UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Sistema de gestión de seguridad de la información de la empresa América Móvil

Tesis para obtener el título profesional en ingeniería informática y de sistemas

Autor

Cherres Odar, Ingrid Melissa

Asesor

Valle Peláez, Miguel

Código ORCID: 0000-0003-3138-9808

CHIMBOTE – PERÚ

2022

Índice

Título

Sistema de gestión de seguridad de la información de la empresa América Móvil Chimbote.

Resumen

La presente investigación tuvo por objetivo el desarrollo de un sistema de gestión de seguridad de la información para la empresa América Móvil en el área de Operaciones con la finalidad de proteger los datos de la mencionada empresa. Para desarrollar el presente trabajo se hizo uso del PMBOK y de la norma estándar ISO 27001 que implementa la seguridad de los trabajadores y clientes. Dichos documentos permiten la flexibilidad a adaptarse a cualquier situación organizacional. Como instrumentos de recolección de datos se emplearon entrevistas y cuestionarios al jefe del área y al personal respectivo. Con los resultados obtenidos se pudo obtener diversas recomendaciones que ayudan a la implementación de un sistema de gestión de la seguridad de la información de la empresa América Móvil.

Abstract

The objective of this investigation was the development of an information security management system for the company América Móvil in the Operations area in order to protect the data of the aforementioned company. To develop this work, use was made of the PMBOK and the ISO 27001 standard that implements the safety of workers and customers. These documents allow the flexibility to adapt to any organizational situation. As data collection instruments, interviews and questionnaires were used with the head of the area and the respective staff. With the results obtained, it was possible to obtain various recommendations that help the implementation of an information security management system for the company América Móvil.

Introducción

Los antecedentes encontrados fueron:

García (2021) en su tesis tuvo el propósito de realizar una propuesta de un sistema de gestión para la seguridad de la información basado en la norma ISO 27001 para las oficinas de tecnologías de la información del Gobierno Regional de Piura. Como tipo de investigación se empleó en cualitativo y con un diseño no experimental. La muestra de la investigación estuvo conformada por 23 colaboradores del gobierno regional. Los resultados indicaron que el 91% de los encuestados sostuvo que no está satisfecho con la situación actual, mientras que el 9% restante afirmó que sí se siente satisfecho. El 100% de los entrevistados afirmó que sí se necesita seguridad en la información con la norma ISO 27001. La conclusión del estudio señala que la propuesta de un sistema de gestión para la seguridad de la información mejora los procesos de seguridad de la información y comunicación del Gobierno Regional de Piura.

Fuentes (2020) tuvo el objetivo de proponer un sistema de gestión para la seguridad de la información encargada de gestionar los procesos más críticos en la Universidad Nacional de Cajamarca. Se usó como marco de referencia fue la norma ISO/IEC 27003 que propone la implementación de un sistema de gestión de la seguridad de información y que a su vez se apoya también en las normas ISO/IEC 27001 e ISO/IEC 27002. Mientras que para analizar los riesgos en TI se usó la metodología MagerIT. Se empleó también un cuestionario como instrumento de recolección de información que se aplicó a los usuarios de TI de la Universidad Nacional de Cajamarca. La conclusión del trabajo señala que la implementación de un sistema de gestión para la seguridad de la información tiene un nivel aceptable.

Cruz y Fukusaki (2017) tuvieron el propósito de diseñar e implementar un sistema de gestión de seguridad de la información con la finalidad de proteger los activos de la información en la empresa Clínica MEDCAM Perú SAC. La metodología empleada fue el método DEMIG o PDCA sugerida por la norma ISO/IEC 27001. Los controles de respuesta se obtuvieron mediante la norma ISO/IEC 27002. Los

resultados de la investigación lograron minimizar los riesgos y amenazas sobre los activos de la información de la empresa, logrando así confidencialidad e integridad en la información. Se concluye que el beneficio de la investigación es asegurar los activos de la información y objetivos de la empresa.

Pardo (2015) presentó una tesis para la Universidad Nacional de Loja, Ecuador, en donde tuvo el objetivo de implementar un modelo de gestión de seguridad en la información para la mencionada universidad basada en la norma ISO/IEC 27001. Se sabe que en la actualidad uno de los bienes más importantes para cualquier empresa en su información; por lo tanto, su adecuado manejo es clave para preservar su identidad y confidencialidad. Este trabajo pretende proporcionar diversos mecanismos de control para proteger los datos, propiedad de la Universidad Nacional de Loja. Además, este trabajo se desarrolló bajo las especificaciones de la Norma ISO/IEC 27001, aplicando diversas entrevistas al personal técnico responsable del área y en donde se puedo observar las necesidades en cuanto a la seguridad. Se consideró la metodología MAGERIT v3 para evaluar la gestión de los riesgos informáticos. Como resultado de la investigación se hizo la valoración de la información obtenida con el personal especializado en TI.

Socialmente, este proyecto permite a la Empresa América Móvil cumplir de manera objetiva a la norma que es exigida por Osiptel, y que le permita garantizar los activos de la información. Además de minimizar y documentar los posibles riesgos o incidentes que puedan atentar contra la seguridad de la información.

Científicamente, este trabajo trata de aportar nuevos conocimientos para el desarrollo de un sistema de gestión de la seguridad de la información en la empresa América Móvil – Chimbote, haciendo uso de la norma ISO 27001 y del PMBOOK, lo cual permite desarrollar la gestión de los activos de la información haciéndolo fácil de usar y auditable en todos sus campos reduciendo así los costos de la empresa.

Con respecto a la problemática, la empresa América Móvil elabora diversos activos de información la cual solamente debe ser usada por los encargados del área responsable. Dichos activos se almacenan y custodian en diferentes medios, de manera física o electrónica. La cual se encuentra disponible para los usuarios y que sirve para la toma de decisiones, generación de reportes, inventarios, estadísticas, entre otros. Pero qué pasa si es que esos activos de información no se utilizan de manera correcta y de acuerdo al objetivo, sino que son utilizados de manera mal intencionada y con otros fines. ¿qué medidas se deben de asumir?.

Ante la problemática encontrada, se formula la siguiente pregunta de investigación:

¿Cómo desarrollar un sistema de gestión de seguridad de la información para la empresa América Móvil?

Sistema de seguridad de la información

De acuerdo con Aguirre (2014), los activos de información son aquellos recursos que tienen cierto valor dentro de una organización. Son necesarios para que una empresa funcione y logre los objetivos trazados.

Los activos de información se clasifican de la siguiente manera:

- Activos de información (datos)
- Documentos (contratos)
- Activos de software (aplicaciones, sistemas)
- Recursos humanos

SEGURIDAD DE INFORMACIÓN

La seguridad de información es el conjunto de medidas preventivas de las empresas que permiten proteger la información.

De acuerdo con Villena (2006) se caracteriza por:

- Confidencialidad, solo es accesible a aquellos que tienen autorización
- Integridad, conserva información exacta durante su procesamiento
- Disponibilidad, asegura el acceso a las personas autorizadas en cualquier momento que sea necesario.

Figura 1: Pilares de la seguridad informática
Fuente: Daniel Sacia

Sistema de gestión de seguridad de información (SGSI)

Villena (2006) sostiene que se refiere a la forma sistemática de administrar la información de una institución para conservarla segura. Un SGSI se compone de personas, equipos informáticos y procesos.

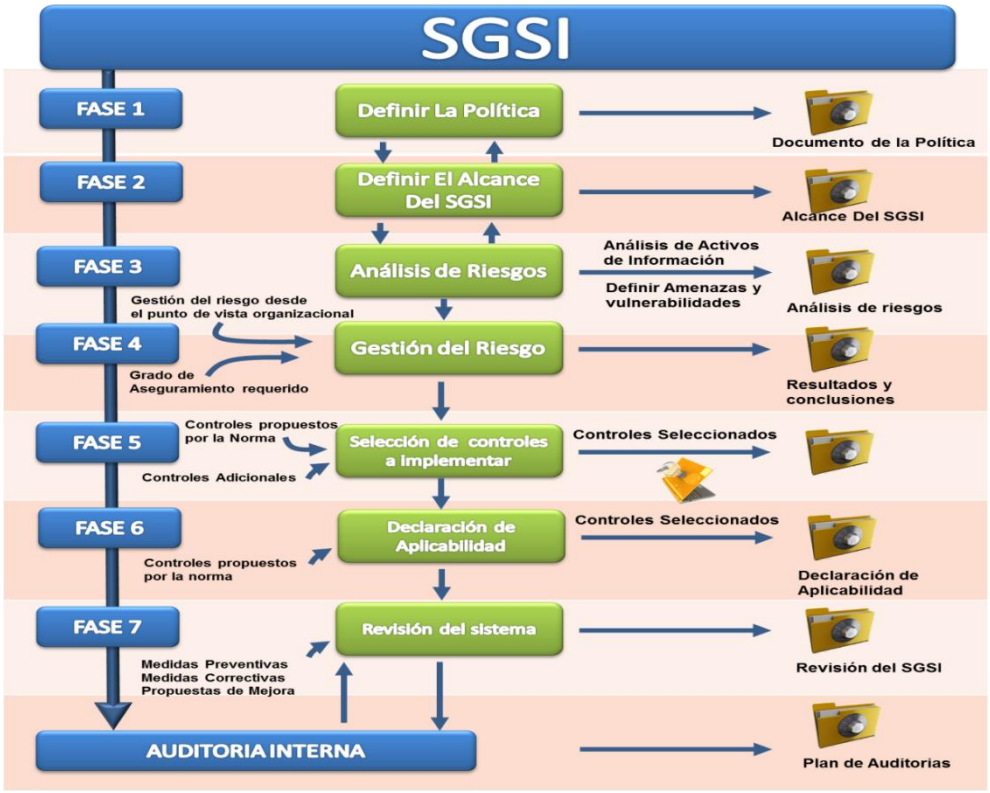


Figura 2: SGSI

Un SGSI sirve para ayudar a tener las políticas claras y procedimientos con relación a los objetivos de la empresa, y con la finalidad de tener un nivel de exposición menor para evitar posibles riesgos.

Figura 3: Riesgos -SGSI
Fuente: Irlenys Tersek

Definición del riesgo

Un riesgo es una amenaza materializada. Mientras más activos sean, más daño hará a la organización.

Además, el riesgo indica lo que podría ocurrir si es que los activos no son protegidos de manera correcta.

Figura 4: Elementos del Riesgo
Fuente: Claudia Villamizar

Identificación de los riesgos:

- Identificar todos los activos con valor para la empresa.
- Se identifican las amenazas más relevantes
- Se identifican las vulnerabilidades
- Se identifica el impacto que tendría la pérdida de integridad y confidencialidad.

Análisis del Riesgo

Se toman en cuenta dos aspectos importantes para analizar el riesgo.

- Probabilidad, consiste en la posibilidad de que un riesgo suceda.
- Impacto, que vienen a ser la consecuencia que puede ocasionar el riesgo.

Evaluación del riesgo

Para evaluar el riesgo se deben comparar los niveles del mismo con los criterios definidos. La finalidad de la evaluación es identificar y evaluar los riesgos.

La evaluación puede llevar también al resultado de no tratar el riesgo.

Tratamiento del riesgo

Conformado por el las decisiones que se toman con cada activo de la información.

En el tratamiento del riesgo se pueden dar las siguientes opciones:

a) *Evitar el riesgo*

b) Aceptar el riesgo

c)Reducir el riesgo

d) Transferir el riesgo

Figura 5:Gestion de Riesgos
Fuente: Secure IT

Tabla 1

Grupo de procesos de gestión de proyectos

Área	Grupos de Procesos de Gestión de Proyectos				
	Inicio	Planificación	Ejecución	Motorización y Control	Cierre
Gestión del proyecto	Se desarrolla el acta de constitución del proyecto	Desarrollo del plan de gestión	Se dirige y ejecuta el proyecto	Supervisar el proyecto Control Integrado de Cambios	Proyecto cerrado
Alcance del proyecto		Planificación del alcance Identificación de los requisitos Se define el alcance Crear EDT		Validación del alcance Control del alcance	
Tiempo del proyecto		Se planifica el cronograma Se definen las actividades Se establecen las secuencias Se estiman los recursos Se estima la duración Desarrollo del cronograma		Control del cronograma	
Costos del proyecto		Se planifica el alcance Requisitos identificados Alcance		Control de Costes	

	Crear EDT			
Calidad del proyecto	Se planifica la gestión de calidad	Asegurar la calidad	Controlar la Calidad	
Gestión del RR.HH. del Proyecto	Planificar la Gestión de Recursos Humanos	Tener los equipos para el proyecto Desarrollar el Equipo del Proyecto Gestión de los equipos		
Gestión de las Comunicaciones del Proyecto	Comunicar	Gestionar	Controlar	

ISO 27001

ISO 27001 es un modelo que comprende un conjunto de lineamientos en donde se especifican los requisitos para establecer, implementar y mejorar un sistema de gestión de seguridad de la información.

Figura 6: ISO 27001

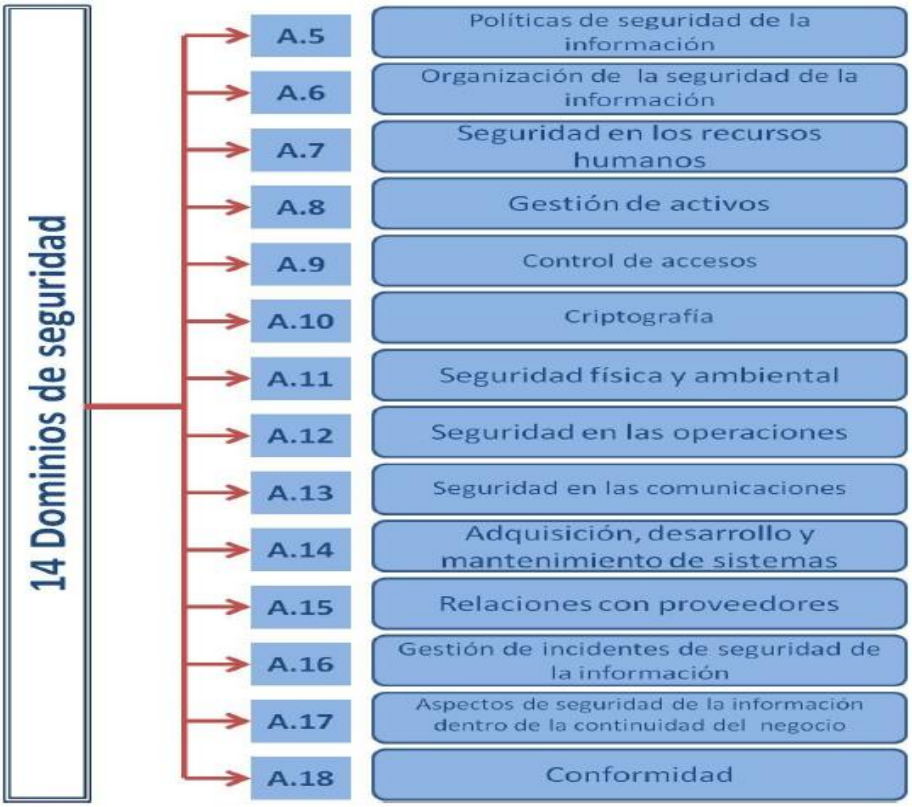


Figura 7: Dominios del ISO 27001

Los objetivos del presente trabajo son:

a) General:

Elaborar un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA AMERICA MOVIL para el área de

b) Específicos:

- Analizar y verificar la situación actual del área de operaciones de la empresa América móvil teniendo en cuenta los antecedentes de violación de los controles del SGSI.
- Elaborar la guía de las buenas prácticas basadas en el PMBOK el cual ayuda a tener documentos como el acta de constitución y la estructura desagregada del trabajo.
- Elaborar la guía de buenas prácticas para la empresa América Móvil, así como seleccionar los controles de Seguridad de Información con la finalidad de cuidar los activos de información.

Metodología

Este trabajo se basó en el tipo descriptivo no experimental, la cual consta en analizar los procesos de gestión de la información de la empresa América Móvil, Chimbote. Y en base a esa investigación elaborar un SGSI gracias a la recolección de la información proveniente de las entrevistas y cuestionarios aplicados.

Mientras que el diseño empleado fue el transversal ya que analiza los datos en un tiempo determinado

Se emplearon las siguientes técnicas e instrumentos de recolección de datos:

Tabla 2
Técnicas, instrumentos, justificación y aplicación

Técnicas	Instrumentos	Justificación	Aplicación
Entrevista presencial	Guía de entrevista a personal especializado.	Permite conocer la situación actual de los procesos y las deficiencias.	Jefe del área de Seguridad Corporativa
Encuestas	Cuestionario	Permite conocer las expectativas de los usuarios sobre el sistema qué cosas se deben de mejorar en base a la seguridad de la información.	Trabajadores del área de Operaciones

Resultados

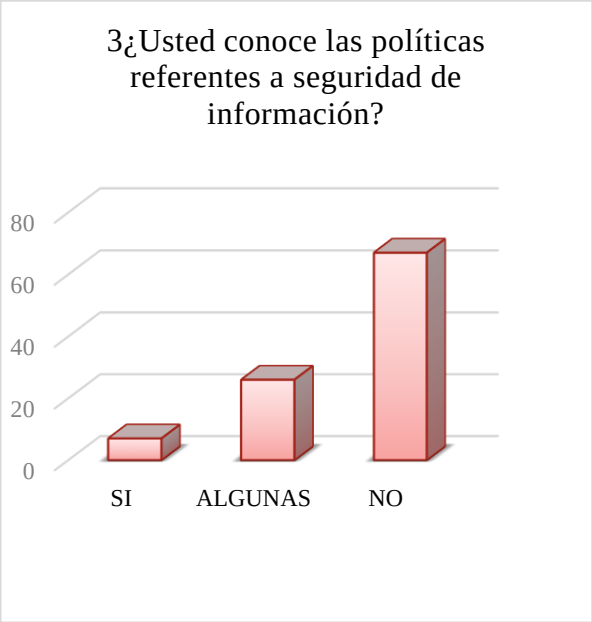
El cuestionario realizado al personal de América Móvil estuvo conformado por 34 ítems. Para el análisis respectivo se tomaron 17 de ellas las cuales se procede a presentar:

Figura 1: Grafico Políticas de Seguridad

Análisis: De acuerdo a la tabla 1, el 77% de los encuestados sostiene que la empresa sí tiene políticas de seguridad de la información, el 13% afirma que no sabe, y el 10% opina que no.

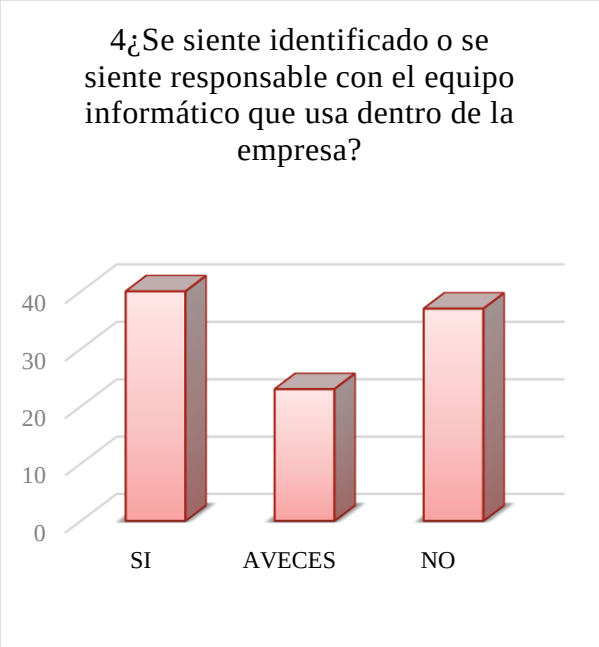
Figura 2: Grafico Practicas de Politicas

Análisis: Según la tabla 2, el 48% de los encuestados afirmó que no se cumplen o se ponen en práctica las políticas de seguridad, mientras que el 30% afirmó que a veces, el 22 sostuvo que sí.



Análisis: De acuerdo a la tabla 3, el 67% de los encuestados afirmó que no conoce las políticas de seguridad de la información, el 26% sostuvo que conoce algunas, y el 7% opinó que sí las conoce.

Figura 3: Grafico conocimiento de Políticas



Análisis: En la tabla 4, el 40% de los encuestados afirmó que sí se siente responsable o se siente identificado con el equipo informático que usa dentro de la empresa, mientras que el 23% afirmó que a veces, y el 37 sostuvo que no se siente responsable o identificado.

Figura 4: Grafico de responsabilidad con el equipo Informático

¿Cuándo se ausenta de su oficina, bloquea su PC?

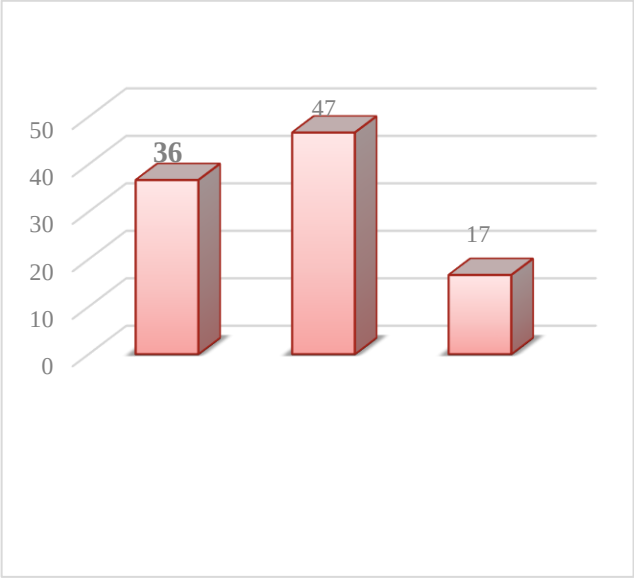


Figura 5: Grafico bloque de PC

Análisis: En la figura se observa que el 36% de los encuestados siempre bloquea su PC cuando se ausente de su oficina, mientras que el 47% lo hace a veces, y el 17% nunca lo hace.

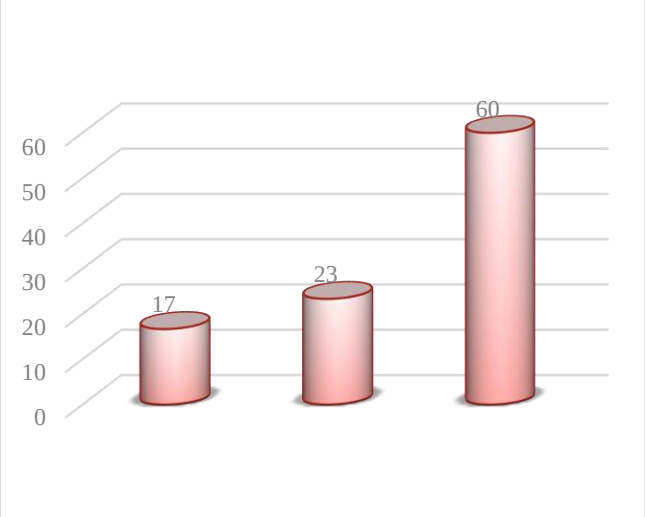


Figura 6: Grafico de Acceso de Almacenamiento

Análisis: En la figura 6 se observa que el 60% de los encuestados afirma que su PC no tiene acceso a los dispositivos de almacenamiento, mientras que el 23% no lo sabe, y el 17% sostiene que sí tiene acceso.

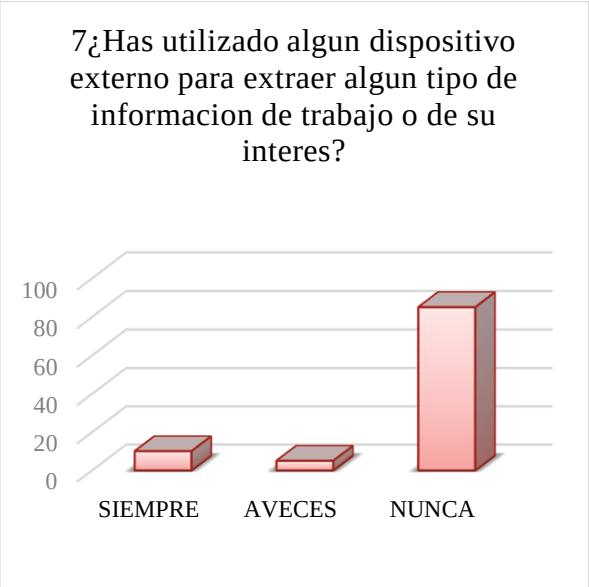


Figura 7: Grafico de uso de Almacenamientos externos

Análisis: De acuerdo a la figura 7, el 85% los encuestados afirmó que nunca ha utilizado algún dispositivo externo para extraer información del trabajo, mientras que el 10% sostuvo que a veces, el 5% afirmó que nunca.

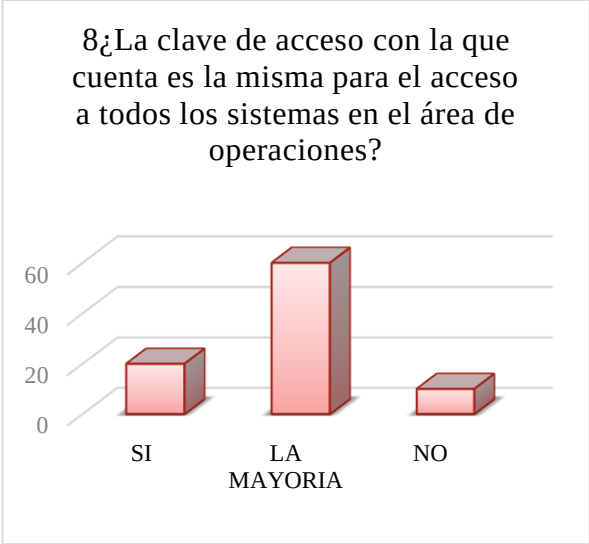


Figura 8: Grafico de Claves de Accesos

Análisis: De acuerdo con la figura 8, el 58% de los encuestados afirmó que en la mayoría de veces la clave es la misma, mientras que el 28% sostuvo que sí es la misma, el 16% afirmó que no es la misma.

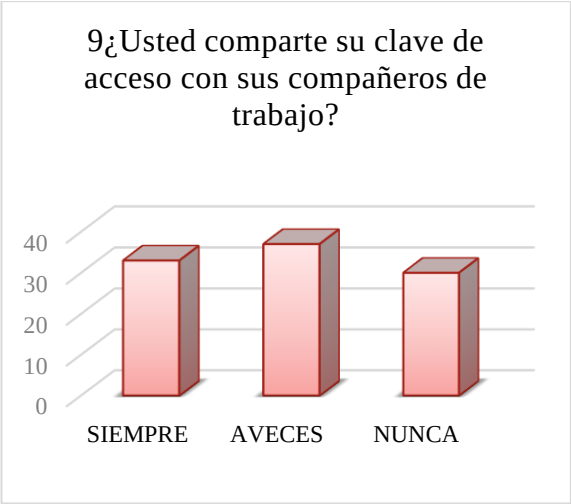


Figura 9: Grafico de compartición de claves

Análisis: De acuerdo a la figura 9, el 37% de los encuestados sostuvo que a veces comparte su clave de acceso con sus compañeros de trabajo, mientras que el 33% afirmó que siempre lo hace, y el 30% opinó que nunca comparte su clave de acceso.

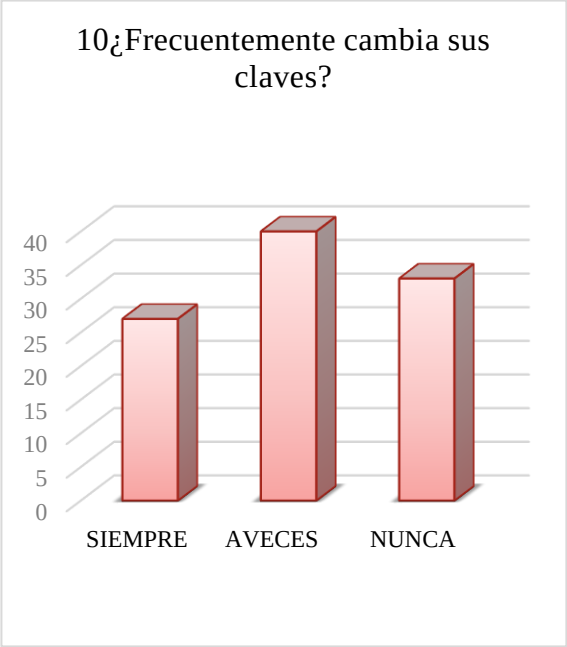


Figura 10: Grafico de Cambio de Claves

Análisis: De la figuras 10 se pude deducir que el 40% de los encuestados sostiene que a veces cambia con frecuencia sus claves de acceso a los sistemas, mientras que el 33% sostuvo que nunca las cambia, el 27% afirmó que siempre las cambia.

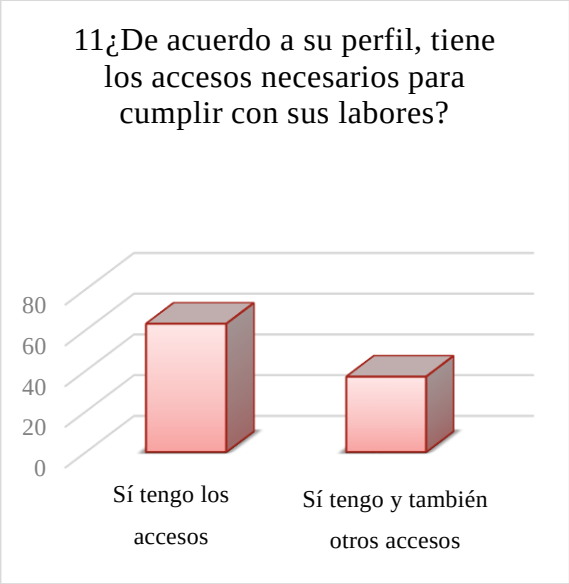


Figura 11: Grafico de Accesos Asignados

Análisis: En la figura 11 se puede observar que el 63% de los encuestados afirmó que sí cuenta con todos los accesos para realizar sus labores, mientras que el 37% restante afirmó que también tiene los accesos necesarios y que también tiene otros accesos que no corresponden a su perfil.

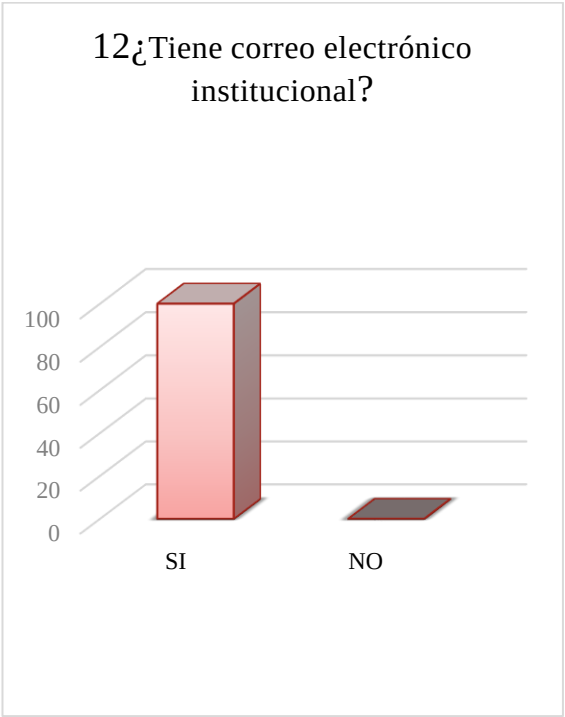
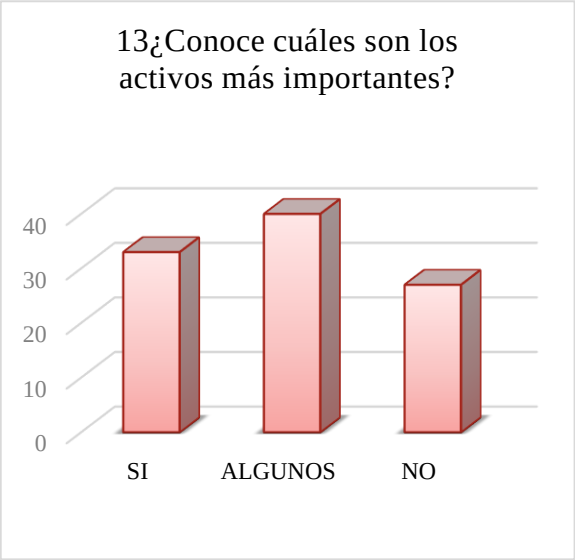


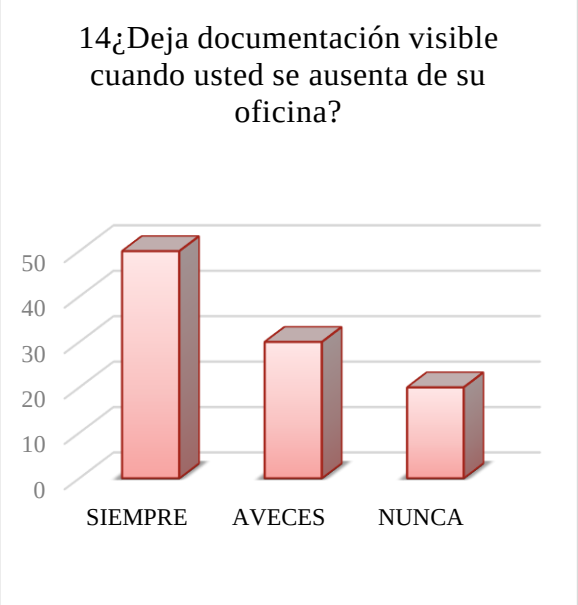
Figura 12: Cuenta de Correo Electrónico

Análisis : En la figura 12 se puede observar que el 95% de los encuestados afirmó que sí tiene correo institucional, mientras que el 5% restante sostuvo que no tiene.



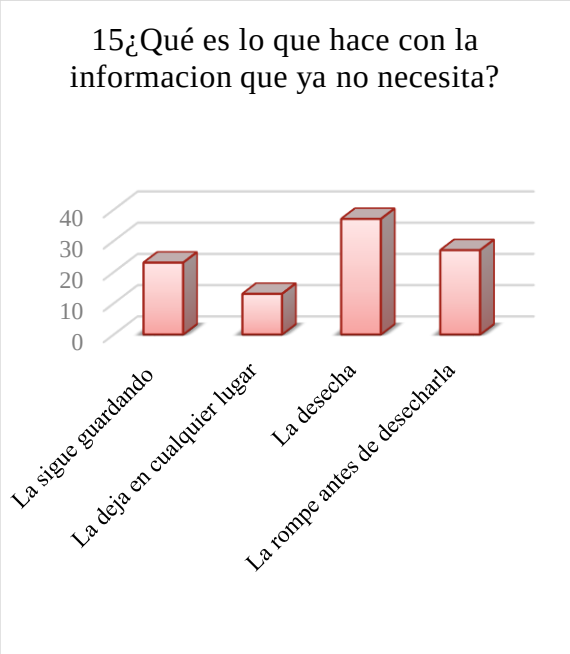
Análisis: En la figura 13 se observa que el 40% de los encuestados afirmó que conoce algunos de los activos más importantes de la empresa dentro del área de operaciones, mientras que el 33% afirmó que sí los conoce, el 27% sostuvo que no los conoce.

Figura 13: Grafico de Conocimiento de Activos



Análisis: En la figura 14 se observa que el 50% de los encuestados sostuvo que siempre deja documentación visible cada vez que se ausenta de su oficina, mientras que el 30% afirmó que a veces lo hace, y el 20% sostuvo que nunca deja documentación visible.

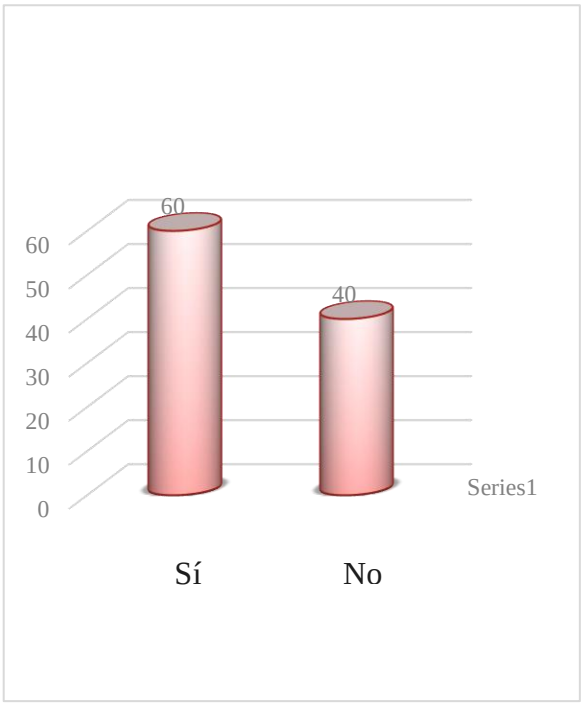
Figura 14: Grafico de Documentos Visibles



Análisis: En la figura 15 se observa que el 37% de los encuestados afirmó que el desecha la información que ya no necesita, mientras que el 27% sostuvo que la rompe antes de desecharla, el 23% opinó que la sigue guardando, y el 13% sostuvo que la deja en cualquier lugar.

Figura 15: Grafico de la Información Innecesaria

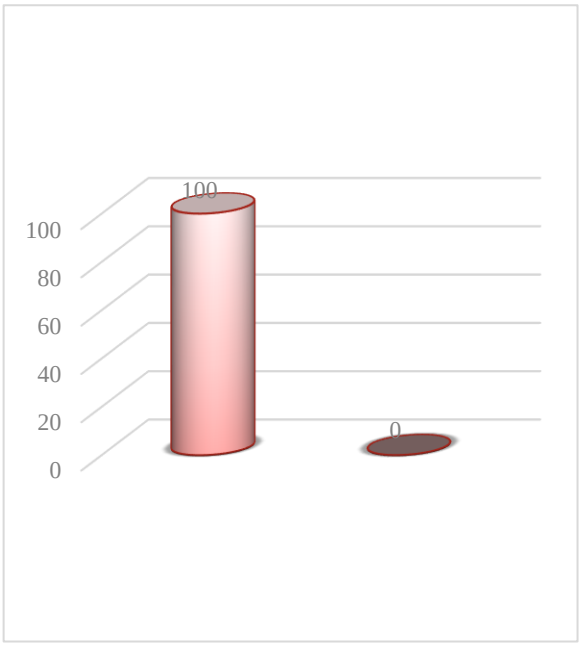
¿Sabe usted diferenciar la información confidencial, interna o pública?



Análisis: En la figura 16 se aprecia que el 60% de los encuestados sostuvo que sí sabe diferenciar entre la información confidencial, interna o pública. Mientras que el 40% restante afirmó que no sabe diferenciar.

Figura 16: Grafico de Información Confidencial

¿Le gustaría conocer un poco más sobre la seguridad de la información?



Análisis: En la figura 17 se observa que el 100% de los encuestados sostuvo que sí le gustaría conocer un poco más sobre la seguridad de la información.

Figura 17: Grafico de Interés de la Seguridad de la Información

Tabla 3

Acta de constitución del proyecto					
PROYECTO	Sistema de Gestión de Seguridad de la Información de la empresa América Móvil				
PATROCINADOR	Gerencia Central				
PREPARADO POR:	Ingrid Melissa Cherres Odar	FECHA	23	04	2017
REVISADO POR:	Maycol Rodriguez Ynguil				
APROBADO POR:	Gerencia Central				

REVISIÓN (Correlativo)	Realizada por: (Motivo y quién lo revisó)	FECHA 04 10 2017
01		
02		

	Descripción del proyecto
	El proyecto denominado "Sistema de gestión de seguridad de la información para la Empresa América Móvil", tendrá la capacidad de proteger los activos de la información de la empresa, llegando así a cumplir los objetivos y reducir los posibles riesgos. Se utilizará lo siguiente: • Políticas de seguridad • Inventarios • Análisis de los riesgos • Gestión de los riesgos • Tratamiento de riesgos • Aplicabilidad

ALINEAMIENTO DEL PROYECTO	
1. OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN (En cuál objetivo estratégico está alineado el proyecto)	**2. PROPÓSITO DEL PROYECTO** Una vez entregado el proyecto, este brindará beneficios a la organización.
El objetivo del negocio de América Móvil es generar el mayor bienestar y desarrollo personal y profesional de nuestros trabajadores, proporcionar bienestar y desarrollo a la comunidad y exceder los objetivos financieros y de crecimiento de nuestros accionistas.	Orientar a la institución a tener el acceso controlado e integro de su información, estableciendo diversos mecanismos de control para identificar los riesgos informáticos y financieros basados en el ISO 27001.

3. **OBJETIVOS**

- Alcance: El presente proyecto sugiere la implementación de un sistema de gestión de seguridad de la información en el área de Operaciones de América Móvil.
- Tiempo: El tiempo estimado es de 5 meses para la culminación del proyecto.
- Costos: Aproximadamente S/. 25,000.00, incluyendo la consultoría.
- Calidad: Se debe tener personal debidamente capacitado en temas de seguridad de la información.
- Elaborar el marco de referencia que garantice todos los elementos del SGSI.
- Se deben de establecer expectativas con la gerencia.
- Se debe de difundir conciencia en todo el personal de la empresa sobre la seguridad de la información, sus compromisos y responsabilidades.

4. FACTORES DE ÉXITO DEL PROYECTO

- Contar con el recurso humano debidamente capacitado en proyectos similares.
- Buena comunicación por parte de todos los actores involucrados.
- Aceptar los resultados de parte del personal.

5. REQUISITOS DE ALTO NIVEL

- Aprobar el acta de constitución del proyecto.
- Elaborar el acta de constitución del proyecto
- Cumplir con la norma ISO 27001.
- Tener al personal debidamente capacitado en el tema
- Tener los documentos de los inventarios de los activos de la información.
- Tener el documento de las políticas de seguridad de la información de la empresa.
- Tener los resultados de las entrevistas al personal y a los usuarios.
- Tener el documento de la declaratoria de aplicación del proyecto.

ALCANCE DEL PROYECTO	
6. FASES DEL PROYECTO	**7. PRINCIPALES ENTREGABLES** Producto que tenga la capacidad de realizar un servicio que debe ser elaborado con la finalidad de completar un proceso o proyecto.
El proyecto está conformado por las fases establecidas en la norma ISO 27001. Inicio	• Acta de constitución del proyecto en mención • Norma ISO 27001 • Objetivos del sistema de gestión de seguridad de la información.
Planificación	• Desarrollo del plan de gestión • Planificar la gestión de los riesgos • Identificación de los riesgos • Hacer el análisis correspondiente • Hacer el análisis cualitativo de los riesgos • Planificación de la respuesta a los riesgos • Análisis situacional de la empresa • Objetivos y metas de la empresa • Análisis de las políticas de seguridad de la información • Análisis de la norma ISO 27001
Ejecución	• Análisis de los riesgos • Identificación de las amenazas • Valoración de los activos • Tratamientos de los riesgos
Seguimiento del proyecto	• Se declara su implementación.
Cierre del proyecto	• Presentación del informe final.

INTERESADOS CLAVES

- Junta de Accionistas
- Directorio de la empresa
- Gerencia General
- Gerencia de Riesgos
- Asesoría Legal
- Área de Imagen
- Área de Recursos Humanos
- Área de T.I.
- Área de Operaciones
- Área de Seguridad
- Unidades de Negocios de Empresa, Personas y Servicios
- Personal de la empresa
- Usuarios

RIESGOS

- Personal poco comprometido.
- Demora en la ejecución de las fases del proyecto
- No hay financiamiento.
- No se cumplen con los plazos de entrega
- Poco personal capacitado

HITOS PRINCIPALES DEL PROYECTO

- El proyecto es aprobado por la Gerencia General
- Se desarrollan las entrevistas al personal encargado y usuarios
- Se verifican que los procesos se realicen dentro de los plazos establecidos
- Se lleva a cabo el inventario de los activos.
- Se entrega el producto dentro del plazo determinado o antes.

PRESUPUESTO DEL PROYECTO		
REQUISITOS DE APROBACIÓN DEL PROYECTO		
FCE	Evaluador Ing Miguel Valle Pelaez	Firma el Cierre del Proyecto Maykol Rodriguez Unguil
• Se asigna al personal capacitado para llevar a cabo los proyectos de automatización de ERP	Jefe de Recursos Humanos.	Gerencia Central
• El personal debe estar a disposición e involucrado totalmente con el proyecto.	Responsables de áreas.	
• El área de operaciones acepta el proyecto.	Supervisor de Operaciones	
• Se entregan los documentos dentro de los plazos.	Gerente del Proyecto Cherres Odar Ingrid Melissa	
GERENTE DE PROYECTO ASIGNADO Ingrid Melissa Cherres Odar		
AUTORIDAD ASIGNADA Maykol Rodriguez Unguil		
Jefe de Operaciones		

DISEÑO METODOLÓGICO DEL ISO 27001

El presente trabajo de investigación está desarrollado bajo la norma ISO 27001. Y sus alcances son los siguientes:

Tabla 4
Fases y consideración.

Fases	Consideración
Norma ISO 27001	• La norma y sus características • Objetivos del sistema de gestión
Análisis de la Empresa	• Descripción del negocio • Objetivos • Alcance • Infraestructura de la seguridad • Políticas relacionadas a la seguridad de la información ○ Personal responsable ○ Manejo de los activos ○ Criptografía ○ Seguridad de las operaciones y comunicaciones ○ Control y monitoreo de los sistemas ○ Comunicación con los proveedores ○ Cumplimiento de plazos
Análisis de Riesgos	• Procedimientos de la empresa • Inventarios de todos los activos • Valoración • Identificar las amenazas • Manejo de riesgos
Aplicabilidad	• Aplicación de los controles

ANÁLISIS DE LA EMPRESA

América Móvil S.A.C es una empresa líder en servicios integrados de telecomunicaciones en Latinoamérica. El despliegue de su plataforma de comunicaciones es de clase mundial que le permite ofrecer a sus clientes un

portafolio de servicios de valor agregado y soluciones de comunicación mejoradas en 25 países de América y Europa, al 30 de junio de 2017, la compañía contaba con 362.6 millones de líneas de acceso, que incluyen 280.0 millones de suscriptores móviles, 33.3 millones de líneas fijas, 27.5 millones de accesos de banda ancha y 21.8 millones de unidades de TV de paga. En América Latina, América Móvil opera bajo las marcas: Telmex, Telcel y Claro.

La Oficina Principal a nivel nacional de América Móvil, se encuentra ubicada en Av. Nicolás Arriola Nro. 480 La Victoria Lima, Perú.

En la actualidad, cuenta con aproximadamente 3500 trabajadores en todo el país.

Visión: Ser la empresa líder en telecomunicaciones en el Perú.

Misión: Proveer servicios de telecomunicaciones con la más alta calidad, más amplia cobertura y constante innovación para anticiparnos a las necesidades de comunicación de nuestros clientes; generar el mayor bienestar y desarrollo personal y profesional de nuestros trabajadores, proporcionar bienestar y desarrollo a la comunidad y exceder los objetivos financieros y de crecimiento de nuestros accionistas.

Objetivo: Generar el mayor bienestar y desarrollo personal y profesional de nuestros trabajadores, proporcionar bienestar y desarrollo a la comunidad y exceder los objetivos financieros y de crecimiento de nuestros accionistas.

Organigrama de América Móvil

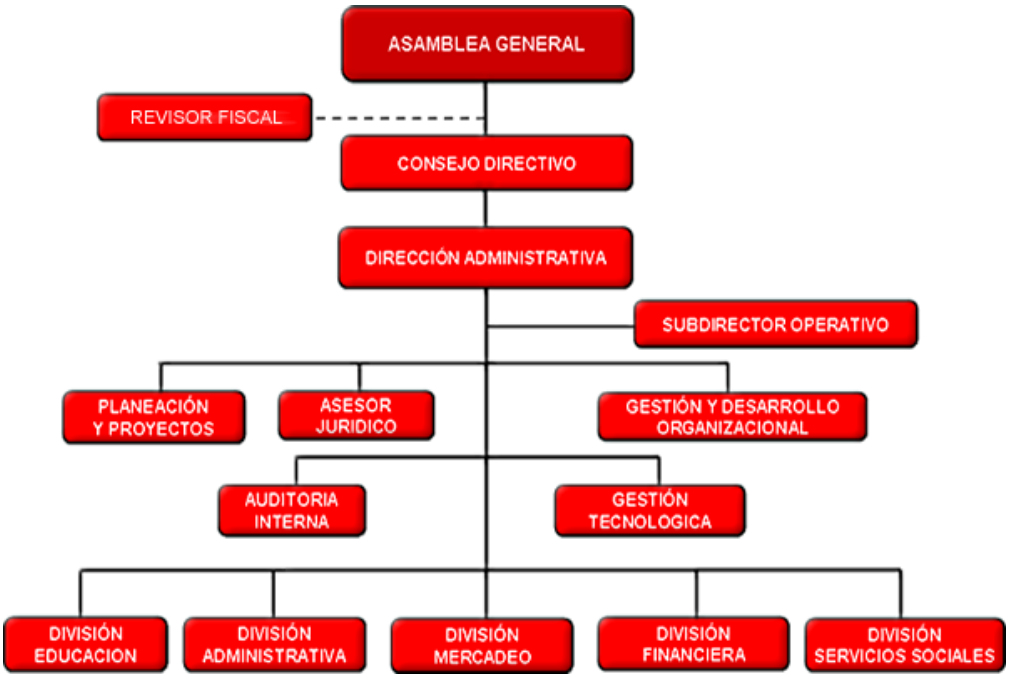


Figura 8: Organigrama de America Movil
Fuente: America Movil

PLAN DE LA GESTIÓN DEL PROYECTO

Tabla 5
Proyecto

Nombre del Proyecto	Siglas del Proyecto

SISTEMA DE GESTION DE SEGURIDAD de la empresa América Móvil	sist_ges_segur_inf_AMERMOV

Procesos:				
ENTRAGABLES	**ENTRADAS**	**MODO DE TRABAJO**	**SALIDAS**	**HERRAMIENTAS Y TÉCNICAS**
Proyect Charter	Acuerdos, Enunciado del Trabajo	Mediante reunión entre el Director de proyecto y el cliente	Contrato	Juicio de Expertos
Cronograma	Lista de Actividades	Reunión del equipo , estimación de la duración de las actividades	Calendario del Proyecto	Ruta crítica
Plan de dirección del Proyecto	Acta de Constitución del proyecto	Reuniones del equipo de proyecto	Plan de dirección del Proyecto Aprobado	Juicio de Expertos
Acta de Comité de Sistemas	Plan de Gestión de Comunicacion es		Actualización documentos	Reuniones
Acta de Reuniones de Trabajo	Plan de Gestión de Comunicacion es	Reuniones formales e informales , distribución documentación	Actualización documentos	Reuniones
Desempeño	Cronograma		Actualización documentos	Excel
Plan de Pruebas	Plan de gestión de Calidad		Solicitudes de cambio	
Informe de Cierre	Plan de Gestión de Comunicacion		Actualización documentos	Formato Excel

	es		
Acta de Cierre	Plan de Gestión de Comunicaciones	Actualización documentos	Reuniones

Metodología de trabajo
• Se define el alcance del proyecto • Se reúnen los documentos. • Se definen los roles y responsabilidad • Se define la fecha de entrega • Reuniones constantes para verificar el estado del proyecto • Cuando el proyecto es entregado se redactan los documentos correspondientes.
Control de Cambios:
Aprobador de cambios: ▪ Autorización de las solicitudes de cambio. ▪ El cambio es autorizado.
Proveedor de Cambios: ▪ Requiere cambios previamente acordados ▪ Requiere de nuevos requerimientos. ▪ Resuelve las consultas sobre los cambios y requerimientos.
Comunicación entre Stakeholders:
COMUNICACIÓN ENTRE LOS STAKEHOLDERS — Técnicas de comunicación a utilizar

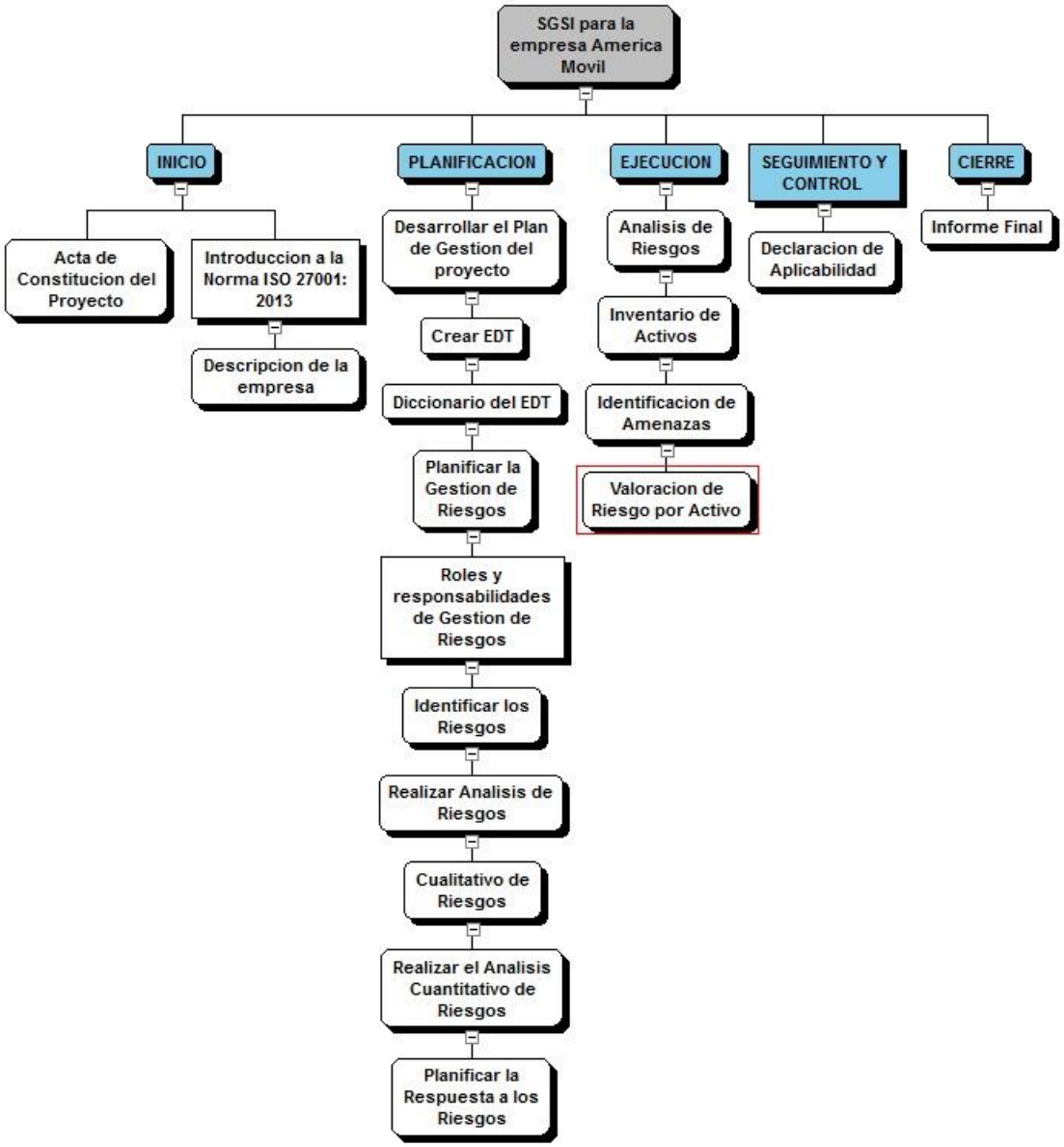
Actas de Comité	Correo Electrónico
Reuniones	Correo Electrónico
Actas de la reunión	Agenda de Reunión
Cronograma del avance	Correo Electrónico

CICLO DE VIDA DEL PROYECTO		**MULTIFASES**	
FASE	Entregable principal de la fase	Consideraciones a tener en cuenta para iniciar esta fase	Consideraciones a tener en cuenta para cerrar esta fase
Inicio	Project charter	Se acepta el Project charter	Se acepta el Project charter
Control y monitoreo	Reportes e informes	Cronogramas	Reportes semanales sobre el avance
Ejecución	Pruebas diversas	Planes de gestión	Se aceptan las pruebas
Cierre	Reporte del cierre	Se acepta el entregable	Fin del proyecto

Revisiones de Gestión:			
TIPO	**CONTENIDO**	**EXTENSIÓN O ALCANCE**	**OPORTUNIDAD**

De avance	Revisiones de avance y desarrollo del cronograma.	Se finaliza con acta de reunión firmada por los asistentes.	Quincenal Regular
De control	Revisiones de indicadores y las mediciones de desempeño y calidad del producto.	Se finaliza con informe interno para monitorear los avances.	Semanal Regular.
Extraordinaria	Problemas generados por riesgos y nuevos requerimientos.	Se desarrolla de manera exclusiva y se redacta un acta con el nuevo cronograma establecido.	En caso de alto riego o cuando se presente problemas.

Estructura detallada de trabajo (EDT)



DICCIONARIO DEL EDT

Tabla 6

Nombre del Proyecto:	**Sistema de Gestión de Seguridad de la Información de la Empresa América Móvil**				
Preparado por:	Ingrid Melissa Cherres Odar		Fecha de Preparación:	23-04-17	
Revisado por:	Raymundo Almika Reyes		Fecha Modific:	05-10-17	
Autorizado por:	Maykol Rodriguez Unguil				
Instrumentos	Encuestas,Entrevistas				
Información	Resultados				
Alcance del proyecto	Analizar los posibles riesgos.				
Responsable	Maykol Rodriguez Unguil				
Tiempo aproximado	150 días	Inicio:	23 Abril	Final:	23 Septiembre
Requisitos de calidad	Analizar los posibles riesgos. Descripción Procesos de los negocios				
Otras referencias					
Hitos del cronograma	Costos				

PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

Tabla 7

Nombre	Siglas del Proyecto
SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA EMPRESA AMERICA MOVIL	sist_ges_segur_inf_AMERMOV

Equipo responsable:

Está compuesto por el director del proyecto, el analista de sistemas y los programadores.

Se realizan talleres con la finalidad de:

- Identificar los posibles riesgos.
- Controlar la respuesta a los riesgos.

Tabla 8

Matriz de impacto y probabilidades

PROBABILIDADES		MUY BAJO	BAJO	MODERADO	ALTO	MUY ALTO
		0.1	**0.2**	**0.4**	**0.6**	**0.9**
MUY ALTO	**9**	0.9	1.8	3.6	5.4	8.1
ALTO	**7**	0.7	1.4	2.8	4.2	6.3
REGULAR	**5**	0.5	1	2.0	3.0	6.3
BAJO	**3**	0.3	0.6	1.2	1.8	2.7
MUY BAJO	**1**	0.1	0.2	0.4	0.6	0.9

	RANGO	**NIVEL**
	8.1 - 2.9.	ALTO
	2.8 - 1.4	MODERADO
	1.3 - 0.1	BAJO

Tabla 9

Roles y responsabilidades de gestión de riesgos

PROCESO	**ROLES**	**PERSONAS**	**RESPONSABILIDADES**
11.1. Planificar la gestión de riesgos	1. Establecer los planes para gestionar los riesgos. 2. Elaborar los elementos de costos para incluirlos en el presupuesto. 3. Revisión de la metodología de trabajo para contener los riesgos.	Equipo de gestión.	1. Gerente de Proyecto 2. Equipo
11.2. Identificar los riesgos	1. Todo el equipo del proyecto debe de identificar los riesgos.	Gerente de Proyecto	1. Gerente de Proyecto
11.3. Realizar el análisis cualitativo de riesgos	1. Evaluar la prioridad de los riesgos mediante la ocurrencia. 2. Evaluar la prioridad de los riesgos sobre los objetivos del proyecto 3. Evaluar la prioridad de los riesgos mediante el plazo de respuesta.	Equipo de gestión.	1. Equipo 2. Gerente de Proyecto
11.4. Planificar la respuesta a los riesgos	1. Asignar a un responsable para dar respuesta a los riesgos. 2. Brindar recursos en el presupuesto de acuerdo al cronograma del proyecto.	Equipo de gestión.	1. Gerente de Proyecto 2. Equipo

11.5. Monitorear y controlar los riesgos	1. Implementar planes de respuesta a los riesgos 2. Rastrear los riesgos identificados 3. Controlar los riesgos 4. Identificar si hay nuevos riesgos. 5. Evaluar qué tan efectivo son los procesos contra los riesgos.	Gerente de Proyecto Equipo de gestión Supervisor	1. Supervisores 2. Equipo 3. Equipo y supervisores 4. Gerente de Proyecto

PERIODICIDAD DE LA GESTIÓN DE RIESGOS			
PROCESO	**MOMENTO DE EJECUCIÓN**	**ENTREGABLE DEL EDT**	**PERIODICIDAD DE EJECUCIÓN**
Planificación de la gestión de los riesgos	Planificación		Mensual
Identificación de los riesgos	Planificación		Semanal
Realizar el análisis cualitativo de riesgos	Planificación		Semanal
Respuesta a los riesgos	Planificación		Semanal
Monitorear y controlar los riesgos	Seguimiento y control		Diario

Tabla 10

Identificación, evaluación plan de respuesta a riesgos

	RIESGO	DESCRIPCIÓN	CAUSA RAIZ	TRIGGER	ENTREG. AFECTADOS	TIPO DE RIEZGO	ESTRATEGIA	RESPONSABLE
R01	Errores en la estimación del presupuesto	No se conocen bien los procesos o tareas a realizarse, lo que ocasiona que no se haya hecho una estimación adecuada	Mal gestión del conocimiento del equipo del proyecto.	Comunicación del cliente o detección de error.	Correspondiente a criterio modificado.	Muy Alta	Adecuado seguimiento y control a información de entrada.	DP, CP.
R02	Cambios en las políticas de gestión	Cambio en información de entrada.	Externo	Comunicación del cliente o detección de error.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a información de entrada.	DP, EP.
R03	Seguridad del software	Cambio en información de entrada. Asignación de tareas a recurso inadecuado que requiere capacitación.	Interno	Consumo de tiempo mayor al programado.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a criterios de diseño.	DP, CP,EP.
R04	Cambios de alcance	Detección de errores en el proceso de revisión.	Externo	Nueva información de entrada, recibida del cliente.	Correspondiente a criterio modificado.	Muy Alta	Adecuado seguimiento y control a información de entrada.	DP, CP.
R05	Desconocimiento del flujo de procesos del cliente	Detección de errores en el proceso de revisión.		Comunicación del cliente o detección de error.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a criterios de diseño.	DP

R06	Desconocimiento de la tecnología usada	Detección de errores en el proceso de revisión.	Externo	Consumo de tiempo mayor al programado.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento a consumo de recursos y llamado de atención oportuno al jefe de diseños.	DP, CP, EP
R07	Las pruebas de funcionamiento no resultan satisfactorias	Asignación de tareas a recurso inadecuado que requiere capacitación.	Interno	Consumo de tiempo mayor al programado.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a criterios de diseño.	DP, EP.

ANÁLISIS DE RIESGOS

Tabla 11
Área de Operaciones

Área de Operaciones	Descripción
Líneas Móviles	▪ Se ingresan los clientes nuevos (Portabilidad o Altas nuevas) ▪ Consulta de Bolsa / Consumo y Saldos. ▪ Cambio de Tope de consumo ▪ Financiamientos de deudas y reintegro de equipo ▪ Renovaciones ▪ Cambio de Plan ▪ Migraciones ▪ Cancelaciones de líneas ▪ Reconocimiento y Desconocimiento de Líneas.
Evaluación Segmento Masivo	▪ Aprobación y Rechazo de Evaluaciones. ▪ Evaluación condicionada a Rentas Adelantadas ▪ Evaluación para cambio de Titularidad de Línea ▪ Evaluación de Clientes Corporativos (Empresas)
Servicio Técnico	▪ Orden de Servicio Técnico ▪ DOA: Se cambia el equipo por fallas constantes. ▪ Servicio Técnico sin orden
Reclamos	▪ Libro de Reclamaciones. ▪ Reclamos: Contratación no solicitada, calidad e Idoneidad, Facturación.
Portal de conocimiento	▪ Claro global ▪ SUIC- Portal de Conocimiento

INVENTARIO DE ACTIVOS

Tabla 12
Inventario de Activos

Aplicaciones	Office 2016, Adobe Acrobat Reader	Aplicaciones	Servidor	Soporte y T.I
S.O.	Windows 8	Software	Servidor	Soporte y T.I
Dispositivos de Almacenamiento	Dvd, discos duros externos,usb.	Dispositivos	Operaciones	Operaciones
Aplicaciones desarrolladas	Siac Pospagp, Siac Prepago, Sistema de Activaciones, SGA, Sistema de Activacione Prepago, Nintex, SistTec, SisCa	Aplicaciones	Servidor	Soporte y T.I
Equipos de Usuario	Impresoras, Scanners, Etiketera,Biometrico,POS	Hardware	Operaciones	Soporte y T.I
Clientes	Datos de Clientes.	Datos	Servidor	Operaciones
Trabajador	Personal de la empresa	Personal	Operaciones	RR.HH
Documentos de clientes	Carpetas Clientes, Contratos de altas, renovaciones, portabilidad, migraciones prepago a postpago, Reposición	Documentos		Usuario asignado.
Reporte de Operaciones	Reportes de Operaciones. Variaciones de Transacciones por línea	Documentos		Usuario asignado.

IDENTIFICACION DE AMENAZAS

En esta sección se identifican las amenazas que puedan dañar a los activos. La amenaza viene a ser un acontecimiento que atente contra la seguridad. Por ejemplo:

- Amenazas naturales: terremotos, tsunamis, inundaciones, huracanes, incendios, etc.
- Amenazas a las instalaciones: incendio, explosiones, falta de energía y fallas mecánicas.
- Amenazas humanas: epidemias, problemas en el transporte, pérdida de personal importante.
- Amenazas tecnológicas: virus, hacking, fallas en las líneas de comunicación.
- Amenazas sociales: huelgas, terrorismo, vandalismo.

DIAGRAMA DE ISHIKAWA : AMENAZAS NATURALES

DIAGRAMA DE ISHIKAWA: AMENAZAS TECNOLOGICAS

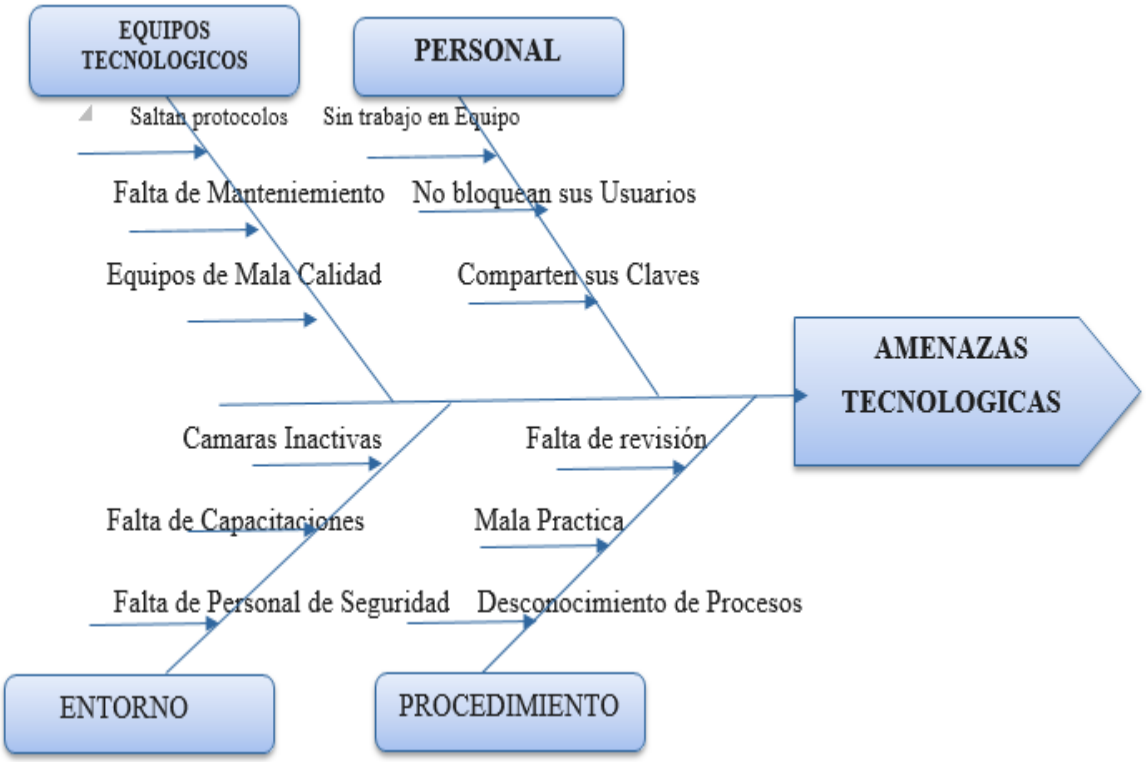
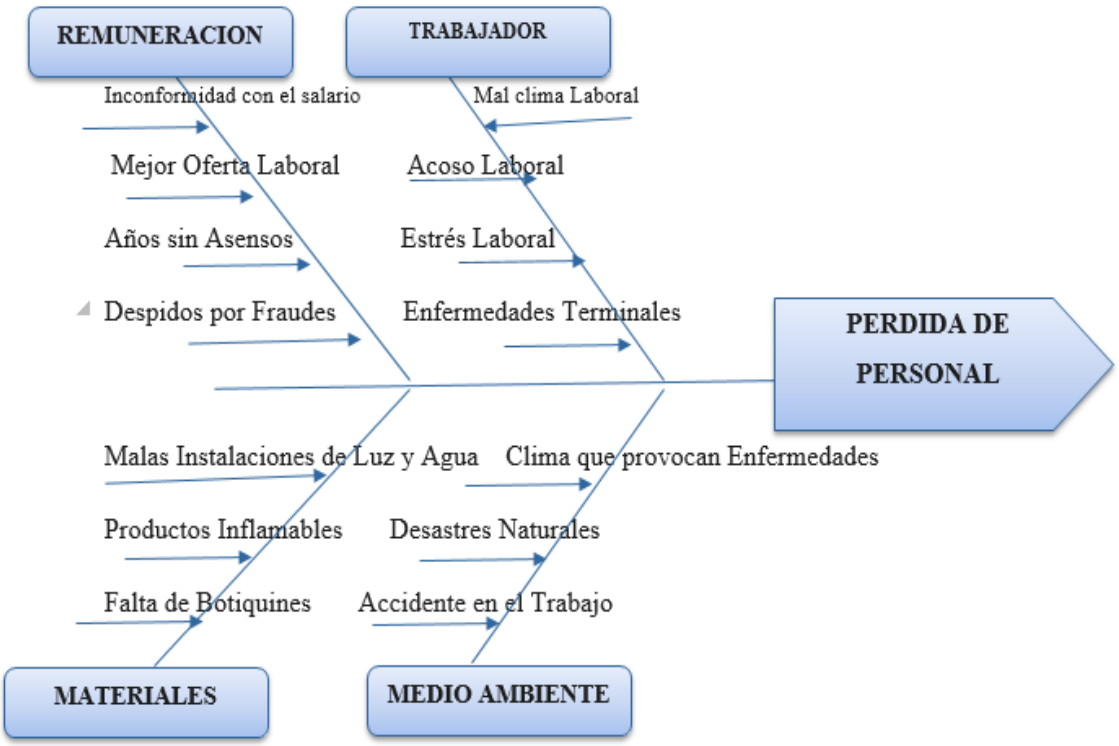


DIAGRAMA DE ISHIKAWA : AMENAZA DE PÉRDIDA DE PERSONAL



VALORIZACIÓN DE ACTIVOS

Tabla 13
Valoración de Activos

Aplicaciones	3	2	2	7
S.O.	4	3	3	10
Dispositivos de Almacenamiento	6	3	2	11
Sistemas desarrollados	4	3	3	10
Equipos	3	4	2	9
Clientes	5	5	3	13
Trabajador	3	4	2	9
Documentos – Cliente	3	3	5	11
Reportes	4	3	3	11
Correo Electrónico	2	4	3	9
Servicios	3	3	5	11

VALORACIÓN DE RIESGO POR ACTIVO

Tabla 14
Riesgo por activo

Naturales	5	2	2	7
Humanas	5	2	2	7
Instalaciones	6	2	2	24
Tecnológicas	6	3	2	36
Operacionales (errores usuario)	6	3	2	14

Tabla 15
Sistemas Operativos

Naturales	9	2	1	18
Humanas	9	1	1	9
Instalaciones	9	2	2	36
Tecnológicas	9	3	2	54
Operacionales	9	3	2	19

Tabla 16

Dispositivos de Almacenamiento

Naturales	11	1	0	0
Humanas	11	1	0	0
Instalaciones	11	1	1	11
Tecnológicas	11	2	3	66
Operacionales	11	3	3	46

Tabla 17

Sistemas Desarrollados

Naturales	11	2	2	44
Humanas	11	3	1	33
Instalaciones	11	3	2	66
Tecnológicas	11	3	2	66
Operacionales	11	3	3	45

Tabla 18
Equipo de Usuario

Naturales	9	2	1	18
Humanas	9	1	0	0
Instalaciones	9	2	1	18
Tecnológicas	9	2	3	54
Operacionales	9	2	2	36

Tabla 19
Cliente (Datos)

Naturales	12	2	1	24
Humanas	12	3	2	72
Instalaciones	12	3	2	26
Tecnológicas	11	3	2	26
Operacionales (errores usuario)	14	4	3	74

Tabla 20
Trabajador

Naturales	9	3	2	18
Humanas	8	1	1	8
Instalaciones	8	1	0	0
Tecnológicas	8	0	0	0
Operacionales (errores usuario)	8	4	3	49

Tabla 21
Carpetas - Clientes

Naturales	12	3	1	36
Humanas	12	2	1	24
Instalaciones	12	2	1	24
Tecnológicas	12	1	1	9
Operacionales	12	4	3	73

Tabla 22
Reporte de Operaciones

Naturales	11	3	1	33
Humanas	11	2	1	22
Instalaciones	11	2	1	22
Tecnológicas	11	1	1	11
Operacionales	11	3	2	66

Tabla 23
Correo Electrónico

Naturales	8	2	0	0
Humanas	8	3	2	48
Instalaciones	8	1	1	8
Tecnológicas	8	3	2	32
Operacionales	8	3	1	18

Tabla 24
Servicios

Naturales	10	2	1	20
Humanas	10	1	1	10
Instalaciones	10	3	2	60
Tecnológicas	10	1	1	10
Operacionales	10	2	2	13

Tratamiento del riesgo

En este caso, para determinar el tratamiento del riesgo, el valor aceptable se establece en 50. Por lo tanto, si se supera o se iguala esa cifra se aplicarán diversos procedimientos.

Tabla 25
Tratamiento de Riesgo

Activos	Riesgo	Tratamiento
Aplicaciones	38	Asumir riesgo
S.O.	52	Asumir riesgo
Dispositivos de Almacenamiento.	64	Asumir riesgo
Sistemas desarrollados	64	Asumir riesgo
Equipos de Usuario	56	Asumir riesgo
Clientes	72	Asumir riesgo
Trabajador	48	Asumir riesgo
Documentos – Cliente	74	Asumir riesgo
Reportes	62	Asumir riesgo
Correo Electrónico	45	Asumir riesgo
Servicios	62	Asumir riesgo

Tabla 26

Aplicabilidad

OBJETIVOS DE CONTROL		CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	POLÍTICAS DE SEGURIDAD	1	APLICAR	Se necesita tener las políticas de seguridad debidamente establecidas para poder definir así a los responsables del proyecto y el sistema a implementar. Los directivos de la empresa deben de brindar el apoyo respectivo. Luego de adoptar las políticas de seguridad de la información estas deberán ser remitidas a todas las partes interesadas.
	REVISAR LAS POLÍTICAS DE SEGURIDAD	2	APLICAR	
ORGANIZACIÓN INTERNA	DETERMINAR RESPONSABILIDADES	3	APLICAR	La empresa deberá definir responsabilidades con respecto a la seguridad de la información. Además, deberá de tener el contacto necesario con las autoridades pertinentes y con profesionales especializados en seguridad de la información.
	SEPARACIÓN DE DEBERES	4	APLICADO	
	CONTACTO CON LAS AUTORIDADES	5	APLICADO	
	CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	6	APLICADO	

	SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	7	APLICAR	
DISPOSITIVOS MÓVILES Y TELETRABAJO	POLÍTICA PARA DISPOSITIVOS MÓVILES	8	APLICADO	La empresa está en la capacidad de limitar el acceso a las redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros.
	TELETRABAJO	9	NO APLICAR	Según la ley 30036 publicada en el año 2013, la empresa cuenta con la modalidad del teletrabajo. Esta modalidad se caracteriza por la no presencia física del trabajador mediante equipos informáticos que le permita cumplir con sus labores.
ANTES DE ASUMIR EL EMPLEO	SELECCIÓN	10	APLICADO	Para este proceso, el área de Recursos Humanos es el encargado de seleccionar el personal correspondiente, siguiendo diversos procedimientos y reglamentos que permitan asegurar la calidad.
	CONDICIONES	11	APLICADO	El personal está en la capacidad de interactuar de manera constante con los activos de la información de la empresa. Para eso se lleva a cabo la firma de aceptación de diversos documentos como: acta de cumplimiento, manual de prevención de lavados de activos, reglamento de seguridad en el trabajo, etc.
DURANTE LA EJECUCIÓN DEL EMPLEO	RESPONSABILIDADES DE LA DIRECCIÓN	12	APLICADO	
	EDUCACION Y FORMACION EN SISTEMAS DE INFORMACIÓN	13	APLICADO	

	DISCIPLINA	14	APLICADO	La empresa está encargada de cumplir con la capacitación respectiva del personal. La disciplina es responsabilidad del superior del área.
TERMINACIÓN Y CAMBIO DE EMPLEO	TÉRMINO RESPONSABILIDADES DE EMPLEO	15	APLICADO	Todo esto es ejecutado por el área de Recursos Humanos
GESTION DE ACTIVOS				
RESPONSABILIDAD POR LOS ACTIVOS	INVENTARIO DE LOS ACTIVOS DE INFORMACION	16	APLICAR	Se identifican los activos de la información del área de operaciones, y se documentan para llevar un control actualizados de dichos activos.
	PROPIEDAD DE LOS ACTIVOS	17	APLICAR	Se identifican a los propietarios de los activos de la información. Luego de eso, se hace el seguimiento a las regularizaciones.
	USO ACEPTABLE DE LOS ACTIVOS	18	APLICAR	Políticas procedimientos para identificar y documentar las respectivas normas.

	DEVOLUCIÓN DE LOS ACTIVOS	19	APLICAR	Los activos son devueltos por los colaboradores cuando se termina la relación contractual. El responsable del área debe asegurar la devolución de los activos en caso de renuncia, cambios o rotaciones de personal.
CLASIFICACIÓN DE LA INFORMACIÓN	CLASIFICACIÓN DE LA INFORMACIÓN	20	APLICAR	La empresa asegura que la información tenga un adecuado nivel de protección. Además, todos los usuarios deben comprometerse en respetar la clasificación de la información.
	ETIQUETADO DE LA INFORMACIÓN	21	APLICAR	Desarrollar e implementar procesos que permitan etiquetar la información siguiendo el modelo propio de la institución. Toda información lleva la etiqueta de “confidencial”.
	GESTIONAR LOS ACTIVOS	22	APLICAR	La empresa debe implementar mecanismos para el manejo de los activos de la información.
MANEJO DE MEDIOS	GESTIONAR LOS MEDIOS EXTRAÍBLES	23	APLICAR	Se implementan diversos procedimientos para mejorar la gestión de aquellos medios extraíbles, tales como el correo institucional, USB, CD, entre otros.

	LOS MEDIOS Y SU DISPOSICION	24	APLICAR	La empresa debe de tener el control de la disposición de los medios cuando estos ya no sean requeridos, siguiendo un procedimiento y formato previamente establecido por el área de seguridad.
	TRANSFERENCIA DE MEDIOS FÍSICOS.	25	APLICAR	La empresa debe de tener procedimientos establecidos en caso del manejo y transferencias de la información y asegurar su traslado de un medio a otro.
CONTROL DE ACCESO				
REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	CONTROLES DE ACCESO	26	APLICAR	Custodiar los activos de información que la empresa genera todos los días. La empresa tiene la responsabilidad de controlar los accesos a los activos de la información.
	ACCESO A LAS REDES	27	APLICAR	La empresa debe de asegurar que los usuarios solamente usen los sistemas debidamente autorizados.
GESTIÓN DE ACCESO DE USUARIOS	REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	28	APLICAR	Implementar un proceso en donde el Registro y Cancelación de cada usuario se lleve a cabo constantemente, y evitar así accesos no autorizados.
	ACCESO A USUARIOS	29	APLICAR	Implementación de un suministro formar para el acceso de los usuarios y asignar o revocar el derecho al acceso a los sistemas según los perfiles de usuarios.

	GESTIONAR LOS ACCESOS	30	APLICAR	La empresa está obligada a tener un control formal de todas las asignaciones y accesos privilegiados a los sistemas y activos de información.
	AUTENTICACION DE USUARIOS	31	APLICAR	Para asignar información debe estar controlado mediante un procedimiento formal y un gestor de identidad web.
	REVISION DE LOS ACCESOS	32	APLICAR	La empresa debe llevar a cabo revisiones de manera continua cada 2 meses para asegurar que los usuarios tengan los accesos necesarios para cumplir con sus funciones.
	AJUSTE DE LOS ACCESOS	33	APLICAR	La empresa debe tener un registro proveniente del área de seguridad y en donde figuren los trabajadores que culminan su contrato o relación laboral para así poder quitarle los acceso a los sistemas respectivos.
RESPONSABILIDADES DE LOS USUARIOS	USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	34	APLICAR	Exigir el cumplimiento de las buenas prácticas de la empresa por parte de los usuarios.
CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	35	APLICADO	Se debe tener cuidado con aquellos usuarios no autorizados a acceder a los sistemas. Además, se recomienda cambiar las claves cada 30 días.
	PROCEDIMIENTO DE INGRESO SEGURO.	36	APLICADO	De ser necesario, los accesos a los sistemas y aplicaciones deben ser controlados mediante procedimientos seguros.

	GESTIÓN DE CONTRASEÑAS.	37	APLICAR	Evaluar los procedimientos de gestión de contraseñas, las cuales deben ser interactivos y garantizar su calidad. Además de promover el cambio de contraseña cada 30 días.
	UTILITARIOS.	38	APLICAR	Controlar el uso de utilitarios que puedan dañar y anular el acceso a los sistemas.
	ACCESO A CÓDIGOS FUENTES.	39	NO APLICAR	No se necesita ejecutar este control, ya que los únicos responsables son los trabajadores del área de Sistemas.
CRIPTOGRAFIA				
CONTROLES CRIPTOGRAFICOS	POLÍTICAS DE CONTROL CRIPTOGRÁFICO	40	APLICADO	Establecer controles criptográficos para los sistemas y garantizar así la confidencialidad e integridad de la información.
	GESTIÓN DE LLAVES	41	APLICADO	La empresa debe implementar políticas y procedimientos acerca del uso y protección de llaves criptográficas.
ÁREAS SEGURAS	PERÍMETRO DE SEGURIDAD FÍSICA	42	APLICADO	La empresa debe de prevenir todo tipo de acceso físico no autorizado, con la finalidad de evitar daños e interferencias a los sistemas de información.

	CONTROLAR LOS ACCESOS FÍSICOS	43	APLICADO	Se debe evitar que personas no autorizadas accedan a los servidores o archivos confidenciales. Para ingresar se deberá contar con la autorización correspondiente del área de Seguridad.
	SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	44	APLICADO	Mantener la información bajo llave y restringir el acceso a la información a quienes no tengan la debida autorización.
	PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	45	APLICADO	La empresa cuenta con aire acondicionado en todos los ambientes, además se cuenta con extintores especiales en caso de incendios.
	TRABAJO EN ÁREAS SEGURAS	46	APLICAR	Diseñar procedimientos para el trabajo en áreas seguras e implementar las políticas de seguridad física y del medio ambiente.
	ÁREAS DE DESPACHO Y CARGA	47	APLICADO	Se controla los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
EQUIPOS	PROTECCIÓN DE EQUIPOS	48	APLICADO	Todo equipo dentro de la empresa se encuentra debidamente protegido en caso de recibir amenazas o peligros que atenten contra la seguridad y de personas no autorizadas. La empresa realiza inventarios cada año de todos sus equipos, tales como PC’s, servidores, escritorios, impresoras, teléfonos, escaners, etc. Esto con la finalidad de evitar pérdidas daños o robos.
	SUMINISTRO	49	APLICADO	
	CABLEADO	50	APLICADO	

	MANTENIMIENTO DE EQUIPOS	51	APLICADO	
	RETIRO DE ACTIVOS	52	APLICAR	Todo equipo o activo de la información de la empresa no debe ser retirado sin la debida autorización. Para esto se debe de contar con el permiso de las áreas correspondientes.
	SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	53	APLICAR	La empresa debe de aplicar ciertas medidas para cuidar la seguridad de los equipos y los activos de información que se encuentren fuera de las instalaciones, y teniendo en cuenta el riesgo que este conlleva.
	DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	54	APLICAR	Se deberían verificar que todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
	EQUIPOS DE USUARIO DESATENDIDO	55	APLICADO	El personal de la empresa vela por la seguridad de los activos de la información que está a su cargo. Además de protegerlos, deben de guardar la confidencialidad, la integridad y la disponibilidad de los mismos. La empresa cuenta con procedimientos y políticas de escritorio limpio y pantallas limpias en los equipos de procesamiento de la información.
	POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	56	APLICADO	

SEGURIDAD DE LAS OPERACIONES				
PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	57	APLICAR	Documentar y poner a disposición de los usuarios los procedimientos de operación, segmentado por área y por perfiles con especificaciones. Además, se podrá entregar un manual que servirá como guía al personal nuevo.
	GESTIÓN DE CAMBIOS	58	APLICAR	La empresa debe de controlar los cambios en cualquier área y en los sistemas de información. Todo cambio debe estar almacenado en un registro histórico, la cual debe considerarse en el área de operaciones y en el área de seguridad.
	GESTIÓN DE CAPACIDAD	59	APLICAR	Se debe de tener un plan de seguimiento de todos los recursos para lograr el desempeño requerido. Además, se realizar ajustes y proyecciones sobre futuros requisitos.
	AMBIENTES SEPARADOS.	60	APLICADO	La empresa tiene la responsabilidad de mantener cada área separada, ya sea de desarrollo, prueba y operación, para así reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

PROTECCION CONTRA CODIGOS MALICIOSOS	CONTROLES CONTRA CÓDIGOS MALICIOSOS	61	APLICAR	Para desarrollar actividades de la empresa se hacen uso de servicios como internet y medios extraíbles, las cuales pueden contener información maliciosa que atente contra el correcto funcionamiento de los activos de información. Por eso se deben de tener controles de seguridad que permitan prevenir y detectar la propagación de códigos maliciosos. Para eso es necesario el mantenimiento de los equipos informáticos y mantener los antivirus actualizados.
COPIAS DE RESPALDO	RESPALDO DE LA INFORMACIÓN	62	APLICAR	Toda información de la empresa, ya sean correos, reportes, informes, entre otros, se encuentran ubicadas en servidores. Es por eso que es necesario implementar controles de acceso y seguridad, y de respaldo de la información (back up) que permita recuperarla en caso de riesgos. De esta manera se permite que la empresa continue con sus actividades sin inconvenientes.

REGISTRO Y SEGUIMIENTO	REGISTRO DE EVENTOS	63	APLICAR	En la empresa se cuenta con perfiles de usuarios y diversos accesos a los activos de información. Esto conlleva a establecer controles de seguridad para registrar todo evento realizado y detectar actividades que no estén autorizadas.
	PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	64	APLICADO	La empresa es la encargada de mantener y proteger el historial de los logs. Para esto, los únicos que tienen acceso a dicha información son los administradores.

	REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	65	APLICAR	La empresa cuenta con el histórico de las actividades de los administradores y operadores de los sistemas gracias a reportes diarios que son generados por los usuarios. Dichos históricos deben guardarse de manera física o virtual para proteger su confidencialidad.
	RELOJES SINCRONIZADOS	66	APLICADO	Los relojes de los sistemas se encuentran debidamente sincronizados con una única fuente de referencia de tiempo.
CONTROL DE SOFTWARE OPERACIONAL	INSTALACIÓN DE SOFTWARES	67	APLICADO	La empresa se encarga de aplicar controles de seguridad para garantizar la protección, control y operación de todos los sistemas operativos. Además, debe de restringir la instalación de nuevos sistemas operativos en los equipos.
GESTION DE LA VULNERABILIDAD TÉCNICA	GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	68	APLICADO	La empresa controla y monitorea los activos de información, puesto que pueden estar dispuestas a diversas amenazas. Por lo tanto debe de establecer diversos controles de seguridad para disminuir los posibles riesgos.
	RESTRINGIR LA INSTALACIÓN DE NUEVOS SOFTWARES	69	APLICADO	La empresa cuenta con diversos sistemas operativos para desarrollar sus actividades. Para eso se estableció controles de seguridad que permitan su protección y correcto uso. Se cuenta demás con restricciones para la instalación de cualquier software.

CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	70	APLICADO	La empresa cuenta diversos sistemas operativos y procesos que estás sujetos a auditoría relacionada a la seguridad de la información. Por eso es importante definir controles de seguridad para garantizar el buen uso de las herramientas de auditoría.
SEGURIDAD DE LAS COMUNICACIONES				
GESTIÓN DE LA SEGURIDAD DE LAS REDES	CONTROL DE LAS REDES	71	APLICADO	La empresa protege de manera segura la información en las redes, instalaciones y equipos de soporte. Tiene mecanismos de seguridad en todos los niveles de servicio y de red.
	SEGURIDAD E N LA REDES	72	APLICADO	
	SEPARACIÓN EN LAS REDES	73	APLICADO	En la empresa los usuarios y sistemas de información están separados de las redes para evitar que el tráfico los afecte.
TRANSFERENCIA DE INFORMACIÓN	POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	74	APLICADO	En el desarrollo de las actividades de la empresa, se pueden encontrar procesos de intercambio de información con clientes u otros colaboradores como parte de prestación de servicios.
	ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	75	APLICADO	

	MENSAJERIA ELECTRÓNICA	76	APLICADO	Para ello es necesario tener controles de seguridad que cumplan con las políticas de la institución.
	CONFIDENCIALIDAD	77	APLICAR	La empresa debe de promover los acuerdos de confidencialidad y la no divulgación por parte de todos los colaboradores de la empresa. Está prohibido que los trabajadores saquen información confidencial de la empresa.
REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	78	NO APLICAR	No es aplicable
	SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	79	NO APLICAR	No es aplicable
	PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	80	NO APLICAR	No es aplicable
CONTROL DE ACCESO AL SISTEMA OPERATIVO	POLÍTICAS PARA UN DESARROLLO SEGURO	81	NO APLICAR	No es aplicable
	PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	82	NO APLICAR	No es aplicable
	REVISIÓN DE LAS TÉCNICAS EN LA PLATAFORMA DE OPERACIÓN	83	NO APLICAR	No es aplicable

	RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	84	NO APLICAR	No es aplicable
	PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	85	NO APLICAR	No es aplicable
	AMBIENTE DE DESARROLLO SEGURO	86	NO APLICAR	No es aplicable
	DESARROLLO CONTRATADO EXTERNAMENTE	87	NO APLICAR	No es aplicable
	PRUEBAS DE SEGURIDAD DE SISTEMAS	88	NO APLICAR	No es aplicable
	PRUEBAS DE ACEPTACIÓN DE SISTEMAS	89	NO APLICAR	No es aplicable
DATOS DE PRUEBA	PROTECCIÓN DE DATOS DE PRUEBA	90	NO APLICAR	No es aplicable
COMUNICACIÓN CON LOS PROVEEDORES				
RELACIONES CON LOS PROVEEDORES	ASEGURAR LAS BUENAS RELACIONES CON LOS PROVEEDORES	91	APLICADO	La empresa se encarga de desarrollar diversas actividades y en la cual necesita comprar varios bienes y productos. Para ello existen controles que controlan la seguridad del negocio y que puedan afectar la seguridad o infraestructura de la empresa.

	TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	92	APLICADO	La empresa tiene diversos acuerdos en materia de seguridad de información con sus proveedores. Dichos requisitos están definidos bajo conceptos técnicos y con condiciones.
	CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	93	APLICADO	Se debe incluir otros requisitos en los acuerdos con terceras personas para mejorar el manejo de los riesgos de la seguridad de la información.
GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	SEGUIMIENTO Y SUPERVISIÓN DE LOS SERVICIOS	94	APLICADO	La empresa se encarga de determinar el cumplimiento de los contratos con los proveedores.
	CONTROLAR LOS CAMBIOS DE LOS PROVEEDORES	95	NO APLICAR	Este control no garantiza la reducción de los riesgos.

GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	RESPONSABILIDADES Y PROCEDIMIENTOS	96	APLICAR	La empresa tiene la obligación de brindar una respuesta rápida y efectiva ante cualquier evento que afecte la seguridad de la información
	REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	97	APLICAR	La empresa debe de asegurar que los eventos o incidentes en la seguridad de la información se reporten de manera oportuna y a las áreas responsables. Los respectivos reportes deben ser remitidos a la brevedad posible.
	INFORME DE LAS DEBILIDADES DE LOS SISTEMAS DE INFORMACION	98	APLICAR	La empresa debe exigir a todos los trabajadores informar de inmediato cualquier debilidad que pueda existir en los sistemas de información.
	EVALUACION DE LOS EVENTOS	99	APLICAR	Todo evento relacionado con la seguridad de la información debería ser evaluado y ser considerado o no como incidente hacia los activos de información.

				Dichos incidentes deben ser manejados por el personal capacitado y correspondiente y que hayan sido asignados por la gerencia.
	RESPUESTA ANTE INCIDENTES	100	APLICAR	La empresa debe contar con un procedimiento para atender cualquier tipo de incidente que afecte a los sistemas de información.
	APRENDIZAJE OBTENIDO DE LOS INCIDENTES	101	APLICAR	El aprendizaje obtenido a raíz de los incidentes, debe de servir para prevenir y mitigar futuros riesgos dentro de la empresa.
	EVIDENCIA RECOLECTADA	102	APLICAR	La empresa se encarga de recolectar y preservar la información correspondiente a las evidencias e incidentes que atenten contra los sistemas de información.
SEGURIDAD EN LOS ACTIVOS DE INFORMACION PARA GARANTIZAR LA CONTINUIDAD DEL SERVICIO				
CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	PLANIFICAR LA CONTINUIDAD	103	APLICAR	La empresa tiene un excelente vínculo en referencia a atención de cliente, por lo que debe tener un buen manejo de la seguridad de la información y garantizar así su continuidad en cualquier situación adversa o amenaza. Por ejemplo, durante un desastre natural o una crisis financiera.
	ASEGURAR LA CONTINUIDAD	104	APLICAR	La empresa se encarga de implementar, documentar y establecer procesos para asegurar la continuidad de los sistemas de

				información en caso exista algún incidente. Además, se debe de nombrar a personas responsables que llegarán a dirigir dichos procesos y que deberán reportar a las áreas respectivas.
	VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	105	APLICAR	La empresa se encarga de verificar y actualizar los controles de seguridad de la información con la finalidad de asegurar su continuidad del servicio.
REDUNDANCIAS	MANTENER LA DISPONIBILIDAD DE LAS INSTALACIONES	106	NO APLICAR	Este control no está considerado a que ayude en la reducción de los riesgos identificados.
CUMPLIMIENTO				
CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	IDENTIFICAR LA LEGISLACIÓN Y REQUISITOS DE CONTRASTE.	107	APLICADO	La empresa cumple con todas las obligaciones legales, ya sean contractuales o reglamentarias, que estén relacionados con la seguridad.
	DERECHOS DE PROPIEDAD INTELECTUAL	108	APLICADO	La empresa garantiza el cumplimiento de todos los trámites legales en relación a normas y contratos que tengan que ver con la propiedad intelectual y el uso de softwares con patente.

	PROTECCIÓN DE REGISTROS	109	APLICADO	La empresa se encarga de proteger adecuadamente los registros de información ante la pérdida, falsificación o algún acceso no autorizado.
	PRIVACIDAD DE LA INFORMACIÓN	110	APLICADO	La empresa se encarga de cuidar las bases de datos y documentación de sus clientes, de sus trabajadores y demás. Esto en relación a las buenas prácticas que tiene la institución y evitar así la violación de la información.
	REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	111	APLICADO	La empresa garantiza el uso de controles criptográficos para el acceso a los sistemas de información con el objetivo de garantizar la confidencialidad e integridad.
REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	112	APLICAR	La empresa haciendo uso de sus políticas de seguridad, mantiene el compromiso de mantener protegido sus activos de información, por lo que está en la obligación de actualizar sus protocolos bajo la norma ISO y bajo la supervisión de OSIPTEL.
	CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	113	APLICAR	El personal encargado mantiene interacción constante con todos los activos de la información. Para eso se han diseñado procedimientos y protocolos correspondientes en relación a la seguridad de la información.

	REVISIÓN DEL CUMPLIMIENTO TÉCNICO	114	APLICAR	Para este control se necesita que la alta dirección se involucre directamente para llegar al éxito en el sistema de gestión de seguridad de la información. Para ello es necesario desarrollar un historial y cumplir con los requisitos mínimos de seguridad.

Análisis y Discusión

El presente trabajo tuvo como objetivo implementar un sistema de gestión de seguridad de la información en la empresa América Móvil – Chimbote.

Luego de haber encontrado los resultados correspondientes se hizo el análisis y comparativa con los trabajos previamente citados. Es así, por ejemplo, se encontró relación con el estudio de García (2021) quien en su tesis tuvo el propósito de realizar una propuesta de un sistema de gestión para la seguridad de la información basado en la norma ISO 27001 para las oficinas de tecnologías de la información del Gobierno Regional de Piura. Los resultados indicaron que el 91% de los encuestados sostuvo que no está satisfecho con la situación actual, mientras que el 9% restante afirmó que sí se siente satisfecho. El 100% de los entrevistados afirmó que sí se necesita seguridad en la información con la norma ISO 27001. La conclusión del estudio señala que la propuesta de un sistema de gestión para la seguridad de la información mejora los procesos de seguridad de la información y comunicación del Gobierno Regional de Piura.

También concuerda con el trabajo de Fuentes (2020) quien tuvo el objetivo de proponer un sistema de gestión para la seguridad de la información encargada de gestionar los procesos más críticos en la Universidad Nacional de Cajamarca. Empleó también un cuestionario como instrumento de recolección de información que se aplicó a los usuarios de TI de la Universidad Nacional de Cajamarca. La conclusión del trabajo señala que la implementación de un sistema de gestión para la seguridad de la información tiene un nivel aceptable.

Finalmente, se encontró relación con la investigación de Pardo (2015) quien presentó una tesis para la Universidad Nacional de Loja, Ecuador, en donde tuvo el objetivo de implementar un modelo de gestión de seguridad en la información para la mencionada universidad basada en la norma ISO/IEC 27001. Como resultado de la investigación se hizo la valoración de la información obtenida con el personal especializado en TI.

Conclusiones

- Se realizaron entrevistas a los colaboradores responsables del área de operaciones, con lo cual se pudo identificar su nivel de conocimiento sobre las políticas de seguridad de la información de la empresa.
- Se desarrolló las guías de las buenas prácticas en donde se tuvo en cuenta diversos procesos de dirección.
- Se subdividió el trabajo del proyecto en partes pequeñas para que sean más manejables orientados a los objetivos de la investigación.
- Se realizaron inventarios de los activos de la información relacionado al área.

Recomendaciones

- Se recomienda verificar y actualizar los diferentes procesos en donde se encuentren vulnerabilidades.
- Se recomienda verificar los perfiles de los usuarios, poniendo más control en los perfiles no autorizados o con acceso temporal al cargo.

- Se recomienda cumplir con los protocolos de seguridad para el caso de las claves de acceso. Además de actualizar constantemente las mismas
- Se recomienda auditar y revisar el historial de cada dispositivo, ya sea externo o removible.
- Se recomienda plantear cuestionarios constantes al personal de la empresa para evaluar así su desempeño y mejorar de ser necesario, con el objetivo de disminuir los riesgos y amenazas.
- Se recomienda revisar de manera constante las políticas de seguridad y verificar su cumplimiento en todo el personal de la empresa.
- Finalmente, se recomienda capacitar constantemente a todo el personal del área.

Referencias Bibliográficas

Aguirre, J. y Aristizábal, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda.* (Proyecto de grado) Universidad tecnológica de Pereira. Colombia. Recuperado de: http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf

Aguirre, D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* (Tesis de título) Pontificia Universidad Católica del Perú. Recuperado de:

https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf?sequence=1&isAllowed=y

Barragán, I., Góngora I., y Martínez, E. (2013). *Implementación de políticas de seguridad informática para la M.I. municipalidad de Guayaquil aplicando la norma iso/iec 27002.* (Tesis de título) Escuela Superior Politécnica del Litoral) Guayaquil, Ecuador. Recuperado de:

http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/21546/ManualTopico.pdf?sequence=2&isAllowed=y

CRUZ, M. Y FUKUSAKI, S. (2017) D*iseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica MEDCAM Perú SAC. U*niversidad San Martin de Porres

De la Cruz, C. (2009). *Elaboración Y Aplicación de un Sistema de gestión de la Seguridad de La Información (SGSI) para la realidad tecnológica de la USAT* (Tesis de título) Universidad Católica Santo Toribio De Mogrovejo. Chiclayo. Recuperado de :

https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/2440/BC-TES-TMP-1311.pdf?sequence=1&isAllowed=y

Espinoza, H. (2013) *Análisis y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Pontificia Universidad Católica del Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957?show=full.

Fuentes, R. (2020) *Sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca.* Universidad Nacional Pedro Ruiz Gallo.

García, R. (2021) *Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de Tecnologías de Información del Gobierno Regional Piura.* Universidad Los Ángeles de Chimbote.

Montoya, N. (2012). *Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional.* (Tesis de título) Pontificia Universidad Católica del Perú. Recuperado de:

https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/5005/MONTOYA_NELSON_DISE%c3%91O_SISTEMA_GESTION_SEGURIDAD_INFORMACION_CENTRO_CULTURAL_BINACIONAL.pdf?sequence=1&isAllowed=y

Pardo, M. (2015) *Modelo de gestión de seguridad de la información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001.* Ecuador

Távara, C. y Navarro, M. (2021) *Sistema de gestión de seguridad de la información basada en la Norma ISO 27001 para la Caja Sullana.* Universidad San Pedro.

Villena, M. (2006). *Sistema de gestión de seguridad de información para una institución financiera.* (Tesis de título) Pontificia Universidad Católica del Perú. Lima. Recuperado de: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/362/VILLENA_MOIS%c3%89S_SISTEMA_DE%20GESTI%c3%93N_DE_SEGURIDAD_DE_INFORMACI%c3%93N_PARA_UNA_INSTITUCI%c3%93N_FINANCIERA.pdf?sequence=1&isAllowed=y

Anexos y Apéndices

Anexo 01: Entrevista Sobre Seguridad De La Información

Dirigido al Jefe del Área de Seguridad Corporativa de América Móvil.

1. ¿América Móvil cuenta con un comité de seguridad de la información?

   SI ( )

   Las funciones del comité se encuentran detalladas en el manual de funciones y organización u otro documento

   _____
   ____

   ¿Quién conforma ese comité?

   _____
   ____

   ¿Ese comité es plenamente identificable por los usuarios América Móvil?

   _____
   ____

   NO ( )

   Si no cuentan con ese comité; ¿Quiénes son los encargados de establecer las políticas de seguridad de la información?

   _____
   ____

   O, ¿Sólo las políticas son establecidas por sí mismo como jefe del área de seguridad Corporativa?

¿Estas políticas son conocidas por todos los usuarios?

_____
____

¿A través de que medio se les dio a conocer?

_____
_

2. ¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información?

_____
____

3. ¿De qué manera controla a sus trabajadores y todo el personal, con respecto al tema de seguridad de la información?

_____
____

4. ¿De qué forma controla los accesos a la red y quién ordena que se genere esos permisos?

_____
____

5. ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?

---

6. ¿Existe un documento donde se especifique las políticas de seguridad de la información?
   SI ( )

¿Quién elaboró ese documento y por quién fue aprobado?

_____
_____

¿Los usuarios conocen este documento?

_____
_____

¿Se aplican estas políticas a todo el personal de America Movil?

_____
_____

¿Cada que tiempo se revisan esas políticas?

_____
_____

NO ( )

¿Según Usted, a que cree que se deba, que hasta ahora no se implementa las políticas de seguridad de la información en America Movil?

_____
_____

¿Cree Usted, que es de suma urgencia la elaboración de políticas de seguridad de la información para America Movil?

_____
_____

Porqué_____
____

Y para su área_____

7. Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?

   SI ( )

   ¿Para ello existen procedimientos documentados para actuar antes, durante y después del desastre?_____
   _____

   ¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro?

   _____
   ____

   Lo cree necesario hacerlo con esta organización_____

   ¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para elaborarlo?

   _____
   ____

   NO ( )

   ¿A qué se debe?_____

8. ¿Cuáles son los errores más comunes cando se usa internet y correo electrónico?

   _____
   ____

9. ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?

MF: Muy frecuente RF: Regularmente frecuente PF: Poco frecuente

Riesgos	MF	RF	PF
Fenómenos Naturales (Terremotos, Inundaciones)			
Fallas mecánicas (Cortes de fluido eléctrico, incendios)			
Divulgación ilícita de la información por el personal			
Destrucción o modificación de la información por el personal			
Intrusos al sistema de la red			
Virus informáticos, gusanos, spam			
Otros:			

10. ¿Los equipos de cómputo en el área tienen fuente de poder ininterrumpible (UPS), generadores de energía, baterías ante cortes de energía eléctrica?

_____

_____

11. ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

_____

_____

12. ¿Quiénes se encargan de capacitar al personal sobre seguridad de la Información?

_____

_____

13. ¿A Usted se le brinda capacitación por parte de la America Móvil acerca de seguridad de la información?

Si ( ) No ( )

Si la respuesta es **Sí;** Cada que tiempo y quien se encarga de hacerlo

_____

_

En caso contrario, ¿cómo se capacitan?

_____

____

14. ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

_____

15. ¿A qué área se le debe de comunicar oportunamente los incidentes de seguridad detectados?

_____

_____

16. ¿Cuáles son sus recomendaciones al personal de America Movil(Área de Operaciones) para un buen uso de la información?

_____

_____

Anexo 02: Encuesta Sobre Seguridad De La Información

1. ¿En America Movil cuentan con políticas de seguridad de la información?

   Si ( ) No lo sé ( ) No ( )

2. ¿Si en la Pregunta 1 respondió si, Se cumplen o se llevan a la práctica estas políticas?

   Si ( ) A veces ( ) No ( )

3. ¿Conoce las políticas de seguridad de la información?

   Si ( ) Algunas ( ) No ( )

4. ¿Cuándo fue la última vez que asistió a un taller o capacitación sobre seguridad de la información?

   Hace 3 meses ( ) Hace 6 meses ( ) Hace 1 año ( ) Nunca ( )

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

   Si ( ) No ( )

6. 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) Capacitaciones, Charlas o conferencias
   c) Como parte de algún curso en tu carrera

7. ¿Puede identificar a las personas que no trabajan en America Movil?

   Si ( ) A Veces ( ) No ( )

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

   a. Fotocheck de la empresa en que trabaja ( )
   b. Fotocheck de visitante (entregado por America Movil) ( )
   c. Otros, Especificar…… ( )
   d. Ninguno ( )

8. ¿Has observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras America Movil?

   Siempre ( ) A veces ( ) Nunca ( )

9. ¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de America Movil?

   Si ( ) A veces ( ) No ( )

10. ¿Tu clave de acceso es la misma para todos los sistemas con los que cuenta el área de Operaciones - America Movil?

    Si ( ) La mayoría ( ) No ( )

    Normalmente tu clave hace referencia a:

    a. Tu nombre y apellido ( )
    b. Tú fecha de nacimiento ( )
    c. Teléfono (de casa o móvil) ( )
    d. Nombre de tu enamorada o enamorado ( )
    e. Otros, Especifique..... ( )

    Y si nunca cambiaste tu clave, cuál es y porque motivo no lo hiciste

    .....

11. ¿Ud. cambia con frecuencia sus Claves de los sistemas de la America Movil?

    Siempre ( ) A veces ( ) Nunca ( )

12. ¿Comparte sus claves de acceso con sus compañeros de trabajo?

    Siempre ( ) A veces ( ) Nunca ( )

13. ¿Usted ha utilizado alguna Laptop dentro de America Movil?

    Siempre ( ) A veces ( ) Nunca ( )

Si su respuesta es **Afirmativa;** Ha recibido algún mensaje en el cual le comunique que su equipo ha sido registrado y puede acceder a la red

Siempre ( ) A veces ( ) Nunca ( )

14. ¿Todos los empleados deben portar su identificación visible durante su permanencia en el centro de labores?

Siempre ( ) A veces ( ) Nunca ( )

15. ¿La responsabilidad por la seguridad de la información debe ser una obligación diaria de quién?

Sólo Jefes ( ) Todo el personal ( ) Área de seguridad corporativa ( )

16. ¿Cuándo se ausenta de su oficina deja bloqueada la PC?

Siempre ( ) A veces ( ) Nunca ( )

17. ¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?
Siempre ( ) A veces ( ) Nunca ( )

18. ¿Qué es lo que hace con la información que ya no necesita?

a. La sigue guardando ( )
b. La deja en cualquier lugar ( )
c. La desecha ( )
d. La tritura o rompe antes de desecharla ( )
e. Otros Explicar ..... ( )

19. Usted apaga los equipos informáticos debidamente después de utilizarlos

Siempre ( ) A veces ( ) Nunca ( )

Si tu respuesta es afirmativa, ¿Cómo apaga el equipo después de trabajar?

a. Apagando directamente el estabilizador. ( )
b. Manteniendo presionando el botón de apagado del CPU. ( )
c. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )

20. Cada vez que sufre algún inconveniente con la PC o aplicación (sistemas) con el cual se desea trabajar, porque medio informa o reporta el inconveniente:

a. Teléfono (anexo) ( )
b. Correo electrónico al área de cómputo ( )
c. Voy físicamente a buscar algún encargado de cómputo ( )
d. Espero que pasen por mi área de trabajo ( )
e. Mesa de Servicios ( )
f. Otros, Especifique…… ( )

21. 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

Siempre ( ) A veces ( ) Nunca ( )

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

Siempre ( ) A veces ( ) Nunca ( )

23. ¿Su PC tiene acceso a los dispositivos de almacenamiento?

Si ( ) No lo sé ( ) No ( )

Si la respuesta es Si, a que dispositivos tiene acceso

……..

24. ¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?

Siempre ( ) A veces ( ) Nunca ( )

Si la respuesta es afirmativa; ¿Cuál fue el medio que utilizo para extraer dicha información?

a. Memoria USB ( )
b. CD ( )
c. DVD ( )
d. Otros ( )

25. ¿Cuenta con correo electrónico?

Si ( ) No ( )

Si su respuesta es **sí;** Que uso le da:

a. Sólo para asuntos Laborales ( )
b. Para asuntos personales ( )
c. Para ambos asuntos (Personales, Laborales) ( )
d. Otros, Especificar…….… ( )

26. ¿Qué haría si recibe un e-mail externo donde se solicita información de carácter personal?

a. No responder e informar al área correspondiente ( )
b. Responder ante lo que solicitan ( )
c. No le doy importancia ( )
d. Otros , Especificar…… ( )

27. ¿Qué recomienda para hacer el uso adecuado del internet de America Movil?

a. Realizar descargar, pero de sitios que sean confiables ( )
b. No realizar descargas de música, programas entre otros. ( )
c. Otros, Especificar…… .. ( )

28. ¿Usted ha detectado que el antivirus de America Movil funciona adecuadamente y que se encuentra actualizado?

Si ( ) No ( )

29. ¿De acuerdo a su perfil, cuenta con todos los accesos asignados para poder realizar sus labores diarias?

    a. Si, cuento con todo lo necesario de acuerdo a mi perfil ( )
    b. Sí, pero también tengo accesos designados que no me corresponde según mi perfil. ( )

30. ¿Reconoce Ud. Cuáles son los activos importantes de America Movil dentro del área de operaciones?

    Si ( ) Algunos ( ) No ( )

31. ¿La información, ya sea documentos entre otros que es de uso interno debe ser divulgada a terceras personas?

    Si ( ) No lo sé ( ) No ( )

32. ¿Ud. sabe distinguir la información que es de estrictamente confidencial, de uso interno o publica?

    Si ( ) No ( )

33. ¿Se cuenta con servicio de vigilancia, personas y/o videocámaras?

    a. Solo Vigilante ( )
    b. Solo videocámara ( )
    c. Ambos ( )

34. Existe alarma para:

    a. Detectar fuego (calor o humo) en forma automática ( )
    b. Avisar en forma manual la presencia del fuego ( )
    c. Otros (Robo) ( )
    d. Existe todas las anteriores ( )
    e. No existe ( )

CENTRO DE ATENCION AL CLIENTE CHIMBOTE

Figura 13:CAC CHIMBOTE

Figura 14:CENTRO DE ATENCION CHIMBOTE II

SERVICIO TECNICO

Figura 15:SERVICIO TECNICO

ALMACEN

Figura 16:ALMACEN CAC CHIMBOTE

SERVIDOR

Figura 17:SERVIDOR

Figura 18:SERVIDOR CAC CHIMBOTE

FILTRO

Figura 19:SERVIDOR CAC CHIMBOTE

SIAC POSTPAGO

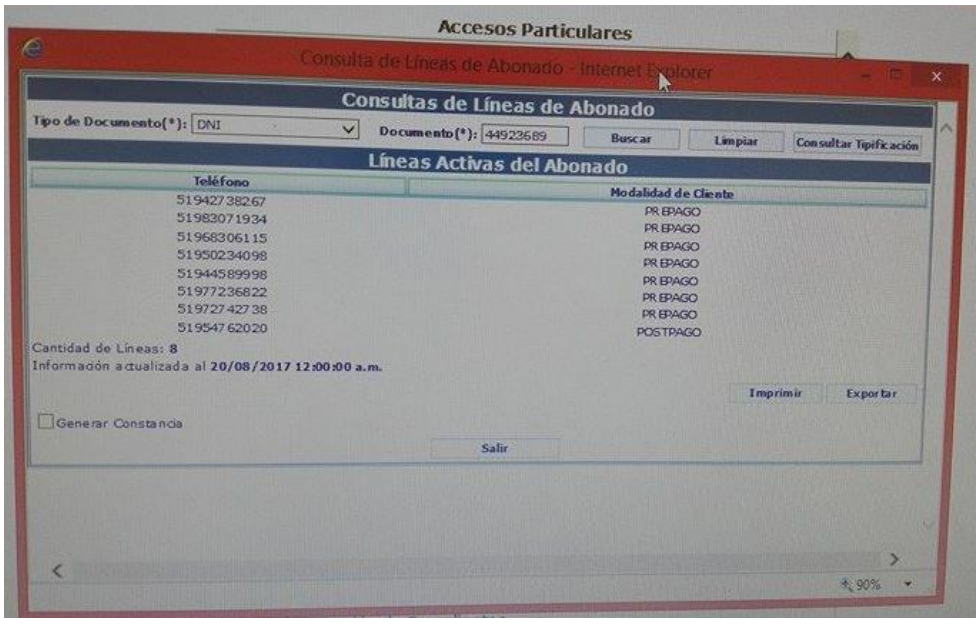


Figura 20:SIAS POSTPAGO

SISTEMA DE ACTIVACIONES

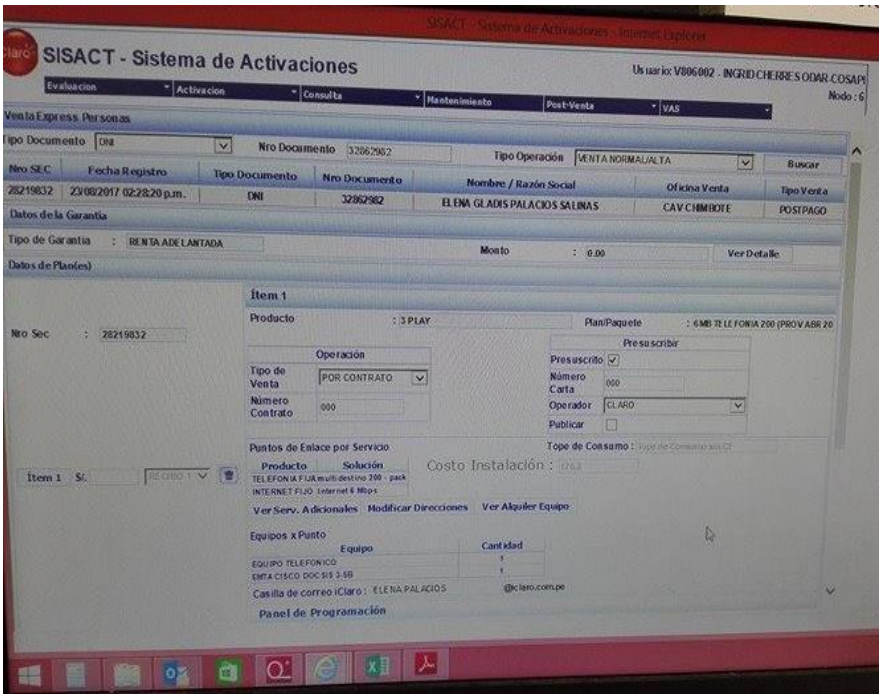


Figura 21:SISITEMA DE ACTIVACIONES

REGISTRO DE CLIENTE EN SISTEMA DE ACTIVACIONES

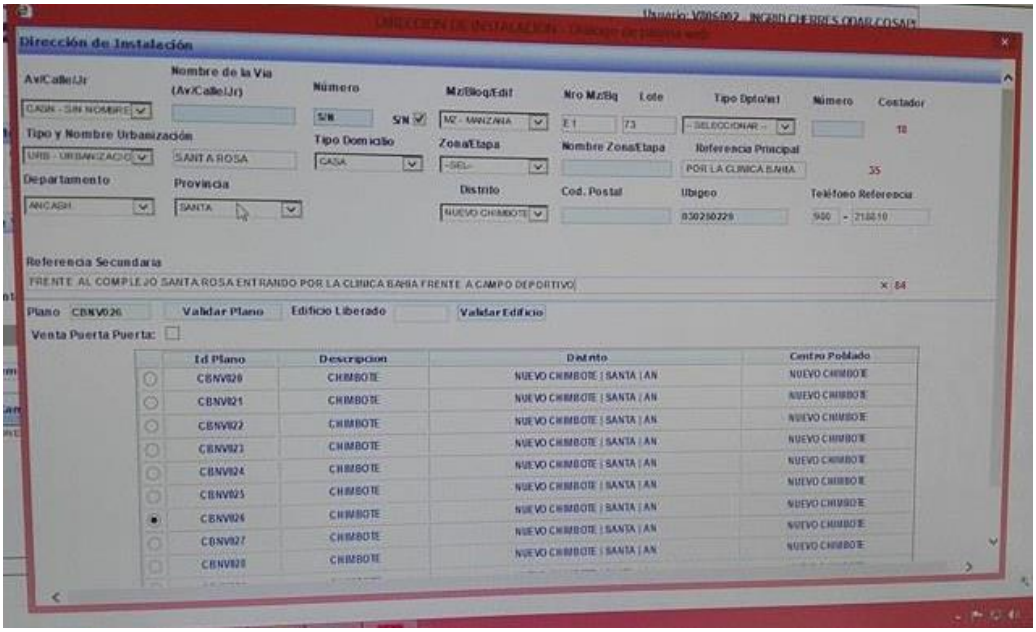


Figura 22: REGISTRO DE CLIENTE EN SISACT

PORTAL DE APLICACIONES

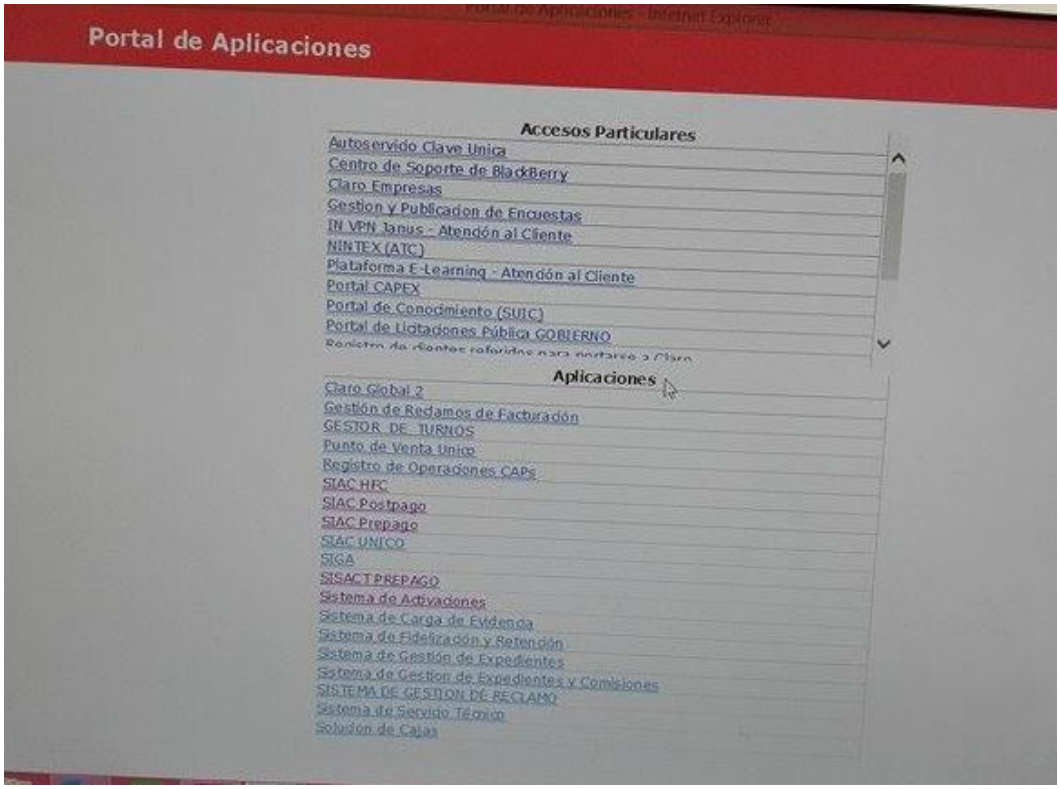


Figura 23:PORTAL DE APLICACIONES