. San Pedro de Andahuaylas lo que me llevo para tener la aprobación de la Presidencia del Consejo de Administración y de la Gerencia General en la realización de este informe.

Ayudó, además, para el momento de conseguir y documentar los pedidos de requerimiento funcionales y no funcionales, calcular los tiempos y equipo y recursos necesarios, definir elementos de comunicación idóneos con los miembros del equipo de trabajo, gestionar el plan de trabajo y reconocer los cambios en su totalidad.

Finalmente las competencias técnicas obtenidas durante mi permanencia en la C.A.C. San Pedro de Andahuaylas, permitieron desarrollarme satisfactoriamente durante el desarrollo del presente proyecto.

CONCLUSIONES

A lo largo de la presente investigación pudimos comprender que un componente principal para la estabilidad y el éxito de las instituciones, es la gestión llevada de forma eficiente de la información y de las TI. Para lograr esto es importante comprometer a la alta dirección y a la plana Gerencial a través de la comprensión básica de los riesgos y limitaciones de nuestras TI para que puedan nuestros directivos proporcionar una orientación eficiente, además de los controles idóneos.

Por lo tanto, las Instituciones financieras en este caso la C.A.C San Pedro de Andahuaylas deberán asumir riesgos en la búsqueda de oportunidades y planificar los procesos de administración y control de riesgos en respuesta a las potenciales amenazas y oportunidades que pudieran ocurrir dentro de la misma. Finalmente las Instituciones deberán alinear sus objetivos estratégicos con sus propios riesgos y controles / procesos.

Aplicar directivas de seguridad es importante, sabemos que hacer de estos planteamientos de seguridad, parte significativo del desarrollo de la labor diaria es vital. Por ende, la C.A.C. San Pedro de Andahuaylas, deberá tener comunicación constante completa y coordinada con los usuarios del sistema, siendo esta la clave para que se conciba una verdadera “cultura de la seguridad” haciendo que estos lineamientos se cumplan.

Se deberá concienciar a toda la Institución que la implantación de una arquitectura de administración de riesgos representa un cambio rotundo en la cultura y en la estructura de la Institución. Como tal, las Instituciones deberán atravesar un proceso típico de administración del cambio.

Sabemos que, en la realidad, no existe un verdadero diseño de seguridad que resguarde en su conjunto los potenciales percances o riesgos; pero es necesario para la continuidad de las organizaciones estar dispuesto y listo a solucionar estos, con prontitud ya que las amenazas y las debilidades se están

generando y actualizando todo el tiempo. Es así que para superar las debilidades encontradas en la auditoría efectuada, hay que considerar realizar primero un Análisis de Riesgos Antes de Implementar el PSI, ver Anexo 4, que constituirá un análisis inicial de los riesgos asociados a las tecnologías de información y luego deberán desarrollar un Análisis de Riesgos Después de Implementar el PSI, ver Anexo 5, en el cual se comprobara la disminución en el porcentaje de vulnerabilidades, consiguiendo de este modo el nivel mínimo de riesgos posibles, esto se puede verificar en la Tabla N° 6.

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
01	Unidad de Sistemas - Gestión de la Dirección de Sistemas	200.00	Políticas de: <ul style="list-style-type: none"> • Seguridad Lógica • Identificación y autenticación • Seguridad en las Comunicaciones • Plan de Contingencia • Control de software • Gestión del centro de procesamiento de data • Resguardo de la información • Seguridad de Personal • Desarrollo y mantenimiento de sistemas • Control de ingreso a nuestros sistemas de información 	100.00	100.00
02	Personal con experiencia en los procesos	133.33	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Identificación y autenticación • Seguridad física • Seguridad de personal • Seguridad en las comunicaciones • Control de software • Desarrollo y mantenimiento de sistemas 	100.00	33.33

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
03	Sistemas de Gestión de Terceros	100.00	Políticas: <ul style="list-style-type: none"> • Seguridad lógica • Seguridad física • Seguridad en las Comunicaciones • Control de ingreso a nuestros sistemas de información 	100.00	0
04	Sistema de Aire Acondicionado	114.29	Política de: <ul style="list-style-type: none"> • Seguridad física • Plan de contingencia 	100.00	14.29
05	Pozos a tierra y Sistema Eléctrico Estabilizado	116.67	Política de: <ul style="list-style-type: none"> • Seguridad física • Plan de contingencia 	100.00	16.67

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
06	Sistema de Telecomunicaciones / MAN	140.00	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Seguridad física • Seguridad en las comunicaciones • Plan de Contingencia 	100.00	40.00
07	Servidores centrales.	146.67	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Control de ingreso a nuestros sistemas de información • Identificación y autenticación • Seguridad de las comunicaciones • Seguridad física • Plan de contingencia • Auditoría y revisiones 	100.00	46.67

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
08	Sistema Transaccional y Administrativo	137.50	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Seguridad física • Seguridad de personal • Plan de contingencia 	100.00	37.50
09	Herramientas de Escritorio y Desarrollo (Programas fuente, sistemas operativos)	150.00	Política de: <ul style="list-style-type: none"> • Seguridad lógica • Identificación y autenticación • Desarrollo y mantenimiento de sistemas • Seguridad en las comunicaciones • Seguridad física • Control de software • Seguridad del personal • Plan de contingencia • Control de ingreso a nuestros sistemas de información • Resguardo de la información • Auditoría y revisiones 	100.00	50.00

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
10	Dispositivos de conectividad y soporte en comunicaciones (Cableado, switch, hubs, módems.)	114.29	Políticas de: <ul style="list-style-type: none"> • Seguridad en las comunicaciones • Seguridad física • Seguridad de personal • Plan de contingencia 	100.00	14.29
11	Sistema Operativo de Red	125.00	Políticas de: <ul style="list-style-type: none"> • Control de ingreso a nuestros sistemas de información • Plan de contingencia • Seguridad lógica • Control de software • Autenticación e identificación • Auditoría y revisiones 	100.00	25.00

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
12	PC's de Escritorio	130.00	Políticas de: <ul style="list-style-type: none"> • Plan de Contingencia • Seguridad física • Seguridad de personal 	100.00	30.00
13	Data generada por los Sistemas de Información	162.50	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Identificación y autenticación • Control de ingreso a nuestros sistemas de información • Seguridad en las comunicaciones • Seguridad física • Seguridad del personal • Plan de contingencia • Resguardo de los datos • Auditoría y revisiones 	100.00	62.50

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
14	Data generada por los Usuarios.	191.67	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Identificación y autenticación • Seguridad física • Seguridad de personal • Control de ingreso a nuestros sistemas de información • Resguardo de la información • Plan de contingencia • Auditoría y revisiones 	100.00	91.67

TABLA N° 6: Nivel mínimo de riesgos posibles

ID DE ACTIVO	ACTIVOS	NIVEL DE VULNERABILIDAD (V) ANTES DEL PSI	MEDIDAS CORRECTIVAS	NIVEL DE VULNERABILIDAD (V) DESPUÉS DEL PSI	REDUCCIÓN DE VULNERABILIDAD
		VALOR		VALOR	VALOR
15	Archivos de hardware, Software, programas, sistemas, manuales, procedimientos administrativos, etc.	171.43	Políticas de: <ul style="list-style-type: none"> • Seguridad lógica • Identificación y autenticación • Seguridad física • Seguridad de personal • Control de ingreso a nuestros sistemas de información • Resguardo de la información • Plan de contingencia 	100.00	71.43
Total		2,133.35		1,500.00	633.35

RECOMENDACIONES

EN RELACIÓN CON EL INFORME DE DEBILIDADES AUDITORIA SEGURIDAD DE INFORMACION

1. Según el punto 3.7.1 carencia del Plan de Seguridad de Información (PSI) y Plan de Continuidad de Negocio (PCN), dispuesto en la Circular G-140-2009-SBS.

Que la Gerencia General disponga que los responsables de la Gestión Informática y de la Unidad de Riesgos, establezcan las acciones respectivas para elaborar el Plan de Seguridad de Información (PSI) y Plan de Continuidad de Negocio (PCN), dispuesto en la Circular G-140-2009-SBS y G139-2009 - SBS, es así que recomendamos la siguiente metodología para la reestructuración de la documentación mencionada. Es por ello que damos unos alcances:

FORMULACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

ETAPA 1: Definición de la Organización de seguridad

ETAPA 2: Identificación de riesgos asociados a factores estratégicos

ETAPA 3: Desarrollo / Completar políticas y arquitectura de seguridad

ETAPA 4: Implementación – Validación

FORMULACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO (PCN)

ETAPA 1: Análisis de Impacto

ETAPA 2: Selección de Estrategia

ETAPA 3: Desarrollo del PCN

ETAPA 4: Prueba y Mantenimiento del PCN

2. Según el punto 3.7.2 Carencia de una Metodología de Administración de Proyectos Definidos

Que la Gerencia General disponga al responsable de la Unidad de Sistemas, la revisión, actualización e implementación de un modelo adaptado a la realidad de la C.A.C. San Pedro de Andahuaylas, referente a los sistemas de información; también, adoptar un estándar para el periodo de vida de desarrollo de sistemas que defina todo el proceso de desarrollo, adquisición, implementación y mantenimiento de las tecnologías de información de la

C.A.C. San Pedro de Andahuaylas. Esta metodología del ciclo de vida de los sistemas seleccionada, deberá ser adaptada para este entorno para el/los futuro(s) sistema(s) a ser desarrollado(s), adquirido(s) e implementado(s). Igualmente, se deben realizar cada cierto tiempo revisiones de estas metodologías a utilizar, para aseverar que incluya técnicas y procedimientos aceptados, en la actualidad.

3. Según el punto 3.7.3 Carencia de un Plan de Mantenimiento a los Servidores y Equipos de Cómputo de la la C.A.C. San Pedro de Andahuaylas. Que la Gerencia General, realice las acciones que correspondan para que la Unidad de Sistemas diseñe en detalle un plan de mantenimiento de los servidores y los equipos de cómputo, el cual especifique los equipos involucrados, los tiempos requeridos y el personal necesario para cumplir con dicho plan. Para ello deberá contar con el consentimiento de la gerencia general para su ejecución.

4. Según el punto 3.7.4 Carencia de aplicativos en áreas específicas que ayuden a la gestión de la C.A.C. San Pedro de Andahuaylas. Que la Gerencia General disponga a los responsables de la gestión informática la evaluación y desarrollo de sistemas para las Áreas de Personal, Logística y Planeamiento, que por lo comprobado requieren sistemas automatizados, lo que reduciría considerablemente el proceso actual, ya que en la actualidad se lleva manualmente, lo que genera mayores costos y tiempos.

5. Según el punto 3.7.5, el Cableado estructurado que utiliza la C.A.C. San Pedro de Andahuaylas, no permite una comunicación eficiente entre las diversas áreas.

Que la Gerencia General disponga a los responsables de la gestión informática, establecer un análisis en detalle de las instalaciones de la red que está instalada en toda la institución, con la finalidad de corregir las deficiencias en las instalaciones y comunicaciones; del mismo modo, diseñar una

infraestructura modelo para tener en cuenta en posibles instalaciones de agencias o locales que adquiera la institución.

6. Según el punto 3.7.6, Carencia de formalización e inobservancia de la metodología del ciclo de vida de desarrollo de sistemas

Que la Gerencia General disponga al responsable de la Unidad de Sistemas, la revisión, actualización e implementación de un modelo adaptado a la realidad de la C.A.C. San Pedro de Andahuaylas, referente a los sistemas de información; también, adoptar un estándar para el ciclo de vida del desarrollo de sistemas (CVDS), con la finalidad de puntualizar los procesos de: Desarrollo, Adquisición, Implementación y Mantenimiento de los sistemas de información de la institución.

Esta metodología del CVDS elegida, deberá ser adaptada para este entorno para los futuros sistemas a ser desarrollados, adquiridos e implementados en nuestra área de sistemas. Igualmente, se deberán efectuar revisiones periódicas de la referida metodología, para certificar que se incluya técnicas y procedimientos actualmente acreditados.

7. Según el punto 3.7.7, Carencia de una Arquitectura Tecnológica que interconecte la Sede Principal con las agencias.

Que la Gerencia General disponga a los responsables de la gestión informática, efectuar un análisis de los riesgos en ese sentido, además realicen una propuesta al directorio que considere entre otros puntos lo siguiente:

- Definición de proyectos específicos, que permitan la expansión e integración de los servicios brindados, a través de la interconexión de las redes de sus agencias con la oficina principal (WAN).
- El desarrollo de sistemas debe orientarse a la integración de los sistemas principales, con una sola base de datos centralizada. Aspecto que resultará más evidente cuando las aplicaciones se encuentren trabajando en ambiente WAN.

- El proyecto de interconexión de redes, debe incluir la interconexión de voz y datos, evaluando la posibilidad de instalar anexos extendidos, lo cual redundaría en la eliminación de los costos por llamadas de larga distancia nacional.

8. Según el punto 3.7.8, Carencia de procedimientos formales para la verificación de la información respaldada; así como, el estado de los dispositivos de seguridad de la sala de servidores.

Que la Gerencia General disponga que los responsables de la gestión informática, establezcan procedimientos para afirmar que los Backups de información sean realizados adecuadamente y que su utilidad y/o estado sea verificada regularmente. Asimismo, evaluar de manera regular el óptimo funcionamiento de los medios y/o dispositivos de seguridad; así como, la capacitación en su uso por parte del personal responsable. Debiendo disponer una preparación cuidadosa de la documentación, el informe de resultados de los exámenes y diseñar un procedimiento de acción de acuerdo con los resultados.

9. Según el punto 3.7.9, Carencia de procedimientos formales para las pruebas y pase a producción de los sistemas de información.

Que la Gerencia General disponga a los encargados de la gestión informática, cumplan con definir e implementar procedimientos formales para controlar el pase de los sistemas de información del ambiente de Desarrollo al de Producción. Debiendo asegurar que las pruebas sean realizadas por un equipo independiente; en concordancia con la evaluación de los recursos e impacto y llevadas a cabo en un lugar de prueba adecuado, antes de iniciar su uso en producción.

10. Según el punto 3.7.10, Deficiente control de las licencias del software instalado.

Que la Gerencia General disponga a los encargados de la gestión informática, realicen el inventario de todas las licencias correspondiente, efectuando los pedidos respectivos coordinando previamente con el área de logística, a efectos de regularizar en el más corto plazo, las licencias de uso del software

que no se encuentren sustentadas. Asimismo, se deberá a la brevedad posible, instalar un software antivirus en el servidor de desarrollo.

Recomendaciones en relación con EL ANÁLISIS DE LA REALIDAD ACTUAL DE LA ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN

1. Que la Alta Dirección como la plana Gerencial de la C.A.C. San Pedro de Andahuaylas, establezcan las acciones respectivas para superar las debilidades y deficiencias encontradas, además considerar se realice la correcta implementación del Plan de Seguridad de Información (PSI); de no ejecutarse esta podría llevar a la Institución, a riesgos innecesarios que se trasluciría en un deficiente desempeño de toda la Institución.

2. La C.A.C. San Pedro de Andahuaylas, deberá disponer que la unidad de Sistemas desarrolle e implemente un Plan de Continuidad de Negocios, basado en un diagnóstico de sus procesos críticos de negocio y que contemple este, procedimientos formales para la prueba del mismo.

3. La C.A.C. San Pedro de Andahuaylas, deberá realizar un monitoreo permanente sobre los resultados de la auditoria para controlar el avance y la correcta implementación de un Plan de Continuidad de Negocio y a la vez de un Plan de Seguridad de Información. Este examen comprenderá la revisión de los procedimientos y políticas vigentes para gestionar de manera óptima, adecuada y prudente los riesgos de las tecnologías de información,

incurriendo en los procedimientos críticos relacionados a dicho riesgo, considerando la ordenanza enumeradas en la Circular N° G-140-2009 y la Circular 139-2009, contenidas en la ordenanza del Sistema de Control Interno, aceptados desde la dación de la Resolución SBS N° 1040-99 del 26 de noviembre de 2009.