PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ANEXOS

Tesis para optar el Título de ***Ingeniero Informático***, que presenta el bachiller:

David Arturo Aguirre Mollehuanca

ASESOR: Moisés Antonio Villena Aguilar

Lima, octubre de 2014

Índice

1. Anexo 1: Política de Seguridad de Información

Serpost
El Correo del Perú

POLITICA DE SEGURIDAD DE INFORMACIÓN

1. INTRODUCCIÓN

La empresa "Servicios Postales del Perú S.A" – SERPOST, claramente comprometida con el resguardo de la seguridad de su información y la de sus clientes, ha decidido incorporar, como parte de su estrategia institucional, la implementación de un sistema de gestión de seguridad de información o SGSI basada en los lineamientos presentados por la Norma Técnica Peruana ISO/IEC 27001:2008 dando cumplimiento a la Resolución Ministerial N° 129-2012-PCM.

2. OBJETIVOS DE LA POLÍTICA

Dar a conocer al personal de SERPOST S.A. y a sus proveedores de bienes y servicios, la importancia de una adecuada Gestión de Seguridad de Información y todos los compromisos adquiridos para proteger, a un nivel aceptable por la empresa, la información que posea, relacionada a la Atención de Clientes Empresariales, en cualquier medio que la contenga.

3. ALCANCE DE LA POLÍTICA

El cumplimiento de la presente política es de carácter obligatorio para todo el personal de SERPOST S.A y para cualquier TERCERO, que tenga una relación de proveedor de bienes o servicio relacionado a los procesos incluidos dentro del alcance del SGSI.

4. ROLES Y RESPONSABILIDADES

La siguiente es una lista de roles y responsabilidades de la seguridad de la información a alto nivel:

Plana Gerencial:

- Conocer y difundir la política de seguridad de la información a todos los trabajadores de la organización.
- Estar comprometidos con el sistema de gestión de la seguridad de la información.

Comité de Seguridad de Información:

- Comunicar la importancia de los objetivos de la seguridad de la información y la necesidad de mantener una mejora continua.
- Estar informados de las necesidades actuales del negocio y de los cambios dados en los procesos pertenecientes al alcance del SGSI.
- Facilitar y dar seguimiento a la asignación de recursos relacionados al SGSI.

Oficial de Seguridad de la Información:

- Diseñar, implementar, monitorear y mejorar el sistema de gestión de seguridad de la información en la empresa.
- Elaborar y ejecutar planes de capacitación para el personal involucrado con el alcance del SGSI.
- Seleccionar y capacitar al personal adecuado para la auditoria interna del SGSI.

Personal de la organización:

- Conocer e identificar aquellos activos de información de los cuales son dueños.
- Asegurar que los activos de información que poseen son manejados y administrados correctamente.
- Reportar al oficial de seguridad de la información sobre cualquier vulnerabilidad detectada que afecte sus activos de información.

Proveedores de Bienes y Servicios:

- Comprometerse por escrito a la adhesión a la presente política.
- Cumplir con lo indicado en el marco regulatorio del SGSI de la institución, en lo que respecta a su relación con terceros.

Serpost
El Correo del Perú

5. POLÍTICA

En SERPOST, se considera que la información, tanto propia como la de nuestros clientes, es un activo clave para la organización, independientemente del medio que la contenga. Por consiguiente, SERPOST se compromete a la búsqueda de la confidencialidad, disponibilidad e integridad de la información según lo indicado en el alcance del SGSI, aumentando así, la confianza de nuestro personal, la de nuestros clientes y de otros grupos de interés.

De acuerdo a ello, la Alta Dirección, se compromete a implementar, operar, mantener y mejorar un sistema de gestión de seguridad de información según los lineamientos indicados por la NTP ISO/IEC 27001:2008, la cual será de aplicación obligatoria a todo el personal y recursos que se encuentren dentro del alcance del mismo.

6. SANCIONES

SERPOST S.A. está obligada a cumplir la Resolución Ministerial N° 129-2012-PCM emitida en mayo del 2012 en la cual se exige la implementación de la NTP ISO/ISO 27001:2008 referente a la implementación de un SGSI.

Debido a ello, en caso se demuestre que algún funcionario o trabajador haya incumplido con las disposiciones que hace referencia este documento, el Comité de Seguridad de la Información, deberá informar, con las pruebas pertinentes, a la Sub Gerencia de Recursos Humanos sobre este hecho, para que se aplique las sanciones correspondientes según los lineamientos y normas vigentes en la empresa.

7. REVISIÓN DE LA POLÍTICA

La revisión de la política del SGSI deberá realizarse una vez al año con la presencia de los miembros del Comité de Seguridad de la Información y la del Oficial de Seguridad de la Información de la empresa.

8. REVISIÓN DEL ALCANCE DEL SGSI

La revisión del alcance del SGSI, se deberá realizar una vez al año o cuando existan cambios importantes en los procesos pertenecientes al alcance actual del SGSI u otros relacionados a los mismos.

9. INFORMACIÓN DE CONTACTO

La persona encargada de velar por el correcto funcionamiento del sistema de gestión de seguridad de la información y de responder por todos los temas relacionados a ella es el Oficial de Seguridad de la Información.

10. DEFINICIONES

- Seguridad de la información: De acuerdo a la NTP ISO/IEC 27001:2008, es la preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.
- Sistema de gestión de seguridad de la información (SGSI): De acuerdo a la NTP ISO/IEC 27001:2008, es parte de un sistema gerencial general, basada en un enfoque de riesgos, para establecer, implementar, operar, revisar, monitorear, mantener y mejorar la seguridad de la información.
- Confidencialidad: De acuerdo a la NTP ISO/IEC 27001:2008, es la propiedad por la que la información está disponible y no es divulgada a personas, entidades o procesos no autorizados.
- Disponibilidad: De acuerdo a la NTP ISO/IEC 27001:2008, es la propiedad de estar disponible y utilizable cuando una entidad autorizada lo requiera.
- Integridad: De acuerdo a la NTP ISO/IEC 27001:2008, es la propiedad de salvaguardar la exactitud e integridad de los activos.

2. Anexo 2: Alcance del SGSI

Serpost
El Correo del Perú

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. PROPOSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir claramente cuáles son los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de SERPOST S.A. y es aplicable a toda la documentación perteneciente al SGSI.

Los únicos usuarios autorizados de este documento son los miembros del Comité de Seguridad de la Información, el Oficial de Seguridad de Información y el personal autorizado de la Sub-Gerencia de Tecnologías de la Información de SERPOST S.A.

2. ALCANCE DEL SGSI

En los cuales se considerarán aquellos activos identificados como los más relevantes de los mismos.

El alcance del sistema de gestión es: "Atención de Clientes Empresariales Locales: Correspondencia empresarial admitida a través del Centro de Clasificación Postal de Lima (CCPL), ubicada en el distrito de Los Olivos, y distribuida en la misma y en la Administración Postal de Miraflores"

Se considerarán los activos identificados como relevantes en el proceso de "Atención de Clientes Empresariales Locales", el cual está conformado por los siguientes sub procesos:

1. Recepción
2. Habilitado
3. Clasificación
4. Distribución Administraciones
5. Control de cargos
6. Digitalización
7. Facturación

Los cuales se desarrollan íntegramente en el CCPL, a excepción del proceso de Distribución Administraciones, el cual se desarrolla tanto en el CCPL como en la Administración Postal de Miraflores.

3. Anexo 3: Objetivos del SGSI

Serpost
El Correo del Perú

OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. PROPOSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir claramente cuáles son los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) de SERPOST S.A., el cual debe ser de conocimiento obligatorio para todo el personal de SERPOST S.A y para cualquier TERCERO, que tenga una relación de proveedor de bienes o servicio relacionado a los procesos incluidos dentro del alcance del SGSI.

Los usuarios autorizados de este documento son los miembros del Comité de Seguridad de la Información, el Oficial de Seguridad de Información y el personal autorizado de la Sub-Gerencia de Tecnologías de la Información de SERPOST S.A.

2. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad de información tiene los siguientes objetivos:

- Buscar la participación de, al menos, un 85% de los colaboradores en las capacitaciones anuales de seguridad de la información
- Reducir los riesgos de seguridad de la información, a un nivel aceptable para la empresa, en un lapso de tiempo previamente definido con los dueños de los procesos.
- Mantener actualizados los procesos y procedimientos relacionados al alcance del SGSI de manera anual o cuando existan cambios en ellos o en su entorno.
- Difundir las políticas de seguridad de información a través de cada uno de los gerentes de SERPOST dentro de sus respectivas áreas.

4. Anexo 4: Modelo de Caso de Negocio – Resumen Ejecutivo

Resumen Ejecutivo

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado, en el cual, las empresas deben tomar decisiones rápidas y eficientes, así como resguardar la información clave de sus clientes. Este escenario convierte a la información en uno de los activos más importantes dentro de las organizaciones llegando a alcanzar una importancia estratégica para muchas de ellas y convirtiéndola, muchas veces, en blanco de ataques de personas mal intencionadas.

En este contexto, la Presidencia del Consejo de Ministros, a través de la resolución ministerial "RM-129-2012-PCM", ha solicitado que todas las entidades públicas implementen un sistema de gestión de seguridad de la información o SGSI por sus siglas en español. De esta forma, se espera poder resguardar a la información tanto de ataques o incidentes físicos, tales como robos o incendios, como de ataques cibernéticos como la explotación de vulnerabilidades de los diversos sistemas de información que se manejan.

Este cambio regulatorio es el principal agente del cambio que discutimos en el documento. Adicionalmente, se debe considerar el cronograma de implementación propuesto por la ONGEI ya que, según el estado actual de la organización, SERPOST se encuentra dentro de la PRIMERA fase del cronograma, cuando se debería ubicar dentro de la CUARTA fase del mismo de las cinco fases propuestas.

Ante esta problemática se analizó cinco posibles soluciones, siendo la más recomendable la implementación de la norma NTP ISO/IEC 27001:2008 con el apoyo de una o más personas externas a la empresa y con los conocimientos necesarios para poder guiar a los colaboradores durante todo el proceso. La toma de esta decisión se basó en tres criterios principales, el cumplimiento del marco legal, el costo efectividad de la implementación de la norma y la recomendación de personal de la ONGEI encargado de ver estos temas a nivel nacional.

Como parte del análisis del proyecto, se presentó un cuadro comparativo entre los requerimientos de capacidades para la implementación de un SGSI y las capacidades actuales de la empresa, como resultado se hizo entrega de una serie de propuestas para preparar a la empresa ante el cambio que deben realizar.

Para la ejecución se recomendó dividir el proyecto en dos, una etapa de análisis y diseño de un SGSI y otra que utilizará los resultados obtenidos para implementar, monitorear y mantener el sistema.

Finalmente, debido a esta división, se recomienda el manejo de un presupuesto para cada etapa ya que no se puede estimar el costo de la implementación del SGSI hasta que no se haya desarrollado el diseño y análisis ya que es ahí donde se identificará cuáles son los riesgos a los que la información de SERPOST se ve expuesta y los controles en los que se deberá invertir para mitigarlos.

5. Anexo 5: Metodología de Valoración de Activos

METODOLOGÍA DE VALORACIÓN DE ACTIVOS

1. INTRODUCCIÓN

El presente documento muestra cual será la metodología utilizada por "Servicios Postales del Perú S.A.", en adelante SERPOST, para la valoración de los activos de información de la empresa, en concordancia con lo propuesto por el anexo B de la ISO/IEC 27005:2008 referente a la identificación y valoración de activos y evaluación de impactos.

2. TÉRMINOS Y DEFINICIONES

Activo: Según la NTP ISO/IEC 27001, un activo es algo que representa valor para la empresa.

3. PERSONAS AUTORIZADAS Y RESPONSABLES

Los únicos usuarios autorizados de este documento son los miembros del Comité de Seguridad de la Información, el personal autorizado de la Sub-Gerencia de Tecnologías de la Información de SERPOST y el Oficial de Seguridad de Información, siendo este último la persona encargada de liderar el equipo que hará uso del documento.

4. METODOLOGÍA DE VALORACIÓN DE ACTIVOS

4.1. Identificación de Activos

Para valorar los activos de información de la empresa, se debe tener un conocimiento previo de que activos se desean valorar, debido a ello, la primera tarea a realizar es la identificación de los activos de información de la empresa.

El oficial de seguridad de la información debe asegurarse de tener actualizada la documentación de los procesos incluidos dentro del alcance del SGSI y de realizar entrevistas a los dueños de los mismos para levantar cualquier información adicional necesaria.

Los activos de información de la empresa serán clasificados de la siguiente manera:

4.1.1.Activos Primarios

Los activos primarios son todos aquellos incluidos dentro de los procesos del alcance del SGSI, así como la información manejada dentro de ellos.

4.1.2.Activos de Soporte

Los activos de soporte son todos aquellos que poseen un vínculo con los activos primarios. Estos pueden ser:

- Hardware (Pc's, Usb, CD's, Servidores)
- Software (Sistemas Operativos, Sistemas In-house, Licencias)
- Redes (Equipos de telecomunicaciones)
- Personal (Personal de la empresa, de proveedores o clientes)
- Lugares (Ambientes dentro y fuera de la organización)

Como resultado de esta identificación se deberá tener un listado de todos los activos involucrados dentro del alcance del SGSI con su descripción, ubicación y su propietario, los cuales deberán ser indicados por los dueños de los procesos del negocio (Ver anexo 1).

4.2. Valoración de Activos

Una vez que se hayan identificado correctamente cuales son los activos involucrados en el alcance del SGSI, el Oficial de Seguridad de la Información debe realizar entrevistas con cada uno de los dueños de los procesos para conocer cuáles son los activos de información más importantes para la organización para protegerlos adecuadamente.

4.2.1.Criterio

Para definir el valor de los activos de información se hará uso de las tres propiedades bases del Sistema de Gestión de Seguridad de la información, la Confidencialidad, la Integridad y la Disponibilidad de los activos.

El nivel de tasación usado para valorar los activos debe responder a la pregunta ¿De qué manera la pérdida del activo impacta a la confidencialidad/integridad/disponibilidad de la información? Para tal efecto se usará la tabla del "Anexo – Escala de Valoración de Activos".

Como resultado, se deberá completar las casillas correspondientes del "Anexo – Inventario y Valoración de Activos" por cada activo de información evaluado.

Aquellos activos cuyo valor promedio de confidencialidad, integridad y disponibilidad sea mayor a 2 deberán ser considerados en el proceso de análisis y evaluación de riesgos.

4.2.2.Herramientas

Las únicas herramientas que se utilizarán para realizar la valoración de los activos serán la entrevista y el Anexo – "Listado y valoración de Activos de Información". La entrevista deberá ser llevada a cabo por el Oficial de Seguridad de la Información o por cualquier persona previamente capacitada y asignada por él.

4.2.3.Frecuencia

Esta valoración deberá ser realizada, como mínimo, una vez al año como parte del proceso de mejora continua del SGSI o cuando exista algún cambio importante en los procesos pertenecientes al alcance actual del SGSI u otros relacionados a los mismos.

6. Metodología de Análisis de Riesgos

METODOLOGÍA DE ANÁLISIS DE RIESGOS

1. INTRODUCCIÓN

El presente documento describe los pasos necesarios para identificar y analizar los riesgos a los que se encuentra expuesta la organización, así como las acciones a realizar para el tratamiento de los mismos, en concordancia con lo propuesto por la ISO/IEC 27005:2008 referente a la Gestión de Riesgos en la Seguridad de la Información.

2. TÉRMINOS Y DEFINICIONES

Amenaza: Según la ISO/IEC 27005:2008, es la causa potencial de un incidente de seguridad de la información no deseado, que puede resultar en un daño para la organización.

Apetito de Riesgo: Es el nivel máximo de riesgo que la organización está dispuesta a aceptar para el logro de sus metas.

Evaluación del Riesgo: Según la NTP ISO 31000:2009, es el proceso general de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Gestión del riesgo: Según la NTP ISO 31000:2009, son las actividades coordinadas para dirigir y controlar una organización en relación al riesgo.

Impacto: Según la ISO/IEC 27005:2008, son cambios adversos al nivel de objetivos de negocio logrados.

Probabilidad: Posibilidad de que se materialice el riesgo, es decir, que se produzca un ataque exitoso de la amenaza, tomando en cuenta las vulnerabilidades y los controles existentes.

Riesgo: Es la combinación de la probabilidad de un ataque exitoso de la amenaza, y las consecuencias que acarrea dicho ataque (impacto).

Riesgo Residual: Según la NTP ISO 31000:2009, es el nivel de riesgo restante luego de realizar el tratamiento de riesgos.

Vulnerabilidad: Es la debilidad de un activo o grupo de activos o controles, que puede ser explotadas por una o varias amenazas de acuerdo a su ubicación. Una vulnerabilidad en sí misma no causa daños.

3. PERSONAS AUTORIZADAS Y RESPONSABLES

La ejecución de lo indicado en este documento se encuentra a cargo del Oficial de Seguridad de la Información, el Comité de Seguridad de la Información y de cualquier persona autorizada por la Sub Gerencia de Tecnologías de Información.

4. METODOLOGÍA DE EVALUACIÓN DE RIESGOS

4.1. Identificación de Amenazas y Vulnerabilidades

Como parte del ciclo de vida del Sistema de Gestión de Seguridad de Información, es necesario realizar la identificación de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de información e identificar las debilidades en la seguridad de la información que puedan amenazar a los activos de información de la empresa.

El Oficial de Seguridad de la Información, deberá llenar el formato del Anexo – "Matriz de Riesgos", con la información obtenida tras entrevistar a los dueños de los procesos según lo descrito en los siguientes pasos:

4.1.1.Identificación de Amenazas

Una amenaza tiene el potencial de dañar activos como sistemas, procesos o información, por ello, es muy importante identificar cuáles son las amenazas principales a los que los activos de información están expuestos.

El Oficial de Seguridad de la Información, junto con un personal debidamente capacitado, debe realizar entrevistas a los dueños de los procesos con la intención de identificar las amenazas a las que los activos se encuentran expuestas, para ello podrá hacer uso de una lista de amenazas ubicadas en el Anexo – "Lista de Ejemplos de Vulnerabilidades y Amenazas" obtenido del "Anexo D" de la ISO/IEC 27005:2008.

4.1.2.Identificación de Vulnerabilidades

Las vulnerabilidades por sí mismas no pueden ocasionar daños en los activos de información ya que necesitan de alguna amenaza que las exploten; sin embargo, es necesario que sean debidamente identificadas en caso suceda algún cambio que implique la aparición de una nueva amenaza.

El Oficial de Seguridad de la Información, junto con un personal debidamente capacitado, debe realizar entrevistas a los dueños de los procesos para la identificación de estas vulnerabilidades, para ello podrá hacer uso de una lista de vulnerabilidades ubicadas en el Anexo – "Lista de Ejemplos de Vulnerabilidades y Amenazas" obtenido del "Anexo D" de la ISO/IEC 27005:2008, el cual servirá como guía para esta labor.

4.2. Identificación y Evaluación de Riesgos

Con ayuda de las amenazas y vulnerabilidades se podrá identificar fácilmente cuales son los riesgos que amenazan la información y se podrá tomar medidas que ayuden a protegerla.

4.2.1.Identificación de Riesgos

El riesgo se definirá como la probabilidad que una amenaza explote una vulnerabilidad de un activo haciéndole perder alguna propiedad relacionada a la seguridad de la información (confidencialidad, disponibilidad, integridad, auditabilidad, etc.)

Una vez identificado el riesgo deberá ser ingresado en el Anexo – "Matriz de Riesgos"

4.2.2.Determinación de Probabilidad e Impacto

El Oficial de Seguridad de la Información en conjunto con los dueños de los activos de información, deben contestar las siguientes preguntas para determinar la probabilidad de ocurrencia de una amenaza:
¿Ya ha sucedido antes?, ¿Pasa muy seguido? y ¿Podría suceder?

Para realizar esta valoración se recomienda revisar la siguiente tabla de lista de probabilidades:

Lista de Probabilidades			
Nivel	**Descripción**	**Escala de porcentaje**	**Probabilidad**
5	Muy Alta	Más de 80%	Ocurrirá en la mayoría de las circunstancias; todos los días o varias veces al mes.
4	Alta	60% - 80%	Probablemente ocurrirá en la mayoría de las circunstancias; al menos una vez al mes.
3	Moderada	40% - 60%	Puede ocurrir en algún momento; al menos una vez al año.
2	Baja	20% - 40%	Podría ocurrir en algún momento; al menos una vez cada dos años.
1	Muy Baja	Menos de 20%	Puede ocurrir en circunstancias excepcionales; como dos veces cada cinco años.

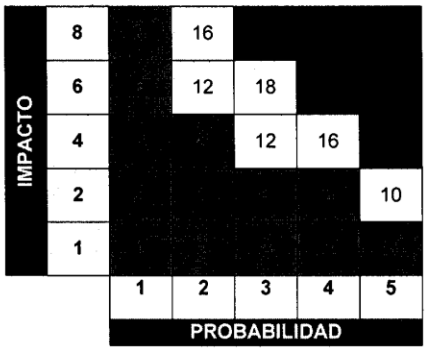
De igual forma, deben determinar cuál es el impacto que tendría la materialización de la amenaza considerando la vulnerabilidad y los controles existentes.

Para realizar esta valoración se recomienda revisar la siguiente tabla de lista de impactos:

Lista de Niveles de Impacto		
Nivel	**Descriptivo**	**Explicación**
8	Catastrófica	Pérdida o daño catastrófico a la reputación de la organización; pérdidas financieras importantes, cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves; pérdida de clientes a gran escala; involucramiento directo de la alta gerencia o directorio.
6	Mayor	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector; cobertura a nivel nacional; investigación del regulador y sanciones por falta grave; involucramiento de la alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
4	Moderado	El impacto sobre la compañía es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio.
2	Menor	Riesgo aceptable en el sector; no hay daño a la reputación, no hay sanciones legales, pero si observaciones por parte de los reguladores, el impacto operacional o financiero es mínimo.
1	Insignificante	No hay impacto directo sobre la organización, no hay daño a la reputación, no existen sanciones legales ni impacto financiero u operacional; no es percibido por los clientes pero si por los colaboradores.

4.2.3. Evaluación del nivel y valor del Riesgo

El nivel de los riesgos se obtendrá de la multiplicación de la probabilidad y el impacto previamente definido por los dueños de los procesos lo cual permitirá ubicar al riesgo en uno de las siguientes celdas:



Una vez se obtenga el nivel de los riesgos, estos deberán ser clasificados según los siguientes niveles de riesgo mostrados en la siguiente tabla.

Riesgo	Nivel de Riesgo
1 – 8	Riesgo Bajo
9 - 18	Riesgo Alto
19 - 40	Riesgo Grave

4.2.4.Apetito del Riego

El Comité de Seguridad de la Información es el responsable de aprobar el apetito del riesgo de la organización, en tal sentido, se ha definido:

- *Riesgos Bajos*: Riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la organización. Es hasta este punto en el cual se define el Apetito de Riesgo de SERPOST, es decir, aquellos riesgos que ***no se encuentren*** en esta zona deberán ser tratados para minimizar su valor.
- *Riesgos Altos*: Riesgos que deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.
- *Riesgos Graves*: Riesgos que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

4.2.5.Tratamiento del Riesgo

El Oficial de Seguridad de la Información debe actualizar el Anexo – "Matriz de Riesgos" con los datos hallados en los pasos anteriores, una vez realizado esto deberá identificar quien o quienes son los responsables del tratamiento de los riesgos y evaluar los tipos de tratamiento más apropiadas teniendo en cuenta el siguiente cuadro:

Tratamiento	Descripción
Mitigar	Reducir los riesgos mediante la implementación de controles que reduzcan el riesgo a un nivel aceptable. Estos controles deberán presentar una documentación adecuada para su implementación y puesta en marcha.
Aceptar	En este escenario se decide no tratar el riesgo debido a no haber identificado controles adecuados para el tratamiento de los riesgos o haber identificado que el costo de implementar algún control es mayor que los beneficios que se obtendrán. Toda aceptación del riesgo debe ser documentada y firmada por el Comité de Seguridad de la Información indicando los criterios de esta decisión. Por último, deberán ser constantemente monitoreados en caso evolucionen y se conviertan en riesgos más graves.
Transferencia	Alternativa más económica en caso sea muy costoso o difícil reducir o controlar un riesgo. Sin embargo, al transferir un riesgo no se transfiere las responsabilidades por lo que deberán ser constantemente monitoreadas para asegurarnos de su correcto tratamiento.
Eliminar	Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un activo, proceso o del área del negocio que es fuente de riesgo. Este plan de tratamiento debe estar debidamente justificado y documentado en caso se decida implementar. Adicionalmente se debe realizar un nuevo Análisis de Riesgo teniendo en cuenta el cambio realizado en la organización.

4.2.6.Controles

Una vez identificados y evaluados cada uno de los riesgos que amenazan a los activos claves de la organización, el oficial de seguridad de la información, con la ayuda de la NTP ISO/IEC 17999, deberá identificar qué controles ha de implementar para reducir el impacto o la probabilidad de los mismos hasta llevarlos a un nivel aceptable e introducir esta información dentro de la matriz de riesgo, a fin de mantener un registro de estos datos.

Adicionalmente, se deberá indicar que tipo control se ha seleccionado, según la tabla que se muestra a continuación:

Tipo de Control	Descripción
Preventivo	Como su nombre lo indica, son controles que buscan prevenir la materialización de un riesgo, mediante un adecuado control de las ***vulnerabilidades*** de un activo.
Detectivo	Este tipo de controles busca ***descubrir*** nuevos riesgos antes que se materialicen, de tal forma, que puedan ser controlados con anticipación
Correctivo	Son controles que se encargan de corregir alguna incidencia minimizando el ***impacto*** del daño o pérdida originada por el riesgo.
Disuasivo	Son controles que buscan reducir la ***probabilidad*** de ocurrencia de algún riesgo.

4.2.7.Riesgo Residual

El Oficial de Seguridad de la Información debe realizar un seguimiento en el tiempo y revisar cada uno de los controles implementados para asegurar que exista una verdadera reducción de la probabilidad o impacto del riesgo.

De igual forma, una vez al año, se deberá evaluar los riesgos residuales, en caso se detecten algunos riesgos con valores superiores al apetito de riesgo de la empresa se tomarán medidas correctivas para disminuir los riesgos a un nivel aceptable.

7. Anexo 7: Inventario y Valoración de Activos

Serpost El Correo del Perú

Anexo 7 - Inventario Total y Valoración de Activos

		Proceso		Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
1	Recepción	Admisión	Recibir una copia del contrato	Orden de Servicio	Documento perteneciente al área comercial, en ella se tiene cada uno de los pedidos realizados por los cliente. Entre los datos que se tienen almacenados se tiene: - Nombre del cliente - Inicio y termino -Plazos de distribución - Tipo (nacional o local)	Primario	Gerencia Postal	---	Area comercial	Files de almacenamiento	---	x				---	2	1	3	2,0
1	Recepción	Habilitado	Habilitar envíos para envíos nacionales o locales	Orden de Servicio		Primario	---	---	Área Comercial	Files de almacenamiento	---	x				---	2	1	3	2,0
2	Recepción	Admisión	Recoger Envíos	Guia de recepción	Documento que viene en forma de talonario, en el se guarda, por numero correlativo, el envío que se esta recibiendo de los clientes. Se trabaja con 3 copias, una es para los postrenes, otra para los clientes y una última para el área Extrapostal	Primario	---	---	Supervisor de Extra Postales	Almacenados en un file de guias de recpción	---	x				---	2	1	1	1,3
2	Recepción	Admisión	Recibe envíos con su guía	Guia de recepción		Primario	---	Postrén Cliente	Supervisor de Extra Postales	Almacenados en un file de guias de recpción	---	x				---	2	1	1	1,3
2	Recepción	Admisión	Verificar Información	Guia de recepción		Primario	---	---	Supervisor de Extra Postales	Almacenados en un file de guias de recpción	---	x				---	2	1	1	1,3
2	Recepción	Habilitado	Recepción y cierre de guía de recepción y salida	Guia de recepción		Primario	---	---	Supervisor de Extra Postales	Almacenados en un file de guias de recpción	---	x				---	2	1	1	1,3
2	Recepción	Admisión	Entrega Envíos al Area de Extra Postales	Guia de recepción		Primario	---	---	Supervisor de Extra Postales	Almacenados en un file de guias de recpción	---	x				---	2	1	1	1,3
3	Recepción	Admisión	Recoger Envíos	Envios	Cada uno de los envíos que el cliente hace entrega para que lleguen a una serie de desinatarios	Primario	Clientes	---	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Admisión	Entrega Envíos al Area de Extra Postales	Envios		Primario	Clientes	---	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Admisión	Contar Envíos Físicos	Envios		Primario	Clientes	---	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Admisión	Verificar Información	Envios		Primario	Clientes	---	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Admisión	Ordenar envíos para habilitado	Envios		Primario	---	Habilitado	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Habilitado	Etiquetado de código de barras	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Habilitado	Habilitar envíos para envíos nacionales o locales	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Habilitado	Enviar paquetes a despacho nacional	Envios		Primario	---	Despachos Nacionales	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Recepción	Habilitado	Enviar paquetes al área de clasificación	Envios		Primario	---	Departamento de Clasificación	Cliente	Ubicada dentro del área	---	x				---	2	1	3	2,0
3	Clasificación	Clasificación	Recepcionar envíos con guía de salida	Envios	Cada uno de los envíos entregados por los clientes que deben ser entregados a sus destinatarios	Primario	Extra Postales	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Clasificación	Recepcionar envíos con la nueva guía de salida	Envios		Primario	Extra Postales	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Clasificación	Preparar envíos para pre clasificación	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Separar grupos de envíos por distritos y/o administraciones	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Seleccionar grupos de envíos por cada guia de salida	Envios		Primario	Adminitración postal	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7

Id Activo	Proceso	Proceso	Proceso	Activo de Información	Activo de Información	Activo de Información	Interacción con otras áreas	Interacción con otras áreas	Propietario del Activo de Información	Ubicación de los Activos de Información	Ubicación de los Activos de Información	Formatos	Formatos	Formatos	Formatos	Clasificación Actual del Activo de Información	Valoración	Valoración	Valoración	Valoración
	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida		Física	Lógica	Papel	Electrónico	Verbal	Otros		Confidencialidad	Integridad	Disponibilidad	Promedio
3	Clasificación	Pre Clasificación	Distribuir los envíos según el cuadro de administración correpondiente	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Contar y comparar los envíos recibidos con las guias de salida	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Clasificación	Devolver a operador envíos y guía de salida	Envios		Primario	---	Extra Postales	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Devolver a operador envíos y guía de salida	Envios		Primario	---	Extra Postales	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Entregar grupos de envíos a clasificadores finales	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Devolver los envios mal asignados para su correcta pre clasificación	Envios		Primario	---	Extra Postales	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Clasificación	Sectorizar envíos de acuerdo a la administración correpondiente	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Clasificación	Separar y remitir los envíos a cada administración por cliente y guía	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Realizar conteo de envíos de la guía registrada	Envios		Primario	---	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Solicitar revisar y resolver inconsistencia	Envios		Primario	---	Extra Postales	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Examinar y corregir la inconsistencia informada	Envios		Primario	Clasificación	Clasificación	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
3	Clasificación	Pre Clasificación	Recibir respuesta por parte del operador extrapostal	Envios		Primario	Extra Postales	---	Cliente	Ubicada dentro del área	---	x				---	2	1	2	1,7
4	Recepción	Admisión	Generar guía de admisión	Computadora de Escritorio	Computadoras utilizadas por el personal para realizar labores como el importado de las bases de datos, impresión de etiquetas, etc.	Soporte	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---				x	---	--	2	3	2,5
4	Recepción	Habilitado	Importar la Base de Datos de los clientes	Computadora de Escritorio		Soporte	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---				x	---	--	2	3	2,5
4	Recepción	Habilitado	Digitar los Envíos	Computadora de Escritorio		Soporte	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---				x	---	--	2	3	2,5
4	Clasificación	Pre Clasificación	Realizar consulta de envíos registrados en el sistema	Computadora de Escritorio	Computadoras utilizadas por el personal para realizar labores como el importado de las bases de datos, impresión de etiquetas, etc.	Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Clasificación	Pre Clasificación	Registrar cada grupo en el sistema según la administración correspondiente	Computadora de Escritorio		Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Clasificación	Pre Clasificación	Eliminar los registros de los envíos por cada guia procesada	Computadora de Escritorio		Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Clasificación	Pre Clasificación	Actualizar y/o corregir registros la inconsistencia registrada en cada administración postal	Computadora de Escritorio		Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Clasificación	Clasificación	Firmar guias de salida conformes e ingresar al datos al sistema	Computadora de Escritorio		Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Clasificación	Clasificación	Enviar copias a otras áreas	Computadora de Escritorio		Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Control de Cargos	Control de cargos	Digitar cargos y rezagos en el sistema	Computadora de Escritorio	Computadoras utilizadas por el personal para realizar labores como el importado de las bases de datos, impresión de etiquetas, envíos de correos, etc.	Soporte	---	---	Supervisor del área de Control de Cargos	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Control de Cargos	Control de cargos	Elaborar y remitir el reporte de cargos pendientes	Computadora de Escritorio		Soporte	---	---	Supervisor del área de Control de Cargos	Ubicada dentro del área	---				x	---	--	3	3	3,0

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
	Proceso			Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
4	Control de Cargos	Control de cargos	Elaborar guía o reporte de devolución	Computadora de Escritorio		Soporte	---	---	Supervisor del área de Control de Cargos	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Control de Cargos	Control de cargos	Remitir reportes de facturación físicos o digitales	Computadora de Escritorio		Soporte	---	---	Supervisor del área de Control de Cargos	Ubicada dentro del área	---				x	---	--	3	3	3,0
4	Digitalización	Digitalización	Digitar cargos y rezagos por fecha y por motivo	Computadora de Escritorio	Computadoras utilizadas por el personal para realizar labores como el importado de las bases de datos, impresión de etiquetas, etc.	Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Digitalización	Transferir imágenes escaneadas a carpetas del servidor	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Elaboración de Reportes y CD's	Elaborar base de datos y remitir información vía email al cliente	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Elaboración de Reportes y CD's	Generar el backup por cliente detallando los meses de los clientes digitalizados	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Digitalización	Generar reporte diario para la devolución de cargos	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Elaboración de Reportes y CD's	Realizar consolidado SAT	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Elaboración de Reportes y CD's	Elaborar cuadro de reporte	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
4	Digitalización	Elaboración de Reportes y CD's	Obtener imágenes y renombrarlas según el número de guía	Computadora de Escritorio		Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	3	3	3,0
5	Recepción	Admisión	Generar guía de admisión	Modulo SUNARP	Modulo de un sistema que srve para la atención del cliente SUNARP	Soporte	---	---	Supervisor de Extra Postales	---	Aplicación		x			---	2	3	3	2,7
6	Recepción	Admisión	Generar guía de admisión	SIM 2.0	Sistema Integrado de Mensajeria, sistema utilizado por los operadores postales para la realización de su trabajo	Soporte	---	---	Supervisor de Extra Postales	---	Aplicación		x			---	2	3	3	2,7
6	Recepción	Habilitado	Etiquetado de código de barras	SIM 2.0		Soporte	---	---	Supervisor de Extra Postales	---	Aplicación		x			---	2	3	3	2,7
6	Recepción	Habilitado	Verificación del Sistema Según Guia de Salida	SIM 2.0		Soporte	---	---	Supervisor de Extra Postales	---	Aplicación		x			---	2	3	3	2,7
6	Control de Cargos	Control de cargos	Contar cargos y rezagos e ingresar datos al sistema	SIM 2.0	Sistema Integrado de Mensajeria, utilizado por los operadores postales para el cumplimiento de sus labores	Soporte	---	---	Operador Postal	---	Aplicación		x			---	2	2	3	2,3
6	Control de Cargos	Control de cargos	Digitar cargos y rezagos en el sistema	SIM 2.0		Soporte	---	---	Operador Postal	---	Aplicación		x			---	2	2	3	2,3
6	Digitalización	Elaboración de Reportes y CD's	Realizar consolidado SAT	SIM 2.0	Sistema utilizado por los operadores postales del área de control de cargos para ingresar el numero de guia, la fecha del cargo, motivo, entregado o rezagado. En el caso del ministerio de producción se especifica quien recibió el cargo y numero DNI.	Soporte	---	---	Encargado del Área	---	Aplicación		x			---	2	3	3	2,7
6	Digitalización	Digitalización	Generar reporte diario para la devolución de cargos	SIM 2.0		Soporte	---	---	Encargado del Área	---	Aplicación		x			---	2	3	3	2,7
6	Digitalización	Digitalización	Digitar cargos y rezagos por fecha y por motivo	SIM 2.0		Soporte	---	---	Encargado del Área	---	Aplicación		x			---	2	3	3	2,7
6	Digitalización	Digitalización	Transferir imágenes escaneadas a carpetas del servidor	SIM 2.0		Soporte	---	---	Encargado del Área	---	Aplicación		x			---	2	3	3	2,7
7	Recepción	Admisión	Generar guía de admisión	Cuaderno de guia de admisión	Cuaderno donde se realizan las guias de admisión, para facilitar el trabajo se inicia una nueva númeración todos los años con un número que termine en 1 (1001,5001,10001, etc)	Primario	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---	x				---	2	1	1	1,3
7	Recepción	Habilitado	Cierre de guías de admisión	Cuaderno de guia de admisión		Primario	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---	x				---	2	1	1	1,3
8	Recepción	Admisión	Ordenar envíos para habilitado	Cuaderno de control de operadores postales	Documento en el cual se queda registrado cada uno de los envios que son entregados para el habilitado	Primario	---	---	Operador Postal	Archivado en el área	---	x				---	2	1	1	1,3
9	Recepción	Habilitado	Etiquetado de código de barras	Etiquetadoras	Se poseen dos maquinas que se encargan de imprimir etiquetas para adjuntar a los envíos	Soporte	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---				x	---	--	--	3	3,0

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
	Proceso			Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
10	Recepción	Habilitado	Digitar los Envíos	Formatos de cargos	Formatos de cargos utilizados por los trabajadores cuando los clientes no tienen una BBDD, usualmente se encuentra dentro de los contratos con los clientes	Primario	Gerencia Comercial	---	Supervisor de Extra Postales	---	Excel guardado en la computadora del supervisor		x			---	2	2	3	2,3
11	Recepción	Habilitado	Imprimir formato de cargos	Impresoras comunes	Herramientas utilizadas para imprimir en el área	Soporte	---	---	Supervisor de Extra Postales	---	---				x	---	--	--	3	3,0
11	Recepción	Habilitado	Imprimir y cortar cargos	Impresoras comunes		Soporte	---	---	Supervisor de Extra Postales	---	---				x	---	--	--	3	3,0
11	Control de Cargos	Control de cargos	Elaborar guía o reporte de devolución	Impresoras comunes	Herramientas utilizadas para imprimir en el área	Soporte	---	---	Supervisor del área de Control de Cargos	---	---				x	---	--	--	3	3,0
11	Control de Cargos	Emitir Reporte de Facturación	Remitir reportes de facturación físicos o digitales	Impresoras comunes		Soporte	---	---	Supervisor del área de Control de Cargos	---	---				x	---	--	--	3	3,0
12	Recepción	Habilitado	Imprimir formato de cargos	Carpeta compartida EXTRAPOSTALES	Carpeta compartida por todo el área de extrapostales para compartir información que crean necesaria	Soporte	---	---	Subgerencia de TI	---	Ubicada en el Servidor		x			---	2	2	3	2,3
12	Recepción	Habilitado	Importar la Base de Datos de los clientes	Carpeta compartida EXTRAPOSTALES		Soporte	---	---	Subgerencia de TI	---	Ubicada en el Servidor		x			---	2	2	3	2,3
13	Recepción	Habilitado	Importar la Base de Datos de los clientes	Backup de los correos recibidos	Backup generado tras archivar los correos recibidos por los cliente con las bases de datos recibidas	Soporte	---	---	Supervisor de Extra Postales	---	Almacenado en la misma computadora del supervisor (archivados)		x			----	2	2	3	2,3
14	Recepción	Habilitado	Importar la Base de Datos de los clientes	Correos de los clientes	Correos enviados por los clientes que poseen las bases de datos con las que trabaja el personal de SERPOST	Primario	Clientes	---	Supervisor de Extra Postales	----	Alamcenada en los correos		x			---	2	2	3	2,3
15	Recepción	Habilitado	Importar la Base de Datos de los clientes	BBDD de los clientes	Base de datos de los clientes dond se muestra quienes deben ser los destinatarios y sus direcciones	Primario	Clientes	---	Supervisor de Extra Postales		Almacenado en la misma computadora del supervisor		x			---	3	2	2	2,3
16	Recepción	Habilitado	Importar la Base de Datos de los clientes	Base original de clientes por año	Base de datos de los envios de los clientes acumulados hasta el momento	Primario	---	---	Supervisor de Extra Postales	---	Almacenado en la misma computadora del supervisor		x			---	3	2	2	2,3
17	Recepción	Habilitado	Imprimir y cortar cargos	Impresora High Speed	Utilizada para imprimir etiquetas High Peed, usado en caso se tengan cantidades masivas (más de 3000 etiquetas)	Soporte	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---				x	---	--	--	3	3,0
18	Recepción	Habilitado	Elaborar la guia de salida	Guia de Salida (SEL)	Documento pre impreso que se realiza a mano. Contiene datos como la fecha, el cliente, el numero de guia de admision, cantidad de envíos.	Primario	---	---	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
18	Recepción	Habilitado	Enviar paquetes a despacho nacional	Guia de Salida (SEL)		Primario	---	Despachos Nacionales	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
18	Recepción	Habilitado	Enviar paquetes al área de clasificación	Guia de Salida (SEL)		Primario	---	Departamento de Clasificación	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
18	Clasificación	Pre Clasificación	Realizar conteo de envíos de la guía registrada	Guia de Salida (SEL)	Documento pre impreso que se realiza a mano. Contiene datos como la fecha, el cliente, el numero de guia de admision, cantidad de envíos.	Primario	Extra Postales	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Clasificación	Recepcionar envíos con guía de salida	Guia de Salida (SEL)		Primario	Extra Postales	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Clasificación	Solicitar correción de datos	Guia de Salida (SEL)		Primario	---	Extra Postales	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Clasificación	Corregir datos de la guía de salida	Guia de Salida (SEL)		Primario	Extra Postales	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Clasificación	Recepcionar envíos con la nueva guía de salida	Guia de Salida (SEL)		Primario	Extra Postales	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Separar grupos de envíos por distritos y/o administraciones	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Realizar consulta de envíos registrados en el sistema	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Seleccionar grupos de envíos por cada guia de salida	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Distribuir los envíos según el cuadro de administración correpondiente	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Contar y comparar los envíos recibidos con las guias de salida	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7

Id Activo	Proceso			Activo de Información			Interacción con otras áreas		Propietario del Activo de Información	Ubicación de los Activos de Información		Formatos				Clasificación Actual del Activo de Información	Valoración			
	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida		Física	Lógica	Papel	Electrónico	Verbal	Otros		Confidencialidad	Integridad	Disponibilidad	Promedio
18	Clasificación	Clasificación	Devolver a operador envíos y guía de salida	Guia de Salida (SEL)		Primario	---	Extra Postales	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Devolver a operador envíos y guía de salida	Guia de Salida (SEL)		Primario	---	Extra Postales	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Solicitar revisar y resolver inconsistencia	Guia de Salida (SEL)		Primario	---	Extra Postales	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Examinar y corregir la inconsistencia informada	Guia de Salida (SEL)		Primario	Clasificación	Clasificación	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Recibir respuesta por parte del operador extrapostal	Guia de Salida (SEL)		Primario	Extra Postales	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Entregar grupos de envíos a clasificadores finales	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Devolver los envios mal asignados para su correcta pre clasificación	Guia de Salida (SEL)		Primario	---	---	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Pre Clasificación	Rectificar las guias de salida con la correcta cantidad de envíos por administración postal	Guia de Salida (SEL)		Primario	---	Extra Postales	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
18	Clasificación	Clasificación	Sectorizar envíos de acuerdo a la administración correpondiente	Guia de Salida (SEL)		Primario	---	Extra Postales	Extra Postales	Ubicada dentro del área	---	x				---	2	3	3	2,7
19	Recepción	Habilitado	Verificación del Sistema Según Guia de Salida	Guia de Salida con Conformidad de Clasificación	Una vez que el área de clasificación realiza sus procesos devuelve la guia de salida SEL con su conformidad	Primario	---	---	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
19	Recepción	Habilitado	Recepción de confirmación de guia	Guia de Salida con Conformidad de Clasificación		Primario	Clasificación Final Despacho Nacional	---	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
19	Recepción	Habilitado	Revisión y cierre de guía de recepción y guia de salida	Guia de Salida con Conformidad de Clasificación		Primario	---	---	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
19	Clasificación	Clasificación	Firmar guias de salida conformes e ingresar al datos al sistema	Guia de Salida con Conformidad de Clasificación	Una vez que el área de clasificación realiza sus procesos devuelve la guia de salida SEL con su conformidad	Primario	---	---	Extra Postales	Ubicada dentro del área	Almacenado en la base de datos del sistema SOP	x	x			---	2	3	3	2,7
19	Clasificación	Clasificación	Enviar copias a otras áreas	Guia de Salida con Conformidad de Clasificación		Primario	---	Extra Postales Control de Cargos	Extra Postales	Ubicada dentro del área	Almacenado en la base de datos del sistema SOP	x	x			---	2	3	3	2,7
20	Recepción	Habilitado	Verificación del Sistema Según Guia de Salida	Pistola lectora de código de barras	Pistola utilizada para agilizar la comprobación de las guias en físico mediante el pistoleado y comprobación con le sistema	Soporte	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---				x	---	--	--	1	1,0
20	Control de Cargos	Control de cargos	Elaborar guía o reporte de devolución	Pistola lectora de código de barras	Pistola utilizada para agilizarel ingreso de guías físicas al sistema	Soporte	---	---	Operador Postal	Ubicada dentro del área	---		x			---	2	2	3	2,3
20	Clasificación	Pre Clasificación	Registrar cada grupo en el sistema según la administración correspondiente	Pistola lectora de código de barras	Pistola utilizada para agilizar la comprobación de las guias en físico mediante el pistoleado y comprobación con el sistema	Soporte	---	---	Supervisor	Ubicada dentro del área	---				x	---	--	--	3	3,0
20	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	Pistola lectora de código de barras	Solo se utiliza en caso de que los cargos tengan código de barra, en caso de contrario se debe digitar el cargo de manera manual , como en el caso del cliente "Ministerio de Justicia"	Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	--	3	3,0
21	Recepción	Habilitado	Verificación del Sistema Según Guia de Salida	Reporte de guia de salida impreso	Se imprimen 4 copias de un reporte de guias de salida.	Primario	---	---	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
21	Recepción	Habilitado	Enviar guia de admisión para aprobación	Reporte de guia de salida impreso	Se envían 4 copias al cliente, una queda para ellos, las otras tres regresan para las áreas interesadas	Primario	---	Cliente	Supervisor de Extra Postales	---	---	x				---	2	1	2	1,7
21	Recepción	Habilitado	Recibir aprobación del cliente	Reporte de guia de salida impreso		Primario	Cliente	---	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7
21	Recepción	Habilitado	Enviar guias de admisión a otras áreas	Reporte de guia de salida impreso		Primario	---	Facturación Control de Cargos	Supervisor de Extra Postales	Files de almacenamiento	---	x				---	2	1	2	1,7

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
	Proceso			Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
22	Clasificación	Clasificación	Solicitar correción de datos	Boletin de verificación de clasificación	Solo se entregan a las administraciones postales que presentaran alguna observación o incidencia. Se envían por medios oficiales para que conozcan que hubo un error a la hora de confeccionar sus despachos	Primario	---	Adm Postales	Supervisor	Administraciones postales	---	x				---	3	2	3	2,7
23	Clasificación	Clasificación	Solicitar correción de datos	File de boletines de verificación de clasificación	Archivador donde se guardan los boletines de verificación una vez se remitieron a las administraciones postales	Primario	---	---	Supervisor	Almacenado dentro del departamento de clasificación	---	x				---	2	2	3	2,3
24	Clasificación	Pre Clasificación	Registrar cada grupo en el sistema según la administración correspondiente	SOP Empresarial	Sistema Operativo Postal, aplicación utilizada por los operadores postales del área de clasificación para el desarrollo de su trabajo	Soporte	---	---	Supervisor	---	Aplicación				x	---	2	3	3	2,7
24	Clasificación	Pre Clasificación	Realizar consulta de envíos registrados en el sistema	SOP Empresarial		Soporte	---	---	Supervisor	---	Aplicación				x	---	2	3	3	2,7
24	Clasificación	Pre Clasificación	Eliminar los registros de los envíos por cada guia procesada	SOP Empresarial		Soporte	---	---	Supervisor	---	Aplicación				x	---	2	3	3	2,7
24	Clasificación	Pre Clasificación	Actualizar y/o corregir registros la inconsistencia registrada en cada administración postal	SOP Empresarial		Soporte	---	---	Supervisor	---	Aplicación				x	---	2	3	3	2,7
24	Clasificación	Clasificación	Firmar guias de salida conformes e ingresar al datos al sistema	SOP Empresarial		Soporte	---	---	Supervisor	---	Aplicación				x	---	2	3	3	2,7
24	Clasificación	Clasificación	Enviar copias a otras áreas	SOP Empresarial		Soporte	---	---	Supervisor	---	Aplicación				x	---	2	3	3	2,7
25	Clasificación	Pre Clasificación	Realizar consulta de envíos registrados en el sistema	Reporte ingreso de envios	Reporte realizado en el SOP para conocer cuantos envios ingresaron en el sistema. Por lo general no se imprime	Primario	---	---	Clasificador	---	Reporte del SOP solo mostrado en pantalla		x			---	2	3	3	2,7
26	Clasificación	Clasificación	Separar y remitir los envíos a cada administración por cliente vgwia	Block de control de envíos SEL	Todo los envíos a administración, guias cantidades desglozados por sectores	Primario	---	---	Clasificador	Ubicada dentro del área	---	x				---	2	1	2	1,7
26	Clasificación	Clasificación	Confeccionar despachos y remitir envios para salida final	Block de control de envíos SEL		Primario	---	---	Clasificador	Ubicada dentro del área	---	x				---	2	1	2	1,7
27	Clasificación	Clasificación	Confeccionar despachos y remitir envios para salida final	Guia general de sacas	Guia general de sacas es el consolidado de todo lo que se está sacando. Una copia se queda en clasificación	Primario	---	Adminitración postal	Clasificador	Administraciones postales	---	x				---	2	1	2	1,7
27	Clasificación	Clasificación	Evacuar carga en vehículos para distribución	Guia general de sacas		Primario	---	Adminitración postal	Clasificador	Administraciones postales	---	x				---	2	1	2	1,7
28	Clasificación	Clasificación	Confeccionar despachos y remitir envios para salida final	Sacas	Paquetes de envíos listos para ser enviados a las distintos centros de distribución	Primario	---	Adminitración postal	Clasificador	Administraciones postales	---				x	---	2	1	2	1,7
28	Clasificación	Clasificación	Evacuar carga en vehículos para distribución	Sacas		Primario	---	Adminitración postal	Clasificador	Administraciones postales	---				x	---	2	1	2	1,7
29	Clasificación	Clasificación	Evacuar carga en vehículos para distribución	Cuaderno de control de despachos	Especifica la cantidad de sacas por centro de distribución	Primario	Adminitración postal	Adminitración postal	Clasificador	Ubicada dentro del área	---	x				---	2	3	3	2,7
30	Clasificación	Clasificación	Evacuar carga en vehículos para distribución	File de guias de salidas	Se archivan las guias de salidad	Primario	---	Callao (Luego de 2 años)	Operador de sistema postal	Ubicada dentro del área	---	x				---	2	3	3	2,7
31	Clasificación	Clasificación	Enviar copias a otras áreas	Cuaderno de control de guias de salida para extrapostales	Cuaderno donde se coloca el numero de guia que se le entrega al área según la fecha	Primario	Extrapostales	Extrapostales	Operador de sistema postal	Ubicada dentro del área	---	x				---	2	3	3	2,7
32	Clasificación	Clasificación	Enviar copias a otras áreas	cuaderno de control de guias de salidas	Cuaderno donde se coloca el numero de guia que se le entrega al área según la fecha	Primario	Control de Cargos	Control de Cargos	Operador de sistema postal	Ubicada dentro del área	---	x				---	2	3	3	2,7
33	Control de Cargos	Control de cargos	Recepcionar despachos de cargos y rezagos	Despacho de cargos y rezagos	Todos los paquetes de cargos que llegan al área de control de cargos	Primario	Administracion Postal	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
33	Control de Cargos	Control de cargos	Verificar y distribuir despachos al personal	Despacho de cargos y rezagos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
33	Control de Cargos	Control de cargos	Verificar cantidades de cargos y rezagos	Despacho de cargos y rezagos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7

Id Activo	Proceso			Activo de Información			Interacción con otras áreas		Propietario del Activo de Información	Ubicación de los Activos de Información		Formatos				Clasificación Actual del Activo de Información	Valoración			
	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida		Física	Lógica	Papel	Electrónico	Verbal	Otros		Confidencialidad	Integridad	Disponibilidad	Promedio
34	Recepción	Habilitado	Imprimir y cortar cargos	Cargos	Cada uno de los cargos que servirán para evidenciar la entrega de los envíos	Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	2	3	2,3
34	Recepción	Habilitado	Imprimir formato de cargos	Cargos		Primario	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---	x				---	2	2	3	2,3
34	Control de Cargos	Control de cargos	Entregar cargos y rezagos al responsable de cada cliente	Cargos	Cada uno de los cargos que envidencia la entrega de algún envío	Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Control de Cargos	Control de cargos	Clasificar cargos y rezagos por cliente y guia de admisión	Cargos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Control de Cargos	Control de cargos	Contar cargos y rezagos e ingresar datos al sistema	Cargos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Control de Cargos	Control de cargos	Efectuar control de calidad según directiva del cliente	Cargos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Control de Cargos	Control de cargos	Devolver cargos y rezagos con memorándum	Cargos		Primario	---	Administracion Postal	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Control de Cargos	Control de cargos	Entregar cargos y rezagos a digitalización	Cargos		Primario	---	Digitalización	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Control de Cargos	Control de cargos	Digitar cargos y rezagos en el sistema	Cargos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
34	Digitalización	Digitalización	Recepcionar cargos y rezagos por cliente	Cargos	Cada uno de los cargos que son enviados por el área de control de cargos pasra su digitalización	Primario	Control de cargos	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
34	Digitalización	Digitalización	Engrapar rezagos	Cargos		Primario	---	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
34	Digitalización	Digitalización	Devolver cargos y rezagos a control de cargos	Cargos		Primario	---	Control de cargos	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
34	Digitalización	Digitalización	Digitar cargos y rezagos por fecha y por motivo	Cargos		Primario	---	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
34	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	Cargos		Primario	---	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
35	Control de Cargos	Control de cargos	Recepcionar despachos de cargos y rezagos	Relación de despachos	Una lista que indica la cantidad de despachos que han ingresado al área	Primario	---	---	Administración Postal	Ubicada dentro del área	---	x				---	2	1	2	1,7
35	Control de Cargos	Control de cargos	Verificar cantidades de cargos y rezagos	Relación de despachos		Primario	Administracion Postal	---	Administración Postal (Provincias o Lima)	Ubicada dentro del área	---	x				---	2	1	2	1,7
36	Control de Cargos	Control de cargos	Verificar y distribuir despachos al personal	Cuaderno de control de ingreso a control de cargos	Cuaderno de control de ingreso al área	Primario	Operador Postal	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
37	Control de Cargos	Control de cargos	Elaborar y remitir el boletin de verificación	Boletin de verificación de control de cargos	Boletin donde se indica a las distintas administraciones postales que la cantidad de envios y/o rezagos que ha llegado al área de control de cargos es distinta de la cantidad que figura en la relación de despachos	Primario	---	Administracion Postal	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
38	Control de Cargos	Control de cargos	Contar cargos y rezagos e ingresar datos al sistema	Control de cargos por despachos	Control de cada uno de los operadores postales sobre la cantidad de cargos y/o rezagos que ha recibido cada uno	Primario	---	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
39	Control de Cargos	Control de cargos	Elaborar guía o reporte de devolución	SIM 2.0 - Módulo de Devoluciones	Modulo de Reporte de Devolución de Cargos, en el se ingresan cada uno de los reportes o guias realizados manualmente	Soporte	---	---	Operador Postal	---	Aplicación		x			---	2	2	3	2,3
40	Control de Cargos	Control de cargos	Efectuar control de calidad según directiva del cliente	Directivas de distribución de clientes	Directivas de cada uno de los clientes en las que se indican como deben haberse realizado las entregas de los envíos y, en caso haya sucedido, como deben haberse colocado los motivos de devolución	Primario	Extrapostales	---	Supervisor Extrapostales	Ubicada dentro del área	---	x				---	2	2	2	2,0
41	Control de Cargos	Control de cargos	Efectuar control de calidad según directiva del cliente	Reporte de control de calidad de cargos y rezagos	Reporte de control de calidad de cada uno de los cargos y rezagos recibidos según las directivas de dsitribución especificadas para cada cliente	Primario	---	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
41	Control de Cargos	Control de cargos	Elaborar cuadros de motivo de entrega y devolución	Reporte de control de calidad de cargos y rezagos		Primario	---	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
41	Control de Cargos	Control de cargos	Entregar cargos y rezagos a digitalización	Reporte de control de calidad de cargos y rezagos		Primario	---	Digitalizacion	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0

Id Activo	Proceso			Activo de Información			Interacción con otras áreas		Propietario del Activo de Información	Ubicación de los Activos de Información		Formatos				Clasificación Actual del Activo de Información	Valoración			
	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida		Física	Lógica	Papel	Electrónico	Verbal	Otros		Confidencialidad	Integridad	Disponibilidad	Promedio
41	Digitalización	Digitalización	Cuadrar cargos y rezagos con la guía de admisión en hoja de control de calidad	Reporte de control de calidad de cargos y rezagos	Se detalla las cantidades entregadas por control de cargo y las cantidades que se han digitalizado, entre los datos que posee se encuentran el número de guia, la fecha que fue admitida y la cantidad admitida.	Primario	---	Control de cargos	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
42	Control de Cargos	Control de cargos	Devolver cargos y rezagos con memorándum	Memorandun de devolución de cargos y/o rezagos	Memorandun de devolución de cargos y/o rezagos que no han pasado el control de calidad según las directivas del cliente	Primario	---	Administracion Postal	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
43	Control de Cargos	Control de cargos	Descargar en el listado de entrega de los clientes los cargos y rezagos	Lista de entrega del cliente	Lista entregada por los clientes en la que se realiza, de forma manual, una revisión de aquellos envios entregados o devueltos (rezagos)	Primario	Cliente	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	3	2,3
44	Control de Cargos	Control de cargos	Elaborar y remitir el reporte de cargos pendientes	Reporte de cargos pendientes locales y nacionales	Reporte de la cantidad de cargos que han sido enviados a las distintas administraciones postales y que aún no han vuelto	Primario	---	Administracion Postal (Locales y Nacionales) Gerencia Postal y Sub Gerencias Inspectoria	Operador Postal	---	Almacenado en los correos de los operadores postales		x			---	1	2	3	2,0
45	Control de Cargos	Control de cargos	Elaborar y remitir el reporte de cargos pendientes	Consolidado de reportes de cargos pendientes locales y nacionales	Consolidado de los reportes de cargos pendientes locales y nacionales enviados	Primario	---	---	Supervisor del área de Control de Cargos	---	Almacenado en la computadora del supervisor		x			---	1	2	3	2,0
46	Control de Cargos	Control de cargos	Elaborar guía o reporte de devolución	Guia de Devolución	Guia donde se indica la cantidad de rezagos que se devolveran al cliente por cada guía de admisión	Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
46	Control de Cargos	Control de cargos	Registrar guía o reporte de devolución en cuaderno de control	Guia de Devolución		Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
46	Control de Cargos	Control de cargos	Entregar guías o reportes de devolución	Guia de Devolución		Primario	---	Postrén	Operador Postal	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
46	Control de Cargos	Control de cargos	Entregar guías o reportes de devolución al cliente	Guia de Devolución		Primario	---	Cliente	Postrén	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
46	Control de Cargos	Emitir Reporte de Facturación	Recibir las guías o reportes de devolución	Guia de Devolución		Primario	Cliente	---	Postrén	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
46	Control de Cargos	Emitir Reporte de Facturación	Verificar la firmas en las guías o reportes de devolución según el cuaderno de control	Guia de Devolución		Primario	Postrén	---	Operador Postal	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
46	Control de Cargos	Emitir Reporte de Facturación	Archivar y ordenar guías o reportes de devolución y hojas de control	Guia de Devolución		Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
47	Control de Cargos	Control de cargos	Elaborar guía o reporte de devolución	Reporte de Devolución	Impresión de lo ingresado en el modulo de devoluciones del sistema SIM	Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
47	Control de Cargos	Control de cargos	Registrar guía o reporte de devolución en cuaderno de control	Reporte de Devolución		Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
47	Control de Cargos	Control de cargos	Entregar guías o reportes de devolución	Reporte de Devolución		Primario	---	Postrén	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
47	Control de Cargos	Control de cargos	Entregar guías o reportes de devolución al cliente	Reporte de Devolución		Primario	---	Cliente	Postrén	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
47	Control de Cargos	Emitir Reporte de Facturación	Recibir las guías o reportes de devolución	Reporte de Devolución		Primario	Cliente	---	Postrén	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
47	Control de Cargos	Emitir Reporte de Facturación	Verificar la firmas en las guías o reportes de devolución según el cuaderno de control	Reporte de Devolución		Primario	Postrén	---	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
47	Control de Cargos	Emitir Reporte de Facturación	Archivar y ordenar guías o reportes de devolución y hojas de control	Reporte de Devolución		Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del operador postal	x	x			---	2	2	2	2,0
48	Control de Cargos	Control de cargos	Registrar guía o reporte de devolución en cuaderno de control	Cuaderno de control de reportes y guías de devolución	En el se anota cada uno de los numeros de reportes o guias de devoluciones que los operadores postales han realizado	Primario	---	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
48	Control de Cargos	Control de cargos	Entregar guías o reportes de devolución	Cuaderno de control de reportes y guías de devolución		Primario	---	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
		Proceso		Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
48	Control de Cargos	Emitir Reporte de Facturación	Verificar la firmas en las guías o reportes de devolución según el cuaderno de control	Cuaderno de control de reportes y guías de devolución		Primario	---	---	Operador Postal	Ubicada dentro del área	---	x				---	2	2	2	2,0
49	Control de Cargos	Control de cargos	Entregar guías o reportes de devolución al cliente	Cuaderno de Control de Postren	Cuaderno de control de cada uno de los postrenes en el que tienen anotados cada uno de los números de guía o reportes que los operadores postales es han entregado	Primario	---	---	Postren	Ubicada dentro del área	---	x				---	2	2	2	2,0
49	Control de Cargos	Emitir Reporte de Facturación	Recibir las guías o reportes de devolución	Cuaderno de Control de Postren		Primario	---	---	Postren	Ubicada dentro del área	---	x				---	2	2	2	2,0
50	Control de Cargos	Emitir Reporte de Facturación	Informar del caso al supervisor del área	Informe de Reportes y Guías de Devolución Faltantes	Informe de Reportes y guías de devolucion no devueltas por el postren pasados el plazo máximo de 48 horas	Primario	---	---	Operador Postal	Archivadores ubicados dentro del área	---	x				---	2	2	2	2,0
51	Control de Cargos	Emitir Reporte de Facturación	Enviar memorándum al postrén para que devuelva los reportes o guías de devolución	Memorándum de reclamo de devolución de reporte o guía de devolución	Memorándum en el cual se le exige al postrén que devuelva el reporte o guía entregada por el operador postal para su envío a los clientes para su aprobación	Primario	---	Postren	Supervisor del área de Control de Cargos	Archivadores ubicados dentro del área	Almacenado en la computadora del supervisor	x	x			---	2	2	2	2,0
52	Control de Cargos	Emitir Reporte de Facturación	Enviar nota informativa al cliente, solicitando entrega de los reportes o guías de devolución	Nota Informativa de entrega de guias o reportes de devolución	Nota Informativa solicitando a los clientes la entrega de los cargos de reportes de devolucion pendientes	Primario	---	Clientes	Supervisor del área de Control de Cargos	Archivadores ubicados dentro del área	Almacenado en la computadora del supervisor	x	x			---	2	2	2	2,0
53	Control de Cargos	Emitir Reporte de Facturación	Remitir reportes de facturación físicos o digitales	Reporte de Facturación de Control de Cargos	Reportes de facturación con los datos de los servicios brindados a los clientes	Primario	---	Cliente	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del supervisor Almacenado en los correos del supervisor	x	x			---	2	2	2	2,0
53	Control de Cargos	Emitir Reporte de Facturación	Revisar y modificar reporte de facturación	Reporte de Facturación de Control de Cargos		Primario	Cliente	---	Operador Postal	Archivadores ubicados dentro del área	Almacenado en la computadora del supervisor Almacenado en los correos del supervisor	x	x			---	2	2	2	2,0
54	Control de Cargos	Emitir Reporte de Facturación	Recepción de reporte de facturación	Reporte de Facturación de Control de Cargos con visto bueno del cliente (Hoja de coordinación)	Reportes de facturación con los datos de los servicios brindados a los clientes con su visto bueno	Primario	Cleinte	Facturacion	Supervisor del área de Control de Cargos	Archivadores ubicados dentro del área	---	x	x			---	2	2	2	2,0
55	Control de Cargos	Control de cargos	Entregar cargos y despachos al responsable de cada cliente	Rezagos	Documentos no entregados a los clientes, no son escaneados, solo se escanea sus cargos	Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Control de Cargos	Control de cargos	Clasificar cargos y rezagos por cliente y guia de admisión	Rezagos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Control de Cargos	Control de cargos	Contar cargos y rezagos e ingresar datos al sistema	Rezagos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Control de Cargos	Control de cargos	Efectuar control de calidad según directiva del cliente	Rezagos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Control de Cargos	Control de cargos	Devolver cargos y rezagos con memorándum	Rezagos		Primario	---	Administracion Postal	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Control de Cargos	Control de cargos	Entregar cargos y rezagos a digitalización	Rezagos		Primario	---	Digitalización	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Control de Cargos	Control de cargos	Digitar cargos y rezagos en el sistema	Rezagos		Primario	---	---	Clientes	Ubicada dentro del área	---	x				---	2	1	2	1,7
55	Digitalización	Digitalización	Recepcionar cargos y rezagos por cliente	Rezagos	Documentos no entregados a los clientes, no son escaneados, solo se escanea sus cargos	Primario	Control de cargos	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
55	Digitalización	Digitalización	Engrapar rezagos	Rezagos		Primario	---	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
55	Digitalización	Digitalización	Devolver cargos y rezagos a control de cargos	Rezagos		Primario	---	Control de cargos	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
55	Digitalización	Digitalización	Digitar cargos y rezagos por fecha y por motivo	Rezagos		Primario	---	---	Control de cargos	Almacenada dentro del área	---	x				---	2	2	2	2,0
56	Digitalización	Digitalización	Recepcionar cargos y rezagos por cliente	Guia de admisión	Contiene datos como el numero de guia, formato físico que procede del área de control de cargos	Primario	Control de cargos	---	Control de cargos	Almacenada dentro del área	---	x				---	2	--	1	1,5
56	Digitalización	Digitalización	Cuadrar cargos y rezagos con la guía de admisión en hoja de control de calidad	Guia de admisión		Primario	---	---	Control de cargos	Almacenada dentro del área	---	x				---	2	--	1	1,5

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
56	Recepción	Admisión	Generar guía de admisión	Guia de admisión	Contiene datos como el numero de guia, formato físico que se genera una vez se recibe un envío	Primario	---	---	Supervisor de Extra Postales	Ubicada dentro del área	---	x				---	2	1	1	1,3
56	Recepción	Habilitado	Cierre de guías de admisión	Guia de admisión		Primario	---	Control de cargos	Supervisor de Extra Postales	Ubicada dentro del área	---	x				---	2	1	1	1,3
57	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	Escaner	Herramienta utilizada para escanear cada uno de los cargos que llegan al area	Soporte	---	---	Encargado del Área	Ubicada dentro del área de digitalización	---				x	---	--	--	3	3,0
58	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	CANONFILE	Software utilizado para el escaneo de imágenes	Soporte	---	---	Encargado del Área	---	Aplicación		x			---	--	--	3	3,0
59	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	Cargos digitalizados	Versión digital de los cargos entregados por el área de control de cargos, se debe relacionar la imagen con el cargo físico mediante la lectura de codigo de barras (escaneado) o el numero de cargo (manual)	Primario	---	---	Encargado del Área	---	Almacenada en la computadora de la encargada del área		x			---	2	2	3	2,3
59	Digitalización	Digitalización	Transferir imágenes escaneadas a carpetas del servidor	Cargos digitalizados		Primario	---	Clientes	Encargado del Área	---	Almacenada en el servidor web		x			---	2	2	3	2,3
59	Digitalización	Elaboración de Reportes y CD's	Generar el backup por cliente detallando los meses de los clientes digitalizados	Cargos digitalizados		Primario	---	Clientes	Encargado del Área	---	Almacenada en el servidor web		x			---	2	2	3	2,3
59	Digitalización	Elaboración de Reportes y CD's	Obtener imágenes y renombrarlas según el número de guía	Cargos digitalizados		Primario	---	---	Encargado del Área	---	---		x			---	2	2	3	2,3
59	Digitalización	Elaboración de Reportes y CD's	Verificar que la información sea correcta	Cargos digitalizados		Primario	---	---	Encargado del Área	---	---		x			---	2	2	3	2,3
59	Digitalización	Elaboración de Reportes y CD's	Grabar imágenes y cuadro de reportes o reporte de devolución de imágenes	Cargos digitalizados		Primario	---	Clientes	Encargado del Área	---	---		x			---	2	2	3	2,3
60	Digitalización	Digitalización	Escanear y enlazar cargos y rezagos por códigos de barras	Partición del disco (D:\)	Unidad donde se guardan cada una de las imágenes escaneadas. Un reporte de la cantidad de guias admitidas en el mes.	Soporte	---	---	Operadores Postales	---	Dentro de cada estación de trabajo				x	---	2	3	3	2,7
61	Digitalización	Digitalización	Transferir imágenes escaneadas a carpetas del servidor	Servidor de imágenes para digitalización	Carpeta donde se guardan los archivos escaneados para mostrarlo en la web, se encuentra ubicado en el área de TI, dentro del CCPL. Se llama TELPERION	Soporte	---	---	Departamento de TI	Ubicada en el datacenter de la empresa	---				x	---	2	3	3	2,7
62	Digitalización	Digitalización	Proceso de elaboración del CD	Proceso para la elaboración de devoluciones de imágenes al cliente mediante CD's	Los procesos para la creación de CD con las imágenes digitalizadas a solicitud del cliente	Primario	---	---	Encargado del Área	---	---			x		---	2	2	2	2,0
63	Digitalización	Elaboración de Reportes y CD's	Realizar consolidado SAT	Consolidado SAT	Reporte de actualización diaria donde se coloca datos como numero de guia SAT y admisión, fecha, plazo de entrega, cantidad admitida, tipo de documento. Tiene información de todo el año	Primario	---	---	Encargado del Área	---	Almacenada en la computadora de la encargada del área		x			---	2	3	2	2,3
63	Digitalización	Elaboración de Reportes y CD's	Elaborar cuadro de reporte	Consolidado SAT		Primario	---	---	Encargado del Área	---	Almacenada en la computadora de la encargada del área		x			---	2	3	2	2,3
64	Digitalización	Elaboración de Reportes y CD's	Elaborar cuadro de reporte	Reporte de Devolución de imágenes diarias para el SAT	Extracto del consolidado SAT con las guias correspondientes a la fecha de vencimiento del dia y actualización detellando las cantidades de información que se devuelve.	Primario	---	---		---	Almacenada en la computadora de la encargada del área		x			---	2	3	2	2,3
64	Digitalización	Elaboración de Reportes y CD's	Grabar imágenes y cuadro de reportes o reporte de devolución de imágenes	Reporte de Devolución de imágenes diarias para el SAT		Primario	---	Cliente	Encargado del Área	---	---		x			---	2	3	2	2,3
64	Digitalización	Elaboración de Reportes y CD's	Almacenar datos para reporte para refacturación por cliente	Reporte de Devolución de imágenes diarias para el SAT		Primario	---	Cliente	Encargado del Área	---	---		x			---	2	3	2	2,3
65	Digitalización	Elaboración de Reportes y CD's	Generar reporte de devolución de imágenes	Reporte de Devolución	Reporte de actualización de datos para otros clientes empresariales detallando cargos y rezagos.	Primario	---	---	Encargado del Área	---	Almacenada en la computadora de la encargada del área. En un Backup almacenado por el personal del departamento de TI		x			---	2	3	2	2,3

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
		Proceso		Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
65	Digitalización	Elaboración de Reportes y CD's	Grabar imágenes y cuadro de reportes o reporte de devolución de imágenes	Reporte de Devolución		Primario	---	Cliente	Encargado del Área	---	Almacenada en la computadora de la encargada del área. En un Backup almacenado por el personal del departamento de TI		x			---	2	3	2	2,3
65	Digitalización	Elaboración de Reportes y CD's	Almacenar datos para reporte para refacturación por cliente	Reporte de Devolución		Primario	---	Cliente	Encargado del Área	---	Almacenada en la computadora de la encargada del área. En un Backup almacenado por el personal del departamento de TI		x			---	2	3	2	2,3
66	Digitalización	Digitalización	Generar reporte diario para la devolución de cargos	Reporte diario para devolución de cargos	Excel que contiene, en cada hoja, las guias digitadas que fueron trabajadas con los campos solicitados por el cliente. Solo para el cliente INDECOPI	Primario	---	Control de cargos	Control de cargos	---	Almacenada en la computadora de la encargada del área. En un Backup almacenado por el personal del departamento de TI		x			---	2	3	2	2,3
67	Digitalización	Elaboración de Reportes y CD's	Verificar que la información sea correcta	Reporte de Guias de Admisión	Reporte de guias de admisión de los cargos admitidos en el mes para la generación de back ups	Primario	---	---	Encargado del Área	---	Almacenada en la computadora de la encargada del área.	x	x			---	2	3	2	2,3
68	Digitalización	Elaboración de Reportes y CD's	Grabar imágenes y cuadro de reportes o reporte de devolución de imágenes	CD	CD con las imágenes y la BD solicitada por el cliente	Soporte	---	Cliente	Encargado del Área	---	---				x	---	2	3	3	2,7
69	Digitalización	Elaboración de Reportes y CD's	Grabar imágenes y cuadro de reportes o reporte de devolución de imágenes	Guia de devolución de imágenes mediante CD's	Se detalla las guias que se vencen en el dia y se le adjunta el reporte impreso que se ha incluido en el CD	Primario	---	Cliente	Encargado del Área	---	---	x				---	2	2	3	2,3
70	Digitalización	Digitalización	Generar reporte mensual por cliente para prefacturación	Reporte de Facturación de digitalización	Puede ser enviado en formato digital (SAT) o físico con los datos de la guia de admisión generada por mes para la facturación.	Primario	---	---	Encargado del Área	Almacenada dentro del área	Almacenada en la computadora de la encargada del área	x	x			---	2	1	2	1,7
70	Digitalización	Elaboración de Reportes y CD's	Enviar a Facturación para conformidad	Reporte de Facturación de digitalización		Primario	---	Facturación.	Encargado del Área	Almacenada dentro del área	Almacenada en la computadora de la encargada del área	x	x			---	2	1	2	1,7
70	Digitalización	Elaboración de Reportes y CD's	Enviar reporte físico buscando aprobación	Reporte de Facturación de digitalización		Primario	---	Cliente Jefe del Dep.	Encargado del Área	Almacenada dentro del área	Almacenada en la computadora de la encargada del área	x	x			---	2	1	2	1,7
71	Digitalización	Elaboración de Reportes y CD's	Entregar a Facturación reporte sellado	Reporte de facturación de digitalización con visto bueno	Reporte de facturación con el visto bueno del jefe inmediato y, en caso haya sido solicitado, del cliente	Primario	---	Facturación	Facturación	Almacenada dentro del área	Almacenada en la computadora de la encargada del área	x	x			---	2	1	2	1,7
71	Digitalización	Elaboración de Reportes y CD's	Enviar reporte físico buscando aprobación	Reporte de facturación de digitalización con visto bueno		Primario	Cliente Jefe del Dep.	---	Facturación	Almacenada dentro del área	Almacenada en la computadora de la encargada del área	x	x			---	2	1	2	1,7
72	Digitalización	Elaboración de Reportes y CD's	Elaborar base de datos y remitir información vía email al cliente	Listado de guías digitalizadas trabajadas por cliente	Listado con la información de todas las guías digitalizadas en el área, este documento solo se envía una vez se haya acabado con la disribución total de loes envíos de una guía	Primario	---	Cliente	Encargado del Área		Almacenada en la computadora de la encargada del área		x			---	2	3	2	2,3
73	Digitalización	Elaboración de Reportes y CD's	Generar el backup por cliente detallando los meses de los clientes digitalizados	CD con backup	Cd que contiene la información de cada uno de los clientes atendidos una vez se completa los envíos de una guía, en el se detalla la cantidad atendida por mes	Primario	---		Encargado del Área	Almacenada dentro del área					x	---	2	2	3	2,3
74	Recepción	Habilitado	Todo el proceso	Operadores Postales	Persona encargada de apoyar en el proceso de atención a clientes empresariales	Personal	---	---	---	---	---				x	---	2	2	2	2,0
74	Clasificación	Clasificación	Todo el proceso	Operador Postal	Persona encargada de apoyar en el proceso de atención a clientes empresariales	Personal	---	---	---	---	---				x	---	2	2	2	2,0
74	Control de Cargos	Control de cargos	Todo el proceso	Operadores postales	Persona encargada de apoyar en el proceso de atención a clientes empresariales	Personal	---	---	---	---	---				x	---	2	2	2	2,0
75	Recepción	Habilitado	Todo el proceso	Supervisor del área de Extra Postales	Persona encargada de supervisar y velar por la correcta operatividad del proceso	Personal	---	---	---	---	---				x	---	2	2	3	2,3
76	Clasificación	Clasificación	Todo el proceso	Clasificador	Persona encargada de clasificar los envíos por clientes, administraciones postales y sectores.	Personal	---	---	---	---	---				x	---	2	2	2	2,0
77	Clasificación	Clasificación	Todo el proceso	Supervisor del departamento de clasificación	Persona encargada de supervisar y velar por la correcta operatividad del proceso	Personal	---	---	---	---	---				x	---	2	2	2	2,0

Id Activo	Proceso	Sub Proceso	Actividad	Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo	Proveedor de la Entrada	Receptor de la Salida	Propietario del Activo de Información	Física	Lógica	Papel	Electrónico	Verbal	Otros	Clasificación Actual del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Promedio
		Proceso		Activo de Información			Interacción con otras áreas			Ubicación de los Activos de Información		Formatos					Valoración			
78	Control de Cargos	Control de cargos	Todo el proceso	Supervisor del área de Control de Cargos	Persona encargada de velar por el correcto funcionamiento de los procesos del área, es apoyada por otro supervisor	Personal	---	---	---	---	---				x	---	2	2	2	2,0
79	Digitalización	Digitalización	Todo el proceso	Encargada del área de Digitalización	Persona encargada de supervisar la operatividad del área y realizar los procesos relacionados a la facturación, siempre y cuando, le competan al área	Personal	---	---	---	---	---				x	---	2	2	3	2,3
80	Digitalización	Digitalización	Todo el proceso	Co-coordinadores del área de digitalización	Personas encargadas de suplantar al encargado del área en caso no se encuentre presente, solo ven el proceso de quemados de CD y envíos de correos	Personal	---	---	---	---	---				x	---	2	2	2	2,0
81	Digitalización	Digitalización	Todo el proceso	Personal de digitalización	Personas encargadas de digitalizar cada uno de los cargos que llevan del área de control de cargos	Personal	---	---	---	---	---				x	---	2	2	2	2,0
82	Todos los Procesos	---	---	Local del CCPL	Local en el cual se realizan cada uno de los procesos descritos anteriormente	Soporte	---	---	---	---	---				x	---	--	--	3	3,0
83	Todos los Procesos	---	---	Sistema de Camaras de Seguridad	Camaras que graban lo sucedido en las áreas de Extra Postales, Control de Cargos, Clasificación y TI	Soporte	---	---	---	---	---				x	---	--	--	3	3,0
84	Todos los Procesos	---	---	Centro de Procesamiento de Datos	Lugar físico en el que se almacenan los servidores y las base de datos	Soporte	---	---	---	---	---				x	---	--	--	4	4,0
85	Todos los Procesos	---	---	Base de datos de desarrollo	Base de datos ubicada en el área de TI en el CCPL, contiene información utilizada como ambiente de prueba. Llamada MISTI2	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	2	2,0
86	Todos los Procesos	---	---	Base de datos en produccion	Base datos ubicada en el área de TI en el CCPL, contiene información utilizada por los usuarios para su trabajo diario. Se llaman ANDURIL01 y ANDURIL02	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	4	4,0
87	Todos los Procesos	---	---	Base de datos de contingencia	Base de datos ubicada en IBM, contiene el respaldo de las bases de datos de producción, llamada SRP STB.	Soporte	---	---	---	Ubicada en el datacenter de IBM	---				x	---	--	--	4	4,0
88	Todos los Procesos	---	---	Servidor de archivos	Servidor utilizado por las distintas áreas operativas y administrativas para compartir archivos. Llamado NIMRODEL	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	4	4,0
89	Todos los Procesos	---	---	Backup del servidor de Archivos	Backup, almacenado en cintas, de la información guardada en el servidor NIIMRODEL.	Soporte	---	---	---	Almacenada en cintas en el datacenter de la empresa	---				x	---	--	--	4	4,0
90	Todos los Procesos	---	---	UPS Power Ware	3 UPS utilizado para mantener la operatividad de los distintos servidores y base de datos del datacenter, tiempo máximo de uso de 30 minutos.	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	4	4,0
91	Todos los Procesos	---	---	Servidor de Aplicaciones	Servidor de aplicaciones que sirve para el control de versiones de los diversos aplicativos manejados en la empresa	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	4	4,0
92	Todos los Procesos	---	---	Cableado estructural	Red de cableado Cat5e en toda la empresa realizado por el personal del área según sus necesidades	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	3	3,0
93	Todos los Procesos	---	---	Gruppo Electrogeno	Grupo Electrogeno utilizado para hacer funcionar cada uno de los equipos del datacenter en caso la carga de los UPS no sea suficiente	Soporte	---	---	---	Ubicada en el datacenter de la empresa	---				x	---	--	--	4	4,0

8. Anexo 8 – Lista de Ejemplos de Vulnerabilidades y Amenazas

Lista de Ejemplos de Vulnerabilidades y Amenazas

Tipo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
Hardware	Mantenimiento insuficiente/instalación fallidade los medios de almacenamiento	Incumplimiento en el mantenimiento delsistema de información
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.
	Susceptibilidad a la humedad, el polvo y lasuciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuracióneficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones detemperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando seabandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios dealmacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos deacceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación alos datos errados en términos de tiempo	Corrupción de datos
	Interfase de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación yautentificación, como la autentificación deusuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claraspara los desarrolladores	Mal funcionamiento del software
	Falta de control eficaz del cambio	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Falta de copias de respaldo	Manipulación con software
	Falta de protección física de las puertas yventanas de la edificación	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Falta de prueba del envío o la recepción demensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha de la comunicación
	Tráfico sensible sin protección	Escucha de la comunicación
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Falta de identificación y autentificación deemisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad derecuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad delpersonal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externoo de limpieza	Hurto de medios o documentos
	Falta de políticas para el uso correcto de losmedios de telecomunicaciones y mensajería	Uso no autorizado del equipo

Lugar	Uso inadecuado o descuidado del control deacceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible deinundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas yventanas de la edificación	Hurto de equipo
Organización	Falta de procedimiento formal para el registroy retiro del registro de usuario	Abuso de los derechos
	Falta de proceso formal para la revisión(supervisión) de los derechos de acceso	Abuso de los derechos
	Falta o insuficiencia de disposiciones (conrespecto a la seguridad) en los contratos conlos clientes y/o terceras partes	Abuso de los derechos
	Falta de procedimiento de monitoreo de losrecursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación yevaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en losregistros de administradores y operador	Abuso de los derechos
	Respuesta inadecuada de mantenimiento delservicio	Incumplimiento en el mantenimiento delsistema de información
	Falta o insuficiencia en el acuerdo a nivel deservicio	Incumplimiento en el mantenimiento delsistema de información
	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento delsistema de información
	Falta de procedimiento formal para el controlde la documentación del SGSI	Corrupción de datos
	Falta de procedimiento formal para lasupervisión del registro del SGSI	Corrupción de datos
	Falta de procedimiento formal para laautorización de la información disponible alpúblico	Datos provenientes de fuentes no confiables
	Falta de asignación adecuada deresponsabilidades en la seguridad de lainformación	Negación de acciones
	Falta de planes de continuidad	Falla del equipo
	Falta de políticas sobre el uso del correoelectrónico	Error en el uso
	Falta de procedimientos para la introducciónde l software en los sistemas operativos	Error en el uso
	Falta de registros en las bitácoras*(logs) deadministrador y operario.	Error en el uso
	Falta de procedimientos para el manejo deinformación clasificada	Error en el uso
	Falta de responsabilidades en la seguridadde la información en la descripción de loscargos	Error en el uso
	Falta o insuficiencia en las disposiciones (conrespecto a la seguridad de la información) enlos contratos con los empleados	Procesamiento ilegal de datos
	Falta de procesos disciplinarios definidos enel caso de incidentes de seguridad de lainformación	Hurto de equipo
	Falta de política formal sobre la utilización decomputadores portátiles	Hurto de equipo
	Falta de control de los activos que seencuentran fuera de las instalaciones	Hurto de equipo
	Falta o insuficiencia de política sobre limpiezade escritorio y de pantalla	Hurto de medios o documentos
	Falta de autorización de los recursos deprocesamiento de la información	Hurto de medios o documentos
	Falta de mecanismos de monitoreoestablecidos para las brechas en la seguridad	Hurto de medios o documentos
	Falta de revisiones regulares por parte de lagerencia	Uso no autorizado del equipo
	Falta de procedimientos para la presentaciónde informes sobre las debilidades en laseguridad	Uso no autorizado del equipo
	Falta de procedimientos del cumplimiento delas disposiciones con los derechosintelectuales	Uso de software falso o copiado

9. Anexo 9 – Matriz de Riesgos

Serpost El Correo del Perú

Anexo 9 - Matriz de Riesgos

		Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
Id Riesgo	Proceso	Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R1	Todos	Backup de base de datos	3	3	4	Se prueban los backups realizados una vez a la semana	Errores al restaurar los backups	Riesgo de pérdida de la integridad de la información almacenada en los backups debido a una restauración fallida de los mismos, a causa de la falta de pruebas de los backups	Baja	Moderado	8	Riesgo Bajo	Transferido Seguir Monitoreando	--	--	--	Jefe del Departamento de Tecnología
R2	Recepción	Backup de los correos recibidos	2	2	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información de los backups de los correos recibidos debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R3	Recepción	Backup de los correos recibidos	2	2	3	Destrucción del equipo o los medios.	Falta de políticas para el respaldo de información	Riesgo de pérdida de la información almacenada en la computadora debido a algún evento que destruya el equipo, a causa de la falta de políticas para el respaldo de información	Moderada	Moderado	12	Riesgo Alto	Mitigar	A. 10.5.1 Recuperación de la información	Se debe obtener un resguardo de la información almacenada en la computadora en un ambiente acondicionado para ello y lejos del área de trabajo	Control Correctivo	Supervisor del área de Extra Postales
R4	Recepción	Backup de los correos recibidos	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de los backups de los correos recibidos debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A. 10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R5	Todos	Backup de servidores	3	3	4	Falta de ambientes adecuados para el almacenamiento de backups	Almacenamiento de los backups dentro del CPD	Riesgo de daño o deterioro de los backups debido a incidentes ocurridos en el CCPL, a causa del almacenamiento de los backups dentro del CPD	Baja	Mayor	12	Riesgo Alto	Transferir	A. 10.5.1 Recuperación de la información	Cada uno de los respaldos o backups de la información almacenada en el CPD debe ser almacenada en un lugar distinto para evitar su perdida en caso un incendio destruya este local.	Control Preventivo	Jefe del Departamento de Tecnología
R6	Todos	Base de datos de contingencia	3	3	4	Abuso de los privilegios	Falta de auditorías (supervisiones) programadas o inopinadas	Riesgo de compromiso de información debido a un ingreso no autorizado a la base de datos de contingencia, a causa de la falta de auditorias a la base de datos	Moderada	Mayor	18	Riesgo Alto	Mitigar	A. 10.10.1 Registro de auditoria	La organización debe producir, analizar y almacenar los logs de auditoria el tiempo que se establezca necesario de tal forma que ayude a investigaciones futuras	Control Detectivo	Jefe del Departamento de Tecnología
R7	Todos	Base de datos de contingencia	3	3	4	Usuarios Mal intencionados	Falta de pruebas de hacking etico	Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección.	Moderada	Mayor	18	Riesgo Alto	Mitigar	A. 10.6.1 Controles de red A. 10.6.2 Seguridad de los servicios de redes	Se deberá desarrollar un plan de análisis de vulnerabilidades que permita identificar los principales problemas en los sitemas y ayude a elaborar procedimientos para corregirlos.	Control Detectivo	Jefe del Departamento de Tecnología
R8	Todos	Base de datos en produccion	3	3	4	Abuso de los privilegios	Falta de auditorías (supervisiones) programadas o inopinadas	Riesgo de compromiso de información debido a un ingreso no autorizado a la base de datos, a causa de la falta de auditorias a la base de datos	Moderada	Mayor	18	Riesgo Alto	Mitigar	A. 10.10.1 Registro de auditoria	La organización debe producir, analizar y almacenar los logs de auditoria el tiempo que se establezca necesario de tal forma que ayude a investigaciones futuras	Control Detectivo	Jefe del Departamento de Tecnología
R9	Todos	Base de datos en produccion	3	3	4	Usuarios Mal intencionados	Falta de pruebas de hacking etico	Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección.	Moderada	Mayor	18	Riesgo Alto	Mitigar	A. 10.6.1 Controles de red A. 10.6.2 Seguridad de los servicios de redes	Se deberá desarrollar un plan de análisis de vulnerabilidades que permita identificar los principales problemas en los sitemas y ayude a elaborar procedimientos para corregirlos.	Control Detectivo	Jefe del Departamento de Tecnología
R10	Clasificación	Boletin de verificación de clasificación	3	2	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación del boletín de verificación de clasificación debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A. 11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R11	Clasificación	Boletin de verificación de clasificación	3	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro del boletin de verificación de clasificación debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A. 10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R12	Todos	Cableado Estructural	--	--	3	No existe un rotulado del cableado estructural	Problemas con algún punto de la red	Riesgo de problemas en la infraestructura de red debido a problemas de conexión en el cableado, a causa de la falta de un rotulado adecuado	Moderada	Moderado	12	Riesgo Alto	Transferir	A.9.2.3 Seguridad del cableado	Se deberá contratar los servicios de una empresa especializada en el rubro para identificar claramente los cables de red en la empresa y evitar errores de manejo al momento de dar mantenimiento a la red	Control Preventivo	Jefe del Departamento de Tecnología
R13	Digitalización	CANONFILE	2	3	2	Usuarios nuevos	Falta de documentación para realizar el proceso	Riesgo de pérdida o daño de la información trabajada con el programa CANONFILE debido a errores de uso del mismo, a causa del desconocimiento de su manejo	Moderada	Moderado	12	Riesgo Alto	Mitigar	A. 10.1.1 Documentación de procedimientos operativos	Se deberá entregar el manual de usuario del programa CANONFILE para facilitar la capacitación de personal nuevo de la empresa	Control Preventivo	Jefe de Departamento de Sistemas de Información
R14	Control de Cargos	Cargos	2	2	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación de los cargos debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Muy Baja	Moderado	4	Riesgo Bajo	Seguir Monitoreando	--	--	--	Oficial de Seguridad de la Información
R15	Recepción	Cargos	2	2	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación de los cargos impresos debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Muy Baja	Menor	2	Riesgo Bajo	Seguir Monitoreando	--	--	--	Oficial de Seguridad de la Información
R16	Recepción	Cargos	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de los cargos debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A. 10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R17	Control de Cargos	Cargos	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de la guía de los cargos debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A. 10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Control de Cargos

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R18	Recepción	Carpeta compartida EXTRAPOSTALES	2	2	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información de la carpeta compartida debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Moderada	Menor	6	Riesgo Bajo	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R19	Recepción	Carpeta compartida EXTRAPOSTALES	2	2	3	Falla del equipo de telecomunicaciones	Perdida de conexión a la red, interna e internet, debido a la falla del equipo	Riesgo de pérdida del acceso a la información de la carpeta compartida debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R20	Digitalización	CD con backup	2	2	3	Desastre Natural o Provocado	Almacenamiento del backup dentro del área	Riesgo de pérdida o deterioro de los CD's con los backups de la información del área debido a un desastre natural o provocado, a causa de su almacenamiento dentro de la misma área	Alta	Moderado	16	Riesgo Alto	Transferir	A.10.5.1 Recuperación de la información	Cada uno de los respaldos o backups de la información almacenada en el área debe ser almacenada en un lugar distinto para evitar su perdida en caso un incendio destruya este local.	Control Preventivo	Jefe del Departamento de Tecnología
R21	Digitalización	CD con backup	2	2	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida de la información almacenada en los CD's de los backups de la organización debido a robos o pérdidas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Baja	Moderado	8	Riesgo Bajo	Seguir Monitoreando	--	--	--	Oficial de Seguridad de la Información
R22	Tecnologías de Información	Centro de Procesamiento de Datos	--	--	4	Destrucción de equipo o medios	Protección física inapropiada para el centro de procesamiento de datos	Riesgo de compromiso de los activos almacenados en el CPD debido a algún acto mal intencionado, causado por la falta de una protección física que evite estos actos	Baja	Catastrofico	16	Riesgo Alto	Mitigar	A.9.2.1 Ubicación y protección de equipos	Se deberá acondicionar el CPD de manera adecuada mediante la instalación de paredes, puertas y ventanas que eviten el acceso no autorizado al mismo	Control Preventivo	Jefe del Departamento de Tecnología
R23	Tecnologías de Información	Centro de Procesamiento de Datos	--	--	4	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño o deterioro de los equipos del CPD debido a un incendio, a causa de la falta de sistemas contra incendios	Alta	Catastrofico	32	Riesgo Grave	Mitigar	A.9.2.1 Ubicación y protección de equipos A.10.5.1 Recuperación de la información	Se deberá adquirir equipos detectores de humo que den la alerta en caso de incendio. Cada uno de los respaldos o backups de la información almacenada en el CPD debe ser almacenada en un lugar distinto para evitar su perdida en caso un incendio destruya este local.	Control Detectivo Control Preventivo	Jefe del Departamento de Tecnología
R24	Tecnologías de Información	Centro de Procesamiento de Datos	--	--	4	Pérdida del suministro de energía	Desconexión de las cámaras de vigilancia	Riesgo de compromiso de información confidencial y activos del CPD debido a la desconexión de camaras de seguridad, a causa de fallas de energía eléctrica	Alta	Mayor	24	Riesgo Grave	Mitigar	A.9.2.2 Suministro eléctrico	Se deberá solicitar la compra de un equipo UPS capaz de brindar de electricidad a las cámaras de seguridad mientras se enciende el grupo electrógeno	Control Preventivo	Encargado de Seguridad Física de la Empresa
R25	Tecnologías de Información	Centro de Procesamiento de Datos	--	--	4	Pérdida del suministro de energía	UPS tiene una duración máxima de 30 minutos	Riesgo de perdida de disponibilidad de los equipos almacenados en el CPD debido a la falta de energía electrica, causados por la poca duración de los UPS adquiridos	Alta	Mayor	24	Riesgo Grave	Mitigar	A.9.2.2 Suministro eléctrico	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los grupos electrógenos de la empresa, indicando las áreas que cubren, el tiempo máximo que pueden estar encendidos y aquellos procesos críticos que deben permanecer operativos durante la contingencia	Control Detectivo	Encargado de Seguridad Física de la Empresa
R26	Tecnologías de Información	Centro de Procesamiento de Datos	--	--	4	Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	Riesgo de daño o deterioro de los equipos del CPD debido al polvo a factores ambientales, a causa de la falta de mecanismos para controlar el medio ambiente	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se deberá adquirir equipos que ayuden a vigilar las condiciones ambiantales que puedan afectar a los equipos del CPD	Control Detectivo	Jefe del Departamento de Tecnología
R27	Clasificación	Computadora de Escritorio	--	3	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "bloqueo de sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Moderada	Menor	6	Riesgo Bajo	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R28	Digitalización	Computadora de Escritorio	--	3	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información de la computadora debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R29	Control de Cargos	Computadora de Escritorio	--	3	3	Demora en la entrega de accesos a los usuarios	Claves compartidas por varios usuarios para el ingreso y uso de correo	Riesgo de pérdida de la información almacenada en la computadora o pérdida del no repudio de mensajes enviados por el correo electrónico debido al intercambio no autorizado de claves, a causa de la demora en la entrega de accesos a los usuarios.	Muy Alta	Menor	10	Riesgo Alto	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Sistemas de Información
R30	Control de Cargos	Computadora de Escritorio	--	3	3	Destrucción del equipo o los medios.	Falta de politicas para el respaldo de información	Riesgo de pérdida de la información almacenada en la computadora debido a algún evento que destruya el equipo, a causa de la falta de politicas para el respaldo de información	Alta	Moderado	16	Riesgo Alto	Mitigar	A.10.5.1 Recuperación de la información	Se debe obtener un resguardo de la información almacenada en la computadora en un ambiente acondicionado para ello y lejos del área de trabajo	Control Correctivo	Supervisor del Departamento de Control de Cargos
R31	Recepción	Computadora de Escritorio	--	2	3	Error en el uso	Uso incorrecto de software y hardware	Riesgo de daño o deterioro de las computadoras debido a errores de uso del usuario, a causa del desconocimiento en el manejo de estas herramientas	Baja	Moderado	8	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Tecnología
R32	Control de Cargos	Computadora de Escritorio	--	3	3	Falla del equipo de telecomunicaciones	Perdida de conexión a la red, interna e internet, debido a la falla del equipo	Riesgo de pérdida de información debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R33	Recepción	Computadora de Escritorio	--	2	3	Introducción de virus, troyanos o software malicioso	Falta de actualización de antivirus	Riesgo de pérdida o daño de la información o de deterioro de la computadora debido a un ataque mal intencionado, a causa de la falta de un software para el tratamiento de código malicioso	Alta	Moderado	16	Riesgo Alto	Mitigar	A.10.4.1 Controles contra Software Malicioso	Se debe adquirir software especializado para la detección y reparación de virus para cada una de las computadoras del personal de la empresa	Control Preventivo	Jefe de Departamento de Tecnología
R34	Clasificación	Computadora de Escritorio	--	3	3	Introducción de virus, troyanos o software malicioso	Falta de actualización de antivirus	Riesgo de pérdida o daño de la información o de deterioro de la computadora debido a un ataque mal intencionado, a causa de la falta de un software para el tratamiento de código malicioso	Alta	Moderado	16	Riesgo Alto	Mitigar	A.10.4.1 Controles contra Software Malicioso	Se debe adquirir software especializado para la detección y reparación de virus para cada una de las computadoras del personal de la empresa	Control Preventivo	Jefe de Departamento de Tecnología
R35	Digitalización	Computadora de Escritorio	--	3	3	Introducción de virus, troyanos o software malicioso	Falta de actualización de antivirus	Riesgo de pérdida o daño de la información o de deterioro de la computadora debido a un ataque mal intencionado, a causa de la falta de un software para el tratamiento de código malicioso	Muy Alta	Moderado	20	Riesgo Grave	Mitigar	A.10.4.1 Controles contra Software Malicioso	Se debe adquirir software especializado para la detección y reparación de virus para cada una de las computadoras del personal de la empresa	Control Preventivo	Jefe de Departamento de Tecnología

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R36	Clasificación	Computadora de Escritorio	--	3	3	Fuego	Poco personal capacitado en el uso de extintores. Destrucción o degradación del activo de información	Riesgo de daño y/o deterioro de las computadoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de la información almacenada en la computadora en un ambiente acondicionado para ello y lejos del área de trabajo	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R37	Digitalización	Computadora de Escritorio	--	3	3	Fuego	Poco personal capacitado en el uso de extintores. Destrucción o degradación del activo de información	Riesgo de daño y/o deterioro de las computadoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de la información almacenada en la computadora en un ambiente acondicionado para ello y lejos del área de trabajo	Control Preventivo	Jefe del Departamento de Seguridad Postal / Encargado del departamento de digitalización
R38	Recepción	Computadora de Escritorio	--	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de las computadoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de la información almacenada en la computadora en un ambiente acondicionado para ello y lejos del área de trabajo	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Área de Control de Cargos
R39	Control de Cargos	Computadora de Escritorio	--	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de las computadoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de la información almacenada en la computadora en un ambiente acondicionado para ello y lejos del área de trabajo	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Control de Cargos
R40	Recepción	Computadora de Escritorio	--	2	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las computadoras debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Tecnología
R41	Clasificación	Computadora de Escritorio	--	3	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las computadoras debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Baja	Moderado	8	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Tecnología
R42	Digitalización	Computadora de Escritorio	--	3	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las computadoras debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Alta	Moderado	16	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá desarrollar un procedimiento que permita establecer una frecuencia fija para el mantenimiento de las distintas herramientas utilizadas en el área de trabajo	Control Preventivo	Jefe de Departamento de Tecnología
R43	Recepción	Computadora de Escritorio	--	2	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de las computadoras debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe del Departamento de Seguridad Postal
R44	Clasificación	Computadora de Escritorio	--	3	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de las computadoras debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.9.2.2 Suministro Eléctrico	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los grupos electrógenos de la empresa, indicando las áreas que cubren, el tiempo máximo que pueden estar encendidos y aquellos procesos críticos que deben permanecer operativos durante la contingencia	Control Preventivo	Jefe del Departamento de Seguridad Postal
R45	Digitalización	Computadora de Escritorio	--	3	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de las computadoras debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.9.2.2 Suministro Eléctrico	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los grupos electrógenos de la empresa, indicando las áreas que cubren, el tiempo máximo que pueden estar encendidos y aquellos procesos críticos que deben permanecer operativos durante la contingencia	Control Preventivo	Encargado de Seguridad Física de la Empresa
R46	Digitalización	Consolidado SAT	2	3	2	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño del consolidado SAT debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R47	Digitalización	Consolidado SAT	2	3	2	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de los consolidados SAT debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Encargado del Departamento de Digitalización
R48	Recepción	Correos de los clientes	2	2	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información de los correos recibidos debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R49	Recepción	Correos de los clientes	2	2	3	Demora en la entrega de nuevos usuarios	Transferencia no autorizada de contraseñas validas	Riesgo de pérdida de la confidencialidad de los correos y daño a la reputación de la empresa debido a la filtración de información confidencial de los clientes causado por compartir una misma contraseña con varias personas	Alta	Menor	8	Riesgo Bajo	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Tecnología
R50	Clasificación	Cuaderno de control de guias de salidas para control de cargos	2	3	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación del cuaderno de control de guías de salida para control de cargos debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R51	Clasificación	Cuaderno de control de guias de salidas para control de cargos	2	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro del cuaderno de control de guías de salida para control de cargos debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R52	Clasificación	Cuaderno de control de despachos	2	3	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación del cuaderno de control de despachos debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R53	Clasificación	Cuaderno de control de despachos	2	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro del cuaderno de control de despachos debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R54	Clasificación	Cuaderno de control de guias de salida para extrapostales	2	3	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación del cuaderno de control de guías de salida para extra postales debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R55	Clasificación	Cuaderno de control de guias de salida para extrapostales	2	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro del cuaderno de control de guías de salida para extra postales debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R56	Tecnologías de Información	Equipo UPS Power Ware	--	--	4	Antigüedad del equipo	El funcionamiento del CPD depende de los UPS	Riesgo de deterioro de los equipos UPS debido a fallas del equipo, a causa de su antigüedad	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los UPS de la empresa destinados al funcionamiento del CPD	Control Detectivo	Jefe del Departamento de Tecnología
R57	Tecnologías de Información	Equipo UPS Power Ware	--	--	4	Incumplimiento en el mantenimiento del sistema	Mantenimiento insuficiente	Riesgo de deterioro de los equipos UPS debido a fallas del equipo, a causa de la falta de mantenimiento	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los UPS de la empresa destinados al funcionamiento del CPD	Control Detectivo	Jefe del Departamento de Tecnología
R58	Digitalización	Escaner	--	--	3	Fuego	Poco personal capacitado en el uso de extintores. Destrucción o degradación del activo de información	Riesgo de daño y/o deterioro de los escaners debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R59	Digitalización	Escaner	--	--	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de los escaners debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Alta	Moderado	16	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá desarrollar un procedimiento que permita establecer una frecuencia fija para el mantenimiento de las distintas herramientas utilizadas en el área de trabajo	Control Preventivo	Jefe de Departamento de Tecnología
R60	Digitalización	Escaner	--	--	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de los escaners debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.9.2.2 Suministro Eléctrico	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los grupos electrógenos de la empresa, indicando las áreas que cubren, el tiempo máximo que pueden estar encendidos y aquellos procesos críticos que deben permanecer operativos durante la contingencia	Control Preventivo	Encargado de Seguridad Física de la Empresa
R61	Recepción	Etiquetadoras	--	--	3	Error en el uso	Uso incorrecto de software y hardware	Riesgo de daño o deterioro de las etiquetadoras debido a errores de uso del usuario, a causa del desconocimiento en el manejo de estas herramientas	Baja	Mayor	12	Riesgo Alto	Mitigar	A.10.1.1 Documentación de procedimientos operativos	Se deben realizar y mantener manuales que den a conocer el correcto uso de las diversas herramientas entregadas a los empleados	Control Preventivo	Jefe de Departamento de Tecnología
R62	Recepción	Etiquetadoras	--	--	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de las etiquetadoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R63	Recepción	Etiquetadoras	--	--	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las etiquetadoras debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Tecnología
R64	Recepción	Etiquetadoras	--	--	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de las etiquetadoras debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe del Departamento de Seguridad Postal
R65	Clasificación	File de boletines de verificación de clasificación	2	2	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación del file de boletines de verificación de clasificación debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R66	Clasificación	File de boletines de verificación de clasificación	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro del file de boletines de verificación de clasificación debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R67	Clasificación	File de guias de salidas	2	3	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación del file de guias de salidas debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R68	Clasificación	File de guias de salidas	2	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro del file de guias de salida debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R69	Recepción	Formatos de cargos	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de los formatos de cargos debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R70	Recepción	Formatos de cargos	2	2	3	Los formatos deben ser digitados en la computadora de manera manual	Personal con poca experiencia puede equivocarse al momento de digitar la información en los cargos	Riesgo de pérdida de la integridad debido a errores en la digitalización causado por la falta de experiencia al llenar los cargos	Moderada	Menor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Supervisor del área de Extra Postales
R71	Tecnologías de Información	Grupo electrogenio	--	--	4	Antigüedad del equipo	Luego de 30 minutos sin electricidad, el funcionamiento del CPD depende del grupo electrógeno	Riesgo de deterioro del grupo electrógeno debido a fallas del equipo, a causa de su antigüedad	Baja	Catastrófico	16	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los grupos electrógenos de la empresa, indicando las áreas que cubren, el tiempo máximo que pueden estar encendidos y aquellos procesos críticos que deben permanecer operativos durante la contingencia	Control Detectivo	Encargado de Seguridad Física de la Empresa
R72	Clasificación	Guia de Salida (SEL)	2	3	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación de la guia de salida de clasificación debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R73	Clasificación	Guia de Salida (SEL)	2	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de la guía de salida debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R74	Clasificación	Guia de Salida con Conformidad de Clasificación	2	3	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación de la guia de salida con conformidad de clasificación debido a robos o modificaciones no autorizadas, a causa de la falta de lugares adecuados donde guardar los documentos importante	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información
R75	Clasificación	Guia de Salida con Conformidad de Clasificación	2	3	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de la guía de salida con conformidad debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Catastrófico	16	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Clasificación
R76	Recepción	Impresora High Speed	--	--	3	Error en el uso	Uso incorrecto de software y hardware	Riesgo de daño o deterioro de la impresora high speed debido a errores de uso del usuario, a causa del desconocimiento en el manejo de estas herramientas	Baja	Mayor	12	Riesgo Alto	Mitigar	A.10.1.1 Documentación de procedimientos operativos	Se deben realizar y mantener manuales que den a conocer el correcto uso de las diversas herramientas entregadas a los empleados	Control Preventivo	Jefe de Departamento de Tecnología
R77	Recepción	Impresora High Speed	--	--	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de la impresora high speed debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R78	Recepción	Impresora High Speed	--	--	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las impresoras high speed debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Tecnología
R79	Recepción	Impresora High Speed	--	--	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de las impresoras high speed debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe del Departamento de Seguridad Postal
R80	Recepción	Impresoras comunes	--	--	3	Error en el uso	Uso incorrecto de software y hardware	Riesgo de daño o deterioro de las impresoras comunes debido a errores de uso del usuario, a causa del desconocimiento en el manejo de estas herramientas	Baja	Mayor	12	Riesgo Alto	Mitigar	A.10.1.1 Documentación de procedimientos operativos	Se deben realizar y mantener manuales que den a conocer el correcto uso de las diversas herramientas entregadas a los empleados	Control Preventivo	Jefe de Departamento de Tecnología
R81	Recepción	Impresoras comunes	--	--	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de las impresoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R82	Control de Cargos	Impresoras comunes	--	--	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de las impresoras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R83	Recepción	Impresoras comunes	--	--	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las impresoras comunes debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Tecnología
R84	Recepción	Impresoras comunes	--	--	3	Perdida del suministro de energia	Inactividad del equipo debido a la falta de energia	Riesgo de pérdida de disponibilidad de las impresoras comunes debido a la pérdida de energía en el área, a causa de la demora en el encendido de los grupos electrógeno de la empresa	Muy Baja	Mayor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe del Departamento de Seguridad Postal
R85	Control de cargos	Lista de entrega del cliente	2	2	3	Hurto o modificación de medios o documentos	Falta de lugares adecuados donde guardar documentación importante Trabajo no supervisado del personal externo de limpieza	Riesgo de pérdida, daño o modificación de la lista de entrega del cliente debido a robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con personal externo y locadores	Muy Baja	Moderado	4	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe del Departamento de Abastecimiento y Servicios Generales Sub Gerente de Logística
R86	Control de cargos	Lista de entrega del cliente	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Perdida de la disponibilidad de la lista de entrega del ciente debido a un incendio	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Supervisor del Departamento de Control de Cargos
R87	Control de cargos	Lista de entrega del cliente	2	2	3	Se almacena toda esta información en cajas distribuidas a lo largo de toda el área	Falta de cuidado en los lugares donde se guardan los documentos	Riesgo de daño y/o deterioro de la lista de entrega del cliente debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.3 Política de Pantalla y escritorio limpio	Se debe adquirir y habilitar lugares especiales donde almacenar la información física que se tiene dentro del área, tales como, armarios o cajones con cerrojos para evitar que sean accedidos por personal no autorizado	Control Preventivo	Oficial de Seguridad de la Información

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R88	Digitalización	Listado de guías digitalizadas trabajadas por cliente	2	3	2	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño del listado de guías digitalizadas trabajadas por cliente debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R89	Todos	Local del CCPL	--	--	3	Camaras de seguridad en el perimetro físico de la empresa cubren el 50% del perimetro físico, solo 2 calles que rodean a la organización	Personal ajeno a la empresa podria ingresar con ayuda de alguien dentro de la organización	Riesgo de pérdida de la confidencialidad, integridad y disponibilidad de la información que se tenga en la empresa debido al ingreso de una persona mal intencionada, a causa de la falta de cámaras de seguridad que protejan todo el perimetro de la organización	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.1 Seguridad Física Perimetral	Se deberá solicitar la compra de camaras de seguridad que permitan establecer un control adecuado de todo el perimetro de la organización	Control Disuasivo	Encargado de Seguridad Física de la Empresa
R90	Todos	Local del CCPL	--	--	3	Descuido del control del acceso físico a las instalaciones donde se llevan a cabo los procesos	Poca cultura de control de acceso a las distintas áreas de la organización	Riesgo de pérdida de la confidencialidad, integridad y disponibilidad de la información que se tenga en la empresa debido a un descuido en el control de acceso físico a las instalaciones, a causa de la poca cultura organizacional para verificar que solo personal autorizado ingrese a las distintas áreas	Baja	Moderado	8	Riesgo Bajo	Mitigar	A.9.1.2 Controles físicos de entradas	Se deberá exigir que todo el personal de SERPOST lleve una identificación visible mientras se encuentre dentro del CCPL, de igual forma, cada uno de los visitantes deberán llevar un carnet de identificación que indique cual es el área que desea visitar.	Control Preventivo	Encargado de Seguridad Física de la Empresa
R91	Todos	Local del CCPL	--	--	3	Poco control a personas externas que ingresan a la organización	Ingreso no autorizado de personas externas a la organización a las distintas áreas	Riesgo de compromiso de información personal y de daño de los equipos del CPD debido al ingreso de personal no autorizado al departamento de Tecnología, a causa del poco control al personal que ingresa a la organización	Muy Alta	Moderado	20	Riesgo Grave	Evitar	A.9.1.1 Seguridad Física Perimetral A.9.1.2 Controles físicos de entradas	Se deberá realizar modificaciones en el departamento de TI que eviten el acceso no autorizado de personal al área, tales como la instalación de puertas y ventanas adecuadas para este local.	Control Preventivo	Jefe del Departamento de Tecnología
R92	Todos	Local del CCPL	--	--	3	Red energética inestable	Grupo electrogeno no abastece a toda la planta	Riesgo de pérdida de la disponibilidad de los servicios realizados en el CCPL debido a que el grupo electrógeno no abastece a toda la organización y causado por una falla eléctrica	Alta	Moderado	16	Riesgo Alto	Mitigar	A.9.2.2 Suministro eléctrico	Se deberá realizar la documentación pertinente que permita dar un mantenimiento adecuado a los grupos electrógenos de la empresa, indicando las áreas que cubren, el tiempo máximo que pueden estar encendidos y aquellos procesos críticos que deben permanecer operativos durante la contingencia	Control Detectivo	Encargado de Seguridad Física de la Empresa
R93	Recepción	Modulo SUNARP	2	3	3	Demora en la entrega de nuevos usuarios	Transferencia no autorizada de contraseñas validas	Riesgo de pérdida de la disponibilidad e integridad de datos en el módulo SUNARP debido al uso de una misma contraseña por varios usuarios causados por la demora en la entrega de accesos a usuarios	Alta	Menor	8	Riesgo Bajo	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Sistemas de Información
R94	Recepción	Modulo SUNARP	2	3	3	Error en el uso	Falta de documentación	Riesgo de pérdida o daño de la información almacenada en el Módulo SUNARP debido a errores de uso del sistema, a causa del desconocimiento en el manejo del sistema	Moderada	Menor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Sistemas de Información
R95	Recepción	Modulo SUNARP	2	3	3	Falla del equipo de telecomunicaciones	Dependencia de la red para el correcto funcionamiento del sistema	Riesgo de pérdida de información del módulo debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R96	Tecnologías de Información	Personal Especializado del área de Tecnologías de Información	--	--	3	Falta de documentación de los procedimientos propios del área	Poco personal especializado para dar mantenimiento a los sistemas	Riesgo de pérdida de disponibilidad de los equipos del área debido a errores de los usuarios, a causa de la falta de documentación de los procedimientos propios del área	Moderada	Moderado	12	Riesgo Alto	Evitar	A.10.1.1 Documentación de procedimientos operativos	Se deberá realizar la documentación de aquellos procesos claves en el área de TI de tal forma que la entrega de servicios del área no se vea afectada por la ausencia de personal clave	Control Preventivo	Jefe del Departamento de Tecnología
R97	Clasificación	Pistola lectora de código de barras	--	--	3	Error en el uso	Uso incorrecto de software y hardware	Riesgo de deterioro de la pistola lectora de código de barras debido a errores de uso del usuario, a causa del desconocimiento en el manejo de estas herramientas	Alta	Moderado	16	Riesgo Alto	Mitigar	A.10.1.1 Documentación de procedimientos operativos	Se deben realizar y mantener manuales que den a conocer el correcto uso de las diversas herramientas entregadas a los empleados	Control Preventivo	Jefe de Departamento de Tecnología
R98	Digitalización	Pistola lectora de código de barras	--	--	3	Fuego	Poco personal capacitado en el uso de extintores. Destrucción o degradación del activo de información	Riesgo de daño y/o deterioro de las pistolas lectoras de códigos de barras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R99	Control de Cargos	Pistola lectora de código de barras	2	2	3	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de las pistolas lectoras de código de barras debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales	Se debe adquirir e instalar equipos contra incendios dentro de la organización	Control Preventivo	Jefe del Departamento de Seguridad Postal
R100	Control de Cargos	Pistola lectora de código de barras	2	2	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de la pistola de código de barras debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Alta	Moderado	16	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá desarrollar un procedimiento que permita establecer una frecuencia fija para el mantenimiento de las distintas herramientas utilizadas en el área de trabajo	Control Preventivo	Jefe de Departamento de Tecnología
R101	Digitalización	Pistola lectora de código de barras	--	--	3	Incumplimiento en el mantenimiento de la herramienta	Mantenimiento insuficiente	Riesgo de daño o deterioro de las pistolas lectoras de códigos de barra debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario	Alta	Moderado	16	Riesgo Alto	Mitigar	A.9.2.4 Mantenimiento de equipos	Se deberá desarrollar un procedimiento que permita establecer una frecuencia fija para el mantenimiento de las distintas herramientas utilizadas en el área de trabajo	Control Preventivo	Jefe de Departamento de Tecnología
R102	Digitalización	Reporte de Devolución	2	3	2	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño del reporte de devolución de imágenes para los clientes, a excepción de SAT, debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R103	Digitalización	Reporte de Devolución	2	3	2	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de los reportes de devolución debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Encargado del Departamento de Digitalización
R104	Digitalización	Reporte de Devolución de imágenes diarias para el SAT	2	3	2	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño del reporte de devolución de imágenes diarias para el SAT debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R105	Digitalización	Reporte de Devolución de imágenes diarias para el SAT	2	3	2	Fuego	Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información	Riesgo de daño y/o deterioro de los reportes de devolución de imágenes diarias para el SAT debido a un incendio, a causa de la falta de capacitación y sistemas contra incendios	Baja	Mayor	12	Riesgo Alto	Mitigar	A.9.1.4 Protección contra amenazas externas y ambientales A.10.5.1 Recuperación de la información	Se debe adquirir e instalar equipos contra incendios dentro de la organización. Se debe obtener un resguardo de esta información en formato digital para evitar la pérdida de los documentos en un incendio	Control Preventivo / Control Correctivo	Jefe del Departamento de Seguridad Postal / Encargado del Departamento de Digitalización
R106	Digitalización	Reporte de Guias de Admisión	2	3	2	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño del reporte de guías de admisión debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R107	Digitalización	Reporte diario para devolución de cargos	2	3	2	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de la sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño del reporte diario para devolución de cargos debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R108	Todos	Sellos Personales	3	--	2	Falta de gavetas con llave para guardar los sellos personales	Hurto de sellos	Riesgo de pérdida de disponibilidad y no repudio debido a la pérdida o robo de los sellos del personal supervisor de cada área, causado por la falta de lugares adecuados para su almacenamiento.	Baja	Moderado	8	Riesgo Bajo	Seguir Monitoreando	--	--	--	Oficial de Seguridad de la Información
R109	Todos	Servidor de archivos	3	3	4	Abuso de los privilegios	Falta de auditorías (supervisiones) programadas o inopinadas	Riesgo de compromiso de información debido a un ingreso no autorizado al servidor de archivos, a causa de la falta de auditorias al servidor	Moderada	Mayor	18	Riesgo Alto	Mitigar	A.10.10.1 Registro de auditoria	La organización debe producir, analizar y almacenar los logs de auditoria el tiempo que se establezca necesario de tal forma que ayude a investigaciones futuras	Control Detectivo	Jefe del Departamento de Tecnología
R110	Todos	Servidor de archivos	3	3	4	Usuarios Mal intencionados	Falta de pruebas de hacking etico	Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección.	Moderada	Mayor	18	Riesgo Alto	Mitigar	A.10.6.1 Controles de red A.10.6.2 Seguridad de los servicios de redes	Se deberá desarrollar un plan de análisis de vulnerabilidades que permita identificar los principales problemas en los sitemas y ayude a elaborar procedimientos para corregirlos.	Control Detectivo	Jefe del Departamento de Tecnología
R111	Digitalización	SIM 2.0	2	3	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "cierre de sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información del SIM 2.0. debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Alta	Menor	8	Riesgo Bajo	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R112	Digitalización	SIM 2.0	2	3	3	Algunas computadoras del área no pueden transferir imágenes al servidor	Los imágenes deben ser transferidas desde una computadora hacia otra para luego ser subidas al servidor y, en algunos casos, se pierde la información	Riesgo de pérdida o daño de la información digitalizada debido a errores en la transferencia de archivos de una computadora a otra, a causa de problemas para transferir los archivos directamente al servidor	Alta	Moderado	16	Riesgo Alto	Evitar	A.11.2.2 Gestión de privilegios	Se debe establecer una directiva en la cual se precise cuales son los perfiles y privilegios que deben tener los usuarios dependiendo de sus roles y responsabilidades para que no afecte su operatividad diaria	Control Preventivo	Jefe de Departamento de Sistemas de Información
R113	Digitalización	SIM 2.0	2	3	3	Defectos conocidos en el Sistema	Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Riesgo de daño o deterioro del sistema SIM 2.0 debido a algún defecto conocido en el sistema sin ser solucionado en el tiempo	Alta	Moderado	16	Riesgo Alto	Mitigar	A.12.6.1 Control de vulnerabilidades técnicas	Se debe tener un registro de los errores reportados por cada uno de los usuarios indicando datos como el error, el sistema, causas y la solución encontrada para el problema	Control Correctivo	Jefe de Departamento de Sistemas de Información
R114	Digitalización	SIM 2.0	2	3	3	Demora en la entrega de credenciales a los usuarios nuevos	Transferencia no autorizada de contraseñas validas mientras se espera por las nuevas credenciales	Riesgo de pérdida de la disponibilidad e integridad de datos en el sistema SIM 2.0 debido al uso de una misma contraseña por varios usuarios causados por la demora en la entrega de accesos a usuarios	Moderada	Menor	6	Riesgo Bajo	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Sistemas de Información
R115	Recepción	SIM 2.0	2	3	3	Demora en la entrega de nuevos usuarios	Transferencia no autorizada de contraseñas validas	Riesgo de pérdida de la disponibilidad e integridad de datos en el sistema SIM 2.0 debido al uso de una misma contraseña por varios usuarios causados por la demora en la entrega de accesos a usuarios	Alta	Menor	8	Riesgo Bajo	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Sistemas de Información
R116	Recepción	SIM 2.0	2	3	3	Error en el uso	Falta de documentación	Riesgo de pérdida o daño de la información almacenada en el SIM 2.0 debido a errores de uso del sistema, a causa del desconocimiento en el manejo del sistema	Moderada	Menor	6	Riesgo Bajo	Seguir Monitoreando	--	--	--	Jefe de Departamento de Sistemas de Información
R117	Recepción	SIM 2.0	2	3	3	Falla del equipo de telecomunicaciones	Dependencia de la red para el correcto funcionamiento del sistema	Riesgo de pérdida de información del SIM 2.0. debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R118	Control de Cargos	SIM 2.0	2	2	3	Falla del equipo de telecomunicaciones	Dependencia de la red para el correcto funcionamiento del sistema	Riesgo de caida del sistema debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R119	Digitalización	SIM 2.0	2	3	3	Falla del equipo de telecomunicaciones	Dependencia de la red para el correcto funcionamiento del sistema	Riesgo de pérdida del acceso a la información del sistema SIM 2.0. debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R120	Control de Cargos	SIM 2.0 - Módulo de Devoluciones	2	2	3	Demora en la entrega de accesos a los usuarios	Claves compartidas por varios usuarios para el ingreso	Riesgo de pérdida de la información y auditabilidad en el sistema SIM debido al intercambio no autorizado de claves, a causa de la demora en la entrega de accesos a los usuarios.	Muy Alta	Menor	10	Riesgo Alto	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Sistemas de Información
R121	Control de Cargos	SIM 2.0 - Módulo de Devoluciones	2	2	3	Falla del equipo de telecomunicaciones	Dependencia de la red para el correcto funcionamiento del sistema	Riesgo de caida del sistema debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R122	Todos	Sistema de Camaras de Seguridad	--	--	3	Pérdida del suministro de energía	Cámaras de seguridad se alimentan directamente de la energía electrica por 10 minutos hasta que se prenda el grupo electrógeno mientras se espera la adquisición de un UPS que se encarge de las camaras	Riesgo de compromiso de información confidencial y activos de la organización debido a la desconexión de camaras de seguridad, a causa de fallas de energía eléctrica	Alta	Moderado	16	Riesgo Alto	Mitigar	A.9.2.2 Suministro eléctrico	Se deberá solicitar la compra de un equipo UPS capaz de brindar de electricidad a las cámaras de seguridad mientras se enciende el grupo electrógeno	Control Preventivo	Encargado de Seguridad Física de la Empresa
R123	Todos	Sistema de Camaras de Seguridad	--	--	3	Usuarios mal intencionados	Lugar inapropiado donde guardar la información de las camaras	Riesgo de daño o pérdida de la grabación del lugar donde se almacena la información del circuito cerrado de television debido a un robo o ataque, a causa de que la grabación se guarda en ese mismo lugar.	Muy Baja	Mayor	6	Riesgo Bajo	Mitigar	A.10.5.1 Recuperación de la información	Aquellas imágenes grabadas por la cámara de seguridad que se encarga de resguardar el centro de almacenamiento de imágenes del sistema cerrado de televisión de la empresa deberán ser almacenadas en un ambiente aparte, debidamente acondicionado para asegurar su disponibilidad ante un posible ataque	Control Correctivo	Encargado de Seguridad Física de la Empresa

Id Riesgo	Proceso	Activo de Información				Identificación del Riesgo			Evaluación del Riesgo				Tratamiento del Riesgo				
		Nombre del Activo de Información	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Valor del Riesgo	Tipo de Tratamiento	Control Alineado a la NTP ISO/IEC 17799	Control Específico	Tipo de Control	Responsable
R124	Clasificación	SOP Empresarial	2	3	3	Acceso de usuarios no autorizados a sistemas o redes	Falta de "bloqueo de sesión" cuando se abandona la estación de trabajo	Riesgo de pérdida o daño de la información debido a la falta de bloqueo de sesión al abandonar la estación de trabajo, a causa de la falta de capacitación de seguridad en el área	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.3.2 Equipo informático de usuario desatendido	Se debe realizar capacitaciones de seguridad de información con los trabajadores de la organización	Control Preventivo	Oficial de Seguridad de la Información
R125	Clasificación	SOP Empresarial	2	3	3	Demora en la entrega de accesos a los usuarios	Transferencia no autorizada de contraseñas validas	Riesgo de pérdida de la disponibilidad e integridad de datos debido al uso de una misma contraseña por varios usuarios causados por la demora en la entrega de accesos a usuarios	Moderada	Moderado	12	Riesgo Alto	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión en la creación de usuarios.	Control Correctivo	Jefe de Departamento de Sistemas de Información
R126	Clasificación	SOP Empresarial	2	3	3	Error en el uso	Falta de documentación	Riesgo de pérdida o daño de la información almacenada en el SOP Empresarial debido a errores de uso del sistema, a causa del desconocimiento en el manejo del sistema	Alta	Moderado	16	Riesgo Alto	Mitigar	A.10.1.1 Documentación de procedimientos operativos	Se deberá realizar y mantener el manual de usuario del sistema SOP para facilitar el trabajo a personal nuevo de la empresa	Control Preventivo	Jefe de Departamento de Sistemas de Información
R127	Clasificación	SOP Empresarial	2	3	3	Falla del equipo de telecomunicaciones	Dependencia de la red para el correcto funcionamiento del sistema	Riesgo de pérdida de información debido a una falla en los equipos de telecomunicaciones	Moderada	Moderado	12	Riesgo Alto	Transferir	A.10.6.1 Controles de redes	Se debe establecer procedimientos y SLA adecuados con los proveedores del servicio de comunicaciones que cubran las necesidades de la organización	Control Preventivo	Jefe de Departamento de Tecnología
R128	Clasificación	SOP Empresarial	2	3	3	Falta de permisos para que cada usuario cambie la contraseña que utiliza	Transferencia no autorizada de contraseñas validas	Riesgo de pérdida de la disponibilidad e integridad de datos debido al uso de una misma contraseña por varios usuarios causados por la falta de un módulo de mantenimiento que permita cambiar las claves al usuario	Alta	Moderado	16	Riesgo Alto	Mitigar	A.11.5.3 Sistema de gestión de contraseñas	Establecer procedimientos para una adecuada gestión de contraseñas dentro del sistema	Control Correctivo	Jefe de Departamento de Sistemas de Información

10. Anexo 10 – Declaración de Aplicabilidad

Anexo 10 - Declaración de Aplicabilidad NTP ISO 27001				
No. De Control	**Control**	**Objetivo de Control**	**Aplicable a la Organización**	**Justificación**
A.5	**Política de Seguridad**			
A.5.1.	***Política de seguridad de la información***	**Dirigir y dar soporte a la gestión de seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones**		
A.5.1.1	Documentos de política de seguridad de la información	La gerencia deberá aprobar, publicar y comunicar a todos los empleados y terceras partes que lo requieran.	SI	Actualmente la organización posee una política de seguridad de la información aprobada por el comité; sin embargo, aún no se ha hecho pública formalmente, esto se debe a que aún se está planificando la manera adecuada para divulgar esta información.
A.5.1.2	Revisión de la política de seguridad de la información	La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva	SI	Dentro de la política aprobada, se ha especificado cuales son los roles y responsabilidades relacionados a la seguridad de la información, adicionalmente, se especificó cada cuanto tiempo se debe revisar la política y el alcance del SGSI para que pueda ser actualizada de ser necesario.
A.6	**Aspectos organizativos para la seguridad**			
A.6.1	***Organización interna***	**Gestionar la seguridad de la información dentro de la organización**		
A.6.1.1	Comité de gestión de seguridad de la información	La gerencia debe respaldar activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de responsabilidades de la seguridad de información	SI	Dentro de la organización se emitió una resolución de gerencia general con N° 026 G/2014 donde se nombró un comité de seguridad de la información asi como un oficial de seguridad de la información los cuales se reunen de manera periodica para la aprobación de documentos y revisión de avances.
A.6.1.2	Coordinación de la seguridad de la información	Las actividades en la seguridad de la información deben ser coordinados por representantes de diferentes partes de la organización que tengan roles relevantes y funciones de trabajo	SI	En la resolución de gerencia general con N° 026 G/2014 se designó como miembros de comité a las siguientes personas: - Sub Gerente de Tecnologias de la Información - Gerente de Desarrollo Corporativo - Gerente Comercial - Gerente Postal - Gerente de Administración de Recursos
A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.	SI	Dentro de la política de Seguridad de la Información, que fue aprobada por el comité de seguridad, se encuentra definido los roles y responsabilidades sobre seguridad de la información
A.6.1.4	Proceso de autorización para las nuevas instalaciones de procesamiento de información	Debe establecerse y definirse un proceso de gestión de autorización para facilitar los nuevos procesamientos de información	SI	Se debe definir un nuevo procedimiento en el cual se indique cual es la gestión adecuada para adquirir o recibir nuevos recursos para el tratamiento de la infromación, algo que por el momento no está normado en la empresa.
A.6.1.5	Acuerdos de confidencialidad	Se debe identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidad de la organización para la protección de información	SI	Actualmente se puede evidenciar la existencia de acuerdos de confidencialidad en los contratos con los proveedores, trabajadores y locadores de la organización para evitar la divulgación de información. Sin embargo, se debe emitir una normativa adecuada en la cual se indique cada cuanto se debe revisar y actualizar estos acuerdos de confidencialidad con los trabajadores
A.6.1.6	Contacto con autoridades	Deben mantenerse contactos apropiados con autoridades relevantes	SI	La entidad encargada de revisar estos temas a nivel nacional es el ONGEI, actualmente se sabe que la ONGEI trata directamente con el oficial de seguridad de la información; sin embargo, aún se debe difundir los temas que tratan ambas partes tanto con la organización, como con el comité de seguridad de la información.
A.6.1.7	Contacto con grupos de interés especial	Se debe mantener contactos con grupos de interés especial u otros foros de especialistas en seguridad así como de asociaciones profesionales	SI	Se debe establecer lazos y conexiones con personal especializado relacionado a seguridad de la información, por el momento la única institución con la que se ha hecho contacto es con la ONGEI, encargada de supervisar la implementación del SGSI a nivel nacional.
A.6.1.8	Revisión independiente de la seguridad de la información	El alcance de la organización para manejar la seguridad de la información, así como su implementación (como por ejemplo: los objetivos de control, los controles, las políticas, procesos y procedimientos) deben ser revisados independientemente durante intervalos planificados o cuando ocurran cambios significativos en la implementación.	SI	Es importante que la organización pueda recibir una opinión externa sobre el estado de la seguridad que posee; es por ello que como parte del proceso de implementación del SGSI, se ha decidido iniciar un proceso de contratación de una empresa consultora especialista en seguridad para que brinde apoyo en el proyecto.
A.6.2	***Seguridad en los accesos de terceros***	**Mantener la seguridad de las instalaciones de procesamiento de la información organizacional que acceden, procesan, comunican o gestionan terceros.**		
A.6.2.1	Identificación de riesgos por el acceso de terceros	Se evaluará los riesgos asociados con el acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementarán controles de seguridad adecuados antes de permitir su acceso.	SI	Es necesario que la organización posea controles adecuados para gestionar e identificar los posibles riesgos de accesos de terceros a la organización, formalmente, no existe un análisis de riegos para ello; sin embargo, en algunos casos, el personal de la organización ha logrado identificar algunos posibles riesgos.
A.6.2.2	Requisitos de seguridad cuando se trata con clientes	Se deben identificar todos los requisitos de seguridad antes de dar acceso a clientes a los activos o la información de la organización	SI	Se debe establecer una documentación formal de cuales son los requisitos de seguridad minimos que se solicitaran a los clientes para darles acceso. Actualmente existen controles para el acceso físico de personal externo; sin embargo, en muchos casos estos controles no se cumplen en su totalidad.
A.6.2.3	Requisitos de seguridad en contratos de outsourcing	Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información organizacional o la adición de productos o servicios a dichas instalaciones, deben cubrir todos los requisitos de seguridad necesarios.	SI	La organización debe establecer una serie de controles para asegurar la seguridad de la información al momento de trabajar con terceros, ya que hasta el momento, solo se ha contemplado el realizar acuerdos de confidencialidad con ellos.
A.7	**Clasificación y control de activos**			
A.7.1	***Responsabilidad por los activos***	**Mantener la protección apropiada de los activos de la organización**		
A.7.1.1	Inventario de activos	Se elaborará y mantendrá un inventario de todos los activos importantes que sean claramente identificados	SI	Como parte del proceso del diseño del SGSI se ha realizado un inventario de activos de información en los procesos involucrados en el alcance.
A.7.1.2	Propiedad de los activos	Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad de una parte designada de la organización	SI	Como parte del proceso del diseño del SGSI se ha realizado un inventario de activos de información en los procesos involucrados en el alcance indicando claramente quienes son los propietarios de los activos y en que procesos estan involucrados.

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.7.1.3	Uso aceptable de los activos	Se debe identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones del procesamiento de la información.	SI	Actualmente en la organización existe un reglamento interno de trabajo en el cual, en el capitulo doce (XII), se hace mención a la correcta utilización de los activos de la empresa; sin embargo, se ha podido verificar que no existe una correcta difusión del mismo
A.7.2	***Clasificación de la información***	**Asegurar que los activos de información reciban un nivel de protección adecuado.**		
A.7.2.1	Guías de clasificación	La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización	SI	Aunque dentro de la organización se maneja información importante y confidencial, actualmente no existe una clasificación adecuada para la misma, por lo que es necesaria su definición.
A.7.2.2	Etiquetado y tratamiento de la información	Se definirá e implementará un conjunto de procedimientos apropiados para etiquetar y manejar información, de conformidad, con el esquema de clasificación adoptado por la organización	SI	Debido a que no se posee una clasificación para la información, tampoco existe una directiva o procedimiento que permita clasificarla adecuadamente, razón por la cual es necesaria su realización.
A.8	**Seguridad en Recursos Humanos**			
A.8.1	***Seguridad antes del empleo***	**Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que sean adecuados a los roles para los cuales han sido considerados, y reducir asi, el riesgo de hurto, fraude o mal uso de las instalaciones**		
A.8.1.1	Roles y Responsabilidades	Se definirán y documentarán los roles de seguridad y las responsabilidades de los empleados, contratistas y usuarios externos en concordancia con la política de seguridad de la información de la organización	SI	Se debe de establecer, en cada uno de los contratos que se hacen firmar a los trabajadores, los roles y responsabilidades que poseerán dependiendo de los cargos a los que ingresen
A.8.1.2	Investigación	Se debe hacer un chequeo y verificación de informaciones anteriores de todos los candidatos para empleo, contratistas y personal externo, en concordancia con las leyes, regulaciones y ética; y proporcional a los requisitos del negocio, la clasificación de la información a ser accedida y a los riesgos percibidos	SI	Como parte del proceso de selección, la sub gerencia de recursos humanos se encarga de revisar los antecedentes penales y policiales de cada uno de los canditatos a un puesto laboral, asi como una verificación si es que lo indicado en el CV del postulante es verdadero; sin embargo, se debe establecer un procedimiento que indique el nivel de investigación necesario dependiendo del cargo que la persona vaya a ocupar en la organización.
A.8.1.3	Términos y condiciones de la relación laboral	Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad como como parte de los términos y condiciones iniciales de su empleo en donde se señalará la responsabilidad del empleado en cuanto a la seguridad de la información.	SI	Dentro del contrato firmado por los trabajadores se establece una clausula de confidencialidad; sin embargo, en ella también se debe establece cuales son los roles y responsabilidades con respecto a la protección de datos, clasificación de información o tratamiento de información de terceros y las sanciones en caso de no cumplir con lo acordado.
A.8.2	***Durante el empleo***	**Asegurar que todos los empleados, contratistas y usuarios externos sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que estén preparados para aplicar la política de seguridad de la organización en el curso de trabajo normal y reducir el riesgo de error humano**		
A.8.2.1	Responsabilidades de la gerencia	La gerencia debe requerir a sus empleados, contratistas y a los usuarios externos aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización	SI	La organización deberá hacer publica, dentro de la organización, cada uno de las políticas y procedimientos relacionados a la seguridad de la información una vez sean aprobadas, hasta el momento solo se ha aprobado el alcance, política y objetivos del SGSI; sin embargo, aún no se ha iniciado con la difusión de los mismos.
A.8.2.2	Concientización, educación y entrenamiento en la seguridad de la información	Todos los empleados de la organización, y donde sea relevante, contratistas y usuarios externos deben recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.	SI	La organización debe de realizar, con cada uno de sus empleados, charlas de concientización y capacitación, relacionadas a seguridad de la información, de manera regular.
A.8.2.3	Proceso disciplinario	Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad	SI	Dentro de la política de Seguridad de la Información, que fue aprobada por el comité de seguridad, se encuentra definida las sanciones que aplicarán al personal que no cumpla con la misma.
A.8.3	***Finalización o cambio del empleo***	**Asegurar que los empleados, contratistas y usuarios externos dejen o cambien de organización de una forma ordenada**		
A.8.3.1	Responsabilidades de finalización	Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados, tan pronto como sea posible.	SI	Se debe establecer procedimientos adecuados para permitir al personal reportar incidentes de seguridad y darles un tratamiento adecuado hasta que sean cerrados por completo.
A.8.3.2	Devolución de activos	Todos los empleados, contratistas y usuarios externos deben realizar la devolución de los activos de la organización que están en su posesión cuando termine su empleo, contrato o acuerdo	SI	Actualmente, la organización tiene un formato para la devolución de laptops y celulares; sin embargo, se debe establecer un procedimiento formal para la devolución de activos en toda la organización
A.8.3.3	Retiro de los derechos de acceso	El derechos de acceso a la información y a las instalaciones de procesamiento de información, que se le otroga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios	SI	En caso exista un cambio en la terminación del empleo de alguna persona, se envía un correo a todas las áreas para saber si esta persona posee alguna deuda con la organización, es gracias a este correo que el área de TI se informa del caso; sin embargo, no hay una comunicación formal en caso rote el personal, debido a ello se debe crear estos procedimientos para dar de baja al usuario correctamente.
A.9	**Seguridad física y del entorno**			
A.9.1	***Áreas seguras***	**Prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización**		
A.9.1.1	Seguridad física perimetral	Las organizaciones usarán perímetros de seguridad (como paredes, puertas con control de entrada por tarjeta o recepciones) para proteger áreas que contienen información e instalaciones de procesamiento de información	SI	La organización posee controles de seguridad alrededor del perímetro del CCPL o sede central; sin embargo, cabe aclarar que no posee camaras de seguridad capaces de monitorear el perimetro al 100%. Adicionalmente, la organización debe establecer procedimientos para controlar el acceso de personal autorizado a las distintas áreas de la organización.

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.9.1.2	Controles físicos de entradas	Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que unicamente personal autorizado pueda ingresar	SI	Se debe establecer un procedimiento para que todo el personal de SERPOST utilice un identificador dentro de las instalaciones, además, todo personal externo debe portar una identificación que indique los lugares a los que tiene permiso para acceder. Por último, existen lugares con información sensible, como el CPD, que no poseen controles adecuados para asegurar la integridad de los equipos.
A.9.1.3	Seguridad de oficinas, despachos y recursos	Se deben designar y mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.	SI	La organización debe mejorar la infraestructura del centro de procesamiento de datos y establecer controles de acceso a las áreas operativas donde se lleva a cabo los procesos pertenecientes al alcance del SGSI
A.9.1.4	Protección contra amenazas externas y ambientales	Se deben designar y mantener protección física contra daños por fuego, inundación, terremoto, explosión, manifestación civil y otras formas de desastre natural o realizado por el hombre.	SI	Se debe instalar detectores de humo dentro de la organización, tanto en el área operativa como en las áreas de soporte pertenecientes al alcance del SGSI. Con respecto al centro de procesamiento de datos, deben establecerse controles ambientales adecuados para evitar el deterioro o daño de los equipos o sus componentes.
A.9.1.5	El trabajo en las áreas seguras	Se debe designar y mantener protección física y pautas para trabajar en áreas seguras	SI	Actualmente, la organización no ha establecido controles adecuados para proteger el CPD por lo que se recomienda modificar la estructura que se encarga de resguardar ese lugar; adicionalmente, dentro de las áreas operativas, se almacena información considerada importante para los dueños de los procesos dentro de cajas, por lo que se recomienda evaluar la posibilidad de adquirir una infraestructura adecuada para el almacenamiento de esta información
A.9.1.6	Areas de carga, descarga y acceso público	Las áreas de carga, descarga y acceso público y otras áreas donde las personas tengan acceso, deben controlarse y, cuando sea posible, aislarse de las instalaciones de procesamiento de información para evitar un acceso no autorizado	SI	Existen controles para dar acceso a personal externo a la organización; sin embargo, estos controles poseen varias deficiencias por lo que deben ser mejorados y monitoreados. No obstante, las áreas de carga y descarga de envíos y paqueterías estan debidamente separadas de las instalaciones de procesamiento de datos.
A.9.2	***Seguridad de los equipos***	**Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización**		
A.9.2.1	Ubicación y protección de equipos	El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidad de acceso no autorizado.	SI	Se debe establecer normas para evitar comer o beber cerca de los equipos. También, se debe establecer controles de acceso a las áreas operativas involucradas en el alcance del SGSI, debido a que los equipos con ángulos de visión muy expuestos a personal no autorizado. Adicionalmente, se debe modificar la infraestructura del centro de procesamiento de datos, debido a que no es la adecuada para almacenar los equipos con la información crítica de la organización.
A.9.2.2	Suministro eléctrico	El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el suministro eléctrico.	SI	Los equipos que forman parte del área de Tecnologías de Información estan protegidos por dos UPS con carga suficiente para 30 minutos, tiempo que demora el grupo electrógeno en encenderse, y que necesitan ser renovados. No obstante, se ha reportado casos en los que el grupo ha fallado, incluso, este no es capaz de cubrir a la organización al 100%, por lo que se debe tomar medidas para la adquisición de un nuevo grupo electrógeno que cubra a toda la organización.
A.9.2.3	Seguridad del cableado	Se protegerá el cableado de energía y telecomunicaciones que transporten datos o respalden servicios de información frente a interceptaciones o daños.	SI	El cableado de la organización fue realizado por personal de la misma empresa a través de los años, como resultado, no esta debidamente rotulada e incluso se puede observar que ha sido instalada de forma desordenada en varias áreas de trabajo, por ello, se debe realizar un proyecto para realizar un correcto cableado estructural dentro de la organización.
A.9.2.4	Mantenimiento de equipos	El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad	SI	Luego de realizar una serie de entrevistas con el personal dueño de los procesos relacionados al alcance del SGSI, se corroboró la falta de un procedimiento adecuado para dar mantenimiento a los equipos utilizados en cada área, tales como computadoras, escaners, impresoras, lectoras de código de barras, etiquetadoras, routers, switches, grupos electrógenos y UPS.
A.9.2.5	Seguridad de equipos fuera de los locales de la organización	Se debe aplicar seguridad al utilizar equipamiento para procesar información fuera de los locales de la organización tomando en cuenta los diferentes riesgos en los que se incurre.	SI	Existe un procedimiento para entregar equipos al personal autorizado; sin embargo, se debe implementar controles para proteger la información que se maneja dentro de los equipos debido a que, en caso de pérdida o robo, solo se realiza una denuncia policial y un pago equivalente al costo del activo físico, más no existe forma de proteger la información que esta llevaba.
A.9.2.6	Seguridad en el re-uso o eliminación de equipos	Todos los equipos que contienen almacenamiento de datos deben ser revisados con el fin de asegurar que los datos sensibles y los software con licencia han sido removido o sobrescritos antes de desecharlos o reutilizarlos.	SI	Hasta el momento este tipo de labores son realizados por el personal de tecnologías de información sin haber sido debidamene documentados, por ello, se deberá realizar un procedimiento formal para la eliminación y re-uso de los equipos electrónicos.
A.9.2.7	Retiro de la propiedad	Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.	SI	Existe un procedimiento para entregar equipos al personal autorizado, asi como un formato para autorizar la salida de las laptops fuera de la organización; sin embargo, se sabe que en muchos casos este formato no es utilizado; por lo que se deberá revisar y actualizar este procedimiento para adecuarlo a las necesidades actuales de SERPOST.
A.10	**Gestión de comunicaciones y operaciones**			
A.10.1	***Procedimientos y responsabilidades de operación***	**Asegurar la operación correcta y segura de los recursos de tratamiento de información**		
A.10.1.1	Documentación de procedimientos operativos	Los procedimientos operativos deberán estar documentados, mantenidos y estar disponibles a todos los usuarios que lo requieran.	SI	Se debe documentar adecuadamente la realización de los procedimientos operativos de la organización. Hasta el momento, estas labores no han sido documentadas y se realizan según los conocimientos de los usuarios.

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.10.1.2	Gestión de cambios	Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información.	SI	La organización posee un formato de transferencia de bienes patrimoniales en caso se necesite cambiar el equipamiento de un área; sin embargo, no existe un formato similar para el cambio de los sistemas. Tampoco existe un procedimiento formal de como realizar estos cambios ni formatos que evidencien los análisis de riesgos ni las pruebas realizadas previas al cambio, por lo que se deberá implementar estos cambios en coordinación con el área de tecnologia y comunicaciones que es la encargada de la realización de estos procesos.
A.10.1.3	Segregación de tareas	Se segregarán las obligaciones y las áreas de responsabilidad con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la organización	SI	Dentro de la organización existen perfiles tanto para los correos, como para el acceso a internet y a los sistemas; sin embargo, se debe elaborar un procedimiento formal para la asignación de perfiles a los usuarios nuevos que lo requieran, el establecimiento un tiempo máximo de atención ante la solicitud de estos perfiles y actualizar los perfiles según las necesidades actuales del negocio.
A.10.1.4	Separación de las instalaciones de desarrollo, prueba y operación	Se separarán las instalaciones de desarrollo, prueba y operación con el fín de reducir el riesgos de acceso no autorizado o cambios en el sistema operacional	SI	En la organización se manejan los tres ambientes solicitados, pero se debe documentar un procedimiento oficial especificando quienes tienen permisos para acceder a dichos entornos y bajo que circunstancias se puede trabajar con cada uno de ellos.
A.10.2	***Gestión de servicios externos***	**Implementar y mantener un nivel apropiado de seguridad de información y servicios de entrega en concordancia con los acuerdos de servicio de entrega por parte de terceros**		
A.10.2.1	Entrega de servicios	Debemos asegurarnos que los controles de seguridad, las definiciones de servicio y los niveles de entrega incluidos en el acuerdo de servicios externos sean implementados, esten operativos y sean mantenidos por el personal externo	SI	En la organización no existe una adecuada gestión de los proveedores debido a la falta de indicadores que permitan medir adecuadamente el cumplimiento de los acuerdos de nivel de servicio establecidos. Adicionalmente, se debe actualizar cada uno de los acuerdos realizados con ellos para contemplar los controles de seguridad que apliquen con cada uno de ellos.
A.10.2.2	Monitoreo y revisión de los servicios externos	Los servicios, reportes y registros provistos por terceras partes deben ser monitoreados y revisados regularmente. Igualmente, se deben llevar a cabo auditorías con regularidad.	SI	La organización debe establecer métricas adecuadas para una adecuado monitoreo de los servicios entregados por los proveedores.
A.10.2.3	Gestión de cambios de los servicios externos	Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de la política de seguridad de información,procedimientos y controles, tomando en cuenta la criticidad de los sistemas de negocio y procesos envueltos en la reevalución de riesgos.	SI	La organización debe realizar un procedimiento adecuado, en el cual se indique como se debe gestionar los cambios en los servicios prestados por los terceros, tanto para modificaciones de políticas de la organización o implementación de nnuevos controles para los proveedores, como para la solicitud del uso de nuevas tecnologías como parte del servicio
A.10.3	***Planificación y aceptación del sistema***	**Minimizar el riesgo de fallos de los sistemas**		
A.10.3.1	Gestión de la capacidad	Se monitorearán las demandas de capacidad y se harán las proyecciones de futuros requisitos de capacidad para asegurar el desarrollo requerido por el sistema	SI	Dentro de la organización existe un procedimiento formal de como se debe realizar la planificación de nuevos proyectos y el analisis de los requerimientos de nuevos sistemas. Sin embargo, se debe evidenciar el correcto cumplimiento de este procedimiento dentro de la organización a través de los años.
A.10.3.2	Aceptación del sistema	Se establecerán los criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones y se llevarán a cabo pruebas adecuadas del sistema antes de su aceptación	SI	Dentro de la organización existe un procedimiento formal para la aceptación de los nuevos sistemas; sin embargo, se debe evidenciar el correcto cumplimiento de estos procedimientos, en muchos casos, no existen manuales de usuario actualizados para cada uno de los sistemas desarrollados por la empresa.
A.10.4	***Protección contra software malicioso***	**Proteger la integridad del software y de la información**		
A.10.4.1	Controles contra software malicioso	Para ofrecer protección frente a software malicioso, se implementarán controles de detección, prevención y procedimientos adecuados de toma de conciencia con los usuarios.	SI	Se debe adquirir un software que permita detectar, prevenir y eliminar código malicioso en los activos que manejan información dentro de la empresa, actualmente se utiliza un antivirus con licencia caducada, por lo que el nivel de protección no es el adecuado. Adicionalmente, se debe capacitar al personal para saber que hacer en caso se detecte algún software malicioso dentro de alguno de los activos que manejen.
A.10.4.2	Controles contra software móvil	Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este opere de acuerdo a una política de seguridad clara y definida. Igualmente, se debe prevenir la ejecución de código movil no autorizado.	SI	El personal de la organización posee roles definidos para navegar en internet, debido a ello, alguno usuarios no poseen permisos para descargar archivos que no esten vinculados a su correo, de igual forma, solo los administradores del sistema poseen permisos para lanzar algún ejecutable; sin embargo, este procedimiento debe ser normado oficialmente.
A.10.5	***Gestión interna de respaldo y recuperación***	**Mantener la integridad y la disponibilidad del procesamiento de información y servicios de comunicación**		
A.10.5.1	Recuperación de la información	Se obtendrán y probarán las copias de recuperación y respaldo de información y software regularmente en concordancia con la política acordada	SI	El área de TI realiza respaldos de la información almacenada en sus centro de datos con con una frecuencia determinada; sin embargo, los usuarios del área operativa no poseen un resguardo de la información que manejan, la única excepción, se da en el proceso de digitalización, pero estos resguardos se almacenan dentro de la misma área. De igual forma, los respaldos de TI se almacenan dentro del centro de datos, por lo que se debe establecer un procedimiento formal para determinar que información debe ser respaldada tanto del área de TI como del área operativa y definir lugares apropiados para el almacenamiento de estos respaldos.
A.10.6	***Gestión de seguridad de redes***	**Asegurar la salvaguarda de información en las redes y la protección de su infraestructura de soporte.**		

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.10.6.1	Controles de red	Se implementará un conjunto de controles para lograr y mantener la seguridad en las redes, y mantener la segurida de los sistemas y aplicaciones usuarios de la red, incluyendo la información en tránsito.	SI	Se debe establecer un procedimiento adecuado para separar las responsabilidades del personal encargado de las redes de la organización y del personal encargado de dar soporte a los equipos, adicionalmente se debe normar la implementación de controles para resguardar la información que viaja a través de las redes, tales como la encriptación de datos y la contratación de servicios para el análisis de vulnerabilidades a las redes de la organización.
A.10.6.2	Seguridad de los servicios de redes	Se deben identificar e incluir en cualquier acuerdo de servicio de red los aspectos de seguridad, niveles de servicio de red los aspectos de seguridad, niveles de servicio y requisitos de gestión, así estos servicios sea provistos interna o externamente.	SI	A través del directorio activo se ha establecido perfiles de acceso a las distintas carpetas compartidas y redes de la organización; sin embargo, se debe establecer procedimientos formales para monitorear y auditar la correcta gestión de accesos a la red. Se debe normar la revisión de los acuerdos de servicio con los proveedores de telecomunicaciones, debido a que este tipo de fallas se están volviendo muy comunes en la organización.
A.10.7	***Utilización y seguridad de los medios de información***	**Prevenir daños, modificaciones o destrucciones a los activos e interrupciones de las actividades del negocio.**		
A.10.7.1	Gestión de medios removibles	Deben de existir procedimientos para la gestión de medios removibles	SI	Se ha implementado una política para restringir el uso de los puertos USB dentro de la organización; sin embargo, no esta normado el correcto uso de estos medios para el almacenamiento de respaldos de información crítica para el negocio, ni la correcta eliminación de información de estos medios.
A.10.7.2	Eliminación de medios	Se eliminarán los medios de forma segura cuando ya no se necesiten, utilizando procedimientos formales	SI	Se debe establecer procedimientos formales para la eliminación de medios de almacenamiento de la información, tanto dígital como física, por el momento, solo se realiza con medios digitales en el área de TI.
A.10.7.3	Procedimientos de manipulación de la información	Se establecerán procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información de divulgaciones no autorizadas o su mal uso	SI	Se debe establecer procedimientos para la correcta manipulación de la información, desde una correcta clasificación, hasta como debe ser enviada a los interesados basados en esta clasificación, algo que no existe dentro de la organización.
A.10.7.4	Seguridad de la documentación de sistemas	La documentación de los sistemas se protegerá de accesos no autorizados	SI	En muchos casos no se posee una documentación adecuada de los sistemas de información desarrollados en la organización, debido a ello, no existe una adecuada difusión de los mismos, por lo que primero se debe actualizar esta documentación para luego establecer procedimientos formales para su correcta distribución.
A.10.8	***Intercambio de información***	**Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas**		
A.10.8.1	Políticas y procedimientos para el intercambio de información	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación	SI	En la organización no existen políticas o controles que permitan asegurar el intercambio de organización, por ello, se deberá establecer una serie de charlas de capacitación explicando a cada uno de los usuarios el cuidado que debe tener con la información sensible enviada a traves de los correos, se debe implementar controles para proteger los correos enviados y recibidos por el personal operativo.
A.10.8.2	Acuerdos de Intercambio	Se deben de establecer acuerdos para el intercambio de información y software entre la organización y entidades externas	SI	Al ser una organización que brinda un servicio de envíos de paqueteria, en los contratos realizados con los clientes, existe clausulas en las cuales se afirma que la información enviada por nuestros clientes deben ser tratadas como confidencial, en caso se pierda algún cargo o envío, se deberá presentar una denuncia policial para informar de este suceso a los clientes; sin embargo, no hay un procedimiento formal donde se establezca controles para asegurar esta información.
A.10.8.3	Seguridad de medios físicos en tránsito	Los medios a ser transportados deberán ser protegidos de acceso no autorizado, mal uso o corrupción durante su transporte fuera de los límites físicos de la organización	SI	El transporte de información de los clientes es realizado por el personal de la organización. Se debe establecer una serie de controles para asegurarla mientras se encuentre en transito. Para el caso de los respaldos de información, se está analizando la adquisicíon de los servicios de un proveedor para su almacenamiento, debido a ello, se deberá establecer una serie de controles para asegurar el correcto translado de esta información.
A.10.8.4	Seguridad del correo electrónico	La información contenida en los correos electrónicos debe ser protegida apropiadamente	SI	Se deberá sensibilizar a los usuarios para evitar que dejen desbloqueada su computadora ya que posee acceso a los correos de cada usuario, adicionalmente, se deberá implementar una serie de controles para asegurar la información ante código malicioso que pueda afectar la información.
A.10.8.5	Seguridad en los sistemas de información de negocios	Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio	SI	Se ha detectado que el sistema integrado de mensajeria presenta una serie de deficiencias al momento de compartir la información entre las áreas, lo que obliga, en muchos casos, a volver a ingresar la información registrada en un módulo para poder trabajar correctamente, debido a ello, se recomienda la verificación de la correcta interoperabilidad del sistema.
A.10.9	***Servicios de comercio electrónico***	**Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso**		
A.10.9.1	Seguridad en el Comercio Electrónico	El comercio electrónico pasando será protegido frente a actividades fraudulentas, controversias contractuales y divulgación o modificación de información.	NO	El presente control no aplica a la organización debido a que no brinda un servicio de comercio electrónico
A.10.9.2	Seguridad en las Transacciones en Línea	La información contenida en línea debe ser protegida para prevenir transmisiones incompletas, ruta incorrectas, alteración no autorizada de mensajes o duplicación no autorizado de mensajes.	NO	El presente control no aplica a la organización debido a que no brinda transacciones en línea
A.10.9.3	Información disponible públicamente	Se protegerá la integridad de la información públicamente disponible para prevenir modificaciones no autorizadas	SI	Se debe desarrollar una serie de procedimientos y responsabilidades para asegurar que la información mostrada dentro de la pagina web sea correcta y actualizada ya que por el momento no esta regulado
A.10.10	***Monitoreo***	**Detectar actividades de procesamiento de información no autorizadas**		

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.10.10.1	Registro de auditoria	Se deben producir y guardar, por un periodo acordado, los registros de auditoria que registran las actividades de los usuarios, excecpiones y eventos de seguridad, con el fin de asistir a investigaciones futuras y al monitoreo del control de acceso	SI	Para los equipos almacenados en el centro de datos, se posee una serie de logs de auditoria; sin embargo, estos no son analizados con regularidad, lo mismo sucede con los sistemas desarrollados para el área operativa; sin embargo, no se tiene logs de lo que realizan los usuarios en la red, por lo que se deberia incluir dentro de un procedimiento para una adecuada auditoria.
A.10.10.2	Uso del sistema de monitoreo	Se deben establecer procedimientos para monitorear las instalaciones de procesamiento de información y los resultados del monitoreo de actividades deben ser revisados regularmente	SI	Se debe establecer una serie de procedimientos para realizar un monitoreo adecuado a los servidores y bases de datos, entre los datos que se deben poseer se encuentra el formato de la bitacora de auditoria ajustado a las necesidades de la organización, la frecuencia con la que se dará este monitoreo, los responsables y las personas a las cuales se entregará los resultados finales.
A.10.10.3	Protección de la información de registro	Las instalaciones e información de registro debe ser registradas	SI	Dentro de la organización se busca proteger los logs de los sistemas y servidores; sin embargo, se debe documentar los procedimientos a seguir para asegurar un nivel adecuado de auditabilidad de las operaciones realizadas
A.10.10.4	Registro de administrador y operador	Las actividades del administrador y de los operadores del sistema deben ser registradas	SI	Dentro de la organización existen logs del sistema y de servidores que contienen cada uno de las acciones de los administradores y operarios; sin embargo, estos logs son almacenados por IBM y no son revisados de manera periodica, por lo que se debe establecer un procedimiento para la realización de esta labor.
A.10.10.5	Registros con faltas	Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas	SI	De las entrevistas realizadas con los usuarios, se detecto que los sistemas SIM y SOP poseen fallas que son reportadas en su momento al departamento de sistemas de información; sin embargo, no existe un registro oficial donde se almacene cuales han sido estos errores, los motivos por los cuales sucedieron ni cuales fueron las soluciones, por lo que se recomienda su inmediata documentación.
A.10.10.6	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo	SI	Existe un servidor de aplicaciones donde se alojan cada una de las aplicaciones de la organización; sin embargo, se debe establecer una documentación formal para la sincronización y/o ajuste del reloj
A.11	**Controles de acceso**			
A.11.1	***Requisitos de negocio para el control de accesos***	**Controlar los accesos a la información**		
A.11.1.1	Política de control de accesos	Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.	SI	Dentro de la organización existen perfiles tanto para los correos, como para el acceso a internet y a los sistemas; sin embargo, se debe documentar los requisitos de seguridad de manera independiente por cada sistema y documentar los perfiles estandar para cada puesto de trabajo dentro de la organización.
A.11.2	***Gestión de acceso de usuarios***	**Asegurar que el acceso de usuarios es autorizado y prevenir accesos no autorizados a los sistemas de información**		
A.11.2.1	Registro de usuarios	Habrá un procedimiento de registro y anulación formal de usuarios para otorgar y eliminar el acceso a todos los servicios y sistemas de información	SI	Como se indicó anteriormente en el control A.8.3.3, no existe una documentación formal para dar a conocer la terminación del empleo de algún trabajador, adicionalmente, tampoco existe un procedimiento formal para dar de alta o de baja a los nuevos usuarios, esta labor se ha ido realizando por el departamento de TI y según lo solicitado por las diversas áreas de la empresa; sin embargo, se debe documentar formalmente estos procedimientos.
A.11.2.2	Gestión de privilegios	Se restringirá y controlará la asignación y uso de privilegios	SI	Se debe generar un procedimiento adecuado, en el cual se indique que cada jefe de área o departamento, debe solicitar los permisos adecuados para cada personal que trabaje bajo su supervisión y establecer roles y responsabilidades para la adecuada gestión de privilegios.
A.11.2.3	Gestión de contraseñas de usuario	Se controlará la asignación de contraseñas a través de un proceso de gestión formal	SI	Se debe establecer una documentación formal en la cual se indique cuales son los pasos para la generación de contraseñas a nuevos usuarios, adicionalmente se deberá solicitar a los usuarios que firmen un compromiso para no compartir su contraseña con otros usuarios y realizar charlas de concientización para explicarles el porque no deben hacerlo.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	La gerencia conducirá un proceso formal y de manera periódica para revisar los derechos de acceso de los usuarios	SI	No existe una comunicación formal al departamento de TI del personal que rota dentro de la empresa, tampoco se realiza una revisión de los perfiles entregados a cada uno de los usuarios luego de un tiempo predeterminado, todas estas acciones deben estar debidamente documentadas en un procedimiento formal.
A.11.3	***Responsabilidad de los usuarios***	**Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento**		
A.11.3.1	Uso de contraseñas	Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas	SI	Existe un procedimiento formal con las reglas para la creación y cambio de contraseñas de los usuarios; sin embargo, se debe realizar una serie de charlas de concientización con los usuarios para evitar que se compartan contraseñas de manera no autorizada y para forzar el cambio de contraseña una vez se entregado por primera vez las credenciales al usuario.
A.11.3.2	Equipo informático de usuario desatendido	Se exige al usuario que asegure protección adecuada a un equipo desatendido	SI	No existe una normativa formal que exiga a los usuarios el bloqueo de las computadoras al momento de ausentarse; sin embargo, se debe realizar charlas de concientización con los usuarios para que adopten esta costumbre, adicionalmente, se debe forzar que las computadoras se bloqueen automaticamente luego de un tiempo de estar desatendidas

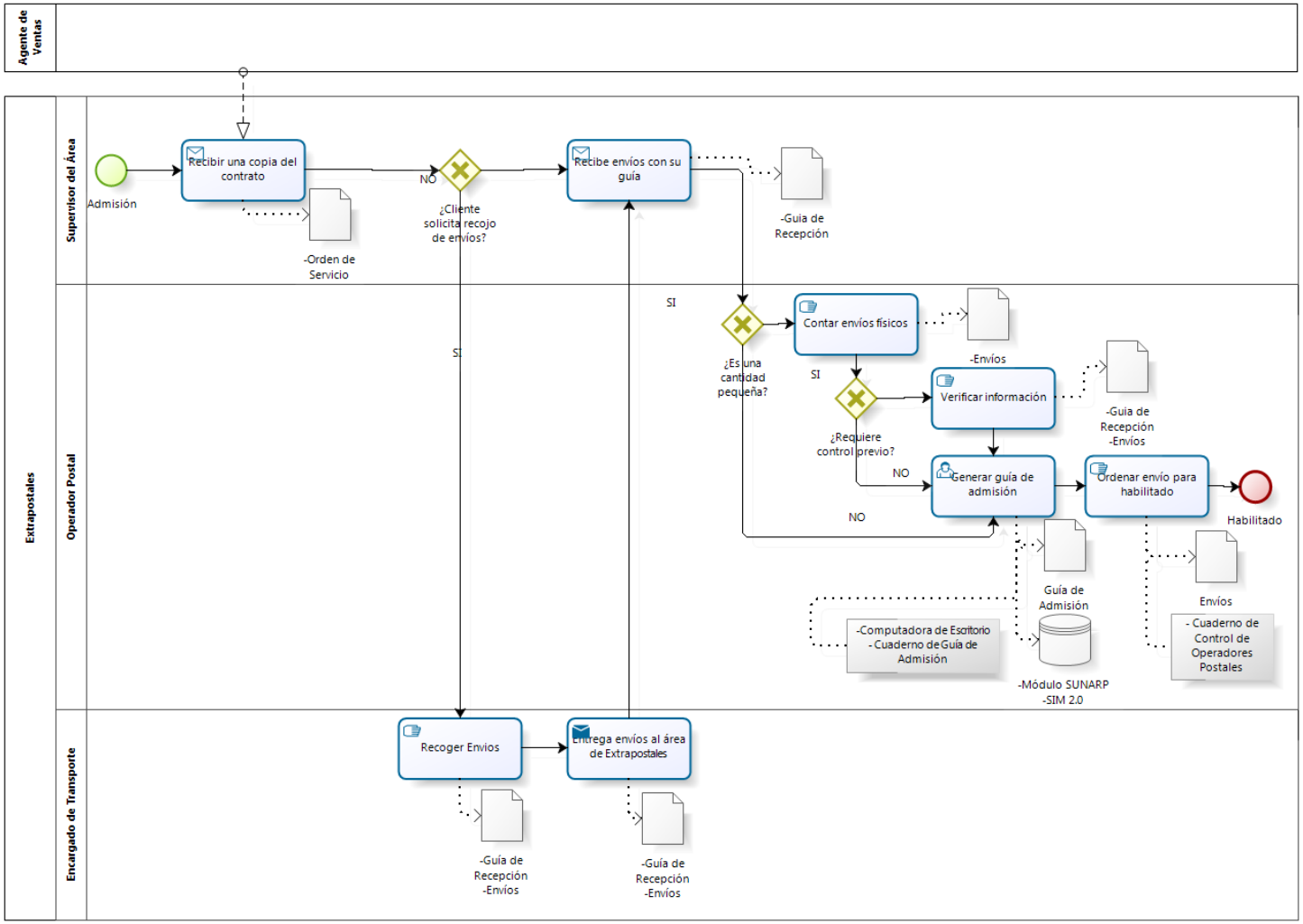
No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.11.3.3	Política de pantalla y escritorio limpio	Se debe adoptar una política de escritorio limpio para papeles y dispositivos de almacenamiento removibles. Igualmente, se debe adoptar una política para instalaciones de procesamiento de información	SI	No existe una política formal para mantener la pantalla y los escritorios de trabajo limpios, se debe establecer una política junto con una adecuada clasificación de la información, para asegurar aquellos activos que son importantes para la organización, adicionalmente, se debe de proveer a las áreas de lugares o equipamiento adecuado para que puedan asegurar este tipo de información.
A.11.4	***Control de acceso a la red***	**Prevenir el acceso no autorizado de los servicios de la red**		
A.11.4.1	Política de uso de los servicios de la red	Los usuarios deben tener acceso directo únicamente a los servicios cuyo uso está especificamente autorizado	SI	El directorio activo restringe el acceso de los usuarios únicamente a los servicios a los que se le ha permitido; sin embargo, se debe realizar una documentación formal de estas acciones.
A.11.4.2	Autenticación de usuario para conexiones externas	Deben usarse apropiados métodos de autenticación para controlar el acceso de usuarios remotos	SI	La organización posee un VPN para que algunos usuarios autorizados, no más de 10, puedan conectarse a la red de manera remota. Este procedimiento debe de documentarse adecuadamente indicando cuales deben ser los perfiles de acceso de cada usuario que se conecta a la red.
A.11.4.3	Autenticación de equipos en la red	Se debería considerar equipos con identificación automática para autentificar conexiones desde ubicaciones y equipos especificos	SI	La organización posee un directorio activo, administrado por IBM, que le permite identificar cada uno de los equipos que se conectan a la red.
A.11.4.4	Protección para la configuración de puertos y diagnóstico remoto	Debe controlarse la seguridad en el acceso físico y lógico para el diagnostico y configuración de puertos	SI	La organización posee un software que le permite administrar adecuamente los puertos de los equipos del departamento de TI; sin embargo, no se posee las licencias suficientes para realizar el mismo procedimiento en toda la organización. El único personal autorizado para acceder a este software es el administrador de red; sin embargo, falta la documentación de un procedimiento formal para realizar un adecuado análisis y configuración de puertos en toda la organización.
A.11.4.5	Segregación en las redes	Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes	SI	No existe un procedimiento formal donde se indique que todas las áreas de la organización deben poseer una red segmentada; sin embargo, se ha logrado realizar a nivel de los distintos locales de la organización, queda pendiente segmentar la red por áreas dentro del CCPL.
A.11.4.6	Control de conexión a las redes	La capacidad de conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden fuera de las fronteras de la organización, debe restringirse de conformidad con la política de control de acceso y los requisitos de las aplicaciones de negocio (vease 11.1)	SI	Se debe establecer una serie de controles para restringir el acceso a las redes compartidas de la organización a ciertos horarios que coincidan con el horario de trabajo.
A.11.4.7	Control de enrutamiento en la red	Se debe implementar controles de ruteo para asegurar que las conexiones de computadores y los flujos de información no violen la política de control de acceso de las aplicaciones de negocios.	SI	En la organización no se ha implementado control alguno para asegurarse que las rutas no hayan sido cambiadas maliciosamente, se deberá analizar y establecer un adecuado control para resguardar el enrutamiento en las redes.
A.11.5	***Control de acceso al sistema operativo***	**Prevenir accesos no autorizados a los sistemas operativos**		
A.11.5.1	Procedimientos seguros de conexión	Se usará un proceso de registro de conexión (login) seguro para acceder a los servicios de información	SI	Se encuentra normado que para acceder a todos las computadoras, se necesita poseer credenciales autorizadas brindadas por el departamento de TI.
A.11.5.2	Identificación y autenticación del usuario	Todos los usuarios tienen un identificador único para su uso propio y exclusivo para sus actividades y debe elegirse una técnica de autenticación adecuada para sustentar la identidad del usuario	SI	Todos los usuarios poseen un identificador único para acceder a las computadoras de la organización; sin embargo, se ha detectado, que en muchos casos, los usuarios comparten contraseñas para iniciar sesión en distintas computadoras, por lo que se debe realizar charlas de concientización a los usuarios para evitar estas practicas.
A.11.5.3	Sistema de gestión de contraseñas	Sistemas de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraselas de calidad	SI	Existen normas y restricciones para la creación de contraseñas de acceso a las computadoras, solicitudes forzadas para el cambio de contraseña cada cierto tiempo y cifrado de las mismas; sin embargo, no existe un procedimiento apropiado para la gestión de creación de usuarios nuevos, lo cual causa que los usuarios compartan contraseñas de manera no autorizada, por lo que se debe realizar charlas de concientización y establecer un procedimiento adecuado para la alta de usuarios
A.11.5.4	Uso de los programas utilitarios del sistema	Se debe registrar y controlar firmemente el uso de programas utilitarios que puedan ser capaces de forzar el sistema y los controles de aplicación	SI	La organización posee una serie de perfiles que restringen la ejecución de ciertos programas que puedan vulnerar los permisos otorgados a cada usuario; sin embargo, no existe un programa de análisis de software malicioso actualizado capaz de proteger los sistemas frente a este tipo de amenazas.
A.11.5.5	Desconexión automática de terminales	Las sesiones inactivas deben cerrarse luego de un período definido de inactividad	SI	Debe existir una documentación adecuada para delimitar los tiempos máximos de duración de las sesiones inactivas conectadas a los distintos sistemas a través de terminales.
A.11.5.6	Limitación del tiempo de conexión	Se usará restricciones de tiempos de conexión para ofrecen seguridad adicional para las aplicaciones de alto riesgo	SI	Se debe implementar una política que indique claramente bajo que horarios se puede iniciar sesión o no, esta política debe contemplar aquellos casos en los que se requiera una ampliación de horarios y solicitudes para habilitar las sesiones en un horario que no pertenezca al horario normal de trabajo
A.11.6	***Control de acceso a las aplicaciones e información***	**Evitar el acceso no autorizado a la información contenida en los sistemas**		
A.11.6.1	Restricción de acceso a la información	El acceso a las funciones de información y de aplicación por usuarios y personal de soporte serán restringidos con la política de control de acceso	SI	Los usuarios autorizados para el manejo de los sistemas poseen los permisos y restricciones adecuados para la realización de su trabajo; sin embargo, estas autorizaciones no estan debidamente documentadas, por lo que se debe realizar procedimientos formales indicando cuales son los perfiles necesarios por sistema y cuales son los permisos que estos deben tener.

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles tendran un ambiente de computo aislado	SI	Dentro de la organización se manejan 2 sistemas y varios módulos separados para la atención de los clientes empresariales; sin embargo, todos los sistemas son albergados dentro de un mismo servidor y tampoco existe documentación formal que indique que un sistema sea sensible.
A.11.7	***Informática móvil y teletrabajo***	**Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de teletrabajo**		
A.11.7.1	Informática y comunicaciones móviles	Se pondrá en práctica una política formal y se adoptarán los controles adecuados para protegerse frente a los riesgos de trabajar con puntos de computadores móviles y medios de comunicación	SI	No existe una política formal para proteger la información almacenada en las computadoras móviles. Dentro del alcance del SGSI solo el jefe del departamento de tecnologia y comunicaciones es el único personal autorizado para tener una computadora móvil de la organización; sin embargo, se debe establecer una serie de controles de encriptación para asegurar que la información almacenada en ese dispositivo no pierda su confidencialidad.
A.11.7.2	Teletrabajo	Se desarrollarán e implementarán políticas, procedimientos y estándares para las actividades de teletrabajo	NO	El presente control no aplica a la organización debido a que no se ha implementado el teletrabajo.
A.12		**Adquisición de sistemas, desarrollo y mantenimiento**		
A.12.1	***Requisitos de seguridad de los sistemas de información***	**Garantizar que la seguridad esté incluida dentro de los sistemas de información**		
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Los requisitos de negocio para nuevos sistemas, o ampliaciones de los sistemas existentes, especificarán los requisitos de control	SI	Se debe implementar dentro de la organización una serie de controles que permitan considerar los requisitos de seguridad dentro del ciclo de vida de los sistemas ya que hasta el momento esto no ha sido considerado, de manera formal, durante el desarrollo de los nuevos sistemas.
A.12.2	***Proceso correcto en aplicaciones***	**Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones**		
A.12.2.1	Validación de los datos de entrada	Se validará el ingreso de datos a los sistemas de aplicacíon para asegurar que sean correctos	SI	Los sistemas desarrollados poseen una validación de los datos ingresados en muchas funcionalidades; sin embargo, se debe elaborar la documentación faltante que evidencie cuales son todos los casos de prueba utilizados para la validación de los datos de entrada.
A.12.2.2	Control del proceso interno	Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados	SI	Durante el desarrollo de los sistema, se ha implementado el manejo de excepciones para evitar que el sistema continue en caso se detecte algún error y se valida la información que se transmite internamente para asegurarse la integridad de datos; sin embargo, no hay una documentación formal de los controles implementados.
A.12.2.3	Integridad de mensajes	Se deben identificar requisitos para la autenticación y protección de la integridad de mensajes. Igualmente, se deben implementar e identificar controles apropiados	SI	Se debe realizar una metodología para identificar aquellos mensajes que deben ser protegidos para implementar controles y asegurar la confidencialidad, integridad y disponibilidad de los mismos.
A.12.2.4	Validación de los datos de salida	Los datos de salida de una aplicación se validarán para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias	SI	Se tiene conocimiento que en los ambientes de prueba y desarrollo se realiza una serie de casos de prueba para asegurar el correcto funcionamiento de los sistemas; sin embargo, no se posee una documentación formal de estas pruebas.
A.12.3	***Controles criptográficos***	**Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos**		
A.12.3.1	Política de uso de los controles criptográficos	Debe desarrollarse e implementrase una política sobre el uso de controles criptográficos para proteger la información	SI	La organización debe realizar una política de encriptación integral para asegurar la información sensible que esta maneja. Se tiene conocimiento que las contraseñas tanto en los sistemas como en el diretorio activo estan encriptadas, pero solo existe una política forma, desarrollada con IBM, para la encriptación de la red WAN.
A.12.3.2	Gestión de claves	Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnicas criptográficas dentro de la organización	SI	La organización debe realizar una política adecuada para una correcta entrega, revocatoria y eliminación de claves a los usuarios que así lo requieran
A.12.4	***Seguridad de los archivos del sistema***	**Asegurar la seguridad de los archivos del sistema**		
A.12.4.1	Control del software en producción	Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales	SI	La organización debe elaborar un procedimiento formal, que hasta el momento no existe, para asegurar una correcta instalación de software en el ambiente de producción o asegurar una correcta reversión del sistema en caso no se haya logrado instalar el software adecuadamente; sin embargo, hasta el momento, si se maneja un repositorio de versiones de los distintos sistemas que se han manejado dentro de la organización.
A.12.4.2	Protección de los datos de prueba del sistema	Se protegerán y controlarán los datos de prueba los cuales deben ser seleccionados cuidadosamente	SI	Se maneja una base de datos paralela para las pruebas de los sistemas de información, la cual es nivelada de manera periodica; sin embargo, es necesario realizar la documentación pertinente para evidenciar cuando es que se debe utilizar esta información y cuales son los controles necesarios en caso se deba utilizar data de prueba en el ambiente de producción.
A.12.4.3	Control de acceso a la librería de programas fuente	El acceso a las librerías de programas fuente debe ser restringido	SI	El acceso al código fuente de los distintos sistemas solo es permitido al jefe del departamento de sistemas de información y al personal que el permita; sin embargo, cabe aclarar que es necesario la elaboración de un procedimiento para el tratamiento de esta información, debido a que muchas personas externas a la organización, trabajadores por recibos por honorarios, tienen acceso a este tipo de información.
A.12.5	***Seguridad en los procesos de desarrollo y soporte***	**Mantener la seguridad del software de aplicación y la información**		
A.12.5.1	Procedimientos de control de cambios	La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios	SI	Se deberá elaborar el procedimiento de control de cambios en el software de la empresa debido a que no existe uno formal dentro de la organización con los requerimientos de hardware necesario, aceptación del usuario, mantenimiento de logs de auditoria del cambio, documentación actualizada del software, entre otros.

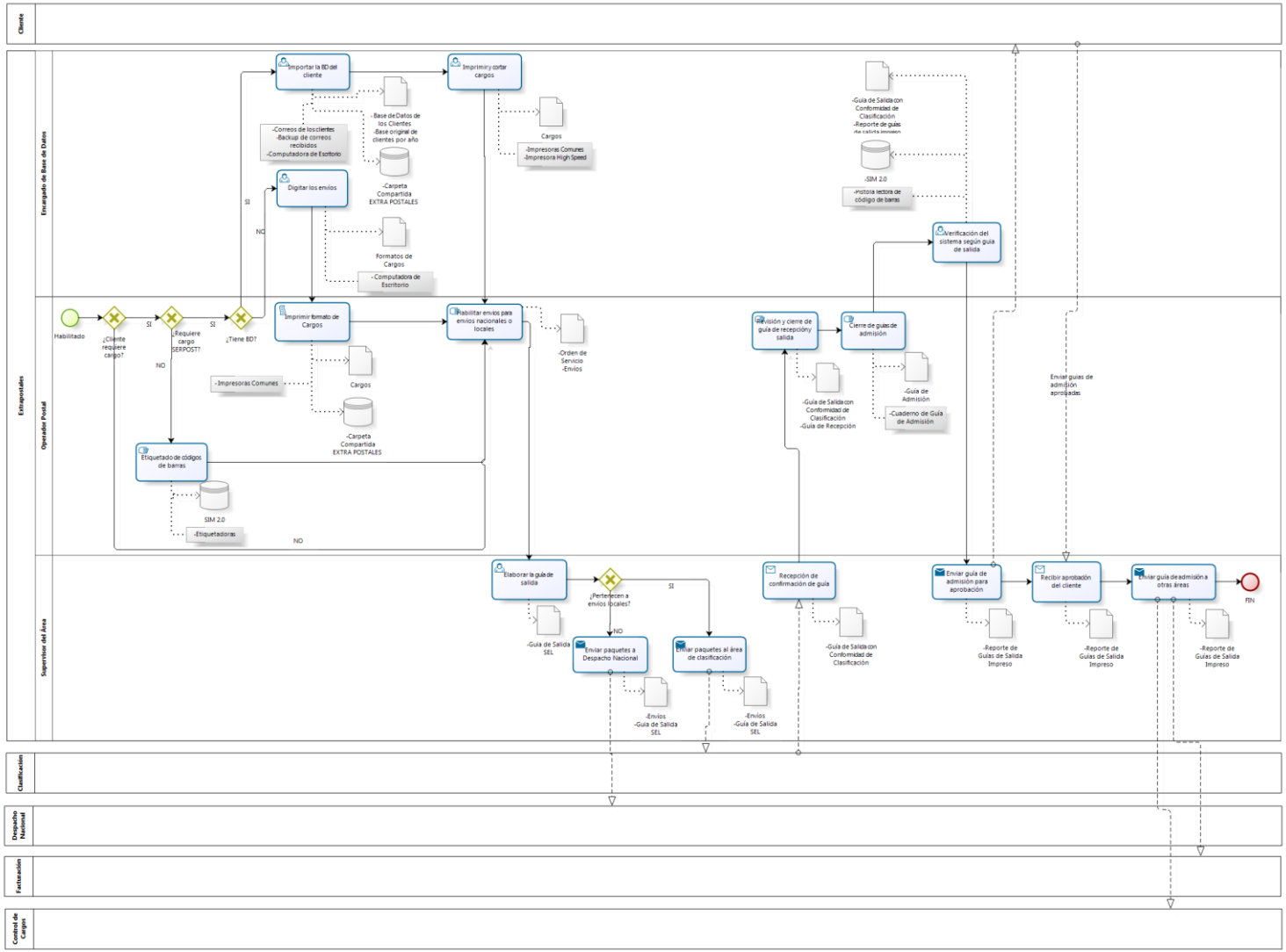
No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.12.5.2	Revisión técnica de los cambios en el sistema operativo	Cuando los sistemas operativos son cambiados, se deben de revisar y probar las aplicaciones críticas de negocio con el fin de asegurar que no existan impactos adversos en las operaciones o seguridad de la organización.	SI	En la organización no ha existido una actualización de sistemas operativos hasta el momento; sin embargo, al momento de adquirir nuevos equipos, estos tenian W7, por esa razon se maneja Windows XP y 7 dentro de la empresa. No existe un procedimiento formal para la actualización de sistemas operativos, por lo que tampoco se realizaron las pruebas pertinentes en los diversos sistemas, ello trajo varios problemas de compatibilidad en los distintos módulos del sistema SIM los cuales tuvieron que ser corregidos en el tiempo.
A.12.5.3	Restricciones en los cambios a los paquetes de software	No se debe fomentar las modificaciones en los paquetes. Se debería limitar a cambios necesarios y todos estos cambios deben ser estrictamente controlados	SI	Se debe elaborar un procedimiento formal para evaluar la modificación de los distintos paquetes de software utilizados en la organización, en este procedimiento se debe especificar como se realizará el análisis de riesgo tras el futuro cambio y como se elaborará el plan de regresión en caso el resultado no sea exitoso
A.12.5.4	Fuga de la información	Se deben de prevenir las oportunidades de fuga de información	SI	Se deberá elaborar un procedimiento para implementar controles que ayuden a evitar la fuga de información a través de los distintos sistemas. Adicionalmente, se cuenta con las clausula de confidencialidad firmadas por cada uno de los trabajadores del local; sin embargo, se debe hacer difusión de la política de seguridad de la empresa ya que en ella se muestra cuales son las sanciones en caso no se cumpla con lo normado referente a seguridad de la información.
A.12.5.5	Desarrollo externo del software	La organización debe supervisar y monitorear el desarrollo externo de software	NO	El presente control no aplica, debido a que la organización posee un área que se encarga del desarrollo de software para la empresa.
A.12.6	***Gestión de la vulnerabilidad técnica***	**Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas**		
A.12.6.1	Control de las vulnerabilidades técnicas	Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan. La exposición de la organización a tales vulnerabilidades debe ser evaluada y se debe tomar medidas apropiadas asociadas al riesgos		La organización debe generar un procedimiento adecuado para crear un registro de errores reportados por los usuarios, en los cuales se deje conocer cual fue el problema, cual fue el impacto, cuando se reporto, cual fue la causa y como se solucionó. Adicionalmente, se debe indicar como es que se gestionará las nuevas vulnerabilidades detectadas o reportadas por los usuarios.
A.13	**Gestión de incidentes en la seguridad de la información**			
A.13.1	***Reportando eventos y debilidades en la seguridad de la información***	**Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita tomar una acción correctiva a tiempo**		
A.13.1.1	Reportando eventos de la seguridad de información	Los eventos en la seguridad de la información deben ser reportados lo más rápido posible a través de canales apropiados	SI	La organización debe generar un procedimiento para gestionar adecuadamente cada uno de los eventos de seguridad de la información reportados por el personal o detectados por cada uno de los controles implementados, además se debe realizar charlas de capacitación con el personal para explicarles cuales son sus roles y responasbilidades dentro del sistema de gestión.
A.13.1.2	Reportando debilidades de seguridad de información	Todos los empleados, contratistas o personal externo usuarios de los sistemas y servicios de información deben estar obligados de notar y reportar cualquier debilidad en la seguridad de los sistemas y servicios	SI	La organización debe capacitar adecuadamente a todo el personal de la organización para que sea capaz de detectar debilidades en el sistema de gestión de seguridad de información y puedan reportarlas adecuadamente, asimismo, se debe recalcar las sanciones que podrian recibir si es que deciden probar las debilidades encontradas.
A.13.2	***Gestión de los incidentes y mejoras en la seguridad de información***	**Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información**		
A.13.2.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de información	SI	Dentro del documento de la política del SGSI, se describe que los miembros del comité tienen la responsabilidad de dar un tratamiento adecuado a los riesgos relacionados a la seguridad de la información detectados; sin embargo, la organización debe establecer un procedimiento en el cual se establezca detalladamente cual es la labor de cada miembro de la alta gerencia y como es que debe desempeñar sus roles.
A.13.2.2	Aprendiendo de los incidentes en la seguridad de información	Debe existir mecanismos que habiliten que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados	SI	La organización debe generar un procedimiento para gestionar adecuadamente cada uno de los eventos de seguridad de la información reportados por el personal o detectados por cada uno de los controles implementados para tener un registro de incidentes y lograr prevenir próximos eventos similares o darles solución en caso se detecten eventos de este tipo
A.13.2.3	Recolección de evidencia	Cuando exista una acción de seguimiento contra una persona u organización, luego de que un incidente en el sistema de información involucre una acción legal (civil o criminal), se debe recolectar, retener y presentar evidencia conforme con las reglas dentro de la jurisdicción.	SI	No existe un procedimiento formal para asegurar la recolección de evidencia de la organización, por lo que se deberá elaborar uno, adicionalmente, se debe evidenciar que los sistemas cumplen con la admisibilidad de la evidencia.
A.14	**Gestión de la Continuidad del Negocio**			
A.14.1	***Aspectos de la gestión de continuidad del negocio en la seguridad de la información***	**Neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna**		
A.14.1.1	Incluyendo la seguridad de información en la gestión de la continuidad del negocio	Se deben establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de la información	SI	La organización debe establecer procedimientos y responsabilidades paragestionar adecuadamente la cotinuidad del negocio, en estos procedimientos se debe colocar explicitamente cuales son los activos relacionados con los procesos críticos del negocio, asegurar la seguridad del personal, establecer planes de continuidad y realizar las pruebas de los mismos.
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Los eventos que pueden causar interrupciones en los procesos de negocio deben ser identificados así como las probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.	SI	La organización debe realizar un analisis de impacto del negocio adecuado según el alcance del SGSI identificando posibles escenarios y evalluando los riesgos tras la materialización de cada uno de ellos.

No. De Control	Control	Objectivo de Control	Aplicable a la Organización	Justificación
A.14.1.3	Desarrollando e implantando de planes de continuidad que incluyen la seguridad de información	Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.	SI	Se debe realizar planes de continuidad de negocio que permitan establecer cuales son los tiempos máximos para la recuperación de los servicios, que tipo de información se debe resguardar y cual se puede perder y las fechas de actualización de los planes
A.14.1.4	Marco de planificación de la continuidad del negocio	Un simple marco de los planes de continuidad del negocio debe ser mantenido para asegurar que todos los planes sean consistentes, que anexen consistentemente los requisitos de seguridad de la información, para identificar prioridades de prueba y mantenimiento	SI	Se debe establecer un estandar único para la elaboración de los planes de contiuidad del negocio, de tal forma que se pueda recolectar toda la información necesaria sobre la planificación de la continuidad del negocio en cada uno de los planes desarrollados.
A.14.1.5	Probando, manteniendo y reevaluando los planes de continuidad del negocio	Los planes de continuidad del negocio deben ser probados y actualizados regularmente con el fin de asegurar que se encuentren actuales y que sean efectivos	SI	Se debe establecer una metodología de pruebas para verificar los planes de continuidad del negocio, en ella debe indicarse textualmente la frecuencia con la cual se harán las pruebas de continuidad en la organización, las simulaciones que se deberán hacer, como regresar a la operatividad luego de las pruebas y como deberán realizarse los ensayos completos ante interrupciones
A.15	**Cumplimiento**			
A.15.1	***Cumplimiento de los requisitos legales***	**Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad**		
A.15.1.1	Identificación de la legislación aplicable	Se definirán y documentarán explícitamente todos los requisitos legales, regulatorios y contractuales relevantes y se deben mantener actualizados cada sistema de información y la organización	SI	Se debe definir planes y procedimientos para verificar el correcto cumplimiento de la legislación aplicable tales como la implementación del SGSI.
A.15.1.2	Derechos de propiedad intelectual (DPI)	Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales en el uso de material con respecto a derechos de propiedad intelectual y uso de productos de software propietario	SI	La organización debe definir un procedimiento para la inscripción de todos los sistemas desarrollados por el departamento de sistemas de información en el INDECOPI y mantener una política de conformidad de los derechos de autor del software adquirido.
A.15.1.3	Salvaguarda de los registros de la organización	Se protegerán los registros importantes de la organización frente a pérdidas, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio	SI	Se debe establecer guías y procedimiento que especifiquen por cuanto tiempo la organización está dispuesta a almacenar la información, cabe aclarar que como parte del proyecto se realizó un inventario de activos de información los cuales fueron valorados según la metodología de svaloración de activos.
A.15.1.4	Protección de los datos y de la privacidad de la información personal	Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales	SI	Se debe establecer un procedimiento para el adecuado manejo de la información personal almacenada dentro de la organización, en conformidad con la ley de protección de datos personales.
A.15.1.5	Prevención en el mal uso de las instalaciones de procesamiento de la información	Los usuarios deben ser disuadidos de utilizar las instalaciones del procesamiento de información para propósitos no autorizados	SI	En la organización está normado, dentro del reglamento interno de trabajo, el prestamo de computadoras autorizadas para el uso personal, siempre y cuando, se solicite con anticipación y de forma escrita; sin embargo, se debe difundir mejor esta normatividad.
A.15.1.6	Regulación de los controles criptográficos	Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos	SI	A nivel nacional existe una directiva que indica que la información sensible debe ser encriptada para asegurar su integridad y confidencialidad, esta directiva es la 007-95-INEI-SJI; sin embargo, la organización no posee una documentación formal que evidencie el cumplimiento de esta directiva, aunque sis se cifren los datos para el manejo de contraseñas en la organización.
A.15.2	***Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico***	**Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales**		
A.15.2.1	Cumplimiento con los estándares y la política de seguridad	Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro de sus área de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de las políticas y estándares de seguridad	SI	Se debe implementar un procedimiento que permita a los gerentes evaluar el cumplimiento de los controles de seguridad de información que se desean implementar, de tal forma que pueda darle un tratamiento adecuado a las no conformidades detectadas.
A.15.2.2	Comprobación del cumplimiento técnico	Debe verificarse regularmente el cumplimiento de la implementación de normas de seguridad en los sistemas de información	SI	Se debe establecer una metodología de trabajo que permita verificar el correcto cumplimiento de la implementación de normas de seguridad en la organización, adicionalmente, se puede incluir un procedimiento para realizar un análisis de vulnerabilidades de los distintos sistemas incluidos en el alcance del SGSI.
A.15.3	***Consideraciones sobre la auditoría de sistemas***	**Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema**		
A.15.3.1	Controles de auditoría de sistemas	Se planificarán cuidadosamene las auditorías de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos del negocio	SI	Se debe establecer un procedimiento para el desarrollo de auditorias planificadas e inopinadas de los sistemas involucrados en el alcance del SGSI ya que hasta el momento no existe rastro alguno de una auditoria a estos sistemas.
A.15.3.2	Protección de las herramientas de auditoría de sistemas	Se protegerá el acceso a las herramientas de auditoria del sistema para prevenir cualquier posible mal uso o daño	SI	Los diversos sistemas y servidores poseen un log que puede ser revisado para temas de auditoria; sin embargo, la organización debe establecer una serie de controles para resguardar la información almacenada dentro de estos logs para evitar la perdida de disponibilidad e integridad de los mismos.

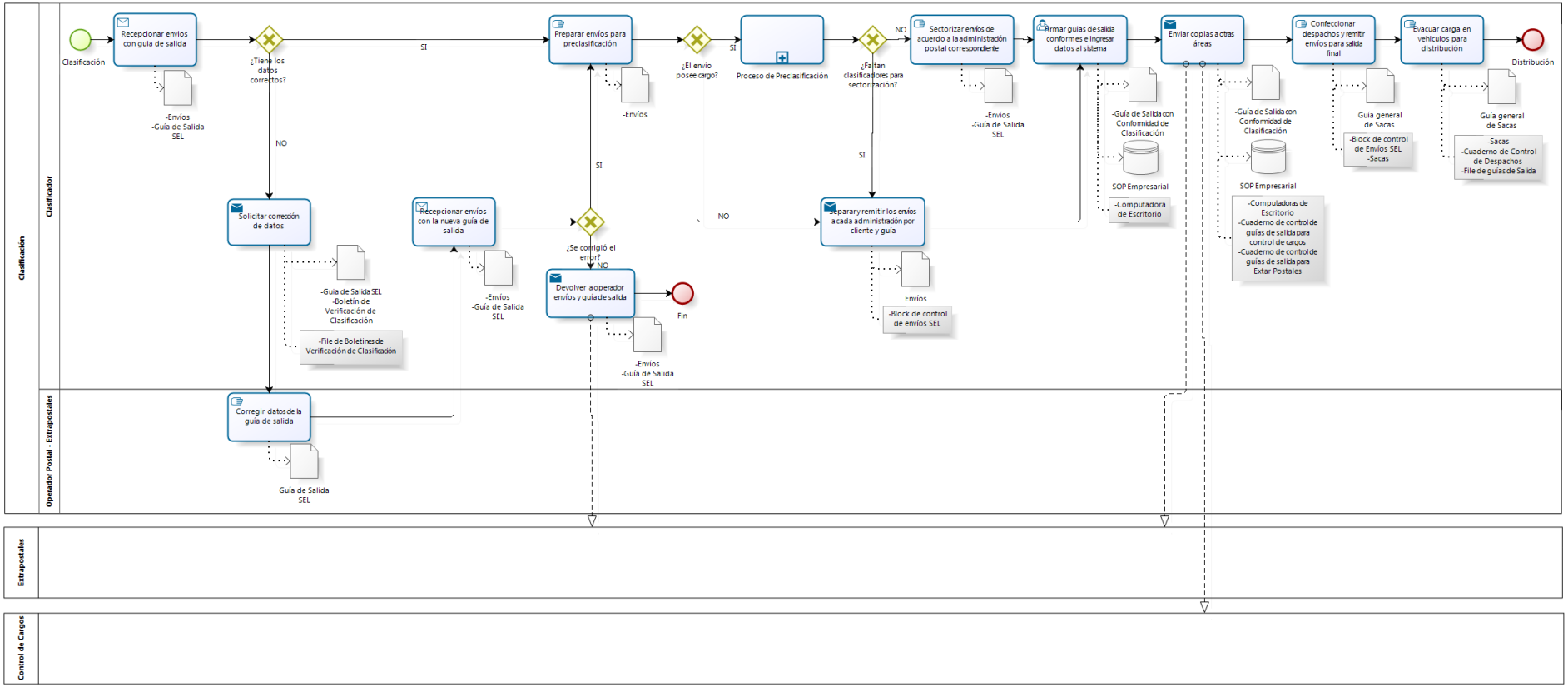
11. Anexo 11 – Proceso de Recepción - Sub Proceso de Admisión



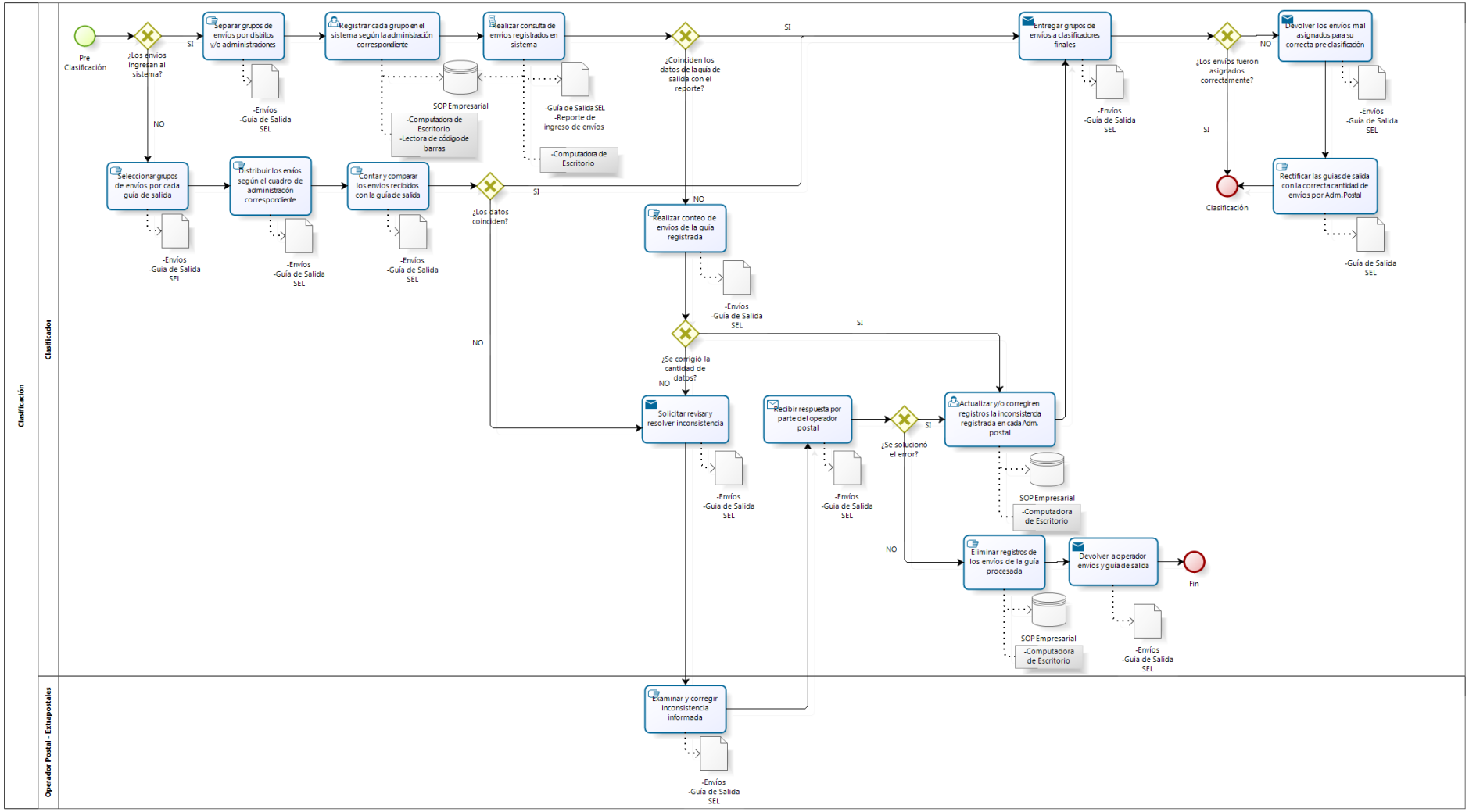
12. Anexo 12 – Proceso de Recepción - Sub Proceso de Habilitado



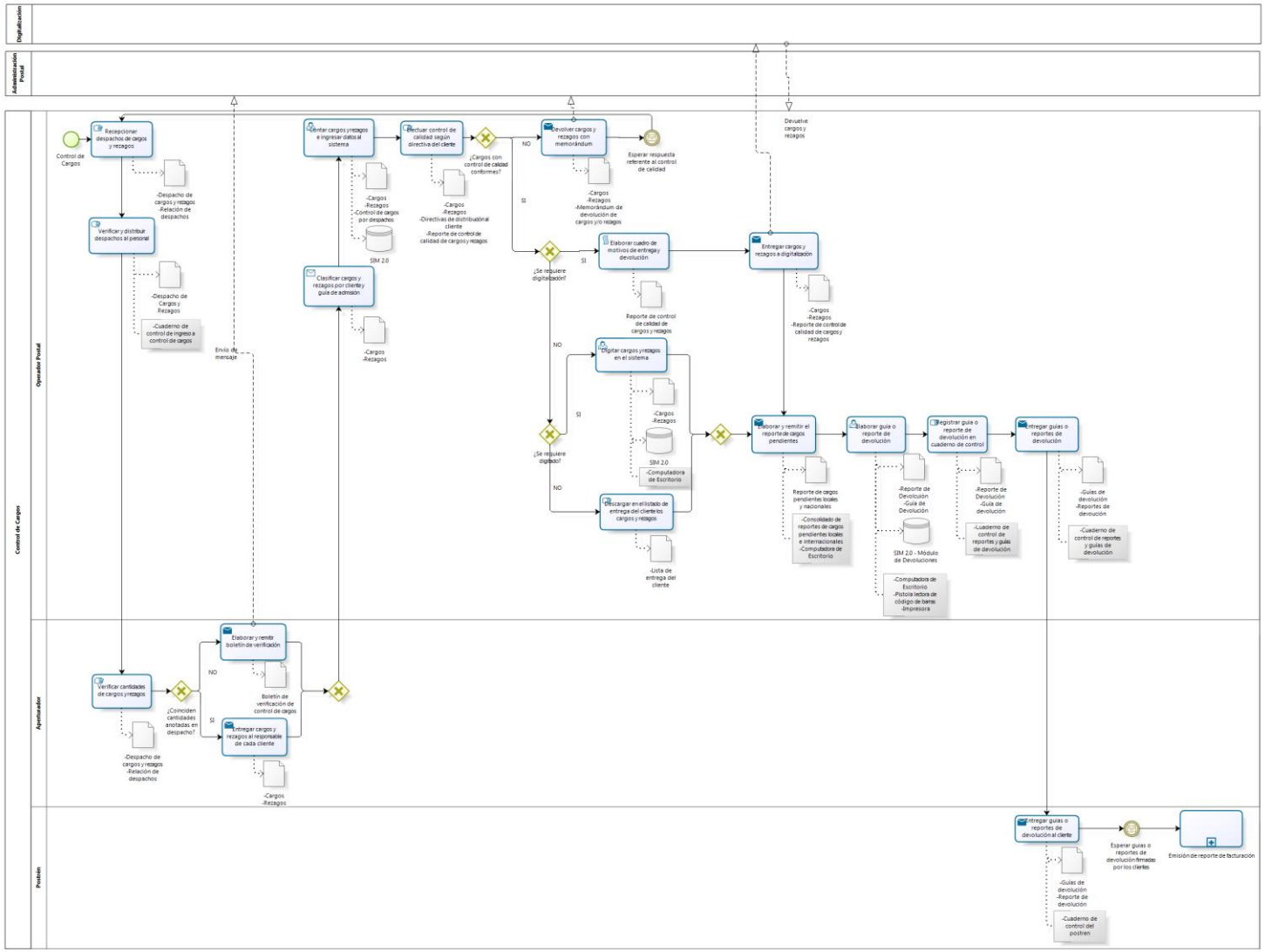
13. Anexo 13 – Proceso de Clasificación



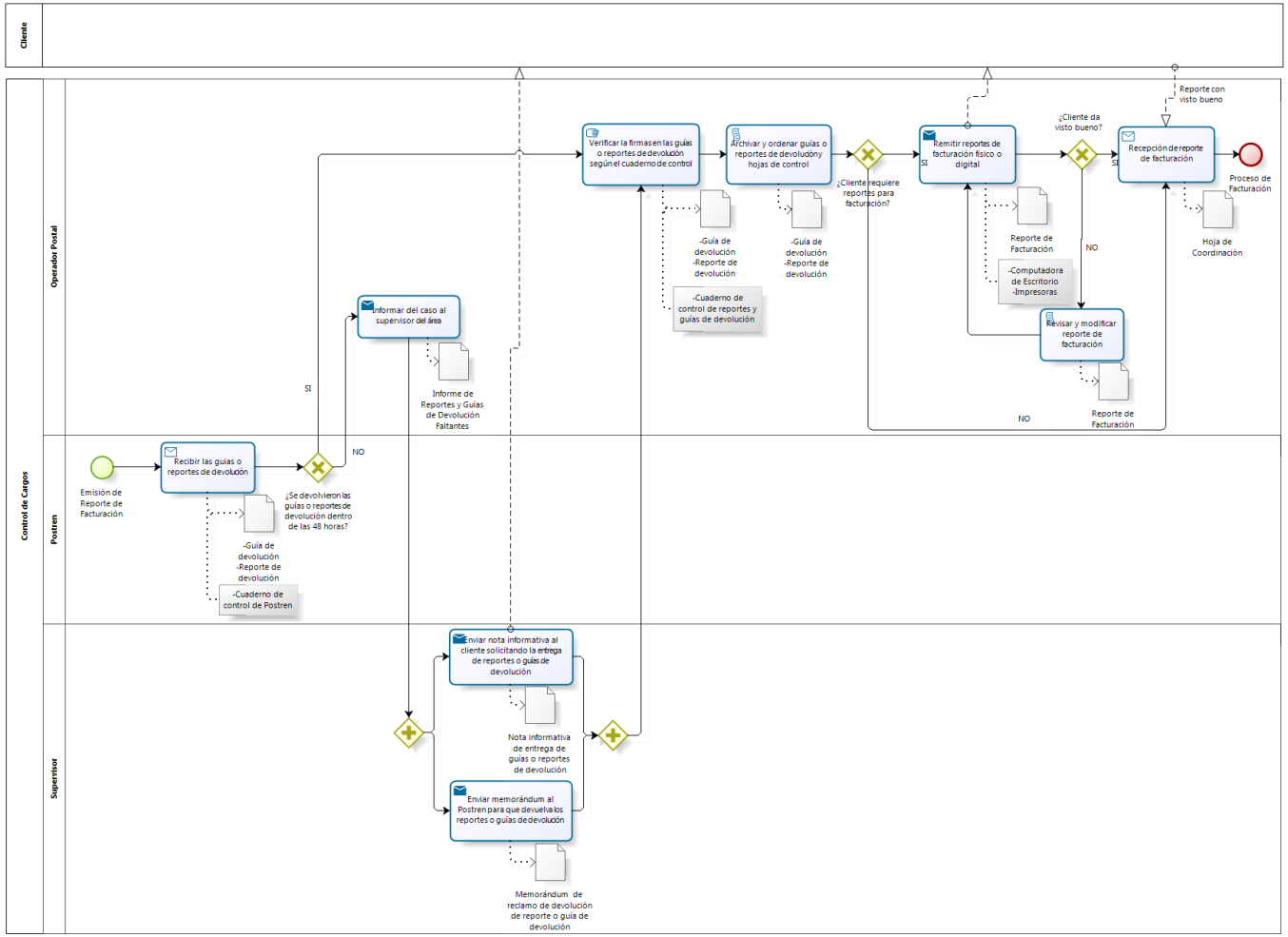
14. Anexo 14 – Proceso de Clasificación - Sub Proceso de Pre Clasificación



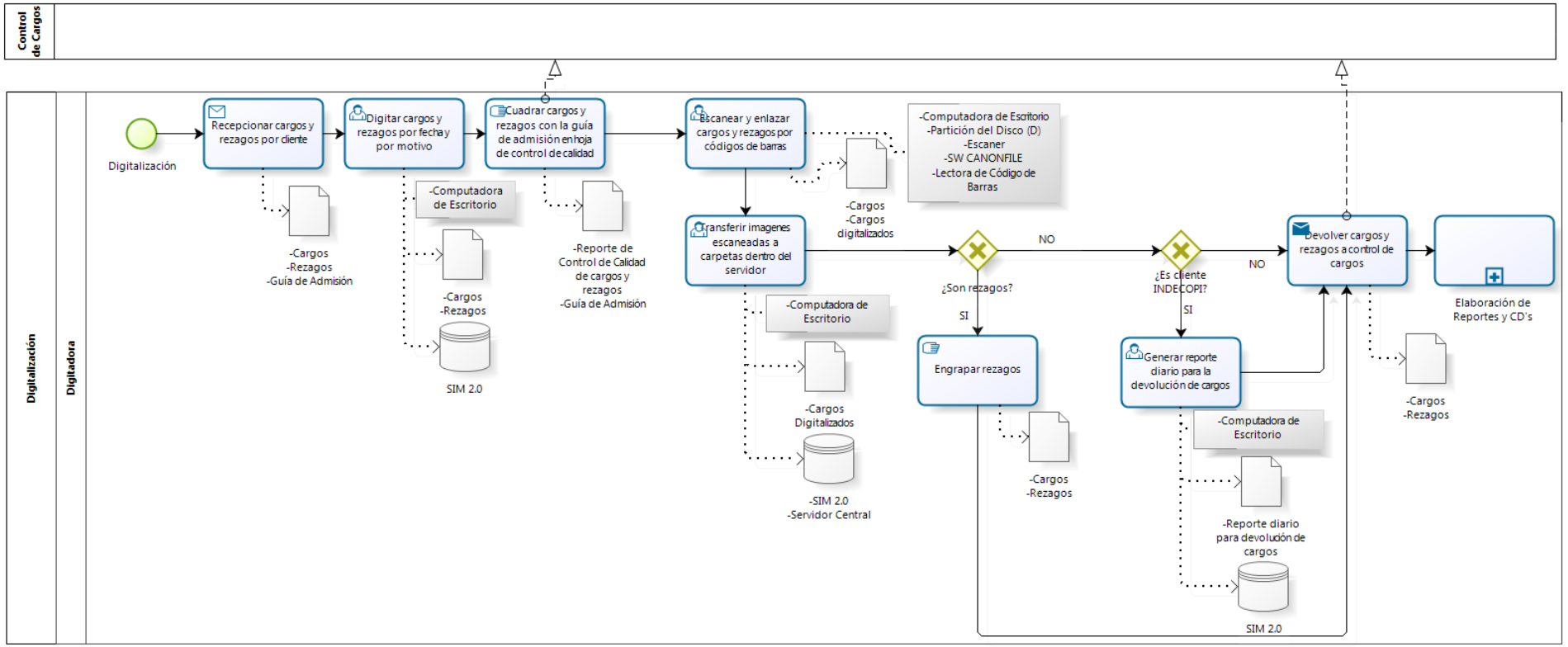
15. Anexo 15 – Proceso de Control de Cargos



16. Anexo 16 – Proceso de Control de Cargos – Sub Proceso de Emisión de Reporte de Facturación



17. Anexo 17 – Proceso de Digitalización



18. Anexo 18 – Proceso de Digitalización – Sub Proceso de Elaboración de Reportes y CD's