UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

"Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015"

INVESTIGADORES:

Rojas Viera Cinthia Katherine.

Zavaleta Verona Tefhany Lisseth.

ASESOR:

Dr. Ing. Jessie Bravo Jaico

Lambayeque, 2019

Rojas Viera Cinthia Katherine

Tesista

Zavaleta Verona Tefhany Lisseth

Tesista

Dr. Jessie Bravo Jaico

Asesor

Dr. Gilberto Carrión Barco

Presidente

Dr. Gisela Maquen Niño

Secretario

Ing. Fuentes Adrianzén Denny John

Vocal

ACTA DE SUSTENTACIÓN

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DECANATO
Ciudad Universitaria - Lambayeque

ACTA DE SUSTENTACIÓN Nº 018-2019-D/FACFyM

(Sustentación Autorizada por Resolución N° 375-2019-D/FACFyM)

En la ciudad de Lambayeque, siendo las 13:00 horas del día 03 de Abril del 2019 se reunieron en la videoteca del laboratorio de física de la FACFyM los miembros del Jurado designados mediante Resolución Nº 1479-2015-D/FACFyM, los docentes:

Dr. Gilberto Carrión Barco, Ing.	Presidente
Dra. Gisella Luisa Elena Maquén Niño, Ing.	Secretario
Ing. Denny John Fuentes Adrianzén	Vocal

Para recibir la tesis titulada:
"Sistema de gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC 27001 para mejorar la Seguridad del Area de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015"

desarrollada por las Bachilleres en Computación e Informática, **Rojas Viera Cinthia Katherine y Zavaleta Verona Tefhany Lisseth.**

Después de escuchar la exposición y las respuestas a las preguntas formuladas por los miembros del Jurado, se acordó APROBAR el trabajo por UNANIMIDAD con el calificativo de REGULAR

En consecuencia, las Bachilleres en referencia quedan aptas para recibir el Título Profesional de **Ingeniero en Computación e Informática,** de acuerdo a la Ley Universitaria, el Estatuto y Reglamento de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque.

Observaciones:

.....

.....

Para constancia del hecho firman.

Dr. Gilberto Carrión Barco, Ing.
Presidente

Dra. Gisella Luisa Elena Maquén Niño
Secretario

Ing. Denny John Fuentes Adrianzén
Vocal

DECLARACIÓN JURADA DE ORIGINALIDAD

Nosotras, Cinthia Katherine Rojas Viera, Tefhany Lisseth Zavaleta Verona investigadoras principales y Dr. Jessie Bravo Jaico asesor del trabajo de investigación "Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015" declaramos bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se demostrara lo contrario, asumimos responsablemente la anulación de este informe y por ende el proceso administrativo a que hubiera lugar.

Que puede conducir a la anulación del título o grado emitido como consecuencia de este informe.

Lambayeque, 03 de Abril de 2019.

Nombre de Investigadores:

Cinthia Katherine Rojas Viera.

Tefhany Lisseth Zavaleta Verona.

Nombre del Asesor:

Dr. Jessie Bravo Jaico.

DEDICATORIA

A mis padres Elmer Rojas y Lucy Viera, quienes son mi motor, que a través de su amor, paciencia y buenos valores ayudaron a trazar mi camino, asimismo a mis hermanos Percy y Ariana que son mi mayor inspiración, ojalá algún día yo me convierta en su fuerza para que puedan seguir avanzando en su camino.

Cinthia Katherine Rojas Viera

A mi familia, en especial a mi madre Marleny Verona, quien, con sus palabras, sonrisas y a veces su silencio, me demuestra su incondicionalidad y amor como mamá en todos los aspectos de mi vida, a mi padre Grover Zavaleta quien ha velado por mi bienestar y con sus consejos para perseverar en este camino, a mi tío Ángel Verona la persona que deposito toda su confianza en mi persona en el largo camino de mi vida y a mi hermano Jorge Luis que es mi bendición.

Tefhany Lisseth Zavaleta Verona

AGRADECIMIENTO

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

De igual manera mis agradecimientos a la Universidad Nacional Pedro Ruiz Gallo, a toda la escuela de Ingeniería en Computación e Informática, a mis profesores quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Finalmente quiero expresar mi más grande y sincero agradecimiento al MSc. Ing. Jessie Bravo Jaico, principal colaboradora durante todo este proceso, quien con su dirección, conocimiento y enseñanza permitió el desarrollo de este trabajo.

A mis amigos, con todos los que compartí dentro y fuera de las aulas, que se convierten en amigos de vida y aquellos que serán mis colegas, gracias por todo su apoyo y amistad.

No puedo dejar de agradecerte especialmente a ti, mi compañera fiel de Universidad, de tesis y ahora de corazón y vida.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

En la presente tesis se pretende elaborar una Guía de implementación de la seguridad basada en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas de información en el Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

Para la obtención de dicha información y recolección de datos se consideró conveniente el uso de la técnica de recolección de datos: encuestas, como medio para poder extraer la información y su posterior interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO/IEC 27001, lográndose determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de dicha área.

Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación. Se logró incrementar los procedimientos utilizados en favor de la empresa permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. Con el Plan de tratamiento de Riesgos, se permitió la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la empresa, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos.

Finalmente se propuso el Plan de Capacitación y Concienciación para poder incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la empresa, teniendo como resultado personal comprometido con la seguridad en favor de la empresa.

Una correcta implementación del SGSI propuesto en el presente trabajo de investigación permitirá incrementar el nivel de la seguridad en beneficio de la empresa.

ABSTRACT

The aim of this titling project is to develop a Safety Implementation Guide based on ISO / IEC 27001, to support the security of information systems in the Operations and Technology Area of the Global BPO Center Allus Chiclayo.

In order to obtain such information and data collection, it was considered convenient to use the data collection technique: surveys, as a means to extract the information and its subsequent interpretation; and in this way measure the problematic reality supported by the use of the ISO / IEC 27001 standard, being able to determine the deficiencies to improve the levels of security and reliability in the information systems of said area.

The results obtained allowed to determine in a real way that, when incorporating the ISO / IEC 27001 standard based on an Implementation Guide. It was possible to increase the procedures used in favor of the company allowing the detection of anomalies in the security of information, reflected in different security mechanisms to safeguard it. With the Risk Treatment Plan, the risk levels were reduced with respect to the information assets, considered threats and vulnerabilities in the company, this manifested in an adequate plan to address them and take the necessary precautions to minimize their impacts.

Finally, the Training and Awareness Plan was proposed in order to increase the percentage of knowledge on the part of the staff in policy-oriented topics, security strategies that benefit the company, resulting in personnel committed to safety in favor of the company.

A correct implementation of the ISMS proposed in this research will increase the level of security for the benefit of the company.

INTRODUCCION

En la presente tesis se lleva a cabo el proceso de análisis y diseño de un Sistema de Gestión de Seguridad de la Información para el área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo. El objetivo primordial de un Sistema de gestión de seguridad de la información es proteger la integridad, confidencialidad e integridad de todos los activos de una organización y este se logra efectuando como primera medida un minucioso análisis de los riegos a los que se enfrentan los activos de información para luego, con este insumo implantar los controles necesarios que protegerán dichos activos.

Se presenta un modelo apoyado en el estándar y norma internacional ISO/IEC 27001:2014, que buscan evitar, disminuir y/o prevenir ataques o desastres informáticos, antes que éstos ocurran. Se iniciará con un proceso de análisis de la situación actual de la empresa, luego se deberá realizar el inventario de activos y a partir de este llevar a cabo la definición del análisis de riesgos, para un posterior diseño de políticas, procesos y procedimientos claros que permitirán determinar y establecer los controles de seguridad que ayuden a gestionar los riesgos identificados.

Hoy en día las empresas privadas se han sistematizado y están utilizando herramientas, equipos informáticos y personal capacitado para facilitar los procesos de trabajo y obtener así un mayor rendimiento laboral. La mayoría de estas empresas no le dan la suficiente importancia a la auditoría de sistemas, creyendo que este tipo de herramienta no les corresponde y lo ven como un gasto y no como una inversión; es por eso que este enfoque es básico y necesario como es el de una Guía de Implementación en la seguridad de sistemas información. ISO/IEC 27001 es la una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI).

CAPITULO I

Diseño Teórico

1.1 Descripción de la Organización

Allus Global BPO Center (Business process outsourcing - Externalización de Procesos de Negocio) nace para que las empresas triunfen en los entornos cada vez más amplios, complejos y competitivos del mundo de hoy.

Especializada en la externalización de procesos de negocios brinda un portafolio de soluciones BPO de medio valor convirtiéndose en una extensión de la empresa del cliente atendiendo los procesos de múltiples industrias.

La gestión global de alta performance enfocada en la optimización de costos y en la excelencia operativa posee la capacidad de llevar adelante un modelo repetible en las plataformas, independientemente de la localización y el momento.

Entonces decimos que Allus Global BPO Center es la compañía encargada en la provisión de soluciones de Contact Centers y BPO. Con prestación de servicios con costos competitivos y eficacia operacional a los mercados de Chile. Brinda servicios de valor y atendiendo sus procesos con innovación, creatividad y conocimiento.

1.2 Misión, Visión y Objetivos de la Organización

1.2.1 Misión

Ser la compañía líder global en BPO a través de una propuesta de soluciones de clase internacional que maximice las capacidades estratégicas de nuestros clientes y los ayude a transformar sus compañías en negocios de alto rendimiento y valor.

1.2.2 Visión

Satisfacer las exigencias de nuestros clientes, colaboradores, accionistas, proveedores y comunidad a través de un modelo de gestión de valor sustentable basado en:

- Excelencia y diferenciación de los servicios.
- Conocimiento profundo de las industrias y sus procesos de negocios.
- Innovación y saber especializado.
- Tecnología de avanzada.
- Flexibilidad y adaptación a las necesidades de los distintos mercados y entornos.
- Procesos de mejora continua y calidad total.
- Gestión eficiente de los recursos disponibles.
- Desarrollo sostenible del talento humano.

1.2.3 Objetivos

- Mejorar el enfoque de la empresa del cliente, al concentrarse en procesos claves del negocio y desligarse de los procesos no centrales al mismo.
- Permitir ganar acceso a las mejores prácticas del sector, al subcontratar los procesos en empresas especializadas.
- Incrementar los beneficios de la reingeniería de procesos. Es decir, los procesos se piensan y ordenan de manera diferente.

- Mejorar la calidad de los procesos y los hace sostenibles en el tiempo.
- Permitir el control de funciones de difícil gestión o fuera de control.
- Incrementar la eficacia operacional y la productividad.
- Permitir la liberación de recursos para otras actividades centrales.
- Reducir costos. El cliente se libera de los costos que provienen de la subutilización de los recursos, capacitación y entrenamiento.
- Es un motor para el cambio, porque el BPO es sinónimo de innovación, investigación, desarrollo y creación de valor sostenido.

1.3 Estructura Orgánica

Organización, a nivel de jerarquías, de Global BPO Center Allus Chiclayo es decir desde el empleado de mayor cargo hasta el empleado de menor cargo.

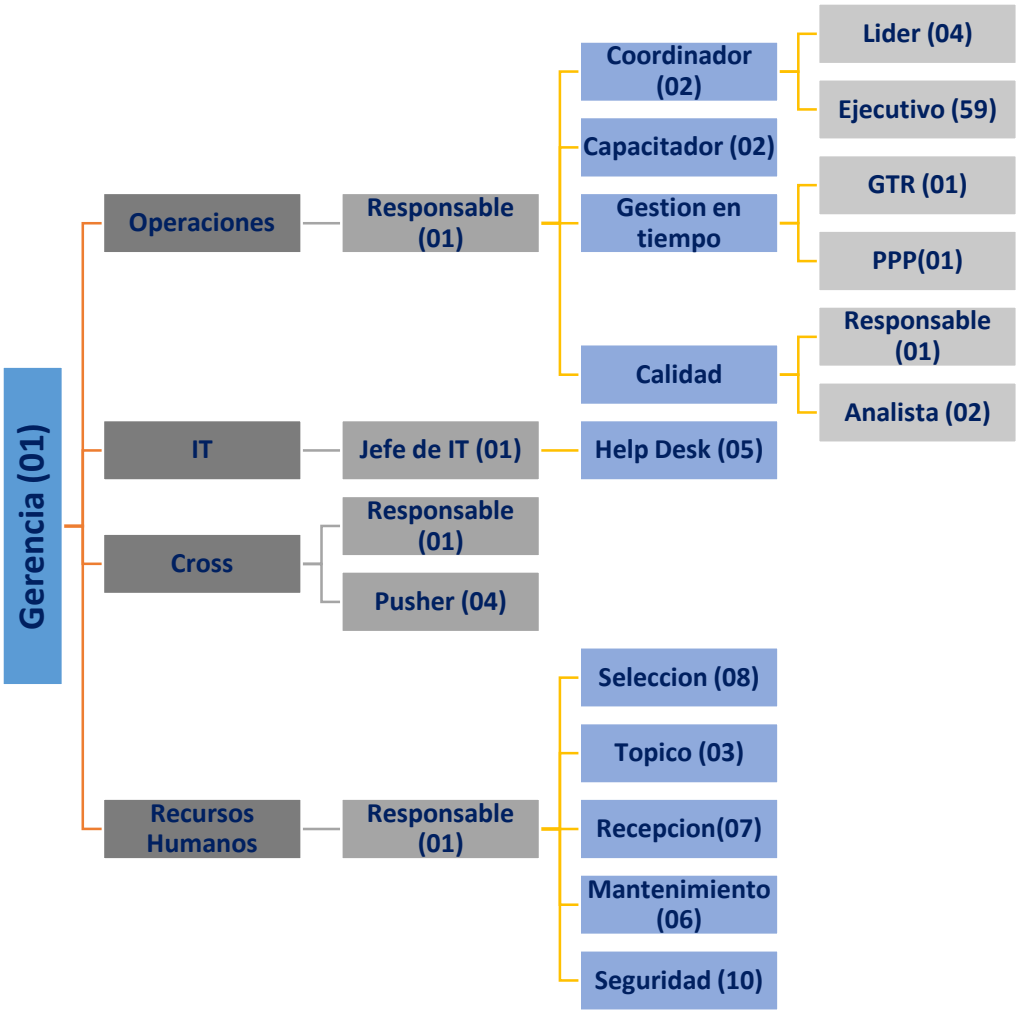


Figura 1. Organigrama de Global BPO Center Allus Chiclayo. Elaboración Propia

1.4 Descripción de la infraestructura tecnológica de la empresa

La empresa Global BPO Center Allus Chiclayo, cuenta con las siguientes áreas:

Gerencia **1**

Área de Operaciones: **(73)**

- Responsable : 1
  - Coordinadores: 2
    - ✓ Líderes: 4
    - ✓ Ejecutivos: 59
  - Capacitador 2
  - GTR(Gestor en tiempo real): 1
    - ✓ PPP(Pronosticador, Planificador y Programador): 1
  - Responsable Control de Calidad: 1
    - ✓ Analistas: 2

Área de Tecnología: **(6)**

- Jefe de IT: 1
  - Help Desk(Mesa de ayuda): 5

Área de Cros (Entrenamiento): **(5)**

- Responsable: 1
  - Pusher(Impulsador): 4

Área de Recursos Humanos: **(14)**

- Responsable: 1
  - Selección: 8
  - Tópico: 3
  - Recepción: 7
  - Mantenimiento 6
  - Seguridad: 10

Cuya infraestructura tecnológica se describe en la **Tabla 1:**

Tabla 1

Infraestructura Tecnológica de Global BPO Center Allus Chiclayo

Item	***Elemento de Análisis***	***Estado***
1	Topología de Red	a). Topología estrella b). Modelo de Red Jerárquico (Núcleo, Distribución y Acceso) c). Diseño Topológico sin redundancia en capa Distribución y Núcleo d). Conectividad a Internet por línea dedicada ISP Telefónica
2		a). Cableado Estructurado de Red Categoría 6a

	Cableado de Red y Normatividad en Centro de Datos	b). Normas EIA/TIA, T568B. TIA-942 Centro de Datos
3	Dispositivos de Red LAN	a). Switch Core (1) Cisco 3750-24SFP b). Switch Distribución (1) Cisco 2960-X Series c). Switches Acceso (8) Cisco 2960-TTL
4	Dispositivos de Telefonía IP	a). Central Telefónica (Call Manager Express - CME) 2600 b). Gateway de Voz Cisco c2811
5	Dispositivos Finales (usuarios)	a). Computadoras de Escritorio (120) Lenovo b). Computadoras Portátiles (8) HP, Lenovo c). Impresoras Multifuncionales de Red (12) HP d). Teléfonos IP (21) Cisco 7960
6	Servidores	Aplicaciones, Base de Datos y Active Directory
7	Dispositivos de Seguridad Perimetral	a). Firewall ASA 5520
8	Dispositivos de Almacenamiento	a). Dispositivo de Almacenamiento IBM Storwize V7000
9	Equipos de Respaldo Eléctrico	No posee una línea eléctrica secundaria de respaldo

10	Equipos de Respaldo de Datos (Backup)	Equipo IBM System X-3550 pero sin Software de Respaldo.
11	Servicio de Protección de los Datos	No posee un servicio de Protección de la Data a respaldar
12	Equipos de Redundancia y Alta Disponibilidad	a). No posee Redundancia en la Capa Núcleo de la Red b). No posee Redundancia en la Capa Distribución de la Red c). No posee Contingencia en Líneas de Internet d). Si posee Servidor de Aplicaciones y Base de Datos de Respaldo pero con déficit de uso.
13	Direccionamiento IP	a). Direccionamiento IP sin clase con red 10.10.0.0/16, subdivido. b). Distribución a través de VLANS VLAN 10: Gerencia 10.10.1.0/27 VLAN 11: Operaciones 10.10.11.0/26 VLAN 12: IT (Tecnologías) 10.10.12.0/27 VLAN 13: Cross 10.10.13.0/26 VLAN 14: RR.HH 10.10.14.0/26 VLAN 15: Admin-Red 10.10.15.0/25

Nota: Elaboración Propia

El diseño de la red actual de Global BPO Center Allus Chiclayo es tal y como se muestra en la ***Figura 2.***

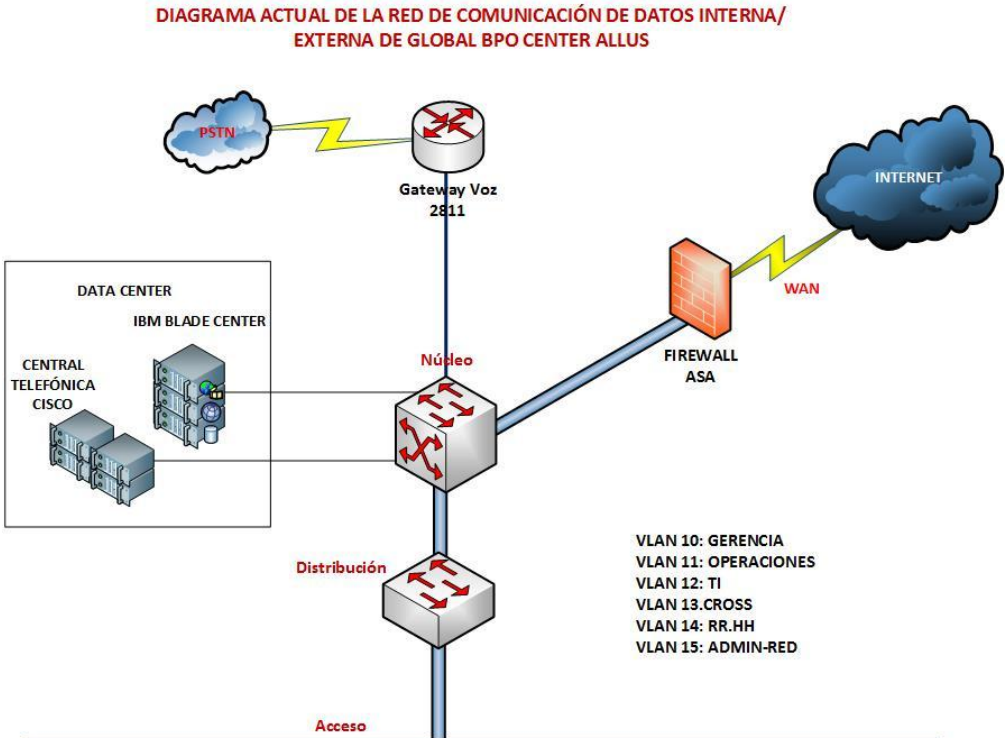


Figura 2. Diseño de Red Actual de Global BPO Center Allus Chiclayo. Elaboración Propia

1.5 Realidad problemática

1.5.1 Planteamiento del Problema

Hace 20 años la expansión del sector BPO Center: Call Center viene presentando un crecimiento, lo que en parte es bueno; ya que permiten optimizar las actividades y procesos del cliente brindándole una atención rápida y objetiva de acuerdo a sus intereses; teniendo el respaldo que su información está segura.

Pero quien puede respaldar la seguridad, en lo que se refiere a una infraestructura de información, es un concepto relacionado con los componentes del sistema (el hardware),

las aplicaciones utilizadas en la empresa (software) y el manejo de la información (usuario); considerando la variedad y cantidad de amenazas que podrían afectar la confidencialidad, disponibilidad e integridad de la información vital para la organización, el negocio y los clientes.

Así como existen especialistas en el mundo de la tecnología, no solo existen especialistas dedicados a desarrollar - por el bien de la comunidad - nuevos software que ayudan a mejorar y facilitar la vida de los seres humanos, sino también existen los llamados "hackers" o piratas cibernéticos, casi siempre jóvenes con avanzados conocimientos de informática que utilizan su inteligencia para robar información de grandes empresas, gobierno y hasta organizaciones sin o con fines de lucro.

Según las entrevistas (VER ANEXO N°1) aplicadas hemos encontrado las siguientes deficiencias con lo que respecta a la seguridad de información de Global BPO Center Allus Chiclayo.

Por ejemplo uno de sus principales procesos es la manipulación de toda la información que respecta al cliente a través de su sistema CITRIX (VER ANEXO N°03) en el cual se puede observar y hacer manejo de : Datos Generales del cliente(DNI, Nombre, Apellidos, Dirección, Teléfono, Fecha de Nacimiento), detalle de llamadas y mensajes de texto realizadas por el cliente de los últimos 180 días, Megas utilizados, recargas , compra de paquetes, boletas , últimos movimientos de pago, evaluación crediticia , reclamos y solicitudes. Toda esta información se encuentra sin respaldo alguno , ya que el personal que labora en Global BPO Center Allus Chiclayo carece de un documento de confidencialidad como parte de sus documentos de contrato; en segundo lugar la infraestructura tecnológica con la que cuenta (79 ordenadores) no

cumplen con los protocolos básicos de seguridad; por ejemplo cualquier tipo de información que se pueda obtener desde la PC o del mismo Sistema CITRIX puede ser copiada en un dispositivo externo (USB) , enviada o guardada a través del correo corporativo hacia cualquier otro correo electrónico.

Otra deficiencia importante es que todos los Ordenadores manejados por Personal de Global BPO Center Allus Chiclayo no cuentan con filtros de seguridad, por ejemplo uno de los más preocupantes es la falta de antivirus o Freeze para protegerlos de cualquier virus informático. En cuanto al acceso a los ordenadores todos los operarios cuentan con un usuario y una clave, que es proporcionada por la empresa. El usuario es creado tomando algunas iniciales del nombre del personal, mientras que la clave es un conjunto de letras y numero escogidos aleatoriamente, pero estos son entregados en una simple hoja de papel escrita a mano, la cual puede ser manipulada maliciosamente por cualquier otra persona.

El Sistema Operativo con el que cuenta cada ordenador es Windows XP sin su respectiva validación, además utilizan para el manejo de su información un software libre (OpenOffice).

Todas estas deficiencias crean la necesidad de control y gestión de la seguridad sobre la información y no solo desde un punto de vista legal en cuanto a datos personales se refiere, sino con carácter general a toda la información manejada por una compañía, convirtiéndose en un complemento importante y que aporta un plus de confianza y compromiso ante clientes y trabajadores.

Por esta misma razón nos preguntamos ¿Qué tan segura esta la información brindada por el cliente en Global BPO Center Allus Chiclayo, con tanto fraude e inseguridad que

se presenta en la actualidad? Como respuesta a esta pregunta es un paso primordial el establecer normativas y estándares que permitan obtener una base de manejo seguro de todo lo relacionado con la infraestructura de comunicación de Global BPO Center Allus Chiclayo, aplicando la cada vez más aceptada e incluso exigida Norma ISO, que es la contratación entre empresas a nivel internacional. Este sistema de gestión es de mucha importancia para que una organización pueda sobrevivir al mercado actual.

1.6 Formulación del Problema

¿Al diseñar un sistema de Gestión de Seguridad de Información basado en la Norma ISO/IEC27001, mejorará la Seguridad Del Área De Operaciones Y Tecnología De Global BPO Center Allus Chiclayo?

1.7 Justificación e Importancia de la Investigación

La información de las organizaciones, se enfrentan en forma creciente con amenazas relativas a la seguridad de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, incendio, etc.

La seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos, esto no prueba que una organización sea 100% segura, la seguridad completa no existe.

Pero en la actualidad se pueden diseñar sistemas que van de la mano con las tecnologías de manera tal que permite facilitar el trabajo del personal en cualquier institución y a la

vez tener un mayor conocimiento de la importancia e implicancia que tiene salvaguardar la información en una organización.

Aquí presentamos algunas de las innegables ventajas que proporcionaría la adopción de un SGSI en una empresa.

Tabla 2

Tabla de ventajas de la adopción de un SGSI en Global BPO Center Allus Chiclayo

Aspecto	Ventaja
Organizacional	El Sistema de Gestión de Seguridad de la información será diseñado con la finalidad de ser utilizados por todo el personal perteneciente al Área De Operaciones Y Tecnología, como guía clara y entendible, con el fin de alcanzar los objetivos trazados por la empresa.
Legal	El Sistema de Gestión de Seguridad de la información facilita el cumplimiento de las distintas normativas que afectan a una empresa u organización en lo que respecta a datos almacenados y privacidad,

	protección de datos y seguridad de la información en general.
Funcional	Permitirá a la organización tener una mejor apreciación y entendimiento de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles, de manera tal maximizar sus beneficios, capitalizar sus oportunidades y ganar ventaja competitiva.
Comercial	El Sistema de Gestión de Seguridad de la información en la organización permite a la misma obtener la certificación reconocida ISO/IEC 27001, lo cual mejora la imagen y el prestigio de la organización ante públicos que conocen la naturaleza de dicho certificado. Se convierte, por tanto, en una demostración de la profesionalidad de la organización y en una garantía de su correcto funcionamiento.

Financiero	Permitirá a los encargados del Área De Operaciones Y Tecnología, adquirir un mejor nivel de servicio en calidad, funcionalidad y facilidad en el uso de la seguridad, de manera tal que minimice costos a la organización.
Humano	Se van a adquirir nuevos conocimientos ante las posibilidades de conocer sobre seguridad de la información la cual nos permitirá fijar los mecanismos y procedimientos que deben adaptar las empresas para salvaguardar los sistemas y la información que estas contienen.

Nota: Elaboración propia

1.8 Objetivos de la Investigación

1.8.1 Objetivo General

Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad Del Área De Operaciones Y Tecnología De Global BPO Center Allus Chiclayo.

1.8.2 Objetivos Específicos

OE1: Realizar un diagnóstico de los procesos de negocio de la seguridad de la información de Global BPO Center Allus Chiclayo.

OE2: Evaluar los activos de información del área de Operaciones y Tecnología a través de una metodología de trabajo con encuestas y entrevistas.

OE3: Identificar los riesgos aplicando la Norma ISO/IEC27001 del sistema de la información de Global BPO Center Allus Chiclayo para gestionarlos o eliminarlos.

OE4: Definir los controles de seguridad de la información a través de la norma ISO 27001 en el área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

OE5: Definir las políticas, normas y procedimientos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

1.9 Limitaciones de la Investigación

- Capacidad de personal por carga laboral – tiempo. No disponen de tiempo suficiente para el desarrollo del proyecto y tenemos que adaptarnos
- Disposiciones presupuestarias
- Mantener recursos informáticos con garantía vencidas (computadoras, impresoras, teléfonos, laptops) origina mayor costo de renovación.

1.10 Antecedentes

1.10.1 Antecedentes en el contexto internacional

CASO EN EUROPA:

Tema: ***"****Proyecto CAMERSEC - Implantación de Sistemas de Gestión de Seguridad de la Información en PyMEs"*

Autor: Andrés García Martínez.

Lugar de investigación: España, Cámara de Comercio, Industria y Navegación de Málaga

Año de investigación: 26 de octubre de 2006

Resumen:

El Proyecto CAMERSEC promueve actuaciones de consultoría para Sistemas de Gestión de Seguridad de la Información realizadas por Grupo Nexus Consultores y Auditores y Tecnotur 3000, siendo decisión de la empresa adherida certificar o no dicho sistema. La iniciativa se está tramitando para que cuente con el apoyo a modo de incentivos por parte de la Agencia IDEA (Consejería de Innovación, Ciencia y Empresa) de cara a la financiación del mismo, así como la obtención de precios en condiciones ventajosas para la consultoría y certificación.

Análisis:

Este proyecto es altamente recomendado para empresas cuyos activos de información tengan un alto valor para la actividad organizacional, la implantación de un sistema de esta naturaleza ayuda a la gestión de la seguridad de sus activos de información ya que afecta a políticas y estrategias de la empresa y constituye un aporte de valor indiscutible para cualquier tipo de actividad empresarial.

CASO EN LATINOAMERICA

Tema: *"Plan de Seguridad Informática"*

Autores: María Dolores Cerini, Pablo Ignacio Prá.

Lugar de investigación: Córdoba – Argentina, EMPRESA ARGENTINA nacional.

Año de investigación: Universidad Católica de Córdoba - 2002

Resumen:

Esta es una empresa concesionaria automotriz que a través del proyecto se quiere desarrollar documentos y directrices que orienten el uso adecuado de las tecnologías de información para obtener el mayor provecho de las ventajas que brindan. De esta manera se va a implementar políticas de seguridad de la información en la compañía para que pueda desarrollarse y mantenerse en su sector de negocios. Las políticas de seguridad de la información van a fijar los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Análisis:

Este trabajo es muy importante ya que su aplicación está basada en un entorno diferente al de nosotros, el cual nos permitirá tener un mejor enfoque al proyecto de investigación que tratamos de llevar a cabo.

1.10.2 Antecedentes en el contexto nacional

Tema: *"Plan de seguridad informática para una entidad financiera."*

Autora: Norma Edith Córdova Rodríguez.

Lugar de investigación: Lima – Perú, BANCO PERUANO de capital extranjero.

Año de investigación: Universidad Nacional Mayor de San Marcos - 2003.

Resumen:

Se puede observar que gracias a la liberación y la globalización de los servicios financieros, junto con la creciente sofisticación de la tecnología financiera, están haciendo cada vez más diversas y complejas las actividad de los bancos en términos de seguridad de información para ello este proyecto busca definir un plan de Seguridad para una entidad financiera, empezando por definir la estructura organizacional (roles y funciones), después pasa a definir las políticas para finalmente concluir con un plan de implementación o adecuación a las políticas anteriormente definidas.

Análisis:

Este tema de investigación nos permite tener un conocimiento más amplio de la seguridad, que se regirá bajo normas para el adecuado uso de la información dentro y fuera de la organización siendo está muy importante dentro de la misma.

Tema*: "Diseño e implementación de un sistema de gestión de Seguridad de Información en Procesos Tecnológicos."*

Autores: Carlos Eduardo Barrantes Porras, Javier Roberto Hugo Herrera

Lugar de investigación: Lima -Universidad de San Martín de Porres

Año de investigación: 2012

Resumen:

En la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos.

El propósito de este trabajo se centró en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001:2005 e ISO 17799:2005.

Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú S.A, que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.10.3 Antecedentes en el contexto local

Tema*: "Sistema de Gestión de Seguridad de Información basado en la norma ISO/IEC 27001 para la Superintendencia de Transporte Terrestre de Personas, Carga y Mercancías (SUTRAN) – Región Lambayeque."*

Autores: Chávez Paz Jorge Homero, Nepo López Giancarlo

Lugar de investigación: Perú - Lambayeque - UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Año de investigación: 2014

Resumen:

En la actualidad el estudio de políticas y reglamentos para la seguridad de la información permite visualizar con mayor claridad la importancia y el valor dela información para la Organización adaptados a la necesidad de protección de datos. Mediante la recopilación de la información de los activos involucrados en los sistemas

de información pertenecientes a SUTRAN, se pudo constatar los problemas actuales de falencias en el mantenimiento, organización y la falta de una metodología de seguridad de la información basadas en normas que garanticen su seguridad. El estudio de la Norma ISO 27001 ha permitido mejorar el conocimiento de los sistemas de seguridad de la información, sus problemas y los medios de protección, además cubre el vacío que ha generado la inexistencia de un método documentado, sobre cómo proceder a implantar un Sistema de Gestión de Seguridad de la Información.

Tema*: "Elaboración Y Aplicación De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Para La Realidad Tecnológica De La Usat."*

Autores: César Wenceslao de la Cruz Guerrero, Juan Carlos Vásquez Montenegro.

Lugar de investigación: Perú – Lambayeque - UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO

Año de investigación: 2008

Resumen:

En la actualidad En la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos.

El propósito de este trabajo se centró en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001:2005 e ISO 17799:2005.

Esta implementación permitió un gran aumento en la seguridad de los activos de información, que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.11 Base teórica

1.11.1 ¿Qué es seguridad? (Venemedia, 2014)

La palabra Seguridad proviene del latín *securitas*, que a su vez deriva de *securus* (sin cuidado, sin precaución, sin temor a preocuparse), que significa libre de cualquier peligro o daño, y desde el punto de vista psicosocial se puede considerar como un estado mental que produce en los individuos (personas y animales) un particular sentimiento de que se está fuera o alejado de todo peligro ante cualquier circunstancia. La seguridad es la garantía que tienen las personas de estar libre de todo daño, amenaza, peligro o riesgo; es la necesidad de sentirse protegidas, contra todo aquello que pueda perturbar o atentar contra su integridad física, moral, social y hasta económica.

En la seguridad se tienen dos dimensiones: individual y social. La primera se refiere al cuido que se da cada persona, para no someterse a riesgos que pongan en peligro la salud y la vida. La seguridad social se refiere al conjunto de leyes, organismos, servicios e instalaciones que cubren y protegen algunas necesidades de la población, como la sanidad, las pensiones, los subsidios, etc. Es muy importante saber que la seguridad implica la forma correcta de hacer las cosas; de allí que sea tan necesario todo el mayor esfuerzo que se dedique en la eliminación de peligros y prevención de accidentes.

El término de seguridad se usa en muchos contextos; se encuentra la seguridad en el trabajo, la cual es un factor muy importante y determinante para el funcionamiento adecuado del lugar en donde se trabaje. También está la seguridad industrial, es el conjunto de conocimientos aplicados para evitar accidentes de trabajo en industrias.

La seguridad nacional que se emplea para hacer referencia a las amenazas o riesgos que provienen del exterior de un Estado y que afectan o ponen en cuestión su soberanía y, por tanto, su capacidad para salvaguardar su propia integridad tanto territorial como institucional.

La seguridad informática es la disciplina, técnicas y herramientas diseñadas para proteger la confiabilidad, integridad y disponibilidad de los datos y de los sistemas. Existen otros tipos de seguridad tales como seguridad alimentaria, seguridad ecológica, seguridad económica, seguridad ciudadana, seguridad vial, entre otros.

1.11.2 ¿Qué es seguridad en TI? (Wikipedia, 2016)

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

1.11.3 ¿Qué es un riesgo? (Mejía, 2014)

La palabra Riesgo viene del Italiano Risicare, que Significa desafiar, retar, enfrentar; también se define como poner en peligro a una persona, en algunos escritos se refiere a la proximidad de un daño. El riesgo también es conocido como la probabilidad de pérdida la cual permite cuantificar el riesgo a diferencia de la posibilidad de riesgo donde este no se puede cuantificar. El riesgo es Incertidumbre relacionado con la duda ante la posible ocurrencia de algo que puede generar pérdidas.

1.11.4 Tipos de Riesgos (Mejía, 2014)

Desde el punto de vista empresarial existen innumerables riesgos, generados tanto por el entorno como por el desarrollo normal de sus actividades.

1.11.4.1 Riesgos Del Entorno

Comprende elementos como el país donde está ubicada la empresa, su naturaleza, la región y ciudad, además del sector, la industria y condiciones económicas, políticas, sociales y culturales. En este orden de ideas se pueden presentar riesgos como:

a. **Riesgo asociado a la naturaleza:** Relacionados con riesgos meteorológicos y climáticos como huracanes, lluvias, maremotos, sequías, que afectan el logro de objetivos.

b. **Riesgos asociados al País:** De acuerdo al País se pueden encontrar riesgos como el riesgo país que hace referencia al grado de peligro que represente este para las inversiones extranjeras

1.11.4.2 Riesgos generados en la empresa:

A nivel de la empresa se pueden presentar un sinfín de riesgos que pueden afectar los procesos, recursos humanos, físicos, tecnológicos, financieros y organizacionales, a los clientes y hasta la imagen de la empresa. En este orden de ideas se pueden presentar riesgos como:

a. **Riesgo de reputación:** es el desprestigio de la empresa que trae como consecuencia la pérdida de credibilidad y confianza del público por fraude, insolvencia, conducta irregular de los empleados, rumores, errores cometidos en la ejecución de alguna operación por falta de capacitación del personal clave o deficiencia en el diseño de los procedimientos, este riesgo puede traer efectos como disminución de la demanda, o la perdida de negocios atribuibles al desprestigio generado.

b. **Riesgo puro:** este riesgo al materializarse origina perdida, como un incendio, un accidente, una inundación.

c. **Riesgo especulativo:** al materializarse genera la posibilidad de generar instantáneamente beneficio o perdida, como una aventura comercial, la inversión en divisas ante expectativas de devaluación o revaluación, la compra de acciones, el lanzamiento de nuevos productos, etc.

d. **Riesgo estratégico:** son las perdidas ocasionas por las definiciones estratégicas inadecuadas y errores en el diseño de planes , programas, estructura, integración del modelo de operación con el direccionamiento estratégico, asignación de recursos, estilo de dirección, además de ineficiencia en la adaptación a los cambios constantes del entorno empresarial, entre otros.

e. **Riesgo operativo:** es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la empresa por fallas en procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos.

f. **Riesgo de mercado:** puede generar ganancias o pérdidas a la empresa al invertir en bolsa, debido a la diferencia en los precios que se registran en el mercado.

g. **Riesgo precio de insumos y productos:** se refiere a la incertidumbre sobre la magnitud de los flujos de caja debido a posibles cambios en los precios que una empresa puede pagar por la mano de obra , materiales y otros insumos de su proceso de producción, y por los precios que puede demandar por sus bienes o servicios.

h. **Riesgo de crédito:** consiste en que los clientes y las partes a las cuales se les ha prestado dinero, fallen en el pago. La mayoría de las empresas se enfrentan ante

este riesgo por cuentas por cobrar, pero esta exposición es más alta en las instituciones financieras.

i. **Riesgo legal:** se refiere a la pérdida en caso de incumplimiento de la contraparte en un negocio y la imposibilidad de exigirle jurídicamente el cumplimiento de los compromisos adquiridos. También se puede presentar al cometer algún error de interpretación jurídica u omisión en la documentación, y en el incumplimiento de normas legales y disposiciones reglamentarias que pueden conducir a demandas o sanciones.

j. **Riesgo tecnológico:** el uso de la tecnología genera riesgos como los virus, el vandalismo puro y de ocio en las redes informáticas, fraudes, intrusiones por hackers, el colapso de las telecomunicaciones que pueden generar el daño de la información o la interrupción del servicio. También está el riesgo del constante cambio de tecnología lo que puede ocasionar que las empresas no estén preparadas para adoptarlas y esto incremente sus costos, menor eficiencia, incumplimiento en las condiciones de satisfacción de los servicios prestados a la comunidad.

k. **Riesgos laborales:** pueden ser accidentes de trabajo y enfermedades profesionales, pueden ocasionar daños tanto a la persona como a la misma empresa.

l. **Riesgos físicos:** afectan a los materiales como por ejemplo; corto circuito, explosión física, daño en la maquinaria, daño en equipos por su operación, por su diseño, fabricación, montaje o mantenimientos; deterioros de productos y daños en vehículos.

1.11.5 ¿Qué es un Activo? (Wikipedia, Wikipedia, 2016)

Es el conjunto de bienes económicos, derechos a cobrar que posee un comerciante o una empresa y aquellas erogaciones que serán aprovechadas en ejercicios futuros. El Marco Conceptual para la Información Financiera del IASB (International Accounting Standards Board (Junta de Normas Internacionales de Contabilidad)), emitido el 1 de enero de 2012, establece la siguiente definición:

«Un activo es un recurso controlado por la entidad como resultado de sucesos pasados, del que la entidad espera obtener, en el futuro, beneficios económicos».

En las registraciones o registros contables cuando se produce una variación de un elemento de activo, ésta puede ser de dos tipos: aumento del activo, se carga o debita anotándose en el debe o disminución del activo se abona o acredita, esto es, se realiza una anotación en el haber.

1.11.6 Tipos de Activos (Empresarial, 2016)

Dentro de los activos de la empresa se pueden diferenciar dos tipos:

1.11.6.1 Activo fijo:

Hace referencia a aquellos bienes y derechos duraderos, que han sido obtenidos con el fin de ser explotados por la empresa. Se trata de aquellos bienes inmuebles, materiales, equipamiento, herramientas y utensilios con los que no se va a comercializar, es decir, que no se van a convertir en líquido, al menos durante el primer año.

En cualquier tipo de empresa se pueden diferenciar dos tipos de activos fijos:

1.11.6.1.1 Activos fijos tangibles.

Dentro de esta categoría se incluyen todos aquellos bienes y materiales tangibles, es decir, se pueden tocar. En función de las características de tu negocio los activos fijos podrán variar de manera notoria. Algunos de los bienes tangibles de los que pueden disfrutar las empresas, acorde a la clasificación establecida por el Plan General Contable, son:

- Terrenos y bienes naturales. Aquellos terrenos y solares que posea la empresa, ya sea urbanos o no.
- Construcciones. Hace referencia a todo tipo de inmuebles, en general, que son propiedad de la organización, como edificios, naves, pisos o locales.
- Instalaciones técnicas. Este concepto hace alusión a todos aquellos elementos que, en conjunto, constituyen una unidad de uso especializada necesaria para la actividad de la empresa. Se trata de montajes en cadena y otro tipo de construcciones similares.

  Maquinaria. Dentro de este apartado se incluyen todas aquellas máquinas, vehículos industriales y herramientas necesarias para la actividad cotidiana.
- Mobiliario. Todas las estanterías, mesas, sillas, mostradores y demás muebles que la empresa posee.
- Equipos para procesos informáticos. Compuesto por ordenadores, impresoras, escáner y demás aparatos electrónicos.
- Elementos de transporte. Dentro de esta categoría se encuentran todos los medios de transporte que formen parte de los bienes de la compañía, como coches,

camiones, motos, barcos, etc., utilizados para el transporte de personas, mercancías, materiales o animales.

- Otros. Aquellos bienes que no se puedan incluir dentro de ninguna de las categorías nombradas.

1.11.6.1.2 Activos fijo intangibles.

Por su parte, los activos intangibles hacen referencia a aquellos bienes y derechos que no son físicos o palpables como tal. Se trata de bienes como marcas, permisos, patentes, derechos de traspaso, fondos de comercio o gastos de investigación.

Marcas registradas. Una marca registrada es un derecho que pude ser adquirido, vendido o arrendarse.

- Patentes. Es un derecho que te otorga un permiso especial y exclusivo, para vender o fabricar un producto o servicio.
- Derechos de autor. Con este derecho se garantiza al autor su derecho a explotar sus productos.
- Franquicias. Por medio de este derecho, la empresa adquiere permiso para poder hacer uso de la marca y productos de otra empresa durante un tiempo determinado.
- Licencias y permisos. Se trata de autorizaciones a través de las que se concede el uso de bienes diferentes, como el caso de recursos software para la empresa.

1.11.6.2 Activo circulante:

Este tipo de activo, también denominado corriente o líquido, hace referencia al dinero del que dispone la empresa o del que puede disponer en un plazo inferior a doce meses. Es decir, aquellos bienes, derechos o créditos, que pueda utilizarse o convertirse en líquido cuando se necesite.

1.11.7 ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), y su origen (de la propia organización o de fuentes externas). (Ampuero Chang, 2011)

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. La Seguridad de la Información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (Alexander G., 2007)

De una manera más estricta una metodología para, un Sistema de Gestión de Seguridad de la Información es aquella parte del Sistema General de gestión de una organización que deberá incorporar:

- La Política.
- La Estructura Organizativa.
- Los Procedimientos.
- Los Controles necesarios para implantar la gestión de la Seguridad de la Información. (Ampuero Chang, 2011)

1.11.8 ¿Para qué sirve un SGSI? (Ampuero Chang, 2011)

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de la información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de la organización para asegurar el máximo beneficio de nuevas oportunidades de mejora de la organización, son algunos de los aspectos fundamentales para la creación de una metodología para la implementación de un SGSI, es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una metodología

sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

1.11.9 Fundamentos de un SGSI (Alexander G., 2007)

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- **Confidencialidad**

  La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad**

  Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad**

  Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

1.11.10¿Qué consideraciones se debe incluir para un SGSI? (Ampuero Chang, 2011)

Una metodología para un Sistema de Gestión de la Seguridad de la Información incluye lo siguiente:

a. Documentos de Nivel 1

Manual de Seguridad: elaborado con la dirección, determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

b. Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información en base a una metodología concreta.

c. Documentos de Nivel 3

Instrucciones y formularios: documentos que describen como se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

d. Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI.

1.11.11Tareas de la Gerencia de un SGSI (Ampuero Chang, 2011)

Uno de los componentes primordiales en la implantación exitosa de una metodología para Sistema de Gestión de Seguridad de la Información es la participación de la dirección.

No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que solo puede tomar la gerencia de la organización. No se debe caer en el error de considerar que una metodología para un SGSI es mera cuestión técnica o documentada relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

- **Compromiso con la Dirección**

  La Dirección tiene varias de las responsabilidades claves en la puesta en marcha y funcionamiento de la metodología para un SGSI.

  Es la Dirección la que debe:

  - ✓ Aprobar la Política y los objetivos de seguridad.
  - ✓ Aprobar los planes de formación y auditorías.
  - ✓ Realizar la revisión del SGSI.
  - ✓ Demostrar su compromiso con la seguridad de la información para promover una cultura efectiva dentro de la organización.

1.11.12Norma ISO 27001 (Center, 2016)

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:

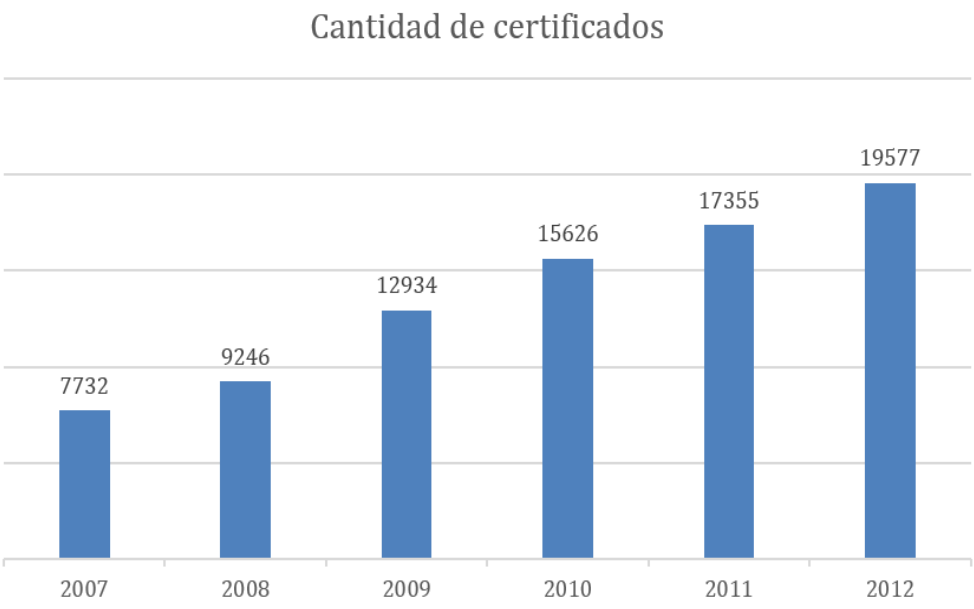


Figura 3. Cantidad de Certificados. Encuesta ISO sobre certificaciones de la norma para Sistemas de Gestión

1.11.13¿Cómo funciona la ISO 27001? (Center, 2016)

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Figura 4. Estructura de ISO 27001. (Center, 2016)

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos).

Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas

organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

1.11.14¿Por qué ISO 27001 es importante para una empresa? (Center, 2016)

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- **Cumplir con los requerimientos legales**

Cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

- **Obtener una ventaja comercial**

Si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

- **Menores costos**

La filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

- **Una mejor organización**

En general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no sabe qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

1.11.15¿Dónde interviene la gestión de seguridad de la información en una empresa?

(Center, 2016)

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciber seguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

1.11.16¿Cómo es realmente ISO 27001? (Center, 2016)

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

- Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
- Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.
- Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
- Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.

- Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
- Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

- Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
- Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
- Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
- Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.
- Anexo A – este anexo proporciona un catálogo de 114 controles

1.11.17¿Cómo implementar ISO 27001? (Center, 2016)

Para implementar la norma ISO 27001 en una empresa, usted tiene que seguir estos 16 pasos:

- Obtener el apoyo de la dirección
- Utilizar una metodología para gestión de proyectos
- Definir el alcance del SGSI
- Redactar una política de alto nivel sobre seguridad de la información
- Definir la metodología de evaluación de riesgos
- Realizar la evaluación y el tratamiento de riesgos
- Redactar la Declaración de aplicabilidad
- Redactar el Plan de tratamiento de riesgos
- Definir la forma de medir la efectividad de sus controles y de su SGSI
- Implementar todos los controles y procedimientos necesarios
- Implementar programas de capacitación y concienciación
- Realizar todas las operaciones diarias establecidas en la documentación de su SGSI
    - ✓ Monitorear y medir su SGSI
    - ✓ Realizar la auditoría interna
    - ✓ Realizar la revisión por parte de la dirección
    - ✓ Implementar medidas correctivas

1.11.18¿Cómo obtener la certificación? (Center, 2016)

Existen dos tipos de certificados ISO 27001: (a) para las organizaciones y (b) para las personas. Las organizaciones pueden obtener la certificación para demostrar que cumplen con todos los puntos obligatorios de la norma; las personas pueden hacer el curso y aprobar el examen para obtener el certificado.

Para obtener la certificación como organización, se debe implementar la norma tal como se explicó en las secciones anteriores y luego se debe aprobar la auditoría que realiza la entidad de certificación. La auditoría de certificación se realiza siguiendo estos pasos:

- 1° Paso de la auditoría (revisión de documentación): los auditores revisarán toda la documentación.
- 2° Paso de la auditoría (auditoría principal): los auditores realizarán la auditoría in situ para comprobar si todas las actividades de una empresa cumplen con ISO 27001 y con la documentación del SGSI.
- Visitas de supervisión: después de que se emitió el certificado, y durante su vigencia de 3 años, los auditores verificarán si la empresa mantiene su SGSI.
- Las personas pueden asistir a diversos cursos para obtener certificados. Los más populares son:
- Curso de Auditor Líder en ISO 27001: este curso de 5 días le enseñará cómo realizar auditorías de certificación y está orientado a auditores y consultores.
- Curso de Implementador Principal de ISO 27001: este curso de 5 días le enseñará cómo implementar la norma y está orientado a profesionales y consultores en seguridad de la información.
- Curso de auditor interno en ISO 27001: este curso de 2 ó 3 días le enseñará los conceptos básicos de la norma y cómo llevar a cabo una auditoría interna; está orientado a principiantes en este tema y a auditores internos.

1.11.19 Otras Normas relacionadas con Seguridad de la Información (Gupta, 2005)

- ISO/IEC 27002 proporciona directrices para la implementación de los controles indicados en ISO 27001. ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799-1.
- ISO/IEC 27004 proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO 27001 ya que explica cómo determinar si el SGSI ha alcanzado los objetivos.
- ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO 27001 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación. ISO 27005 ha surgido de la norma británica BS 7799-3.
- ISO 22301 define los requerimientos para los sistemas de gestión de continuidad del negocio, se adapta muy bien con ISO 27001 porque el punto A.17 de esta última requiere la implementación de la continuidad del negocio aunque no proporciona demasiada información.
- ISO 9001 define los requerimientos para los sistemas de gestión de calidad. Aunque a primera vista la gestión de calidad y la gestión de seguridad de la información no tienen mucho en común, lo cierto es que aproximadamente el 25% de los requisitos de ISO 27001 y de ISO 9001 son los mismos: control de documentos, auditoría

interna, revisión por parte de la dirección, medidas correctivas, definición de objetivos y gestión de competencias. Esto quiere decir que si una empresa ha implementado ISO 9001 le resultará mucho más sencillo implementar ISO 27001.

1.11.20 MAGERIT:

MAGERIT es la metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que en la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, esto supone beneficios para los usuarios; y da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si éstos, son valiosos, MAGERIT permitirá saber cuánto valor está en juego y ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Actualmente se encuentra en la versión 2.0; durante el periodo transcurrido desde la publicación de la primera versión de MAGERIT (1997), el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad

1.11.20.1 Descripción General De MAGERIT:

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC, como pueden ser guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista, según esto.

MAGERIT persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.11.20.2 Ventajas de MAGERIT: Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles

1.11.20.3 Desventajas de MAGERIT: El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa

1.11.20.4 El Método:

En la Planificación del Análisis y Gestión de Riesgos se establecen las consideraciones necesarias para arrancar el proyecto, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del proyecto**.**

1.11.20.4.1 Análisis de Riesgos:

En el Análisis de riesgos se identifican y valoran los elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables. Es la consideración sistemática del daño probable que puede causar un fallo en la seguridad de la información, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

- **Elementos Del Análisis De Riesgos:**

  En la realización de un Análisis y Gestión de Riesgos según MAGERIT, el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

- ✓ **Activos:** Recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información o dato.
- ✓ **Amenazas:** Determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza
- ✓ **Vulnerabilidades:** Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- ✓ **Impactos:** Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto.
- ✓ **Riesgo:** Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia.
- ✓ **Salvaguardas (Funciones, Servicios y Mecanismos):** Un salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas.

- **Activos**

Identificación de los Activos protegibles del Dominio MAGERIT tiene en cuenta cinco grandes categorías de Activos:

- ✓ El entorno o soporte del Sistema de Información, que comprende activos tangibles (como edificaciones, mobiliario, lugares de trabajo), equipamiento de suministro auxiliar (energía, climatización, comunicaciones) y personal.

- ✓ El sistema de información propiamente dicho del Dominio (hardware, redes, software, aplicaciones).
- ✓ La propia información requerida, soportada o producida por el Sistema de Información que incluye los datos informatizados, así como su estructuración (formatos, códigos, claves de cifrado) y sus soportes (tratables informáticamente o no).
- ✓ Las funcionalidades del Dominio que justifican al Sistema de Información, incluido desde el personal usuario a los objetivos propuestos por la dirección del Dominio.
- ✓ Otros Activos, de naturaleza muy variada, por ejemplo la imagen de la organización, la confianza que inspire, el fondo de comercio, la intimidad de las personas, etc.

- **Riesgos:**

El riesgo es la posibilidad de que se produzca un impacto en un Activo o en el Dominio.

Para MAGERIT el cálculo del riesgo ofrece un Indicador que permite tomar decisiones por comparación explícita con un Umbral de Riesgo determinado; o sea una propiedad de la relación Vulnerabilidad /Impacto y por tanto de la relación entre Activos y Amenazas.

- **Amenazas**

Las amenazas se definen como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

[N] Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[I] De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

[E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas.

[A] Ataques intencionados: Fallos deliberados causados por las personas.

Errores y amenazas constituyen frecuentemente las dos caras de la misma moneda: algo que le puede pasar a los activos sin animosidad o deliberadamente. Se pueden dar hasta tres combinaciones:

- ✓ Amenazas que sólo pueden ser errores, nunca ataques deliberados.
- ✓ Amenazas que nunca son errores: siempre son ataques deliberados.
- ✓ Amenazas que pueden producirse tanto por error como deliberadamente.

MAGERIT considera distintos 'productores' de las Amenazas (no humanos, humanos involuntarios o humanos voluntarios) para tener en cuenta la diversidad de sus causas, independientemente de sus consecuencias.

Cada tipo de productores genera un tipo de causas de los cambios del estado de seguridad en los Activos: accidentes, errores e intervenciones intencionales, éstas realizadas con presencia del agresor por 'tele-acción' (usando medios de comunicación). Las Amenazas se clasifican así:

Grupo A de Accidentes

A1: Accidente físico de origen industrial: incendio, explosión, inundación por roturas, contaminación por industrias cercanas o emisiones radioeléctricas.

A2: Avería: de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema

A3: Accidente físico de origen natural: riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe.

A4: Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, fluidos y suministros diversos.

A5: Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática.

Grupo E de Errores

E1: Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema.

E2: Errores de diseño existentes desde los procesos de desarrollo del software (incluidos los de dimensionamiento, por la posible saturación).

E3: Errores de ruta, secuencia o entrega de la información en tránsito.

E4: Inadecuación de monitorización, trazabilidad, registro del tráfico de información.

Grupo P de Amenazas Intencionales Presenciales

P1: Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura).

P2: Acceso lógico no autorizado con intercepción pasiva simple de la información.

P3: Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración; es decir, reducción de la confidencialidad para obtener bienes o servicios aprovechables (programas, datos).

P4: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración: es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje inmaterial, infección vírica).

P5: Indisponibilidad de recursos, sean humanos (huelga, abandono, rotación) o técnicos (desvío del uso del sistema, bloqueo).

Grupo T de Amenazas Intencionales Teleactuadas.

T1: Acceso lógico no autorizado con intercepción pasiva (para análisis de tráfico).

T2: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración.

T3: Acceso lógico no autorizado con modificación (Inserción, Repetición) de información en tránsito.

T4: Suplantación de Origen (del emisor o reemisor, 'man in the middle') o de Identidad.

T5: Repudio del Origen o de la Recepción de información en tránsito.

- **Vulnerabilidades**:

La Vulnerabilidad de un Activo se define como la potencialidad o posibilidad de ocurrencia de la materialización de una Amenaza sobre dicho Activo. Es una propiedad de la relación entre un Activo y una Amenaza y se clasifica de acuerdo con éstos (conviene centrarse en las amenazas más fácilmente materializables y/o más impactantes).

La vulnerabilidad se expresa con un valor decimal, comprendido entre los valores extremos: 0 (la Amenaza no afecta al Activo) y 1 (no alcanzable pues significa la agresión permanente). MAGERIT evita cuidadosamente los términos probable y probabilidad al definir la Vulnerabilidad, mientras que emplea los conceptos de potencial y potencialidad como más cercanos al tránsito de amenaza materializable en agresión.

Esa potencialidad se convierte en frecuencia para los casos de calculabilidad definida (cifra de cuántas veces falla una disquetera por año) y en posibilidad para los casos de calculabilidad más difusa (que MAGERIT también trata con técnicas avanzadas especiales).

MAGERIT mide la Vulnerabilidad por la frecuencia histórica cuantitativa de la materialización de la Amenaza sobre el Activo, cuando es factible (fiabilidad de un componente hardware, número de fallos de software); o bien por la potencialidad cualitativa de dicha materialización, cuya primera aproximación lleva a emplear una escala vista en las Amenazas potenciales (consideradas ahora reales, o sea agresiones).

1.11.21Cobit

La información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante.

La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios. Como resultado, hoy más que nunca, las empresas y sus ejecutivos se esfuerzan en:

- Mantener información de alta calidad para soportar las decisiones del negocio.
- Generar valor al negocio con las inversiones en TI, por ejemplo, alcanzando metas estratégicas y generando beneficios al negocio a través de un uso de las TI eficaz e innovador.

- Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- Mantener los riesgos relacionados con TI en un nivel aceptable.
- Optimizar el coste de los servicios y tecnologías de TI.
- Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Durante la pasada década, el término "gobierno" ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión.

Además, cada vez se aprueba más legislación y se implementan regulaciones para cubrir esta necesidad.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

Figura 5. Principios de Cobit. (ISACA, 2012)

COBIT 5 se basa en cinco principios claves (mostrados en la Figura N° 5) para el gobierno y la gestión de las TI empresariales:

- *Principio 1 - Satisfacer las Necesidades de las Partes Interesadas*

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

- *Principio 2 - Cubrir la Empresa Extremo a Extremo*

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- ✓ Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- ✓ Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

- *Principio 3 - Aplicar un Marco de Referencia único integrado*

  Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

- *Principio 4 - Hacer Posible un Enfoque Holístico*

  Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa.

  Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo

  COBIT 5 define siete categorías de catalizadores:

  - ✓ Principios, Políticas y Marcos de Trabajo
  - ✓ Procesos
  - ✓ Estructuras Organizativas
  - ✓ Cultura, Ética y Comportamiento
  - ✓ Información
  - ✓ Servicios, Infraestructuras y Aplicaciones
  - ✓ Personas, Habilidades y Competencias

- *Principio 5 - Separar el Gobierno de la Gestión*

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

- ✓ **Gobierno**

  El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

- ✓ **Gestión**

  La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

1.12 Conceptos y definiciones

- **Amenazas:** Cualquier acción o evento que puede ocasionar consecuencias adversas (Wikipedia, 2016)
- **Archivo Log:** Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o IP´s involucradas en el proceso, etc.) (Manual de politicas y normas de seguridad informatica)

- **Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema. (JEANNELLYS, 2009)
- **Confidencialidad:** Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información. (Quispe Arroyo)
- **Control de Accesos**: Consiste en controlar el acceso a recursos de usuario autorizados. (Chávez Paz Jorge Homero, 2014)
- **Cuenta:** Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático. (JORGE, 2014)
- **Desastre o Contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio. (Seguridad de la información y auditoría de sistemas)
- **Disponibilidad:** Consiste en la posibilidad de acceder a la información o a utilizar un servicio siempre que se necesite. (Chávez Paz Jorge Homero, 2014)
- **Integridad:** Consiste en garantizar que una información o mensaje no han sido manipulados. (Seguridad Informatica, 2015)
- **Malware:** Todo software dañino para los sistemas, englobándose dentro del término a virus, gusanos y troyanos
- **Remota:** Forma de administrar los equipos informáticos o servicios a través de terminales o equipos remotos, físicamente separados de la Empresa.

- **Riesgo:** posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización. (Seguridad de la información y auditoría de sistemas)
- **Soporte Técnico: (Personal en Outsourcing):** Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la Empresa. (Manual de politicas y normas de seguridad informatica)
- **Terceros:** Empresas, proveedores de software, convenios educativos que tengan anexos con la Empresa. (Chávez Paz Jorge Homero, 2014)
- **Usuario:** Defínase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red Empresarial y tenga una especie de vinculación laboral con la Empresa. (Ayub, 2012)
- **Virus:** Son programas normalmente dañinos que se añaden a ficheros ejecutables y tiene la propiedad de ir replicándose por los sistemas y/o ficheros adyacentes. Los virus informáticos pueden causar "muertes" de sistemas (HENAO ACOSTA)
- **Vulnerabilidad:** Punto en el que un recurso es susceptible de ataque. Al realizar esta relación, se puede cuantificar el daño que se causaría si la amenaza cumpliera su objetivo y obviamente sería directamente proporcional al grado de vulnerabilidad del sistema. (HENAO ACOSTA)

CAPITULO II

Métodos y Materiales

2.1 Tipo de Investigación

Investigación Tecnológica Formal

2.2 Hipótesis

Si se diseña un Sistema de Gestión de Seguridad de Información basado en la Norma ISO/IEC27001, mejorará la seguridad del Área de Operaciones y Tecnológica de Global BPO Center Allus Chiclayo.

2.3 Variables

2.3.1 Variable Independiente

Sistema de Gestión de Seguridad de Información.

2.3.2 Variable Dependiente

Seguridad del Área de Operaciones y Tecnología.

2.4 Selección de la Metodología a utilizar para el desarrollo de la investigación

2.4.1 PDCA: Plan-Do-Check-Act (STANDARDIZATION, 2013)

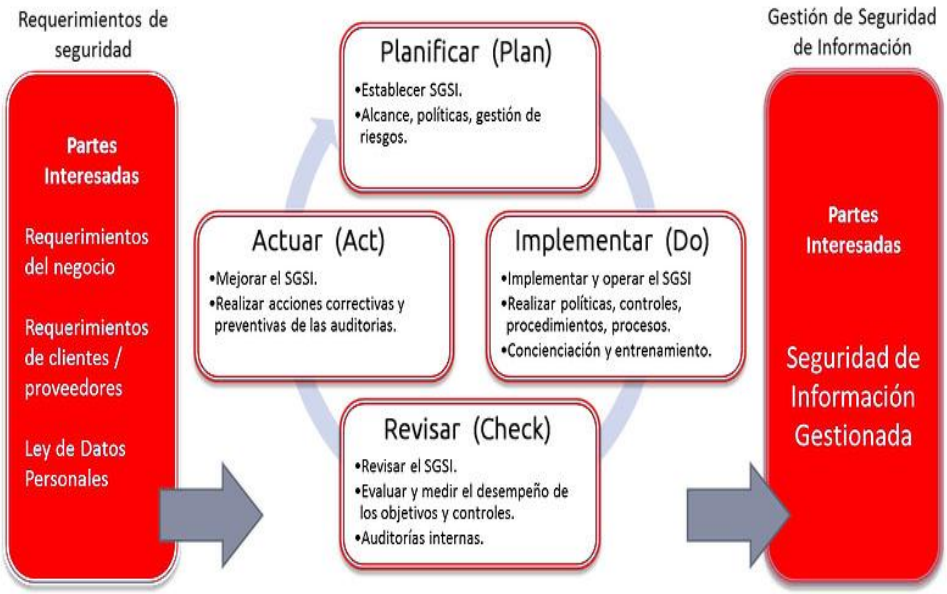


Figura 6. Implementación de un (SGSI). (REDSER, 2016)

Para establecer y gestionar una metodología adecuada para la implementación de un Sistema de Gestión de Seguridad de la Información se debe garantizar la interpretación del ciclo continuo PDCA, optimo en los sistemas de gestión de la calidad, y de esta manera poder incorporar estos aspectos en el desarrollo de la misma.

1. **PLAN: Establecer el SGSI**

   Planificar y establecer los objetivos de seguridad de la información, para escoger los controles adecuados (la norma contiene un catálogo de 133 posibles controles) Planificar y diseñar una metodología para un SGSI implica:

   a) **Establecer el alcance del SGSI.** Es el primer paso. Hay que decidir que parte de la organización va a ser protegida, o toda la organización.

b) **Establecer las responsabilidades.** Se asignará un responsable de seguridad, que coordine las tareas y esfuerzos en materia de seguridad.

c) **Definir política de seguridad.** La política de la organización es la que va a sentar las bases de lo que se va a hacer, mostrará el compromiso de la dirección con el SGSI y servirá para coordinar responsabilidades y tareas.

2. **DO (Hacer): Implementar y utilizar el SGSI**

Implementar y operar todo lo planificado en la fase anterior.

Algunas medidas de corte técnico requerirán poca documentación, pero otras más de índole organizativa, como son el caso de la gestión de la o de los recursos humanos, necesitarán ser documentadas. (Ampuero Chang, 2011)

Una tarea importante dentro de esta fase es la formación. Desde luego la formación e información continua al personal dentro del proyecto debe comenzar con el mismo, se debe involucrar a todos aquellos que se vean afectados por el SGSI tanto de forma directa como indirecta.

3. **CHECK (Comprobar): Monitorizar y revisar el SGSI**

Comprobar el funcionamiento y verificar si los resultados cumplen lo establecido.

Una vez puesto en marcha el plan de seguridad, se deben revisar periódicamente de manera que se detecten posibles desviaciones. Pueden haberse producido retrasos en las acciones a tomar o bien haber surgido problemas que no fueron previstos y que hay que solucionar para continuar con el plan.

4. **ACT (Actuar): Mantener y mejorar el SGSI**

Actuar para mejorar todos los incumplimientos detectados en la fase anterior.

Cuando mediante cualquiera de las actividades de comprobación realizadas o incluso durante la operativa habitual del SGSI se descubren no conformidades, reales o potenciales, deben tomarse medidas para solucionarlas. Hay maneras para ello:

a) Adoptar acciones correctoras. Las decisiones de qué hacer y cómo deben estar basadas en una identificación precisa de la causa del problema para evitar malgastar recursos simplemente arreglando provisionalmente un incidente que volverá a repetirse si no se ataca la causa que lo originó.

b) Adoptar acciones preventivas. Son aquellas que se toman para prevenir que ocurra algo no deseado. La gran ventaja de estas acciones es que evidentemente es más eficaz y sencillo poder prevenir los problemas que solucionarlos. De todos modos es fundamental también en este caso determinar cuál es la posible fuente de problemas con el objeto de eliminarla.

c) Definir acciones de mejora. Las acciones de mejora no surgen de la necesidad de solucionar un problema sino de la dinámica del sistema de gestión, que impulsa a refinar procesos y superar objetivos continuamente.

2.4.2 Criterios de Selección de la Metodología empleada

La metodología para identificar y analizar los riesgos de la seguridad de la información en las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo será la combinación entre la metodología COBIT y la metodología MAGERIT, de ellas sólo tomaremos los puntos concernientes a evaluación de riesgos y como complemento se desarrollaran algunos agregados de acuerdo a nuestras investigaciones realizadas. Como resultado se buscará conocer los puntos débiles concernientes a tecnologías de información, concluyendo con definir una estrategia de aceptación de riesgo.

CAPITULO III

Resultados y Discusión

3.1 Planificar

La norma menciona que se debe establecer el contexto para la gestión de riesgo y como primera instancia identificaremos los activos de Global BPO Center Allus Chiclayo.

3.1.1 Establecer el alcance del SGSI.

El Sistema de Gestión de Seguridad de Información protegerá las áreas de Operaciones y el área de Tecnología de la Información (TI) De Global BPO Center Allus Chiclayo, y esta dirigido exactamente a los jefes de dichas áreas y sus operarios ya que ellos son los que laboran directamente con los activos de la empresa.

En la figura N°01 se muestra la estructura orgánica de la empresa y la cantidad de personas que laboran en cada área. Las áreas a estudiar solo son las que mencionamos a continuación.

Área de Operaciones: **(73)**

- Responsable : 1
  - Coordinadores: 2
    - ✓ Líderes: 4
    - ✓ Ejecutivos: 59
  - Capacitador 2
  - GTR: 1
    - ✓ PPP: 1
  - Responsable Control de Calidad: 1
    - ✓ Analistas: 2

Area de IT: **(6)**

- Jefe de IT: 1
  - Help Desk: 5

3.1.2 Establecer las responsabilidades. Se asignará como Oficial de Seguridad de la Información al Jefe de TI actual el cual coordinara las tareas en materia de seguridad.

3.1.3 Definir política de seguridad.

- Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información del Área de Operaciones y del área de Tecnología De Global BPO Center Allus Chiclayo.
- Los activos de información deI Area de Operaciones y Tecnología De Global BPO Center Allus Chiclayo, serán identificados y clasificados para establecer los mecanismos de protección necesarios.
- El Sistema de Gestión de Seguridad de Información (SGSI) definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por Global BPO Center Allus Chiclayo .
- Todos los clientes internos serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

- No será permitido el ingreso a páginas no autorizadas o que permitan intercambiar información.
- Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información del Area de Operaciones y Tecnología De Global BPO Center Allus Chiclayo.
- Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por Global BPO Center Allus Chiclayo.
- Es responsabilidad de todos los clientes internos reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

3.1.4 Gestión de Riesgos

3.1.4.1 Activos

A continuación, se muestra una lista de activos más importantes de Global BPO Center Allus Chiclayo, y están clasificados según las cinco grandes categorías que MAGERIT tiene en cuenta.

Tabla 3

Lista de activos más importantes de Global BPO Center Allus Chiclayo

Tipo de Activo	***Activo***
	Oficinas

El entorno o soporte del Sistema de Información (edificaciones, mobiliario, lugares de trabajo, energía, climatización, comunicaciones, personal)	Teléfonos Puertas Ventanas Escritorios Box Sillas
El sistema de información propiamente dicho del Dominio (hardware, redes, software, aplicaciones)	CPUs Monitores Teclados Mouses Scanners Impresoras Headset Servidores Router Open Office Windows XP Software de audio Windows Media Player Switch Cableado de red

La propia información requerida, soportada o producida por el Sistema de Información (formatos, códigos, claves de cifrado)	CITRIX Windows(contraseña) Cuentas de Usuario Password Token
Las funcionalidades del Dominio que justifican al Sistema de Información (personal usuario)	Operarios Jefes de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo

Nota: Elaboración propia

3.1.5 Amenazas

A continuación, se muestra una lista de posibles amenazas que podrían afectar los activos de Global BPO Center Allus Chiclayo.

Tabla 4

Lista de posibles amenazas que podrían afectar los activos de Global BPO Center Allus Chiclayo

Tipo de Activo	Amenazas
El entorno o soporte del Sistema de Información	Fuego Daños por agua Fenómeno sísmico Fallo del sistema de suministro de aire acondicionado o de agua Pérdida del suministro de energía
El sistema de información propiamente dicho del Dominio	Interceptación de señales Humedad y Polvo Robo de documentos Robo de equipos Mal funcionamiento de equipo Mal funcionamiento de software Uso de software falsificado o copiado Ataques al sistema Escucha ilegal

La propia información requerida, soportada o producida por el Sistema de Información	Uso de equipo sin autorización Copia fraudulenta de software Tratamiento ilegal de datos Intrusión, accesos forzados al sistema Acceso no autorizado al sistema Venta de información personal
Las funcionalidades del Dominio que justifican al Sistema de Información	Abuso de los derechos Falsificación de derechos Negación de acciones Incumplimiento de la disponibilidad de Personal Suplantación de identidad Chantaje

Nota: Elaboración propia

3.1.6 Vulnerabilidades

En el siguiente cuadro se muestra aquellas vulnerabilidades a las que están expuestos los activos de Global BPO Center Allus Chiclayo.

Tabla 5

Vulnerabilidades a las que están expuestos los activos de Global BPO Center Allus Chiclayo

Tipo de Activo	Vulnerabilidades
El entorno o soporte del Sistema de Información	✓ Red energética inestable ✓ Deterioro de techo
El sistema de información propiamente dicho del Dominio	✓ Susceptibilidad a la humedad, el polvo y la suciedad ✓ Copia no controlada ✓ Interfaz de usuario complicada ✓ Fechas incorrectas ✓ Falta de registro de las llamadas ✓ Descarga y uso no controlados de software ✓ Falta de copias de respaldo ✓ Uso incorrecto de software y hardware ✓ Gestión deficiente de las contraseñas ✓ Almacenamiento sin protección

Nota: Elaboración propia

La propia información requerida, soportada o producida por el Sistema de Información	✓ Falta de "terminación de la sesión" cuando se abandona la estación de trabajo ✓ Falta de políticas sobre el uso del correo electrónico.
Las funcionalidades del Dominio que justifican al Sistema de Información	✓ Procedimientos inadecuados de contratación ✓ Entrenamiento insuficiente en seguridad ✓ Falta de conciencia acerca de la seguridad ✓ Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería ✓ Falta de procedimiento formal para el registro y retiro del registro de usuario ✓ Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con el personal usuario

3.2 Hacer (DO)

La preparación y planificación de SGSI, son pasos importantes, pero en definitiva, lo importante de todo este proceso es que desencadena en una serie de controles a considerar y documentar, que se puede afirmar, son uno de los aspectos fundamentales del SGSI.

Cada uno de ellos se encuentra en estrecha relación a todo lo que especifica la norma ISO/IEC 27001:2014 en los puntos 5 al 13 y del 15 al 18.

La evaluación de cada uno de ellos está quedando claramente documentada. El estándar especifica en su "Anexo A" el listado completo de cada uno de ellos. Para cada uno de ellos define el objetivo y lo describe brevemente.

A continuación, se mostrará los controles de seguridad que no son más que las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que objetivos serán alcanzados.

Los controles que aquí mencionamos han sido seleccionados e implementados de acuerdo a los requerimientos identificados a través de los riesgos.

Se está tomando como numeración según el ANEXO A(Normativo) de la norma ISO/IEC 27001:2014.

A.5 Políticas de seguridad de la información

Este dominio proporciona las directrices generales de gestión y apoyo a la seguridad de la información en concordancia con los requerimientos del servicio de Global BPO Center Allus Chiclayo. El comité de seguridad establecerá claramente las directrices de la política en línea con los objetivos del servicio y demostrará su apoyo y su compromiso con la seguridad de la información a través de la publicación y mantenimiento de una política de seguridad de la información. Al ser un dominio de posicionamiento general respecto a la seguridad de la información, debe de cubrir todas las garantías definidas en la introducción: confidencialidad, integridad y disponibilidad de la información.

Tabla 6

Políticas de seguridad de la información

Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.			**Análisis**
A.5.1.1	Políticas para la seguridad de la información	*Control* Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.	La organización ha identificado los riesgos de información, en tal sentido es necesario establecer una **política de seguridad** de la información para informar y concientizar a todos los colaboradores y partes interesadas sobre los riesgos a los que están expuestos, así como los controles implementados para evitar la materialización de estos riesgos.
A.5.1.2	Revisión de las políticas para la seguridad información	*Control* Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos	

	para asegurar su conveniencia, adecuación y efectividad continúa.	Igualmente, la política de seguridad de la información deberá definir claramente responsables de su desarrollo e implementación. La política de seguridad de la información de la compañía deberá ser frecuentemente revisada para asegurar su idoneidad con respecto a los riesgos de información. Está política será comunicada a todas las partes interesadas.

Nota: A.5.1 Dirección de la gerencia para la seguridad de la información.

Elaboración propia.

A.6 Organización de la seguridad de la información

Este dominio proporciona dos objetivos de seguridad: gestionar la seguridad de la información dentro del Área de Operaciones y Tecnología y mantener la seguridad de los recursos y de los activos de información que son accesibles por externos. Para la consecución del primer objetivo es importante que la empresa apruebe la política de

seguridad de la información, asigne los roles de seguridad, coordine y revise la implementación de la seguridad en las áreas.

Tabla 7

Organización de la seguridad de la información

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			**Análisis**
A.6.1.1	Roles para la seguridad de la información	Control Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	La organización mediante su política de seguridad de la información establecerá el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma velará por mantener protegido la información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad,
A.6.1.2	Segregación de funciones	Control Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no	

		autorizada o no intencional o mal uso de los activos de la organización.	manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior se establecerá un comité de seguridad de la información que tengan responsables que cumplan con los roles definidos anteriormente.
A.6.1.3	Contacto con autoridades	Control Contactos apropiados con autoridades relevantes deben ser mantenidos.	
A.6.1.4	Contacto con grupos especiales de interés	Control Contactos apropiados con grupos especiales de interés u otros foros de seguridad y asociaciones profesionales deben ser mantenidos.	

Nota: A.6.1 Organización interna Organización de la seguridad de la información

Elaboración propia.

A.7 Seguridad de los recursos humanos

Este dominio trata de asegurar que cualquier persona que tenga acceso a los activos descritos sepan y acepten sus responsabilidades en materia de seguridad de los sistemas de información y recursos con los cuales trabajan durante todo el ciclo de vida del empleado (antes de la contratación, durante la contratación y una vez finalizado la relación laboral). La principal garantía que se quiere cubrir es la confidencialidad mediante el uso de cláusulas referentes a obligaciones y responsabilidades del empleado. Otro de los objetivos es reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Tabla 8

Seguridad de los recursos humanos - Antes del empleo

Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.			**Análisis**
A.7.1.1	Selección	Control Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las	Para el desarrollo de las actividades la organización requiere contratar personal, los cuales tienen acceso a la información, por tanto es importante implementar controles basándose en los

		leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	reglamentos, la ética y las leyes pertinentes, que aseguren un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales previo acceso a la información.
A.7.1.2	Términos y condiciones empleo	Control Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	

Nota: A.7.1 Antes del empleo

Elaboración propia.

Tabla 9

Seguridad de los recursos humanos - Durante el empleo

Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.			**Análisis**
A.7.2.1	Responsabilidades gerencia	Control La gerencia debe requerir a todos los empleados aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	El personal de la organización en el desarrollo de las actividades para las cuales fueron contratados interactúa permanentemente con la información, en tal sentido es necesario establecer controles para asegurar que son conscientes de los riesgos, responsabilidades y deberes con respecto a seguridad de la información, igualmente es necesario capacitar y concienciar al personal permanentemente en temas de seguridad de la
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben	

		recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	información según sea pertinente para sus funciones laborales. También se hace preciso establecer un proceso disciplinario que permita a la organización saber cómo actuar en caso de que los colaboradores cometan alguna violación de la seguridad, sin embargo, para evitar al máximo que se presente incidentes la dirección exigirá a los colaboradores el cumplimiento de las políticas y procedimientos establecidos.
A.7.2.3	Proceso disciplinario	Control Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la	

		seguridad de la información.	

Nota: A.7.2 Durante el empleo

Elaboración propia.

Tabla 10

Seguridad de los recursos humanos - Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.			**Análisis**
A.7.3.1	Terminación o cambio responsabilidades empleo.	Control Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.	La organización permite un acceso de la información a los operarios desde el inicio de su contrato, por esta razón es necesario establecer controles que permitan asegurar la devolución de los activos de la organización y el retiro o cambio de los derechos de acceso cuando se presentan renuncias, terminaciones o

			cambios de la contratación del personal.

Nota: A.7.3 Terminación y cambio de empleo

Elaboración propia.

A.8 Gestión de activos

Este dominio proporciona una protección adecuada de los, identificando a los propietarios de estos activos, cuya responsabilidad es el mantenimiento de los controles adecuados sobre los mismos. A tener en cuenta todos los medios o soportes que transmiten, almacenan y procesan información. También se debe realizar una clasificación de los mismos ya que hay que asegurar que la información recibe un nivel de protección apropiado. La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

Tabla 11

Seguridad de los recursos humanos - Responsabilidad por los activos

Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.			**Análisis**
A.8.1.1	Inventario de activos	Control Información, otros activos asociados con información e	La organización dentro del proceso de implementación y mantenimiento del sistema de gestión de seguridad de la

		instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	información debe realizar un inventario de todos sus activos de información, los cuales le permitan desarrollar su labor, y también garantizar el uso adecuado de los mismos a través de reglas documentadas e implementadas.
A.8.1.2	Propiedad de los activos	Control Los activos mantenidos en el inventario deben se propios.	
A.8.1.3	Uso aceptable de los activos	Control Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	

A.8.1.4	Retorno de activos	Control Todos los empleados deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	Los activos de la organización deberán ser regresados por los colaboradores al finalizar su relación contractual. La organización debe asegurar la devolución de los activos cuando se presentan renuncias, terminaciones o cambios de la contratación del personal.

Nota: A.8.1 Responsabilidad por los activos

Elaboración propia.

Tabla 12

Seguridad de los recursos humanos - Manejo de los medios

Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.			**Análisis**
A.8.3.1	Gestión de medios removibles	Control Se debe implementar procedimientos para la	Para el desarrollo de las actividades diarias se utilizan medios para el intercambio de

		gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	información, tales como correo electrónico empresarial, servicios de mensajería e incluso las computadoras tienen acceso USB o CD, por lo anterior es necesario establecer controles para asegurar que se eviten eventos como divulgación, modificación, retiro o destrucción de información no autorizada.
A.8.3.2	Disposición de medios	Control Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.	
A.8.3.3	Transferencia de medios físicos	Control Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o	

	la corrupción durante el transporte.

Nota: Manejo de los medios

Elaboración propia.

A.9 Control de acceso

Este dominio cubre uno de los aspectos más importantes y evidentes respecto a la seguridad: la problemática del control de acceso a los sistemas de información. Para ello plantea los siguientes objetivos de control: requisitos del negocio para el control de acceso, gestión de los accesos de los usuarios, responsabilidades del usuario, control de acceso de red, control de acceso del sistema operativo, control de acceso a las aplicaciones y a la información y teletrabajo y movilidad en el ámbito de la e-Administración. Las garantías que cubre este dominio son autenticidad y confidencialidad. También es el control base que asegure una buena trazabilidad. Los permisos de acceso a las redes, sistemas y a la información que esos soportan se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Tabla 13

Control de acceso - Requisitos

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.			**Análisis**
A.9.1.1	Política de control de acceso	Control Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	En organización los activos de información son manejados por los operarios todo el tiempo, en tal sentido es importante establecer controles de seguridad que permitan asegurar y controlar el acceso a la información.
A.9.1.2	Acceso a redes y servicios de red	Control Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	La organización cuenta con una red LAN única la cual soporta las actividades de los diferentes usuarios, por lo tanto, es necesario establecer controles de seguridad para asegurar que los usuarios solo tienen acceso a los servicios

			para los cuales están autorizados.

Nota: A.9.1 Requisitos de la empresa para el control de acceso

Elaboración propia.

Tabla 14

Control de acceso - Gestión de acceso de usuario

Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.			**Análisis**
A.9.2.1	Registro y baja de usuarios	Control Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	El personal está permitido de manejar información, pero no debe tener acceso a las cuentas de los jefes ya que ellos manejan información adicional, por esta razón es muy importante gestionar de forma adecuada el acceso de los usuarios de acuerdo con el área o puesto que manejan. En tal sentido es importante
A.9.2.2	Aprovisionamiento de acceso a usuario	Control Un proceso formal de aprovisionamiento de	

		acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	establecer controles de seguridad aseguren el acceso de usuarios autorizados, así como evitar el acceso de usuarios no autorizados a información fuera de su área o puesto de trabajo.
A.9.2.3	Gestión de derechos de acceso privilegiados	Control La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	
A.9.2.4	Gestión de información de autentificación secreta de usuarios	Control La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.	

A.9.2.6	Remoción o ajuste de derechos de acceso	Control Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.	

Nota: A.9.2 Gestión de acceso de usuario

Elaboración propia

Tabla 15

Control de acceso - Responsabilidades de los usuarios

Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.			**Análisis**
A.9.3.1	Uso de información de	Control Los usuarios deben ser exigidos a que sigan	El personal de la compañía manejará para acceder a los servicios de red un usuario

	autentificación secreta	las prácticas de la organización en el uso de información de autentificación secreta.	único e intransferible al cual se le asignan las respectivas credenciales, las cuales se deberán actualizar cada treinta (30 días).

Nota: A.9.3 Responsabilidades de los usuarios

Elaboración propia.

Tabla 16

Control de acceso - Control de acceso a sistema y aplicación

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			**Análisis**
A.9.4.1	Restricción de acceso a la información	Control El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	El personal de la compañía manejará para acceder a los servicios de red un usuario único e intransferible al cual se le asignan las respectivas credenciales, las cuales se deberán actualizar cada treinta (30 días).

A.9.4.2	Procedimientos de ingreso seguro	Control Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.
A.9.4.3	Sistema de gestión contraseñas	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	Control El uso de programas utilitarios que podrían ser capaces de pasar

		por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.
A.9.4.5	Control de acceso al código fuente de los programas	Control El acceso al código fuente de los programas debe ser restringido.

Nota: A.9.4 Control de acceso a sistema y aplicación

Elaboración propia.

A.10 Criptografía

Este dominio asegura la confidencialidad y autenticidad de datos mediante el proceso de reemplazarlos por una versión transformada. Esta puede ser reconvertida a la forma original sólo por alguien que posea el algoritmo criptográfico y las claves adecuadas.

También es el nombre que se le da a la disciplina que incluye los principios, medios y métodos para transformar los datos con intención de ocultar la información y prevenir la modificación y los usos no autorizados de la misma.

Tabla 17

Criptografía - Controles criptográficos

Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.			**Análisis**
A.10.1.1	Política sobre el uso de controles criptográficos	Control Una política sobre el uso de controles criptográficos para la protección de la información debe implementada.	La organización para el sistema de información que se va a manejar debe establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.
A.10.1.2	Gestión de claves	Control Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.	

Nota: A.10.1 Controles criptográficos

Elaboración propia.

A.11 Seguridad física y ambiental

Este dominio trata de asegurar los activos físicos (tangibles) a través del control de acceso y la protección contra contingencias externas (medioambientales). Las garantías que cubre este dominio son la disponibilidad, la integridad, la disponibilidad y la confidencialidad de la información.

La infraestructura que sustenta las aplicaciones informáticas que sirven de soporte a la tramitación telemática, así como los soportes de almacenamiento que éstos usan, que residan en su local, deben estar protegidos contra daño físico o hurto utilizando mecanismos de control de acceso físico.

Tabla 18

Seguridad física y ambiental - Áreas seguras

Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.			**Análisis**
A.11.1.1	Perímetro de seguridad física	Control Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen	La organización para el desarrollo de sus actividades cuenta con una infraestructura física, ubicada el sector central de

		información sensible o crítica e instalaciones de procesamiento de la información.	la ciudad Chiclayo, en la cual se ubican los activos de información, en tal sentido es importante establecer los controles de seguridad para evitar el acceso físico no autorizado, el daño a la infraestructura y activos de información de la compañía.
A.11.1.2	Controles de ingreso físico	Control Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	
A.11.1.3	Asegurar oficinas, áreas e instalaciones	Control Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.	
A.11.1.4	Protección contra amenazas externas y ambientales	Control	

		Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	
A.11.1.5	Trabajo en áreas seguras	Control Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.	

Nota: A.11.1 Áreas seguras

Elaboración propia

Tabla 19

Seguridad física y ambiental - Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.			**Análisis**
A.11.2.1	Emplazamiento y protección de los equipos	Control Los equipos deben ser ubicados y protegidos	Para el desarrollo de las actividades la organización utiliza

		para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	equipos tales como servidores, computadores de escritorio, impresoras, escáneres, entre otros, en estos equipos se procesa la información de los clientes y de la empresa por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la organización.
A.11.2.2	Servicios de suministro	Control Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	
A.11.2.3	Seguridad del cableado	Control El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	

A.11.2.4	Mantenimiento de equipos	Control Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	
A.11.2.5	Remoción de activos	Control Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.	Para el desarrollo de las actividades la organización utiliza equipos tales como servidores, computadores de escritorio, impresoras, escáneres, entre otros, en estos equipos se procesa la información de los clientes y de la empresa por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro
A.11.2.7	Disposición o reutilización segura de equipos	Control Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier	

		dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.	como fuera de la organización.
A.11.2.8	Equipos de usuario desatendidos	Control Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.	El personal de la organización es responsable de los activos de información que se encuentran a su cargo, así como de la protección de estos activos en cuanto confidencialidad, integridad y disponibilidad, de tal forma que se han definido responsabilidades claras en cuanto a seguridad de la información en los manuales de funciones que son entregados al personal, en tal sentido es necesario
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las	

	instalaciones de procesamientos de la información debe ser adoptada.	establecer controles de seguridad para asegurar que se evita el acceso de usuarios no autorizados y el robo de información.

Nota: A.11.2 Equipos

Elaboración propia.

A.12 Seguridad de las operaciones

Este dominio trata de asegurar que la explotación de la infraestructura se realiza de forma segura y controlada, se supervisa su estado y se reportan incidencias. Para ello, define varios objetivos de control como: procedimientos y responsabilidades operacionales, protección contra código malicioso, copias de seguridad, gestión de la seguridad de red, gestión de dispositivos de almacenamiento, control sobre el intercambio de información entre trabajadores y monitorización de sistemas.

Tabla 20

Seguridad de las operaciones - Procedimientos y responsabilidades operativas

Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.	**Análisis**

A.12.1.1	Procedimientos operativos documentados	Control Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.	La compañía para el desarrollo de sus actividades utiliza herramientas ofimáticas y tecnológicas, con las cuales interactúan permanentemente el personal a través de los equipos asignados para su labor, en tal sentido es necesario establecer controles de seguridad que garanticen que todos los cambios se controlan, revisan y someten a pruebas para no comprometer la seguridad del sistema ni el entorno operativo y también evitar así la fuga de información.
A.12.1.2	Gestión del cambio	Control Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.	
A.12.1.3	Gestión de la capacidad	Control El uso de recursos debe ser monitoreado,	

		afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	

Nota: A.12.1 Procedimientos y responsabilidades operativas

Elaboración propia

Tabla 21

Seguridad de las operaciones - Protección contra códigos maliciosos

Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.			**Análisis**
A.12.2.1	Controles contra códigos maliciosos	Control Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en	Para el desarrollo de las actividades de la organización se utilizan servicios como Internet, medios extraíbles, los cuales pueden afectar el correcto funcionamiento de activos de información como equipos, software entre otros,

		combinación con una concientización apropiada de los usuarios.	por lo tanto, es importante establecer controles de seguridad que permitan detección y prevención de la acción de códigos maliciosos, así como también procedimientos de concientización de los usuarios.

Nota: A.12.2 Protección contra códigos maliciosos

Elaboración propia.

Tabla 22

Seguridad de las operaciones - Respaldo

Objetivo: Proteger contra la pérdida de datos			**Análisis**
A.12.3.1	Respaldo de la información	Control Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y	La información de la empresa, que los ejecutivos descargan se encuentra ubicada en los equipos asignados a los colaboradores, en tal sentido es importante establecer

		probadas regularmente en concordancia con una política de respaldo acordada.	controles de seguridad que aseguren la ejecución de procedimientos de backup y recuperación que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la empresa continué con sus actividades habituales sin ningún inconveniente.

Nota: A.12.3 Respaldo

Elaboración propia.

Tabla 23

Seguridad de las operaciones - Registros y monitoreo

Objetivo: Registrar eventos y generar evidencia			**Análisis**
A.12.4.1	Registro de eventos	Control Registros (logs) de eventos de actividades de usuarios,	La compañía para el desarrollo de sus actividades cuenta con colaboradores que tienen acceso a los diferentes

		excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	activos de información para la ejecución de sus actividades, en tal sentido se establecerá controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información.
A.12.4.2	Protección de información de registros.	Control Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	
A.12.4.3	Registros del administrador y del operador	Control Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los	

		registros(logs) deben ser protegidos y revisados regularmente.
A.12.4.4	Sincronización de reloj	Control Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.

Nota: A.12.4 Registros y monitoreo

Elaboración propia.

Tabla 24

Seguridad de las operaciones - Control del software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales			**Análisis**
A.12.5.1	Instalación de software en sistemas operacionales	Control Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	La organización para el desarrollo de sus actividades utiliza el sistema operativo, WINDOWS XP, pero sin licencia, en tal sentido es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos que restrinja la posibilidad de instalación de programas y/o aplicativos.

Nota: A.12.5 Control del software operacional

Elaboración propia.

Tabla 25

Seguridad de las operaciones - Gestión de vulnerabilidad técnica

Objetivo: Prevenir la explotación de vulnerabilidades técnicas			**Análisis**
A.12.6.1	Gestión de vulnerabilidades técnicas	Control Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	La compañía tiene activos de información tecnológicos los cuales están expuestos a vulnerabilidades de tipo técnico, por lo tanto, es necesario establecer controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas.
A.12.6.2	Restricciones sobre la	Control	La organización para el desarrollo de sus actividades

	instalación de software	Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	utiliza el sistema operativo, WINDOWS XP, pero sin licencia, en tal sentido es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos.

Nota: A.12.6 Gestión de vulnerabilidad técnica

Elaboración propia.

Tabla 26

Seguridad de las operaciones - Consideraciones para la auditoría de los sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.			**Análisis**
A.12.7.1	Controles de auditoría de sistemas de información	Control Requisitos de las auditorías y las actividades que	La compañía no cuenta con sistemas operativos que pueden ser objeto de auditoria de seguridad de la

	involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	información, al momento no se realizan auditorias, pero tiene en proyecto realizarse, por lo tanto, es importante establecer controles de seguridad que garanticen un adecuado uso de las herramientas de auditoria y minimizar la interrupción de los sistemas durante el proceso.

Nota: A.12.7 Consideraciones para la auditoría de los sistemas de información

Elaboración propia.

A.13 Seguridad de las comunicaciones

Este dominio detalla más controles técnicos que organizativos respecto a dominios anteriores. Las garantías que cubre son disponibilidad, confidencialidad, integridad y conservación de la información. Se establecerán responsabilidades y procedimientos para la gestión y operación de todos los medios de tratamiento de información. Esto incluye elaborar de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Tabla 27

Seguridad de las comunicaciones - Gestión de seguridad de la red

Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.			**Análisis**
A.13.1.1	Controles de la red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	La cuenta con una red LAN única sobre que la desarrollan todas las aplicaciones ejecutadas por los usuarios, es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar su infraestructura de soporte.
A.13.1.2	Seguridad de servicios de red	Control Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se	

		provean internamente o sean tercerizados.	

Nota: A.13.1 Gestión de seguridad de la red

Elaboración propia.

Tabla 28

Seguridad de las comunicaciones - Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			**Análisis**
A.13.2.1	Políticas y procedimientos de transferencia de la información	Control Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	Dentro del desarrollo normal de las actividades de la compañía se presentan actividades de intercambio de información, por lo cual es importante establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos de la empresa para el intercambio de información

			y para garantizar que no se presente uso inadecuado o corrupción cuando la información sale de la organización.
A.13.2.2	Acuerdo sobre transferencia de información	Control Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	
A.13.2.3	Mensajes electrónicos	Control La información involucrada en mensajería electrónica debe ser protegida apropiadamente.	
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Control Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la	La organización mediante su política de seguridad de la información establecerá su compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma vela por mantener

	información deben ser identificados, revisados regularmente y documentados.	protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para la organización interna de seguridad de la información.

Nota: A.13.2 Transferencia de información

Elaboración propia.

A.15 Relaciones con los proveedores

Este dominio detalla que en el momento en que una organización considera compartir una parte de su proceso productivo con otra, también acepta compartir información vital y confidencial que, eventualmente, puede poner en riesgo la operación en caso de ser

divulgada. Antes de suscribir un acuerdo o firmar un contrato, conviene asegurarse de que la organización que actuará como proveedor hace uso de las mejores prácticas en cuanto a gestión de la calidad y de la seguridad de la información. La tercerización siempre implicará un riesgo. Eso es algo que debemos tener claro antes de subcontratar un proceso o establecer un acuerdo con algún proveedor.

Tabla 29

Seguridad de las comunicaciones - Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores			**Análisis**
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Control Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	La compañía requiere realizar diferentes tipos de compras, en tal sentido es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la

		Control	seguridad de la información
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	de la organización
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y	La organización al momento de contratar deberá exigir el cumplimiento de las buenas prácticas y cumplimiento de las políticas de la organización para su desarrollo.

		comunicaciones y la cadena de suministro de productos.	

Nota: A.15.1 Seguridad de la información en las relaciones con los proveedores

Elaboración propia.

Tabla 30

Seguridad de las comunicaciones - Gestión de entrega de servicios del proveedor

Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.			**Análisis**
A.15.2.1	Monitoreo y revisión servicios proveedores	Control Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	La compañía requiere realizar diferentes tipos de compras, en tal sentido es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de gestionar compras que de bienes o servicios que afecten la seguridad de la información
A.15.2.2	Gestión de cambios a los servicios de proveedores	Control Los cambios a la provisión de servicios	

	por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	e la organización y la infraestructura que sobre la cual esta soportada.

Nota: A.15.2 Gestión de entrega de servicios del proveedor

Elaboración propia.

A.16 Gestión de incidentes de seguridad de la información

Este dominio trata de garantizar que los eventos y debilidades en la seguridad asociados al Área de Operaciones y Tecnología sean comunicados para, de este modo,

poder realizar las acciones correctivas oportunas y adecuadas. Este es un dominio que está enfocado principalmente a cubrir las garantías de disponibilidad, confidencialidad e integridad.

Tabla 31

Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.			**Análisis**
A.16.1.1	Responsabilidades y procedimientos	Control Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	La organización mediante su política de seguridad de la información establecerá su compromiso, organización y asignación de para su cumplimiento, de igual forma vela por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de

			confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para la organización interna de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	Control Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.	La compañía tiene activos de información a los que se les ha realizara su respectivo análisis, evaluación y tratamiento del riesgo, los cuales pueden ser objeto de incidentes de seguridad de la información, por lo cual es importante establecer controles que aseguren que
A.16.1.3	Reporte de debilidades de	Control	

	seguridad de la información	Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	los eventos y debilidades de seguridad de la información son comunicados oportunamente a través de los canales de gestión apropiados al área de seguridad de la información para su respectiva gestión tan pronto como sea posible.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Control Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.	

A.16.1.5	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	La compañía activos de información los cuales pueden ser objeto de incidentes de seguridad de la información y deben ser analizados por el personal de seguridad informática designado por la gerencia para identificar acciones de mejora, en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente de los incidentes de seguridad de la información.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	
A.16.1.7	Recolección de evidencia	Control La organización debe definir y aplicar procedimientos para la	

	identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	

Nota: A.16.1 Gestión de incidentes de seguridad de la información y mejoras

Elaboración propia.

A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio

Este dominio trata de establecer un plan de acción para minimizar los efectos de una catástrofe. Las garantías que este dominio cubre son la integridad, la disponibilidad y la conservación de la información. El objetivo es establecer un proceso de gestión de continuidad de actividad para garantizar la recuperación de los procesos críticos en el Área de Operaciones y Tecnología, reduciendo el tiempo de indisponibilidad a niveles aceptables, mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental, tanto preventivos como de recuperación.

Tabla 32

Aspectos de seguridad de la información en la gestión de continuidad del negocio - Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización			**Análisis**
A.17.1.1	Planificación de continuidad de seguridad de la información	Control La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	La compañía debería estar comprometida en garantizar el cumplimiento total del objeto de estos, en tal sentido ante cualquier interrupción en las actividades del negocio por fallas tecnológicas importantes o desastres, la empresa debe contar una gestión de continuidad del negocio que permita minimizar el impacto generado en su capacidad, establecer controles para asegurar una adecuada
A.17.1.2	Implementación de continuidad de seguridad de la información	Control La organización debe establecer, documentar, implementar y mantener procesos,	

		procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	gestión de continuidad del negocio.
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Control La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	

Nota: A.17.1 Continuidad de seguridad de la información

Elaboración propia.

Tabla 33

Aspectos de seguridad de la información en la gestión de continuidad del negocio - Redundancias

Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información			**Análisis**
A.17.2.1	Instalaciones de procesamiento de la información	Control Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	La organización deberá contar con equipos de respaldo para aquellos servicios críticos, como firewall e internet, entre otros para garantizar la disponibilidad de las instalaciones de procesamiento de información.

Nota: A.17.2 Redundancias

Elaboración propia.

A.18 Cumplimiento

Este dominio trata de evitar el incumplimiento del marco normativo y cualquier requerimiento de seguridad que éste obligue mediante el cumplimiento en los sistemas de información de las políticas y estándares de seguridad desarrollados.

Este dominio es horizontal y cubriría las garantías definidas: confidencialidad, integridad y disponibilidad de la información.

Tabla 34

Cumplimiento - Cumplimiento con requisitos legales y contractuales

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.			**Análisis**
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Control Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes, así como el enfoque de la organización para	La organización para los sistemas de información que se manejan en los diferentes proyectos deberá establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.

		cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.
A.18.1.3	Protección de registros	Control Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.

		Control
A.18.1.4	Privacidad y protección de datos personales.	La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.
		Control
A.18.1.5	Regulación de controles criptográficos	Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.

Nota: A.18.1 Cumplimiento con requisitos legales y contractuales

Elaboración propia.

Tabla 35

Cumplimiento - Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.			**Análisis**
A.18.2.1	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o	La organización mediante su política de seguridad de la información establece su compromiso, organización y asignación de para su cumplimiento, de igual forma vela por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la

		cuando ocurran cambios significativos.	revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para la organización interna de seguridad de la información.
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Control Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	El personal de la organización interactúa permanentemente con los activos de información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, en tal sentido es importante establecer controles de seguridad que garanticen que todo el personal de la empresa conoce y aplica las políticas de seguridad de la información y los respectivos controles.
A.18.2.3	Revisión del cumplimiento técnico.	Control Los sistemas de información deben ser revisados regularmente	

		respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.

Nota: A.18.2 Revisiones de seguridad de la información

Elaboración propia.

En conclusión:

Tal y como se mencionó en el punto 1.4 "Descripción de la infraestructura tecnológica de la empresa", el estado de la infraestructura tecnológica es como se muestra en la *Tabla 1* y el diseño de red tal y como se muestra en la ***Diagrama N° 2***, por lo tanto, para soportar los controles que estamos proponiendo anteriormente tenemos que realizar cambios para asegurar el cumplimiento del SGSI y los mostramos en la siguiente tabla:

Tabla 36

Propuesta de la infraestructura tecnológica para Global BPO Center Allus Chiclayo

Item	Elemento de Análisis	Observación/Recomendación
1	Topología de Red	a). La Topología de Red es optima b). El Modelo de Red cumple con los requerimientos de un SGSI

		c). Se recomienda implementar enlaces redundantes
2	Cableado de Red y Normatividad en Centro de Datos	El cableado estructurado cumple con las normas y estándares internacionales para el soporte tecnológico del SGSI
3	Dispositivos de Red LAN	Los dispositivos de Red LAN descritos cumplen con las normas y estándares del SGSI
4	Dispositivos de Telefonía IP	a). Los dispositivos de Telefonía IP cumplen con las expectativas de comunicación.
5	Dispositivos Finales (usuarios)	Los dispositivos finales como computadoras de escritorio, computadoras portátiles, impresoras y teléfonos IP, cumplen con las normas y estándares internacionales para el soporte tecnológico del SGSI.
6	Servidores	Aplicaciones, Base de Datos y Active Directory cumple con los estándares y normas para redes de Almacenamiento SAN
7	Dispositivos de Seguridad Perimetral	Adquirir un Firewall de mejores prestaciones incluyendo filtros UTM IPS, IDS, APPLICATTION CONTROLS, WEB FILTER, DDOS, ETC Dispositivos Recomendados: a). CheckPoint (VER ANEXO N°02)

8	Dispositivos de Almacenamiento	El Dispositivo de Almacenamiento IBM Storwize V7000 cumple con las normas internacionales, pero se recomienda la distribución correcta de almacenamiento considerando los niveles de crecimiento en un TAPE Backup con cintas.
9	Equipos de Respaldo Eléctrico	Se recomienda adquirir un Generador Eléctrico con cuchilla de intercambio automático.
10	Equipos de Respaldo de Datos (Backup)	Se recomienda la adquisición urgente de un Software de Almacenamiento Backup (Tivoly Storage Manager) que permita al dispositivo IBM System X-3550 realizar el respaldo de la Data en Cintas.
11	Servicio de Protección de los Datos	Se recomienda la contratación del Servicio de Protección y custodia de la Data en Cintas como PROSEGUR o HERMES.
12	Equipos de Redundancia y Alta Disponibilidad	a). Adquirir un Dispositivo Switch Core Cisco 3750-24SFP adicional para la integración de Alta Disponibilidad en Capa de Núcleo con Protocolo PVST+ Rápido b). Adquirir un Dispositivo Switch Distribución Cisco 2960-X Series adicional para la integración de Alta Disponibilidad en Capa de Distribución con Protocolo PVST+ Rápido en enlaces troncales

		c). Adquirir una Línea de Internet de respaldo con Alta disponibilidad con la integración del protocolo HSRP d). Adquirir e Implementar un Servidor de Respaldo en el caso sea posible, de lo contrario implementar nuevas cuchillas de Servidores con Alta disponibilidad
13	Direccionamiento IP	a). El Direccionamiento IP sin clase con red 10.10.0.0/16 es óptimo. b). En Distribución a través de VLANS, se recomienda configurar y agregar las Vlans DMZ para separar los servidores de la Admin-Red, y además considerar una Vlan VPN para los trabajadores a Distancia: VLAN 10: Gerencia 10.10.1.0/27 VLAN 11: Operaciones 10.10.11.0/26 VLAN 12: IT (Tecnologías) 10.10.12.0/27 VLAN 13: Cross 10.10.13.0/26 VLAN 14: RR.HH 10.10.14.0/26 VLAN 15: Admin-Red 10.10.15.0/25 VLAN 16: DMZ 10.10.16.0/25 VLAN 17: VPN 10.10.17.0/28

Nota: Elaboración propia

Después de la siguiente propuesta el diseño de la red quedaría de la siguiente manera (Ver diagrama N°07):

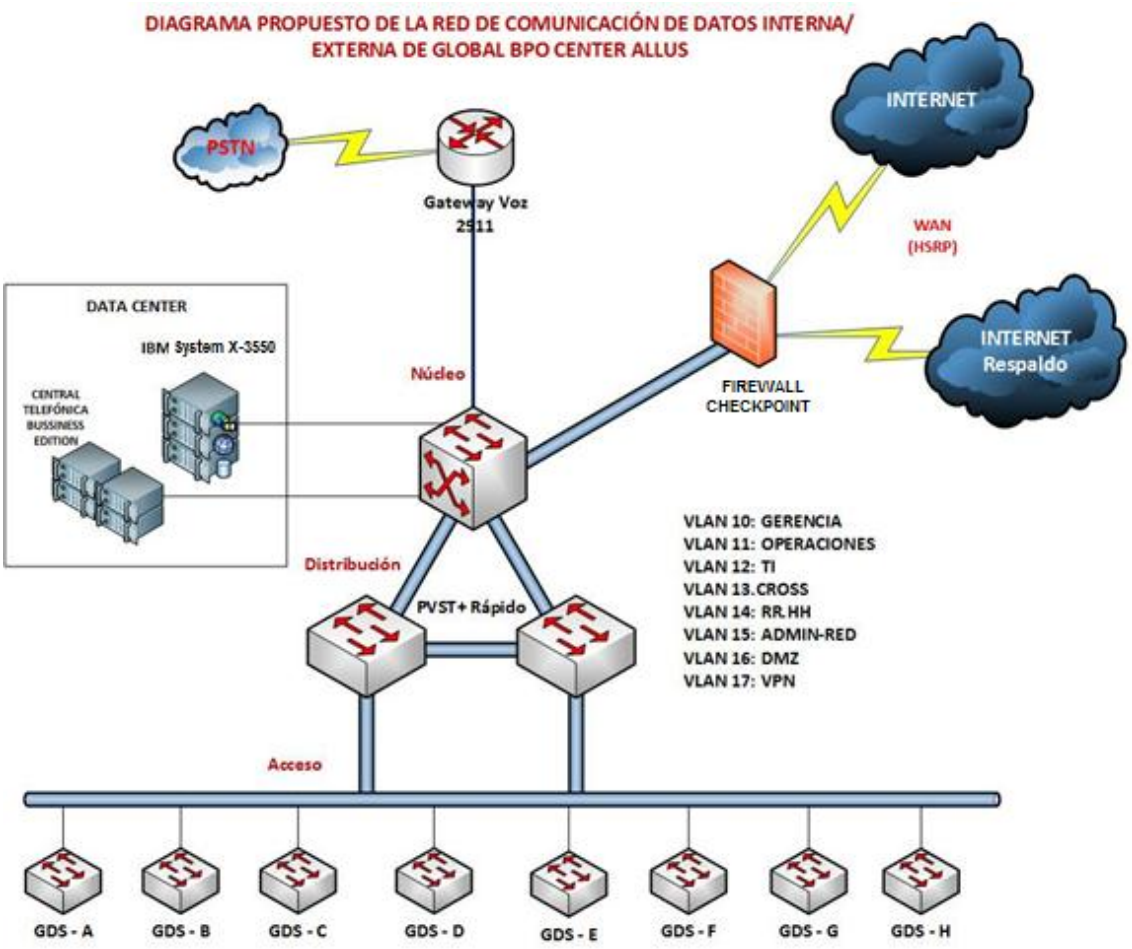


Figura 7. Propuesta El Diseño De La Red. Elaboración propia

3.2.1 Políticas de Seguridad de la Información: *[ISO/IEC 27001:2014 A.5.1]*

- **Política corporativa**

En Global BPO Center Allus Chiclayo la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes.

Conscientes de sus necesidades actuales, implementamos un modelo de gestión de seguridad de la información como herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en Global BPO Center Allus Chiclayo, específicamente en las Áreas de Operaciones y Tecnología. Este proceso será liderado de manera permanente por el Oficial de Seguridad de la Información.

Esta política será revisada con regularidad o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

- **Políticas generales**

Hemos establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan el objetivo de este proyecto en cuanto a la protección de los activos principales de información de Global BPO Center Allus Chiclayo:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de Global BPO Center Allus Chiclayo.

2. Los activos de información de Global BPO Center Allus Chiclayo, serán identificados y clasificados para establecer los mecanismos de protección necesarios.
3. Se definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.
4. Todos los operarios serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de Global BPO Center Allus Chiclayo.
6. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.
7. Es responsabilidad de todos los operarios de Global BPO Center Allus Chiclayo reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

3.2.2 Concienciación y educación sobre normas de seguridad: *[ISO/IEC 27001:2014 A.7.2.2]*

Para que los usuarios puedan colaborar con la gestión de la seguridad, se les debe concienciar e informar a fin de que cumplan con las medidas establecidas por la organización en el desempeño habitual de sus funciones.

Es preciso instruir al personal de forma apropiada sobre seguridad y el uso correcto de los sistemas de información y sus recursos, así como sobre la importancia de la seguridad en el tratamiento de los datos en la organización.

Se formará a todo el personal de la empresa que vaya a tratar datos del sistema de información sobre las normas de utilización y medidas de seguridad. Esto conseguirá que todo usuario conozca las instrucciones para tratar los recursos, la respuesta ante incidencias de seguridad y el mantenimiento de los recursos, y así disminuir los errores de tratamiento y los malos usos de los recursos del sistema de información.

3.2.3 Uso adecuado de los activos: [ISO/IEC 27001:2014 A.8.1.3]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los operarios determinadas por los jefes de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

Para la consulta de la información que contiene el software se establecerán privilegios de acceso a los operarios de acuerdo con el desarrollo de sus funciones y competencias.

Todos los operarios que manipulen información en el desarrollo de sus funciones deberán firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerado como un "incidente de seguridad".

3.2.4 Gestión de medios removibles: [ISO/IEC 27001:2014 A.8.3]

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de Global BPO Center Allus Chiclayo, estará autorizado para aquellos operarios cuyo perfil del cargo y funciones lo requiera.

Las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo son responsables de implementar los controles necesarios para asegurar que en los sistemas de información de Global BPO Center Allus Chiclayo, sólo los operarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

Así mismo, el operario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información que éste contiene.

3.2.5 Control de acceso: *[ISO/IEC 27001:2014 A.9]*

- **Acceso a internet**

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de Global BPO Center Allus Chiclayo, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

✓ El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- ✓ El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Messenger, Skipe y otros similares, que tengas como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de Global BPO Center Allus Chiclayo.
- ✓ El intercambio no autorizado de información de propiedad de Global BPO Center Allus Chiclayo, de sus clientes y/o de sus operarios, con terceros.
- ✓ La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus autores, o que contengas archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en internet debe ser autorizada por el jefe de las Áreas de Operaciones y Tecnología.

b) Se realizará un monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los operarios. Así mismo, se podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la **legislación nacional vigente**.

c) Cada uno de los operarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) El uso de internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de Global BPO Center Allus Chiclayo.

- **Acceso a los Recursos Tecnológicos**

El uso adecuado de los recursos tecnológicos asignados por las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo a sus operarios se reglamenta bajo los siguientes lineamientos:

e) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de Global BPO Center Allus Chiclayo es responsabilidad de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo, y por tanto son los únicos autorizados para realizar esta labor.

f) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

g) Las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo van a definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

h) Únicamente los funcionarios y terceros autorizados por las Áreas de Operaciones y Tecnología pueden conectarse a la red inalámbrica de Global BPO Center Allus Chiclayo.

3.2.6 Responsabilidad de los usuarios: *[ISO/IEC 27001:2014 A.9.3]*

Todos los recursos de información críticos de Global BPO Center Allus Chiclayo tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada operario requiera para el desarrollo de sus funciones, definidos y aprobados por las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

Todo operario que requiera tener acceso a los sistemas de información de Global BPO Center Allus Chiclayo debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la organización.

3.2.7 Control de acceso físico: *[ISO/IEC 27001:2014 A.11.1]*

La Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo, destinadas al procesamiento o almacenamiento de información sensible y donde se encuentran los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, serán consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma deberán contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

3.2.8 Protección y ubicación de los equipos: *[ISO/IEC 27001:2014 A.11.2]*

Los equipos que hacen parte de la infraestructura tecnológica Global BPO Center Allus Chiclayo tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los operarios que tengan acceso a los equipos que componen la infraestructura tecnológica Global BPO Center Allus Chiclayo no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

3.2.9 Escritorio y pantalla limpia: *[ISO/IEC 27001:2014 A.11.2.9]*

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los operarios de Global BPO Center Allus Chiclayo deben mantener la información

restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

3.2.10 Protección contra software malicioso: *[ISO/IEC 27001:2014 A.12.2]*

Se establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus (McAfee), antispam (Zimbra), antispyware (Safety Anti-Spyware) y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso. Será responsabilidad de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, se define los siguientes lineamientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad previamente avaladas.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

3.2.11 Copias de respaldo: *[ISO/IEC 27001:2014 A.12.3]*

La información contenida en la plataforma tecnológica de Global BPO Center Allus, es un activo importante para la empresa, ya que en ella encontramos una réplica del sistema de movistar Chile (SGU) la cual contiene la información de cada cliente, también encontraremos la grabación de todas las llamadas realizadas en la plataforma; es por ello que se asegurará de manera periódica mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Esto se realizará al finalizar el mes. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo establecerán procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá

conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

3.2.12 Correo electrónico: *[ISO/IEC 27001:2014 A.13.2.3]*

Los operarios a quienes Global BPO Center Allus Chiclayo les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de Global BPO Center Allus Chiclayo, así mismo podrá ser utilizadas para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de Global BPO Center Allus Chiclayo y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo de acuerdo con las necesidades de cada usuario.

d) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico asignada como punto de contacto en comunidades de contacto social, tales como facebook, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

e) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo proporciona.

f) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

g) Toda información generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo.

h) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por Global BPO Center Allus Chiclayo y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

3.2.13 Acuerdos de Confidencialidad: *[ISO/IEC 27001:2014 A.13.2.4]*

Todos los operarios del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo deben aceptar los acuerdos de confidencialidad definidos, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

3.2.14 Reclutamiento

Cada nuevo empleado de Global BPO Center Allus es una apuesta de futuro. La empresa le asignará una serie de tareas y responsabilidades al nuevo empleado, y proporcionará los medios materiales y la información necesaria para que pueda llevarlas

a cabo. Existirá un procedimiento de reclutamiento que tenga en cuenta los siguientes aspectos relativos a la seguridad:

- **Definición del puesto:** Para cada nueva vacante se deberá definir cada criterio del puesto a cubrir según su responsabilidad y la información que manejará. Global BPO Center Allus deberá definir su criterio propio.
- **Selección:** En la selección de candidatos a puestos críticos se deben comprobar los antecedentes penales y las referencias profesionales.
- **Contrato:** El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad y protección de datos.

- **Inicio:** Durante los primeros días de trabajo, es recomendable que el empleado:
    - ✓ Asista a unas sesiones de formación donde se le introduzca en la normativa interna y de seguridad de la empresa. De este modo todo empleado conoce sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del email e internet, clasificación de la información, etc.
    - ✓ Firme un acuerdo de confidencialidad donde aceptará el cumplimiento del mismo. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.

- **Accesos:** Los accesos a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del empleado (Coordinador de

Operaciones) al Área de Tecnología. Dichos accesos deben ser siempre justificables por la labor que se va a realizar, y en caso de ser privilegiados, el Comité de Seguridad debe aprobar su concesión.

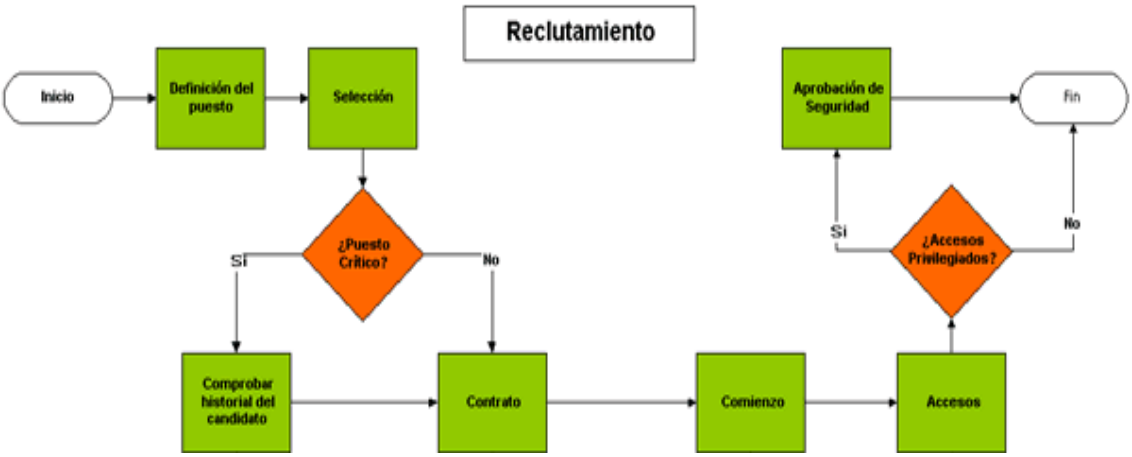


Figura 8. Diagrama de flujo propuesto para el reclutamiento de personal. Elaboración propia

3.2.15 Salida de empleados

La salida de un empleado es un punto crítico de riesgo para la Empresa. En casos de problemas laborales y despidos, un empleado puede convertirse en una seria amenaza. Pudiendo presentarse casos de sabotaje o substracción de información por parte de empleados disgustados.

Para evitar todo esto, existirá un nuevo procedimiento de bajas que tenga en cuenta los siguientes aspectos de seguridad:

- ✓ **Clasificación de las bajas:** El responsable del empleado junto con Recursos Humanos debe clasificar la baja según las circunstancias que la rodean. Un ejemplo de posibles categorías sería:
  - ✓ Renuncia
  - ✓ Muerte
  - ✓ Jubilación obligatoria
  - ✓ Jubilación anticipada
  - ✓ Destitución
  - ✓ Supresión de puestos

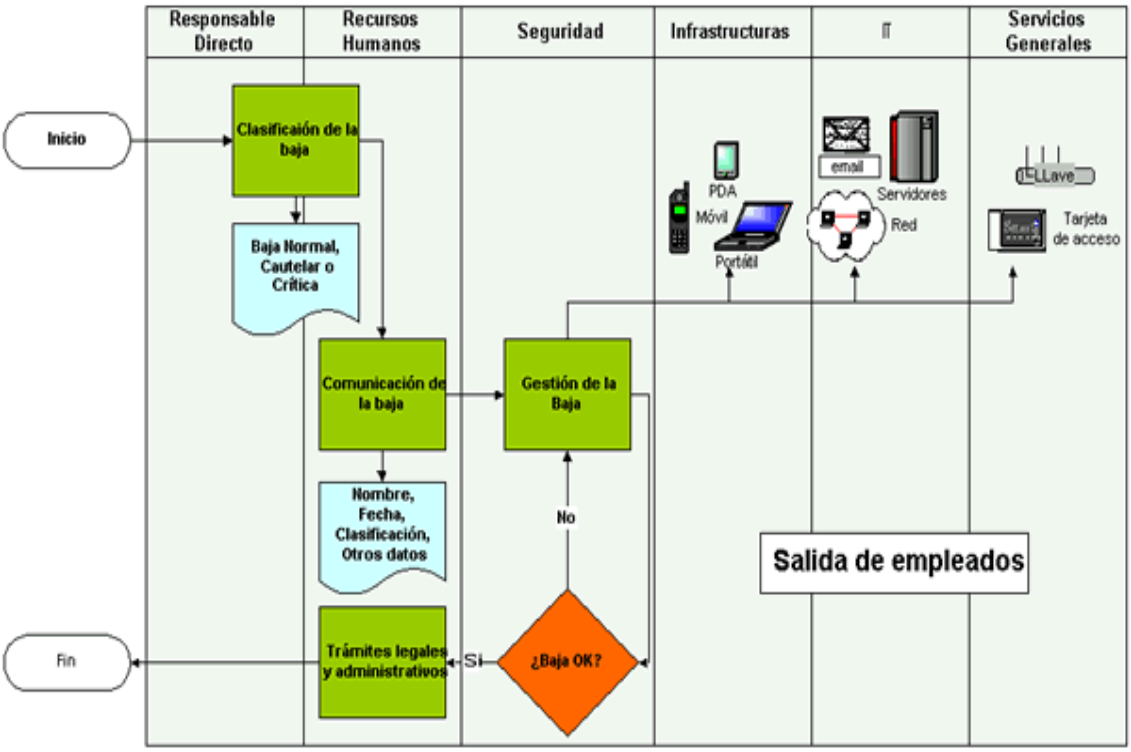


Figura 9. Diagrama de flujo propuesto para la salida de personal. Elaboración propia

3.3 Check: Monitorizar y revisar el SGSI

3.3.1 Gestión del SGSI

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización.

- **Formación del comité de seguridad de la información**

  El Comité de Seguridad de la Información será formado por los mismos jefes u operarios de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo. El Comité de Seguridad de la Información procederá a revisar y proponer junto con el Gerente de Global BPO Center Allus Chiclayo la aprobación de la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; promover la difusión y apoyo a la seguridad de la información dentro del Organismo y coordinar el proceso de administración de la continuidad de las actividades del Organismo.

  El cargo de **Oficial de Seguridad de la Información** será asignado al Jefe del área de Tecnología de la Información (TI), él será responsable de coordinar las

acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El cargo de **Responsable de Seguridad Informática** será asignado a un Help Desk, quien cumplirá funciones relativas a la seguridad de los sistemas de información de Global BPO Center Allus Chiclayo, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política. Además, cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de las Áreas de Operaciones y Tecnología de Global BPO Center Allus Chiclayo. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El cargo de **Responsable del Área de Recursos Humanos** será asignado a Coordinador de recursos humanos de Global BPO Center Allus Chiclayo, este cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El cargo de **Responsable del Área Reglamentaria** será asignado al Jefe del Área de Operaciones, quien verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con sus empleados y con terceros.

Los **usuarios de la información y de los sistemas** son los mismos operarios de la empresa. Ellos son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

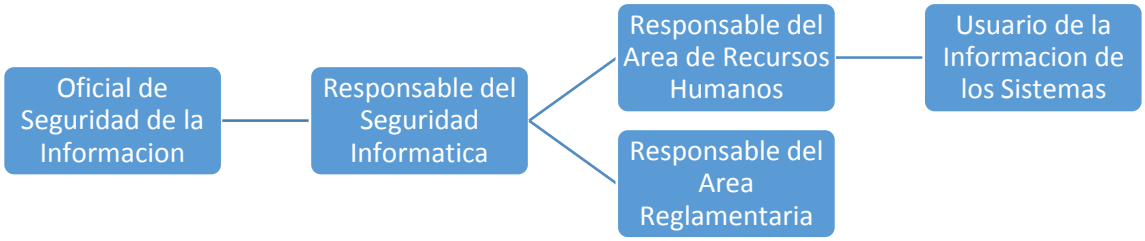


Figura 10. Comité de seguridad de la información. Elaboración propia

- **Procedimientos del Comité de Seguridad de la información**

En este punto se planteará los procedimientos a seguir por parte de Comité de Seguridad de la Información el cual deberá:

✓ Ejecutar procedimientos de monitorización y revisión para:

– Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.

– Identificar brechas e incidentes de seguridad.

- Ayudar a determinar las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.
- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

✓ Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

✓ Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

✓ Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.

✓ Realizar periódicamente auditorías internas del SGSI en intervalos planificados realizadas por empresas externas.

✓ Revisar el SGSI periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- ✓ Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- ✓ Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

3.4 Análisis de costos

3.4.1 Costo de Servicios y Materiales

A continuación, se presenta el costo referencial para implementación del SGSI, para así cumpla con la normativa ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo:

Tabla 37

Costo Referencial Para Implementación Del SGSI

Descripción	Costo
Servicio de implementación del Servidor BLADE IBM.	S/. 5,000.00
Adquisición Firewall : CheckPoint	S/. 20,000.00
Servicio de configuración de LUNS(unidad lógica de red) del Dispositivo de Almacenamiento IBM Storwize V7000	S/. 5,000.00
Generador Eléctrico con cuchilla de intercambio automático.	S/. 7,000.00
Software de Almacenamiento Backup.(Tivoly storage manager)	S/. 8,000.00

Servicio de Protección y custodia de la Data en Cintas.	S/. 1,500.00
Switch Core Cisco 3750-24SFP adicional.	S/. 15,000.00
Switch Distribución Cisco 2960-X Series adicional.	S/. 15,000.00
Línea de Internet 8 Mbps de respaldo por 12 meses	S/. 10,000.00
COSTO TOTAL (Referencial):	S/. 86,500.00

Nota: Elaboración propia

3.5 Recuperación de la Inversión

En la siguiente tabla N°9 se muestra ahorro supuesto anual para contar con el SGSI propuesto anteriormente; seguido de la tabla N° 21 beneficio/costo:

Tabla 38

Ahorro supuesto anual al contar con un SGSI

Descripción	Ahorro
Pérdida de la información accidental	S/. 100,000.00
Pérdida de la información por desastres naturales y/o provocados	S/. 250,000.00
Pérdida o robo de información por problemas de comunicación	S/. 50,000.00
Interrupción de los procesos de negocio	S/. 300,000.00
Robo de información de los clientes personal interno y/o proveedores	S/. 50,000.00
TOTAL AHORRO (Supuesto Anual)	S/. 750,000.00

Nota: Elaboración propia

Tabla 39

Beneficio / Costo

Beneficio:	S/. 750,000.00
Costo:	S/. 86,500.00
B/C	S/. 663,500.00

Nota: Elaboración propia

3.5.1 Cuadro financiero del VAN:

Las siguientes tablas presentan un análisis de sensibilidad sobre el VAN, considerando variaciones en los costos, precios de venta, servicios y total de egresos. En la tabla N° 11 mostramos un cuadro con el flujo de caja económica sin los servicios propuestos del SGSI, tal como en la tabla N°12 mostramos el flujo de caja económica ya con los servicios propuestos del SGSI:

Tabla 40

Flujo de caja económico (sin los servicios propuestos del SGSI)

Concepto / Años	**Año 0**	**Año 01**	**Año 02**	**Año 03**	**Año 04**
		I. INGRESOS			
1.-Total Ingreso		150,000	150,000	150,000	150,000
Ventas y Servicios.		150,000	150,000	150,000	150,000

II. EGRESOS

Egresos por Actividad				
2.-Total Egresos (Gastos Administrativos)	44,400	44,400	44,400	44,400
LINEA DEDICADA (PPP) 10Mb	44,400	44,400	44,400	44,400
Utilidad Operativa	105,600	105,600	105,600	105,600
Utilidad antes de Impuestos	105,600	105,600	105,600	105,600
Impuesto a la Renta (Asociación sin fines de lucro)	0	0	0	0
FCE	105,600	105,600	105,600	105,600

Nota: Elaboración propia

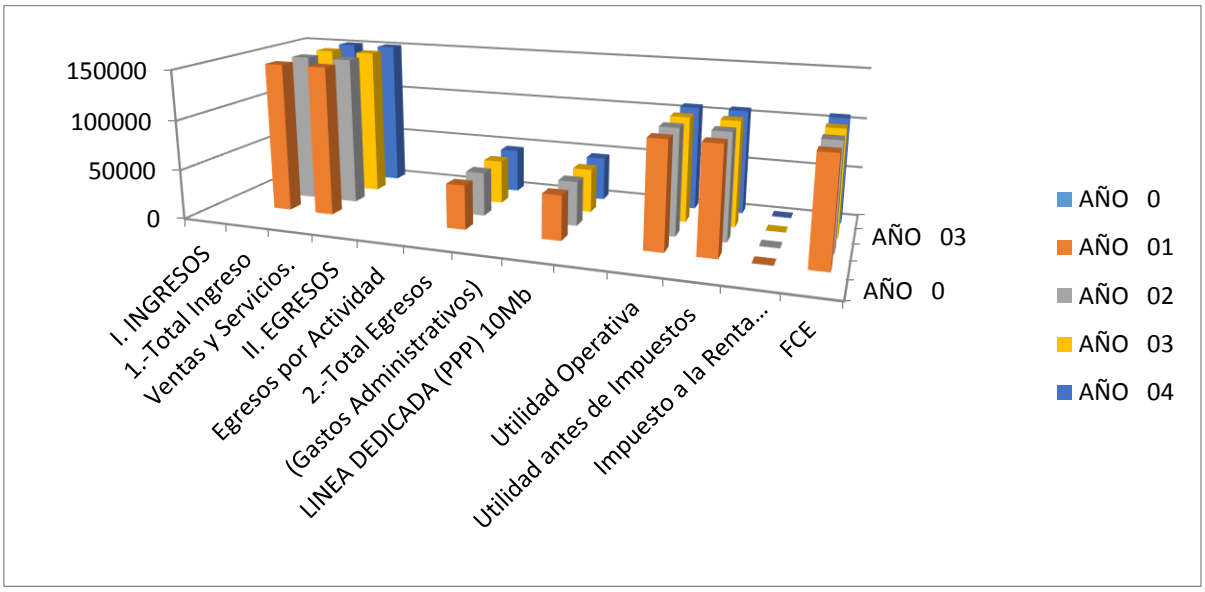


Figura 11. Diagrama de barras con los resultados del flujo de caja económico (SIN LOS SERVICIOS PROPUESTOS DEL SGSI). Elaboración Propia.

Tabla 41

Flujo de caja económico (con los servicios propuestos del SGSI)

Concepto / Años	**Año 0**	**Año 01**	**Año 02**	**Año 03**	**Año 04**
		I. INGRESOS			
		S/.	S/.	S/.	S/.
1.-Total Ingreso		150,000.00	150,000.00	150,000.00	150,000.00
Ventas y servicios		150,000	150,000	150,000	150,000

II. EGRESOS

Costo de Inversión	
Servicio de implementación del Servidor BLADE IBM.	5,000
Adquisición Firewall : CheckPoint	20,000
Servicio de configuración de LUNS del Dispositivo de Almacenamiento IBM Storwize V7000	5,000
Generador Eléctrico con cuchilla de intercambio automático.	7,000
Software de Almacenamiento Backup.(Tivoly storage manager)	8,000

Servicio de Protección y custodia de la Data en Cintas.	1,500				
Switch Core Cisco 3750-24SFP adicional.	15,000				
Switch Distribución Cisco 2960-X Series adicional.	15,000				
IMPLEMENTACION (TESISTA)	-				
(Imprevistos 1%)	-	30,000			
(Total de Inversión)	76,500				
Egresos por Actividad					
2.-Total Egresos (Gastos Administrativos)	S/. 76,500.00	S/. 54,400.00	S/. 54,400.00	S/. 54,400.00	S/. 54,400.00
LINEA DEDICADA (PPP) 10Mb		44,400	44,400	44,400	44,400

Línea de Internet 8 Mbps de respaldo por 12 meses		10,000	10,000	10,000	10,000
Utilidad Operativa		95,600	95,600	95,600	95,600
Utilidad antes de Impuestos		95,600	95,600	95,600	95,600
		0	0	0	0
(Inversión)	-76,500				
FLUJO DE CAJA ECONOMICO		S/. 95,600.00	S/. 95,600.00	S/. 95,600.00	S/. 95,600.00

Nota: Elaboración propia

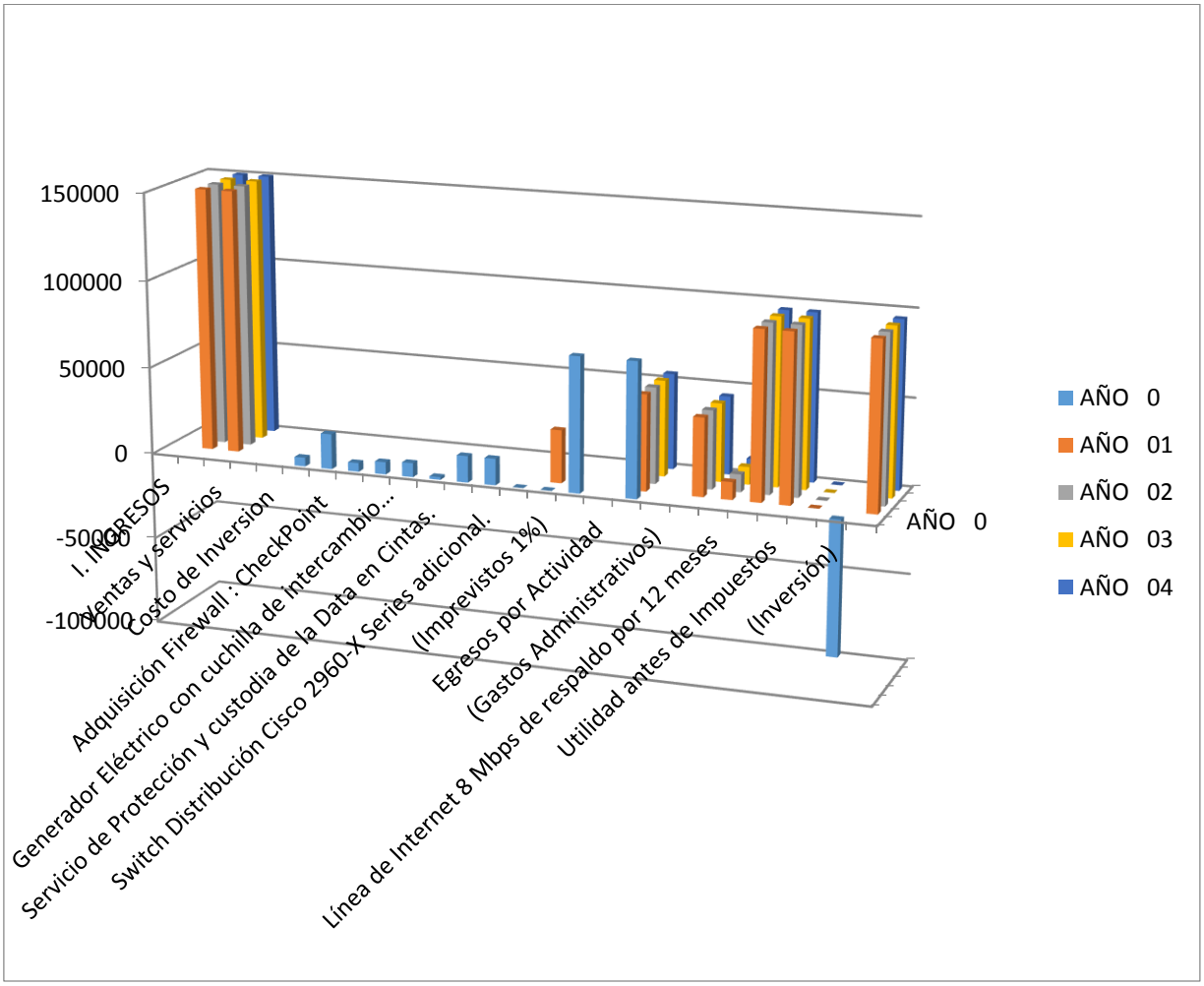


Figura 12. Diagrama de barras con los resultados del flujo de caja económico (CON LOS SERVICIOS DE LA PROPUESTAS DEL SGSI). Elaboración Propia.

EVALUACIÓN ECONÓMICA

Variables	
Tasa de descuento económico	12%
Inversión total	76,500

VANE(12%)=290,371

EL ANÁLISIS BENEFICIO/COSTO ES:

FORMULA DE BENEFICIO COSTO DE UNA INVERSIÓN

B/C E= VAN(Ingresos) = 455,602 **1.88**

VAN (Egresos) 241,372

B/C E = 1.88

Figura 13. Evaluación económica. Elaboración Propia.

Tabla 42

Valor presente de los ingresos y egresos para hallar el beneficio costo

	0	**1**	**2**	**3**	**4**	**Total**
VANI(12%)=		133,928.57	119,579.08	106,767.04	95,327.71	455,602.40
VANE(12%)=	136,500.00	48,571.42	43,367.34	38,720.84	34,572.18	241,731.80

Nota: Elaboración Propia.

Tabla 43

Resumen de evaluación económica

	VAN	B/C
Evaluación Económica	290,370.59	1.88
Resumen de Evaluación Económica		

Nota: Elaboración Propia.

Tabla 44

Periodo de recuperación económico

Año	Inversión	Año 01	Año 02	Año 03	Año 04
Flujo de Caja Económico		95,600	95,600	95,600	95,600
Inversión	-76,500				
Flujo de Caja Acumulado		S/.19,900.00	S/. 114,700.00	S/. 210,300.00	S/.305,900.00

Nota: Elaboración Propia.

Periodo anterior al cambio del signo	1	
Valor absoluto del flujo acumulado	60900	***FORMULA DE PERIODO DE RECUPERACION***
Flujo de caja en siguiente periodo	75600	
PERIODO DE RECUPERACION DE INVERSION	1.81	*1 AÑO Y 8 MESES*

$$\text{Periodo anterior al cambio del signo} + \frac{\text{Valor absoluto del flujo acumulado}}{\text{Flujo de caja en siguiente periodo}}$$

Figura 14. Formula de Periodo de Recuperación. Elaboración Propia.

En cuanto a evaluación económica, Por cada S/. 1.26 que recuperamos gastamos S/.1.00, teniendo en cuenta que el periodo de recuperación de la inversión económica es de 1 año y 8 meses.

Como se observa, el B/C es > a 1 (1.26), esto quiere decir que la inversión adicional para el SGSI en la empresa es aceptable, lo que representa un beneficio de S/ 229,624

3.6 Beneficios Tangibles

- ✓ Mejora de productividad de los trabajadores.
- ✓ Mayor confianza de nuestro cliente para la garantía de calidad y confidencialidad comercial.
- ✓ Disponibilidad de la información.
- ✓ Ayuda a identificar los activos de información y a protegerlos adecuadamente.
- ✓ Provee a la gerencia dirección y apoyo para la seguridad de la información

3.7 Beneficios Intangibles

- ✓ Reduce la pérdida o robo de información.
- ✓ Diferencia en la competencia a nivel regional y/o nacional.
- ✓ Mejorará la seguridad, autenticidad, confiabilidad de la información ante algún incidente de seguridad.
- ✓ Confianza y reglas claras para los trabajadores de la organización.
- ✓ Fortalece los conocimientos de los trabajadores respecto a temas de seguridad de la información.

- ✓ Asegura una correcta y segura operación de información de la empresa, reduciendo el riesgo del error humano.
- ✓ Incrementa sustancialmente los controles de accesos a la información.
- ✓ Minimiza la interrupción en el funcionamiento de las actividades de la empresa y lo protege de desastres.

CAPITULO IV

Conclusiones

6.1 . Conclusiones

- ✓ Se identificó los procesos de negocio haciendo uso de la herramienta de Magerit con los siguientes elementos: activos, amenazas, vulnerabilidades, Impactos, Riesgo, Salvaguardas permitió establecer como se delimitaría nuestro sistema de gestión
- ✓ Se identificó los activos de información aplicando la Norma ISO/IEC 27001 encontrándose un total de 29 (*Tabla N° 1*) cuya criticidad tenían un valor alto los cuales se tomaron en cuenta para el desarrollo del SGSI.
- ✓ La evaluación de los riesgos aplicando la Norma ISO/IEC 27001 se inició con los riesgos con criticidad alta los cuales se usaron para trabajar las vulnerabilidades y amenazas a mitigar a través de un plan de tratamiento de riesgos.
- ✓ Los controles seleccionados de la Norma ISO/IEC 207001 para su implementación son un total de 13 los cuales se eligieron para mitigar los riesgos más críticos dentro del Área de Operaciones y Tecnología de Global BPO Center.
- ✓ Se definieron las políticas, normas y procedimientos de seguridad exigida por la norma ISO7IEC 27001 quedando estructurado de la siguiente manera: el alcance del SGSI, políticas y objetivos de seguridad de la información, metodología de evaluación y tratamiento de riesgos, la declaración de aplicabilidad, plan de tratamiento de riesgos, inventario de activos, política de control de acceso, procedimiento para gestión de incidentes, procedimientos de la continuidad de negocios, garantizando la confidencialidad, integridad y disponibilidad de la información.

CAPITULO V

Recomendaciones

7.1 . Recomendaciones:

- ✓ Realizar campañas de concientización periódicas para el personal de la empresa con respecto a la seguridad de información, de tal manera que todos los empleados de los diversos niveles jerárquicos existentes, conozcan la importancia y las consecuencias de no seguir los lineamientos de seguridad en el día a día.

- ✓ Se recomienda que se establezca el comité de seguridad que pueda dedicarse a la continuidad del sistema de gestión.

- ✓ Actualizar periódicamente el SGSI. El plazo recomendado es cada **3** años ya que este periodo implica la posible adquisición de nuevas tecnologías dentro del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo**.**

- ✓ Realizar ejercicios de escritorio para comprobar los controles establecidos dentro del SGSI. Por lo menos una vez al año se deberían realizar dichas pruebas.

Bibliografía Referenciada

- Alexander G., A. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información / Óptica ISO/ IEC 27001:2005.* Bogota: Primera edición , Alfaomega Colombiana S.A.
- Ampuero Chang, C. (2011). *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros. Tesis para optar por el título de Ingeniero Informático.* Lima: Pontificia Universidad Católica del Perú, Facultad de Ingeniería Informática.
- Ayub, D. T. (Julio de 2012). MANUAL DE POLITICAS Y NORMAS DE SEGURIDAD INFORMATICA.
- Center, O. C. (2016). *27001*. Obtenido de http://advisera.com/27001academy/es/que-es-iso-27001/
- Cesar Wenceslao de la Cruz Guerrero, J. C. (2008). *Elaboracion y Aplicacion de un Sistema de Gestion de la Seguridad de la informacion(SGSI) para la Realidad Tecnológica de la USAT.* Lambayeque-Peru.
- Chávez Paz Jorge Homero, N. L. (2014). *Sistema de Gestion de Seguridad de Información basada en la norma ISO/IEC 27001 para la Superintendencia de Transport Terrestre de Personas, Carga y Mercancías (SUTRAN) - Region Lambayeque.* Lambayeque-Peru.
- Empresarial, L. (2016). *Retos Directos*. Obtenido de Retos Directos: http://retos-directivos.eae.es/el-activo-fijo-tipos-y-caracteristicas/
- Gupta, P. (2005). *ISO 27000.es*. Obtenido de http://www.iso27000.es/iso27000.html

- HENAO ACOSTA, C. (s.f.). *DIAGNOSTICO DE LA SEGURIDAD INFORMÁTICA EN APOSTAR S.A.* Obtenido de docplayer: http://docplayer.es/1722934-Diagnostico-de-la-seguridad-informatica-en-apostar-s-a-carolina-henao-acosta.html
- ISACA. (2012). *COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.*
- *JEANNELLYS*. (09 de FEBRERO de 2009). Obtenido de SEGURIDAD DE INFORMATICA: http://jeannellys.blogspot.pe/2009/02/seguridad-de-los-sistemas-de.html
- JORGE, C. A. (2014). *POLÍTICAS Y NORMAS DE SEGURIDAD.* CORDOBA.
- *Manual de politicas y normas de seguridad informatica.* (s.f.). Obtenido de scribd: http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica#scribd
- María Dolores Cerini, P. I. (2002). *Plan de Seguridad Informatica.* Córdova - Argentina.
- Martinez, A. G. (2006). *"proyecto CAMERSEC - Implatacion de Sistemas de Gestion de Seguridad de Informacion en PyMEs".* España - Malaga.
- Mejía, R. C. (2014). *Definición y Tipos de Riesgos.* Obtenido de eafit.
- Quispe Arroyo, J. C. (s.f.). *slideshare*. Obtenido de Políticas de seguridad: http://es.slideshare.net/xjuan12x/polticas-de-seguridad-16925175
- REDSER. (2016). *ISO 27001 - Sistema de Gestión de Seguridad de la Información.* . Obtenido de http://www.redser.com/servicios/iso-27001.asp
- Rodriguez, N. E. (2003). *Plan de Seguridad Informática para una Entidad Financiera.* Lima-Peru.

- *Seguridad de la información y auditoría de sistemas*. (s.f.). Obtenido de monografias: http://www.monografias.com/trabajos61/seguridad-informacion-auditoria-sistemas/seguridad-informacion-auditoria-sistemas.shtml
- *Seguridad Informatica*. (15 de Junio de 2015). Obtenido de Prezi: https://prezi.com/esieqjirveuy/seguridad-informatica/
- STANDARDIZATION, I. O. (2013). *"Information technology - Security techniques - Information security management systems – Overview and Vocabulary".* International Standard ISO/IEC 27000:2012. Switzerland, 2012.
- Venemedia. (2014). *CONCEPTODEFINICION.DE*. Obtenido de CONCEPTODEFINICION.DE: http://conceptodefinicion.de/seguridad/
- Wikipedia. (08 de 03 de 2016). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- Wikipedia. (2016). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Activo_(contabilidad)#Tipos_de_activo

ANEXOS

- **ANEXO A (NORMATIVA)**

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

Los objetivos de control y controles listados en la Tabla A.1 son directamente derivados desde y alineados con los listados en ISO/IEC 27002:2013[1], Cláusulas 5 a 18 y se utilizan en el contexto con el Apartado 6.1.3.

A.6.1 Objetivos de control y controles

A.6.1.4	Contacto con grupos especiales de interés	*Control* Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.

A.6.2 Dispositivos móviles y teletrabajo

Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.

A.6.2.1	Política de dispositivos móviles	*Control*

		Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.

A.7 Seguridad de los recursos humanos

A.7.1 Antes del empleo

Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.

A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.

A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.

A.7.2 Durante el empleo

Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.

A.7.2.1	Responsabilidades de la gerencia	*Control* La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	*Control* Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y

		procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.
A.7.2.3	Proceso disciplinario	*Control* Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.

A.7.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

A.7.3.1	Terminación o cambio de responsabilidades del empleo.	*Control* Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.

A.8 Gestión de activos

A.8.1 Responsabilidad por los activos

Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.

A.8.1.1	Inventario de activos	*Control* Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben ser propios.
A.8.1.3	Uso aceptable de los activos	*Control* Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.
A.8.1.4	Retorno de activos	*Control* Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización

		en su posesión a la conclusión de su empleo, contrato o acuerdo.

A.8.2 Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.

A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.
A.8.2.2	Etiquetado de la información	*Control* Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.
A.8.2.3	Manejo de activos	*Control* Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia

		con el esquema de clasificación de la información adoptado por la organización.

A.8.3 Manejo de los medios

Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.

A.8.3.1	Gestión de medios removibles	*Control* Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de medios	*Control* Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.

A.9 Control de acceso

A.9.1 Requisitos de la empresa para el control de acceso

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

A.9.1.1	Política de control de acceso	*Control* Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y servicios de red	*Control* Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.

A.9.2 Gestión de acceso de usuario

Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.

A.9.2.1	Registro y baja de usuarios	*Control* Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.

A.9.2.2	Aprovisionamiento de acceso a usuario	*Control* Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	*Control* La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.
A.9.2.4	Gestión de información de autentificación secreta de usuarios	*Control* La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.
A.9.2.5	Revisión dede derechos acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Remoción o de ajuste derechos de acceso	*Control* Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes

		externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.

A.9.3 Responsabilidades de los usuarios

Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.

A.9.3.1	Uso de de información autentificación secreta	*Control* Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.

A.9.4 Control de acceso a sistema y aplicación

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.
A.9.4.2	Procedimientos de ingreso seguro	*Control* Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe

		ser controlado por un procedimiento de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.
A.9.4.5	Control de acceso al código fuente de los programas	*Control* El acceso al código fuente de los programas debe ser restringido.

A.10 Criptografía

A.10.1 Controles criptográficos

Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

A.10.1.1	Política sobre el usode controles criptográficos	*Control* Una política sobre el la uso de criptográficos para ser controles información debe protección de implementada. la desarrollada e
A.10.1.2	Gestión de claves	*Control* Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.

A.11 Seguridad física y ambiental

A.11.1 Áreas seguras

Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.

A.11.1.1	Perímetro de seguridad física	*Control* Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen

		información sensible o crítica e instalaciones de procesamiento de la información.
A.11.1.2	Controles de ingreso físico	*Control* Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	*Control* Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
A.11.1.5	Trabajo en áreas seguras	*Control* Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.
A.11.1.6	Áreas de despacho y carga	*Control* Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser

		controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.

A.11.2 Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.

A.11.2.1	Emplazamiento y protección de los equipos	*Control* Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
A.11.2.2	Servicios de suministro	*Control* Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.

A.11.2.4	Mantenimiento de equipos	*Control* Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.
A.11.2.5	Remoción de activos	*Control* Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Disposición o reutilización segura de equipos	*Control* Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.

A.11.2.8	Equipos de usuario desatendidos	*Control* Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.

A.12 Seguridad de las operaciones

A.12.1 Procedimientos y responsabilidades operativas

Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.

A.12.1.1	Procedimientos operativos documentados	*Control* Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión del cambio	*Control* Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la

		información y sistemas que afecten la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de la capacidad	*Control* El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	*Control* Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

A.12.2 Protección contra códigos maliciosos

Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.

A.12.2.1	Controles contra códigos maliciosos	*Control* Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser

		implementados, en combinación con una concientización apropiada de los usuarios.

A.12.3 Respaldo

Objetivo: Proteger contra la pérdida de datos

A.12.3.1	Respaldo de la información	*Control* Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.

A.12.4 Registros y monitoreo

Objetivo: Registrar eventos y generar evidencia

A.12.4.1	Registro de eventos	*Control* Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.
A.12.4.2	Protección de información de registros.	*Control* Las instalaciones para registros (logs) y la información de los registros (logs) deben ser

		protegidas contra la adulteración y el acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.
A.12.4.4	Sincronización de reloj	*Control* Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.
A.12.5 Control del software operacional		
Objetivo: Asegurar la integridad de los sistemas operacionales		
A.12.5.1	Instalación de software en sistemas operacionales	*Control* Procedimientos deben ser implementados s para controlar la instalación de software en sistemas operacionales.

A.12.6 Gestión de vulnerabilidad técnica

Objetivo: Prevenir la explotación de vulnerabilidades técnicas

A.12.6.1	Gestión de vulnerabilidades técnicas	*Control* Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.

A.12.7 Consideraciones para la auditoría de los sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

A.12.7.1	Controles de auditoría de sistemas de información	*Control* Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados

		para minimizar la interrupción a los procesos del negocio.

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de seguridad de la red

Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

A.13.1.1	Controles de la red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.
A.13.1.2	Seguridad de servicios de red	*Control* Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.
A.13.1.3	Segregación en redes	*Control*

		Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.

A.13.2 Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

A.13.2.1	Políticas y procedimientos de transferencia de la información	*Control* Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdo sobre transferencia de información	*Control* Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.
A.13.2.3	Mensajes electrónicos	*Control* La información involucrada en mensajería electrónica debe ser protegida apropiadamente.

A.13.2.4	Acuerdos de confidencialidad o no divulgación	*Control* Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.

A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.

A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	*Control* La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de

		contratos o divulgación no autorizada y modificación.
A.14.1.3	Protección de transacciones en servicios de aplicación	*Control* La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.

A.14.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del

ciclo de vida de desarrollo de los sistemas de información.

A.14.2.1	Política de desarrollo seguro	*Control* Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambio del sistema	*Control*

		Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	*Control* Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones sobre cambios a los paquetes de software	*Control* Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.
A.14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.

A.14.2.6	Ambiente de desarrollo seguro	*Control*	Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.
A.14.2.7	Desarrollo contratado externamente	*Control*	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.
A.14.2.8	Pruebas de seguridad del sistema	*Control*	Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.
A.14.2.9	Pruebas de aceptación del sistema	*Control*	Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.

A.14.3 Datos de prueba

Objetivo: Asegurar la protección de datos utilizados para las pruebas

A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.

A.15 Relaciones con los proveedores

A.15.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores

A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	*Control* Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	*Control* Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.

A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.

A.15.2 Gestión de entrega de servicios del proveedor

Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.

A.15.2.1	Monitoreo y revisión de servicios de los proveedores	*Control* Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.
A.15.2.2	Gestión de cambios a los servicios de proveedores	*Control* Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la

		criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.

A.16 Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.

A.16.1.1	Responsabilidades y procedimientos	*Control* Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Empleados y contratistas que usan los sistemas y servicios de información de la organización deben

		ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	*Control* Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección,

		adquisición y preservación de información que pueda servir como evidencia.

A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio

A.17.1 Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización

A.17.1.1	Planificación de continuidad de seguridad de la información	*Control* La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.
A.17.1.2	Implementación de continuidad de seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de continuidad	*Control*

	de seguridad de la información	La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.

A.17.2 Redundancias

Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información

A.17.2.1	Instalaciones de procesamiento de la información	*Control* Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.

A.18 Cumplimiento

A.18.1 Cumplimiento con requisitos legales y contractuales

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.

A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	*Control* Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el

		enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	*Control* Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.
A.18.1.3	Protección de registros	*Control* Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de datos personales.	*Control* La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.

A.18.1.5	Regulación de controles criptográficos	*Control* Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.

A.18.2 Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.

A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento de políticas y normas de seguridad	*Control* Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de

		responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información deben ser revisados regularmente respecto al cumplimieto de las políticas y normas de seguridad de la información de la organización.

- **ANEXO Nº 01:**

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

(Encuesta Verbal)

Dirigido a los **trabajadores** de Global BPO Center Allus Chiclayo.

Objetivos:

- Conocer que tan involucrados se encuentran los trabajadores en el resguardo de la Tecnología de Información.
- Saber si los trabajadores utilizan de manera óptima las tecnologías de información y de qué manera ayudarían a salvaguardar la misma.

1. Cargo del Informante: **……..……**

2. A qué área pertenece:**……..**

3. Puede identificar a las personas que no trabajan en Allus.

   SI ( ) NO ( )

   Si tu respuesta es **Sí,** fue por medio de:

   a. Fotosheck de la empresa. ( )
   b. Indumentaria ( )
   c. Otros, Especificar**……** ( )

4. Usted apaga los equipos informáticos debidamente después de utilizarlos

   SI ( ) NO ( )

   Si tu respuesta es **Sí,** Cómo apagas tu equipo después de trabajar

   a. Desenchufando el cable de energía de la computadora. ( )
   b. Manteniendo presionando el botón de apagado del CPU. ( )
   c. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )

5. Se siente seguro en los ambientes donde se encuentran los equipos informáticos frente a cualquier desastre natural.

   SI ( ) NO ( )

6. Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar

   SI ( ) NO ( )

7. Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de Global BPO Center Allus Chiclayo

SI ( ) NO ( )

8. Si en el transcurso del uso de su equipo informático se detecta alguna actividad sospechosa como ingresando a lugares restringidos (redes sociales, correos personales, páginas de entretenimiento), usted sería capaz de afrontarla (por la responsabilidad que asume en ese determinado momento sobre el equipo asignado)

SI ( ) NO ( )

9. Hace usted uso de los antivirus en los equipos informáticos de la Global BPO Center Allus Chiclayo cuando ingresa al ordenador.

Si ( ) A veces ( ) No tiene conocimiento ( )

10. Usa usted algún tipo de dispositivo de almacenamiento para sacar información del ordenador.

Si ( ) No ( )

11. ¿Cómo obtienes tus claves de acceso para los aplicativos que utilizas?

a. A través de un correo ( )
b. Verbalmente ( )
c. A través de un documento ( )

12. Alguno de tus compañeros de trabajo tiene acceso a tus cuentas y/o contraseñas.

Si ( ) No ( )

13. Cada que tiempo cambias la contraseña de tus cuentas.

Semanal ( ) Mensual ( ) Nunca ( )

14. Utiliza el servicio de correo electrónico que le asigna Global BPO Center Allus Chiclayo para uso personal.

SI ( ) NO ( )

15. Usted recibió alguna capacitación acerca de Seguridad de la Información en Global BPO Center Allus Chiclayo.

SI ( ) NO ( )

16. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información

SI ( ) NO ( )

Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:

a. Folletos y boletines ( )
b. Charlas o conferencias ( )
c. Otros, Especifique: **……** ( )

17. Usted ha realizado alguna de las siguientes actividades en su PC:

    a. Instalando algún software que necesitaba ( )

    b. Haciendo limpieza de componente de su PC (teclado, mouse, cpu, etc.) ( )

    c. Desarmando el CPU por algún sonido o falla ( )

    d. Otros, Especifique…….. ( )

    e. Ninguna ( )

18. ¿Qué hace usted cuando uno de sus componentes o aplicativos no funcionan correctamente en su PC?

    a. Intenta arreglarlo ( )

    b. Lo arregla mi compañero de trabajo más cercano ( )

    c. Llamo a mi jefe directo para que me de una solución. ( )

19. ¿Con qué frecuencia solicita usted que se le realice mantenimiento a la PC que se le asigno?

    Mensual ( ) Trimestral ( ) Semestral ( ) Anual ( ) Nunca ( )

20. ¿Con qué frecuencia solicita que le revisen su PC frente a cualquier falla?

    A veces ( ) Casi Siempre ( ) Nunca ( )

21. Cree usted que su equipo se encuentra seguro frente a cualquier peligro como:

    a. Acceso a sus cuentas personales ( )

    b. Ingreso de Virus ( )

    c. Existencia de un extinguidor o medida de seguridad de los equipos cerca ( )

d. No lo sé ( )

e. Otros, Especificar…….. ( )

22. Cada vez que sufre algún inconveniente con la PC o aplicación la cual desea trabajar, porque medio informa o reporta el inconveniente:

a. Teléfono ( )

b. Correo electrónico. ( )

c. Voy físicamente a buscar algún encargado. ( )

d. Espero que pasen por mi área de trabajo ( )

e. Otros, Especifique…… ( )

f. Ninguna ( )

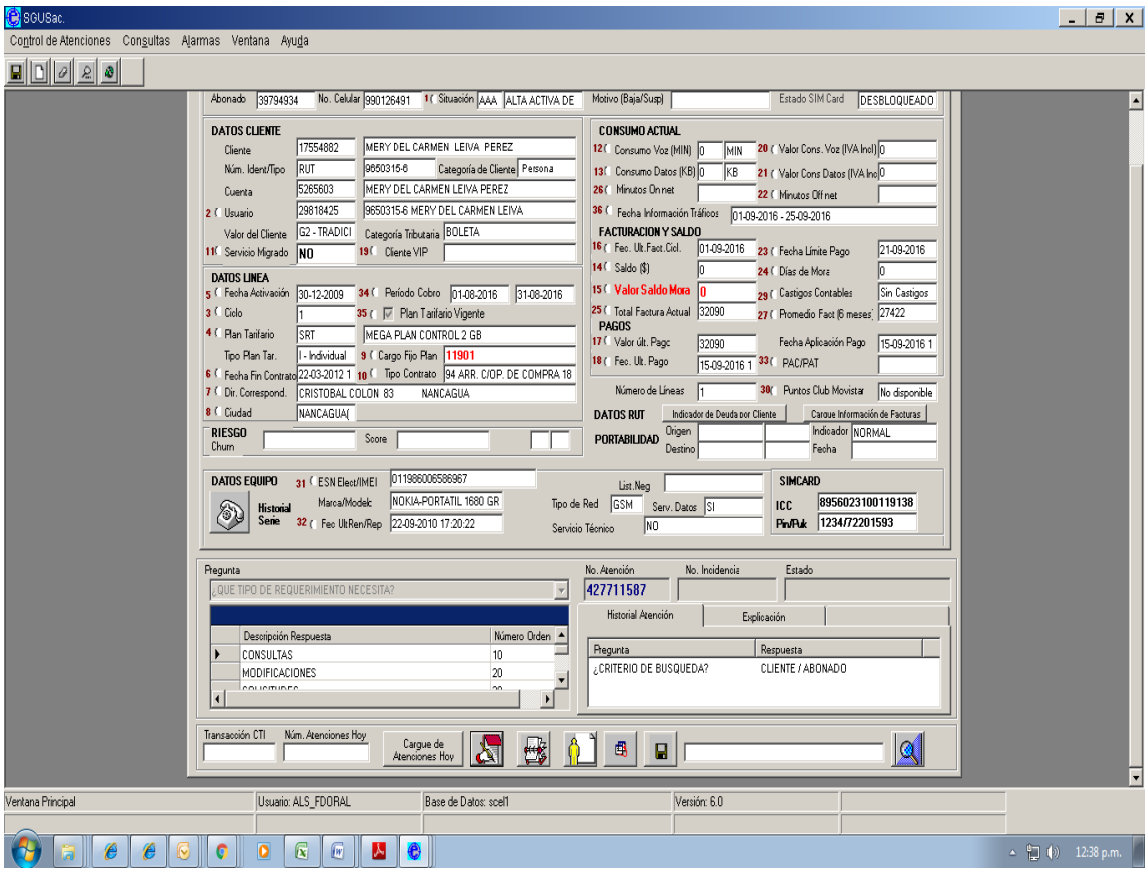
- **ANEXO Nº 02:**

Gartner 2016 para los Firewalls de Redes Empresariales.

- **ANEXO Nº 03:**

Plataforma utilizada en la Empresa Global BPO Center Allus Chiclayo

✓ **CITRIX:**



Prepago Movistar V 2.1.8 - Windows Internet Explorer

movistar

VERONICA SANHIESA AR | Tecnología : GSM | Plan Actual : NUMFREC

997233992 | Modelo Equipo : PORTATIL L6 | Valor : BLUE_1

Estado: ALTA ACTIVA DE ABONADO | Tipo : PREPAGO | Sistema : SCL

No. Abonado : Buscar

- Consulta On Line
  - Consulta de Saldo
  - Consulta Voucher
  - Consulta Tráfico y Recarga OnLine
- Recarga On Line
- Consultas PSM
- Consultas Comerciales
- Consulta SVA Activos
- Números Frecuentes
- Aplicar Recarga
- Aplicar Cambio Plan
- Combos y Bolsas Prepago
- Salir

Trafico y Recargas On Line >

Informacion Comverse

Fecha Activación : 0001-01-01 00:00:00 | Estado Actual : Activo con saldo | Estado Anterior :

Código Plan Actual : NUMFREC | Saldo Actual : 9045 | Fecha Vigencia Saldo : 17-10-2016

Fecha Expiraci?n Saldo : 16-03-2017

						SALDO FINAL				
Fecha	Tipo	Descripción	No Tarjeta No LLamado	Duración	Monto	Min Núm preferido	Min on promo	Min on	Min todo destino	Saldo
2016-09-26 19:44:41	Llamada	Llamada	103	00:05:00	$0	-	-	-	-	$9045
2016-09-26 18:58:52	Ajuste	c4-10-179-5-114-EPGMMT1.epc.mnc	-	-	$590	-	-	-	-	$9045
2016-09-25 02:31:30	MTR	EXP_BALS	-	-	$0	-	-	-	-	$9635
2016-09-23 12:54:51	Llamada	Llamada	996592901	00:13:14	$0	02:35:41	-	-	-	$9635
2016-09-20 15:51:50	Llamada	Llamada	228446743	00:00:19	$20	-	-	-	-	$9635
2016-09-20 15:49:37	Llamada	Llamada	992283000	00:00:23	$25	-	-	-	-	$9656
2016-09-20 11:11:26	Llamada	Llamada	996592901	00:05:08	$0	02:48:55	-	-	-	$9682
2016-09-19 21:12:25	Llamada	Llamada	226222081	00:03:27	$0	02:54:03	-	-	-	$9682
2016-09-19 13:39:19	Llamada	Llamada	226222081	00:02:15	$0	02:57:30	-	-	-	$9682
2016-09-19 13:33:51	Llamada	Llamada	226222081	00:03:46	$0	02:59:45	-	-	-	$9682
2016-09-19 12:26:01	Llamada	Llamada	226222081	00:02:39	$0	03:03:31	-	-	-	$9682
2016-09-18 13:42:11	Llamada	Llamada	226222081	00:03:12	$0	03:06:10	-	-	-	$9682
2016-09-18 02:33:37	MTR	EXP_BALS	-	-	$0	-	-	-	-	$9682
2016-09-17 20:13:59	Llamada	Llamada	996592901	00:02:07	$0	03:09:22	-	-	-	$9682
2016-09-17 19:29:56	Llamada	Llamada	226222081	00:05:22	$0	03:11:29	-	-	-	$9682
2016-09-17 19:15:15	Llamada	Llamada	996592901	00:03:09	$0	03:16:51	-	-	-	$9682
2016-09-17 15:54:26	MTR	POS_MCAJAS	-	-	$2000	03:20:00	-	-	-	$9682
2016-09-17 15:54:26	Recarga	Recarga	0 0	-	$2000	03:20:00	-	-	-	$9682

12:39 p.m.