



EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.
EMPAS S.A.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código:PLGI-03


Versión:00

Pág. 1 de 13

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN


EMPAS S.A.

| CUADRO DE CONTROL DE CAMBIOS | | |
|------------------------------|-------|---------------------------------------|
| Versión | Fecha | Descripción de la modificación |
| 00 | | Creación y codificación del documento |

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 2 de 13 |

CONTENIDO

| | |
|---|----|
| INTRODUCCIÓN | 3 |
| 1. OBJETIVOS | 4 |
| 2. MARCO NORMATIVO | 5 |
| 3. DOCUMENTOS DE REFERENCIA | 5 |
| 4. ALCANCE..... | 6 |
| 5. GOBIERNO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN..... | 6 |
| 6. METODOLOGÍA..... | 6 |
| 7. FASE DIAGNÓSTICO | 7 |
| 8. FASE DE PLANIFICACIÓN | 10 |
| 9. FASE DE IMPLEMENTACIÓN | 10 |
| 10. FASE DE EVALUACIÓN | 11 |
| 11. FASE DE MEJORAMIENTO CONTINUO | 11 |


| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 3 de 13 |

INTRODUCCIÓN

La Estrategia de Gobierno Digital es una política definida en el Decreto Único Reglamentario del sector de las Tecnologías de la Información y las Comunicaciones, con el fin de promover una adecuada gestión interna de las entidades públicas, así como una buena relación con el ciudadano, a través de la participación y la prestación de servicios de calidad.

La Empresa Pública de Alcantarillado de Santander - EMPAS S.A E.S.P, es una empresa prestadora del servicio público domiciliario de alcantarillado con un equipo humano altamente calificado y criterios de excelencia, que garantiza la gestión integral de sus procesos en procura de una mejor calidad de vida y la protección del medio ambiente.

EMPAS S.A., consciente de la importancia de la información como recurso valioso para la entidad, los grupos de interés y para la ciudadanía, documenta el Plan de Seguridad y Privacidad de la Información, herramienta a través de la cual la empresa define su estrategia y políticas de seguridad para el tratamiento de la información. Para tal fin, EMPAS S.A. propone una serie de actividades fundamentadas en el ciclo PHVA, cuyo objetivo es garantizar la integridad, disponibilidad, confidencialidad, respaldo y acceso a la información.

| | | |
|---|---|----------------|
|  | <p align="center">EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A.</p> <p align="center">PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p> | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 4 de 13 |


1. OBJETIVOS

Objetivo general

Ejecutar acciones que ayuden a proteger los activos de información administrados por la Empresa Pública de Alcantarillado de Santander – EMPAS S.A E.S.P, mediante la creación e implementación de una política que defina actividades de mejora continua.

Objetivos específicos

1. Analizar la situación actual al año 2021 de la empresa con respecto a las acciones que se realizan en seguridad de la Información.
2. Desarrollar en la empresa el Manual de Seguridad y Privacidad de la Información.
3. Identificar los controles de seguridad definidos por la norma ISO 27001 que se requieran implementar en EMPAS para el año 2021.
4. Comunicar e implementar las estrategias de seguridad de información definidas durante el año 2021.
5. Cumplir con la normatividad vigente que establece una buena gestión de seguridad de la información definida por la Política de Gobierno Digital.

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 5 de 13 |


2. MARCO NORMATIVO

| Norma | Descripción |
|---|--|
| Ley 44 de 1993 | “Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” |
| Ley 1273 de 2009 | “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. |
| Ley 1712 de 2014 | “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”. |
| Ley 1581 de 2012 | “Por la cual se dictan disposiciones generales para la protección de datos personales”. |
| Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 | Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPÍ de MINTIC. |
| Decreto 1499 de 2017 | El cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión. |
| CONPES 3854 de 2016 | Política de Seguridad Digital del Estado Colombiano. |
| | Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL |
| | Norma Técnica Colombiana ISO27001:2013. |
| Resolución No. 000268 de 2013 | Por la cual se derogan las Resoluciones No 000035 de 2007 y No 000122 de 2007. Comité Interno de Archivo. |
| Resolución No. 000036 de 2014 | Por medio de la cual se deroga la Resolución No. 000019 e 2007 y se estructura el EQUIPO MECI SIGC del Sistema Integrado de Gestión y Control |
| Resolución No. 000494 de 2016 | Por medio de la cual se determinan las políticas de uso de los equipo de cómputo de la Empresa Pública de Alcantarillado de Santander S.A ESP - EMPAS S.A., y los servicios institucionales de correo electrónico e internet, el manejo, instalación y desinstalación de software y la conservación y cuidado de la información afectada al funcionamiento de la empresa |
| DEDE-03 | Política de tratamiento de datos personales de EMPAS S.A |

Tabla 1. Marco legal para el plan.

3. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001:2013
- Modelo de Seguridad y Privacidad de la Información – MINTIC
- Manual de Administración de Tecnología de la Información – MAGI-01.

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 6 de 13 |

- Manual de Gobierno Digital – MINTIC
- Modelo Integrado de Planeación y Gestión – MIPG
- NTC ISO 9001:2015

4. ALCANCE

La Empresa Pública de Alcantarillado de Santander – EMPAS S.A E.S.P., establece la Política de Seguridad y Privacidad de la Información para su implementación en el periodo contemplado 2020 – 2024, con actualizaciones anuales. El Plan de Seguridad y Privacidad de la Información aplica para el proceso de Gestión informática de EMPAS S.A. donde se recolecte, procese, almacene, consulte o intercambie información relevante para el cumplimiento de los objetivos estratégicos de la empresa.

5. GOBIERNO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN


EMPAS S.A. contempla un esquema de gobierno para la seguridad de la información. En primer lugar, existe una política general de seguridad y privacidad de la información que define las reglas de comportamiento que debe seguir la organización en procura de la protección de los activos de información. Estas políticas se encuentran documentadas en el Manual de Administración de Tecnología de la información, MAGI-01.

Como apoyo a la política general, se definen exigencias respecto a la manera en que se va a llevar a cabo el cumplimiento de la estrategia de seguridad de la información al interior de EMPAS S.A.

Finalmente, se definen aquellas políticas y estándares de seguridad de la información asociados al respaldo de las políticas de gestión de tecnología en la empresa.

6. METODOLOGÍA

De acuerdo a lo establecido por la Política de Gobierno Digital, la metodología para el desarrollo del plan se soporta en un ciclo PHVA que incluye una fase previa de diagnóstico. Con esto se pretende que las entidades puedan gestionar de manera asertiva sus activos de información.

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 7 de 13 |

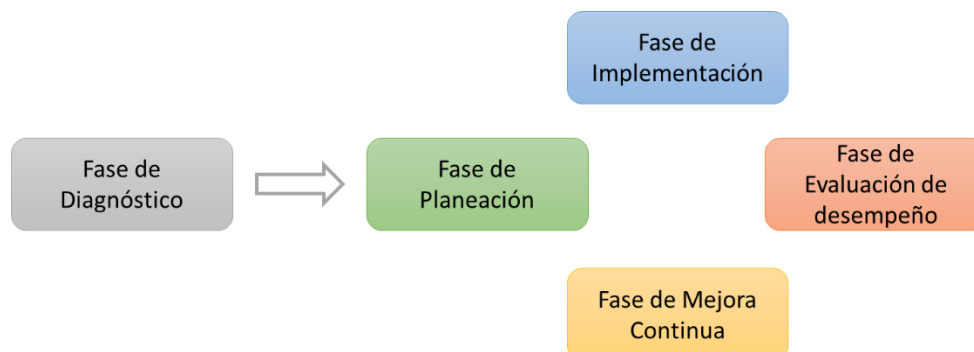


Figura 1. Metodología

7. FASE DIAGNÓSTICO


El objetivo de la primera fase es identificar el estado actual de EMPAS S.A. con respecto a temas de seguridad y privacidad de la información. Para tal fin, se hace uso de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información, desarrollada por el Ministerio de las TIC, a partir de la cual se puede valorar el grado de implementación y efectividad de los controles de seguridad de la información, establecidos en la norma ISO 27001. El resultado de esta etapa será el nivel de madurez y permitirá definir la hoja de ruta de la empresa para consolidarlo.

5.1. Contexto Estratégico

El presente plan se encuentra alineado al Plan Estratégico de Gestión y Resultados Institucional de EMPAS S.A., Específicamente aporta el logro del objetivo estratégico del programa de Consolidación y Fortalecimiento al Desarrollo Institucional “Propender por el fortalecimiento del desarrollo institucional basándose en el mejoramiento continuo de los procesos internos”. En cuanto al Modelo Integrado de Planeación y Gestión – MIPG, el Plan de Seguridad de la Información aporta en el logro de la implementación de la Política de Gobierno Digital, la Política de Seguridad Digital y la Política de Transparencia, acceso a la información pública y lucha contra la corrupción.

5.2. Estado actual

Con base en la norma técnica ISO 27001, se desarrolló el diagnóstico de los controles de seguridad de la información. Se establece que EMPAS implementa criterios de control de seguridad definidos por la norma de manera efectiva, con un promedio de evaluación del 53% de 100%, con respecto a la gestión administrativa y técnica en seguridad de la información que se desarrolla en la empresa. La

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 8 de 13 |

valoración de controles establece que los procesos y los controles siguen un patrón regular, están documentados y son conocidos por la mayoría de personas relacionadas con la organización, son efectivos y se aplican consistentemente durante la operación de los procesos de la empresa. A pesar de esto, es poco probable que se pueda realizar un monitoreo constante de tal forma que se detecte algún tipo de desviación cuando el control no se aplique oportunamente o de manera incorrecta.

Existen fortalezas en algunos de los dominios, particularmente en la seguridad de los recursos humanos, el control de acceso y la seguridad de las operaciones. Las principales debilidades se encuentran en la implementación de controles criptográficos y las relaciones con proveedores.

| | DOMINIO | Calificación Actual | Calificación Objetivo |
|---|---|----------------------------|------------------------------|
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 50 | 100 |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 47 | 100 |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 70 | 100 |
| A.8 | GESTIÓN DE ACTIVOS | 53 | 100 |
| A.9 | CONTROL DE ACCESO | 76 | 100 |
| A.10 | CRIPTOGRAFÍA | 20 | 100 |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 63 | 100 |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 72 | 100 |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 62 | 100 |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 45 | 100 |
| A.15 | RELACIONES CON LOS PROVEEDORES | 20 | 100 |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 63 | 100 |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 50 | 100 |
| A.18 | CUMPLIMIENTO | 54 | 100 |
| <i>PROMEDIO EVALUACIÓN DE CONTROLES</i> | | 53 | 100 |

Tabla 2. Evaluación de controles de seguridad

Para lograr un avance se requiere:

- Aplicar los controles de seguridad oportunamente y de la manera indicada
- Monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no están funcionando eficientemente.

- Realizar seguimiento periódico para que la implementación de controles ejerza buenas prácticas de seguridad en la entidad.

El avance en cumplimiento de la línea de seguridad por años establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones es de 39% de 100%, debido que la entidad se encuentra en proceso de documentación, estandarización y aprobación por parte de la dirección, del modelo de seguridad de la información, sin embargo, si existen controles de seguridad en cada uno de los procesos, metodología de riesgos aprobados por la alta dirección, un plan de tratamiento de riesgo, un plan de comunicación para los funcionarios de la entidad con respecto a la seguridad de la información y un control de operaciones en espera de ser aprobados por la dirección.


| | COMPONENTE | % de Avance Actual | % Avance Esperado |
|-------|-------------------------|--------------------|-------------------|
| 2021 | Planificación | 21% | 40% |
| 2021 | Implementación | 7% | 20% |
| 2021 | Evaluación de desempeño | 5% | 20% |
| 2021 | Mejora continua | 6% | 20% |
| TOTAL | | 39% | 100% |

Tabla 3. Porcentaje de avance ciclo PHVA

5.3. Nivel de Madurez

En este componente se mide el nivel de madurez en la que se encuentra EMPAS S.A. con respecto al modelo de seguridad y privacidad de la información. Para la medición el nivel de madurez se toma en cuenta el resultado obtenido del avance administrativo, técnico y PHVA anteriormente analizado, arrojando como resultado:

- Los controles de seguridad establecidos por la entidad, deben alinearse con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información, es decir, no se determina el grado de criticidad de la información.
- Se desarrollan y ejecutan procesos de gestión de seguridad de la información.
- Se cuenta con documentos que manifiestan criterios de seguridad aprobados por calidad, pero no se cuenta con un documento que permita plasmar las acciones a realizar tomando como base el modelo de seguridad y privacidad de la información aprobado por la alta dirección.
- Si bien se incluyen aspectos de seguridad de la información en el Plan de Auditoría Interna de EMPAS S.A. debe fortalecerse la evaluación y el mejoramiento continuo de los procesos y procedimientos de seguridad.

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 10 de 13 |

8. FASE DE PLANIFICACIÓN

El objetivo de esta fase es definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de la metodología de gestión del riesgo. Como insumo se utiliza la herramienta de diagnóstico desarrollada en la fase anterior, con base en la cual EMPAS S.A. establecerá el alcance, las políticas, procedimientos y objetivos del Modelo de Seguridad y Privacidad de la Información. Todas estas actividades, así como las de fases subsiguientes, son puntos de mejora con los que se busca contribuir para alcanzar un mayor nivel de madurez de la gestión de la seguridad digital en la organización.


| Actividad | Resultado | Fecha |
|--|--|------------------|
| Establecer la política general de seguridad y privacidad de la información de EMPAS S.A. | Manual de seguridad y privacidad de la información aprobado por la dirección y socializado. | 31 de Marzo 2021 |
| Definir roles y responsabilidades de seguridad y privacidad de la información | | 31 de Marzo 2021 |
| Identificar, valorar y tratar los riesgos de seguridad de la información. | Matriz de riesgos actualizada. Plan de tratamiento de riesgos de seguridad de la información. | 31 de Mayo 2021 |
| Plan de comunicaciones del MSPI para EMPAS S.A. | Plan de socialización de políticas de seguridad | 31 de Marzo 2021 |

Tabla 4. Actividades Fase de Planificación

9. FASE DE IMPLEMENTACIÓN

Con base en los resultados de la fase de planificación, se procede a la implementación de las políticas, cuyo objetivo es materializar las acciones contempladas para garantizar la seguridad de la información. En esta etapa se establecen los controles de seguridad de la información que haya lugar de acuerdo a la valoración de riesgos.

| Actividad | Resultado | Fecha |
|--|--|----------------------|
| Desarrollar la declaración de aplicabilidad de los controles de seguridad. | Documento de declaración de aplicabilidad de controles | 31 de mayo 2021 |
| Implementar y monitorear el Plan de tratamiento de | Seguimiento del plan de tratamiento de riesgos de | 31 de Diciembre 2021 |

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 11 de 13 |

| | | |
|---|---|---------------------|
| riesgos de seguridad y privacidad de la información | seguridad de la información. | |
| Seguimiento al plan de transición a IPV6 | Informe de estado de la transición a IPV6 | 31 de Marzo de 2021 |

Tabla 5. Actividades Fase de Implementación

10. FASE DE EVALUACIÓN

El propósito de esta fase es hacer seguimiento y monitorear el plan, con base en los resultados que arrojan los indicadores de seguridad y privacidad de la información, ideados para validar los controles, su eficiencia y eficacia.

| Actividad | Resultado | Fecha |
|---|---|----------------------|
| Revisión del Manual de Seguridad y Privacidad de la Información por parte de la dirección de EMPAS S.A. | Manual revisado y actualizado. | 31 de Agosto de 2021 |
| Creación de indicador para seguimiento del plan. | Indicador creado | 31 de marzo de 2021 |
| Seguimiento a los controles de los riesgos de Seguridad y Privacidad de la Información | Evidencias de controles a los riesgos de Seguridad y Privacidad de la Información | 31 de Diciembre 2021 |

Tabla 6. Actividades Fase de Evaluación

11. FASE DE MEJORAMIENTO CONTINUO


La Fase final del ciclo para el desarrollo del Plan tiene como fin la mejora continua de los procesos y procedimientos de seguridad y privacidad de la información de EMPAS S.A., con base en el resultado de la evaluación de la fase anterior.

| Actividad | Resultado | Fecha |
|---|--|----------------------|
| Desarrollar plan de mejoramiento continuo de los procesos y procedimientos de seguridad y privacidad de la información. | Planes de mejoramiento continuo en el área de sistemas de información. | 31 de Diciembre 2021 |

Tabla 7. Actividades Fase de Mejora Continua



| Planificación | | | | |
|--|---|----------------------|------------------------|---|
| Actividad | Resultado | Fecha | Recursos | Responsable |
| Establecer la política general de seguridad y privacidad de la información de EMPAS S.A. | Manual de Seguridad y Privacidad de la Información aprobado por la dirección y socializado. | 31 de Marzo 2021 | Humanos | Equipo de Sistemas de Información Profesional Planeación corporativa |
| Definir roles, responsabilidades Y autoridades de seguridad y privacidad de la información | | 31 de Marzo 2021 | Humanos | Gerencia |
| Identificar, valorar y tratar los riesgos de seguridad de la información. | Matriz de riesgos actualizada Plan de tratamiento de riesgos de seguridad de la información. | 31 de Mayo 2021 | Humanos y Tecnológicos | Contratista Gobierno Digital |
| Plan de comunicaciones del MSPi para EMPAS S.A. | Plan de socialización de políticas de seguridad | 31 de Marzo 2021 | Humanos | Profesional Planeación corporativa y calidad |
| Implementación | | | | |
| Actividad | Resultado | Fecha | Recursos | Responsable |
| Desarrollar la declaración de aplicabilidad de los controles de seguridad. | Documento de declaración de aplicabilidad de controles | 31 de Mayo 2021 | Humanos y Tecnológicos | Equipo de sistemas de información |
| Implementar y monitorear el Plan de tratamiento de riesgos de seguridad y privacidad de la información | Evidencias de ejecución del plan de tratamiento de riesgos de seguridad de la información. | 31 de Diciembre 2021 | Humanos y Tecnológicos | Equipo de Sistemas de Información Profesional Planeación corporativa |
| Seguimiento al plan de transición a IPV6 | Informe de estado de la transición a IPV6 | 31 de Marzo de 2021 | Humanos y Tecnológicos | Profesional infraestructura – Sistemas de Información |
| Evaluación | | | | |
| Actividad | Resultado | Fecha | Recursos | Responsable |
| Revisión del estado del Manual de | Manual revisado y actualizado. | 31 de Agosto de 2021 | Humanos | Profesional Sistemas de |

| | | |
|---|---|----------------|
|  | EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P. EMPAS S.A. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Código:PLGI-03 |
| | | Versión:00 |
| | | Pág. 13 de 13 |

| | | | | |
|---|---|----------------------|------------------------|--|
| Seguridad y privacidad de la Información por parte de la dirección de EMPAS S.A. | | | | Gestión |
| Creación de indicador para seguimiento del plan. | Indicador creado | 31 de marzo de 2021 | Humanos | Contratista Gobierno Digital |
| Seguimiento a los controles de los riesgos de Seguridad y Privacidad de la Información | Evidencias de controles a los riesgos de Seguridad y Privacidad de la Información | 31 de Diciembre 2021 | Humanos | Control Interno |
| Mejora Continua | | | | |
| Actividad | Resultado | Fecha | Recursos | Responsable |
| Desarrollar plan de mejoramiento continuo de los procesos y procedimientos de seguridad y privacidad de la información. | Planes de mejoramiento continuo en el área de sistemas de información. | 31 de Diciembre 2021 | Humanos y Tecnológicos | Asesor de Gerencia – Sistemas de Información |

Tabla 8. Consolidado PHVA

| | | |
|---|--|--|
| Actualizo | Revisó | Aprobó |
| Contratista Área de Sistemas de información | Asesor de Gerencia Sistemas de información | Comité Institucional de Gestión y Desempeño |