

## CHECK LIST ISO 27001:2013

ACTIVIDAD	COMPLETO
<b>1.1 Requisitos del SGSI</b>	<b>7</b>
<b>NUMERAL 4</b>	<b>2</b>
4.1 Comprender la organización y su contexto	
4.2 Comprender las necesidades y expectativas de las partes interesadas	
4.3 Alcance del SGSI documentado	X
4.4 Sistema de Gestión de la seguridad de la información	X
<b>NUMERAL 5</b>	<b>3</b>
5.1 Liderazgo y compromiso	X
5.2 Política general del SGSI	X
5.3, Roles, organizaciones , responsables y autoridades - 7.2 Competencia - A.6.1.1 roles y responsabilidades para la seguridad de la información	X
<b>NUMERAL 6</b>	<b>0</b>
6.1 Acciones para abordar los riesgos y oportunidades	
6.2 objetivos de seguridad de informacion y planes para alcanzarlos	
<b>NUMERAL 7</b>	<b>0</b>
7.1 Recursos	
7.3 Toma de conciencia	

7.4 Comunicación	
7.5 Información documentada	
<b>NUMERAL 8</b>	<b>1</b>
8.2 Valoración de riesgos de la seguridad de la información- A.8.1.1 inventario de activos,A.8.1.2 propiedad de los activos	X
8.3 Tratamiento de riesgos en seguridad de la información	
<b>NUMERAL 9</b>	<b>1</b>
9.1 Seguimiento, medición, análisis y evaluación	X
9.2 Auditorías internas al SGSI	
9.3 Revisión por la dirección	
<b>NUMERAL 10</b>	<b>0</b>
10.1 No conformidades y acciones correctivas	
10.2 Mejora continua	
<b>1.2 Controles de seguridad de la información (Anexo A)</b>	<b>114</b>
<b>POLÍTICAS</b>	<b>14</b>
A.5.1.1 Políticas para la seguridad de la información:	X
A.6.2.1 política para dispositivos móviles,	X
A 8.1.3 uso aceptable de los activos,	X

A.8.2 Clasificación de la información	X
A.9.1.1 política de control de acceso,	X
A.10.1.1 política sobre el uso de controles criptográficos,	X
A.11 Seguridad física y del entorno	X
A.11.2.9 política de escritorio limpio y pantalla limpia,	X
A.12.6.2 Política de restricción de software no autorizado	X
A.13.2.1 políticas y procedimientos de transferencia de información,	X
A.14.2.1 Política de desarrollo seguro	X
A.15.1.1 política de seguridad de la información para las relaciones con proveedores	X
A.18.1. Política de Protección de datos personales	X
A.5.1.2 revisión de las políticas para la seguridad de la información	X
<b>6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</b>	<b>5</b>
A.6.1.2 separación de deberes (Segregación de funciones)	X
A.6.1.3 contacto con las autoridades	X
A.6.1.4 contacto con grupos de interés especial	X
A.6.1.5 seguridad de la información en la gestión de proyectos	X
A.6.2.2 teletrabajo	X
<b>7. SEGURIDAD DEL RECURSO HUMANO</b>	<b>6</b>

A.7.1.1 selección	X
A.7.1.2 términos y condiciones del empleo	X
A.7.2.1 responsabilidades de la dirección	X
A.7.2.2 toma de conciencia, educación y formación en la seguridad de la información	X
A.7.2.3 proceso disciplinario	X
A.7.3.1 terminación o cambio de responsabilidades de empleo	X
<b>8. GESTIÓN DE ACTIVOS</b>	<b>7</b>
A.8.1.4 devolución de activos	X
A.8.2.1 clasificación de la información	X
A.8.2.2 etiquetado de la información	X
A.8.2.3 manejo de activos	X
A.8.3.1 gestión de medios removibles	X
A.8.3.2 disposición de los medios	X
A.8.3.3 transferencia de medios físicos	X
<b>9. CONTROL DE ACCESO</b>	<b>7</b>
A.9.1.2 acceso a redes y a servicios de red	X
A.9.2.1 registro y cancelación del registro de usuarios	X
A.9.2.2 suministro de acceso de usuarios	X
A.9.2.3 gestión de derechos de acceso privilegiado	X
A.9.2.4 gestión de información de autenticación secreta de usuarios	X
A.9.2.5 revisión de los derechos de acceso de usuarios	X
A.9.2.6 retiro o ajuste e los derechos de acceso	X
<b>9.3 RESPONSABILIDADES DE LOS USUARIOS</b>	<b>1</b>

A.9.3.1 uso de información de autenticación secreta	X
<b>9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES</b>	<b>5</b>
A.9.4.1 restricción de acceso a la información	X
A.9.4.2 procedimiento de ingreso seguro	X
A.9.4.3 sistema de gestión de contraseñas	X
A.9.4.4 uso de programas utilitarios privilegiados	X
A.9.4.5 control de acceso a códigos fuente de programas	X
<b>10. CRIPTOGRAFÍA, CONTROLES CRIPTOGRAFICOS</b>	<b>1</b>
A.10.1.2 gestión de llaves	X
<b>11. SEGURIDAD FÍSICA Y DEL ENTORNO</b>	<b>14</b>
A.11.1.1 perímetro de seguridad física	X
A.11.1.2 contorles de acceso físicos	X
A.11.1.3 seguridad de oficinas, recintos e instalaciones	X
A.11.1.4 protección contra amenazas externas y ambientales	X
A.11.1.5 trabajo en áreas seguras	X
A.11.1.6 áreas de despacho y carga	X
A.11.2.1 ubicación y protección de los equipos	X
A.11.2.2 servicios de suministro	X
A.11.2.3 seguridad del cableado	X
A.11.2.4 mantenimiento de equipos	X
A.11.2.5 retiro de activos	X
A.11.2.6 seguridad de equipos y activos fuera de las instalaciones	X
A.11.2.7 disposición segura o reutilización de equipos	X
A.11.2.8 equipos de usuario desatendido	X
<b>12. SEGURIDAD DE LAS OPERACIONES</b>	<b>14</b>

<i>A.12.1.1 procedimientos de operación documentados</i>	X
<i>A.12.1.2 gestión de cambios</i>	X
<i>A.12.1.3 gestión de capacidad</i>	X
<i>A.12.1.4 separación de los ambientes de desarrollo, pruebas y operación</i>	X
<i>A.12.2.1 controles contra códigos maliciosos</i>	X
<i>A.12.3.1 respaldo de la información</i>	X
<i>A.12.4.1 registro de eventos</i>	X
<i>A.12.4.2 protección de la información de registro</i>	X
<i>A.12.4.3 registros de administrador y del operador</i>	X
<i>A.12.4.4 sincronización de relojes</i>	X
<i>A.12.5.1 instalación de software en sistemas operativos</i>	X
<i>A.12.6.1 gestión de las vulnerabilidades técnicas</i>	X
<i>A.12.6.2 restricciones sobre la instalación de software</i>	X
<i>A.12.7 controles de auditorías de sistemas de información</i>	X
<b>13. SEGURIDAD DE LAS COMUNICACIONES</b>	<b>6</b>
<i>A.13.1.1 controles de redes</i>	X
<i>A.13.1.2 seguridad de los servicios de red</i>	X
<i>A.13.1.3 separación de las redes</i>	X
<i>A.13.2.2 acuerdos sobre transferencia de información</i>	X
<i>A.13.2.3 mensajería electrónica</i>	X
<i>A.13.2.4 acuerdos de confidencialidad o de no divulgación</i>	X
<b>14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS</b>	<b>9</b>
<i>A.14.1.1 análisis y especificación de requisitos de seguridad de la información</i>	X
<i>A.14.1.2 seguridad de servicios de las aplicaciones en redes públicas</i>	X

A.14.1.3 protección de transacciones de los servicios de las aplicaciones	X
A.14.2.2 procedimientos de control de cambio de sistemas	X
A.14.2.5 principios de construcción de los sistemas seguros	X
A.14.2.6 ambiente de desarrollo seguro	X
A.14.2.7 desarrollo contratado externamente	X
A.14.2.8 pruebas de seguridad de sistemas	X
A.14.2.9 prueba de aceptación de sistemas	X
A.14.3.1 protección de datos de prueba	X
<b>15. RELACIONES CON LOS PROVEEDORES</b>	<b>4</b>
A.15.1.2 tratamiento de la seguridad dentro de los acuerdos con proveedores	X
A.15.1.3 cadena de suministro de tecnología de información y comunicación	X
A.15.2.1 seguimiento y revisión de los servicios de los proveedores	X
A.15.2.2 gestión de cambios en los servicios de los proveedores	X
<b>16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>7</b>
A.16.1.1 responsabilidades y procedimientos	X
A.16.1.2 reporte de eventos de seguridad de la información	X
A.16.1.3 reporte de debilidades de seguridad de la información	X
A.16.1.4 evaluación de eventos de seguridad de la información y decisiones sobre ellos.	X
A.16.1.5 respuesta a incidentes de seguridad de la información	X
A.16.1.6 aprendizaje obtenido de los incidentes de seguridad de la información	X
A.16.1.7 recolección de evidencia	X
<b>17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO</b>	<b>4</b>
A.17.1.1 planificación de la continuidad de la seguridad de la información	X
A.17.1.2 implementación de la continuidad de la seguridad de la información	X
A.17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información	X

A.17.2.1 disponibilidad de instalaciones de procesamiento de información	X
<b>18. CUMPLIMIENTO</b>	<b>10</b>
A.18.1.1 identificación de la legislación aplicable y de los requisitos contractuales	X
A.18.1.2 derechos de propiedad intelectual	X
A.18.1.3 protección de registros	X
A.18.1.4 privacidad y protección de información de datos personales	X
A.18.1.5 reglamentación de controles criptográficos	X
A.18.2.1 revisión independiente de la seguridad de la información	X
A.18.2.2 cumplimiento con las políticas y normas de seguridad	X
A.18.2.3 revisión del cumplimiento técnico	X
A.18.2.2 cumplimiento con las políticas y normas de seguridad	X
A.18.2.3 revisión del cumplimiento técnico	X





DOCUMENTADO?		
PARCIAL	NINGUNO	PORCENTRAJE
12	1	93%
2	0	21%
X		Aun Falta, Acelera ritmo
X		
0	0	21%
		Aun Falta, Acelera ritmo
2	0	7%
X		Aun Falta, Acelera ritmo
X		
4	0	14%
X		Aun Falta, Acelera
X		

X		ritmo
X		
1	0	11%
		Aun Falta, Acelera ritmo
X		
1	1	11%
X		Aun Falta, Acelera ritmo
	X	
2	0	7%
X		Aun Falta, Acelera ritmo
X		
0	0	100%
0	0	100%









0	0	100%
0	0	100%
0	0	100%







## EVIDENCIA

Se encuentra integrado al manual del Sistema de Gestión, dentro del contexto

Se encuentra integrado al manual del Sistema de Gestión, dentro de la ,matrriz de partes interesadas.

Se encuentra integrado al manual del Sistema de Gestión, dentro del alcance del sistema.

Se encuentra integrado al manual del Sistema de Gestión, dentro del Mapa de procesos y la caracterización de procesos.

El liderazgo y compromiso de la alta gerencia se evidencia a travez de la oficina asesora de planeación e información quien apoya, coordina y hace seguimiento al avance de la implemetacion del sistema en las fases de planear, hacer, verificar y actuar

Se encuentra formalizada y publicada en la pagian web - Resolucio 0199 del 2020

Este documento hace parte del manual de poliitcas específicas de segurifsd y privacidad de la informacion, que se encuentra publicado en el proceso de gestion tecnologica. - **MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1**

Se cuenta con un instrumento para la gestion de riesgos de seguridad digital, se iniciaron mesas de trabajo donde se socializó el instrumento y la metodologia, se aprovisionaron los recursos en el sharepoint y se esta iniciando el diligenciamiento del instrumento por los procesos para su posterior consolidación

Validar los objetivos del Sistema de gestion de seguridad de la informacion y realizar el seguimiento con corte al 2021 - Seguimiento Política Integral MIPG-SIG Trim III 2021 - copia

Se cuenta con un anteproyecto de presupuesto de la OAPI (SIG) asociado al equipo tecnicos del SGSI

Dentro del plan de seguridad y privacidad de la información hay un item que hace referencia a la toma de conciencia a traves de - **Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital** (Boletines informacitivos, correos)

Dentro del plan de seguridad y privacidad de la información hay un item que hace referencia a la toma de conciencia a través de - **Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital** (Boletines informativos, correos)

Se está elaborando, revisando, actualizando y/o formalizando los documentos obligatorios del SGSI.

Se cuenta con un instrumento para la gestión de riesgos de seguridad digital, se iniciaron mesas de trabajo donde se socializó el instrumento y la metodología, se aprovisionaron los recursos en el sharepoint y se está iniciando el diligenciamiento del instrumento por los procesos para su posterior consolidación.

Se cuenta con el inventario de activos de información levantado y actualizado de acuerdo a las TRD vigentes. (Sharepoint).

Para el caso de los servidores públicos, proveedores y terceros se tienen definidos requisitos de seguridad para el acceso a la información Clasificada y Reservada de la entidad. (Clausulas de contratos, acuerdos de confidencialidad, procedimientos de contratación entre otros).

Se está construyendo en la herramienta de riesgos de seguridad digital

Se tienen identificados y se les hace seguimiento trimestral - Informe de Indicadores

Se realizaron auditorías internas a los procesos misionales, pero no se cuenta con el informe de auditoría y los hallazgos generados en este.

Revisar el programa de auditoría que incluya los aspectos de SGSI.

Se tienen insumos del desempeño del SGSI, pero no están alineados con TODOS los elementos de entrada definidos en la norma ISO 27001:2013 en el numeral 9.2

Se tiene documentado el PROCEDIMIENTO DE GESTIÓN DE MEJORA.

No hay acciones de mejora reportadas

Se tiene documentado el PROCEDIMIENTO DE GESTIÓN DE MEJORA.

No hay acciones de mejora reportadas

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.

Se está formalizando la guía de uso aceptable de activos

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.  
Los activos de información se encuentran clasificados de acuerdo al nivel de importancia respecto a la confidencialidad, integridad y disponibilidad de la información. Este ejercicio se hizo alineado a la Ley 1712.

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.  
Se cuenta con acuerdos de confidencialidad multipropósito que sirven para servidores públicos, proveedores y terceros.

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.  
Hay una política de protección de datos personales publicada en la página web de la entidad.

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.  
Actualmente estamos en proceso de actualización de las políticas, derivados de los cambios en los roles y responsabilidades de la seguridad de la información, adicionalmente ajustar el término funcionario por servidores públicos.

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.  
Se participa en mesas de trabajo con CCOCI, Mintic y el CSIRT Gobierno

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.

Se viene trabajando en la formalización de la guía de etiquetado de información

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1.

Procedimientos de identificación, valoración y clasificación de activos de información.  
Guía de uso aceptable de activos.

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1







Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1

Este control se encuentra contemplado en el MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-MA-02-V1





## OBSERVACIONES

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.

Entregar avance con corte al 2021

Contar con mínimo dos personas para la gestión del SGSI con las competencias e idoneidad.

Mejorar la estrategia de comunicación de los planes para la toma de conciencia.

Mejorar la estrategia de comunicación del sistema de gestión de seguridad de la información.

Diligenciar la herramienta por los líderes y/o responsables de cada proceso.  
Identificar los procedimientos de tecnologías de la información asociados a la seguridad de la información

Revisar el informe y el programa de auditoría y tomar acciones para el mejoramiento de este.

Establecer plan de mejoramiento

Documentar y hacer seguimiento a las acciones generadas en el proceso que evidencien acciones correctivas

Mejorar la estrategia de comunicación del Manual del sistema de gestión para que se garantice que todas las partes interesadas lo conozcan.


































































































































































































