PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Requerimientos Tecnológicos

2023

INTRODUCCIÓN

El Instituto de Desarrollo de Arauca IDEAR tiene por objeto principal el fomento del desarrollo económico y social en el ámbito local, municipal, departamental y regional mediante la prestación de servicios relacionados con la ejecución de actividades financieras y las conexas para ejecutar estas, dirigidas a la obtención, administración y colocación de recursos que se utilicen para gestión y ejecución de programas y proyectos de inversión en los sectores económicos y sociales destinatarios, constitucional y legalmente de la inversión Estatal; todo lo anterior en el marco legal que como establecimiento público del orden territorial le corresponde y puede desplegar al pertenecer a la categoría de instituto para el financiamiento y desarrollo territorial.

El IDEAR, es un establecimiento público de carácter departamental, descentralizado, de fomento, promoción y desarrollo, regulado por los artículos 70 a 81 de la Ley 489 de 1998, el Decreto Nro. 1221 de 1986, dotado con personería jurídica, autonomía administrativa y patrimonio propio y hace parte de las instituciones denominadas en el Estado Colombiano como Institutos de Fomento y Desarrollo Territorial -INFIS-.

El IDEAR ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones. En la gestión de los procesos estratégicos, misionales y de apoyo, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa que puede ir desde un dato personal hasta secretos empresariales que no deben ser divulgados a personal no autorizado, suceso que puede poner en riesgo la gestión pública.

En atención a lo anterior, la entidad asumió el reto de implementar el SGSI, siguiendo los lineamientos del MSPI de la Estrategia de Gobierno en Línea, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, el SGSI del IDEAR adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

Así mismo, el SGSI del IDEAR define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en

continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoria y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

Lo anterior se complementa con los programas de formación y transferencia de conocimiento en seguridad de la información y las campañas de sensibilización que se lideran al interior de la entidad.

Así pues, la entidad expone a través de este manual el modelo del SGSI adoptado por la entidad de acuerdo con el ciclo PHVA (planear, hacer, verificar y actuar), con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada. Dicho manual describe las disposiciones acogidas por la entidad para establecer el contexto, las políticas, los objetivos, el alcance, los procedimientos, las metodologías, los roles, las responsabilidades y las autoridades del SGSI; de acuerdo con los requisitos legales, los contractuales y los normativos, que le aplican a la entidad, en el marco de seguridad de la información.

Para tal fin, la entidad ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

1. OBJETIVO

Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad según el modelo del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, adoptado por el Instituto de Desarrollo de Arauca, en adelante IDEAR; este documento expone las prioridades de implementación de los controles en relación a seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

2. OBJETIVOS ESPECÍFICOS

- ✓ Comunicar e implementar la estrategia de seguridad de la información.
- ✓ Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- ✓ Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- ✓ Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- ✓ Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos del IDEAR, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para el IDEAR.

4. DEFINICIONES

- ✓ **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- ✓ **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- ✓ **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ **Contratistas**: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

- ✓ **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

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

- ✓ **Guía**: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

- ✓ **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- ✓ **Norma**: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

- ✓ **Parte interesada**: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- ✓ **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.

- ✓ **Política**: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

- ✓ **Privacidad de datos:** La privacidad de datos, también llamada protección de datos es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.
- ✓ **Procedimiento**: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

- ✓ **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- ✓ **Rol:** Papel, función que alguien o algo desempeña.

- ✓ **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- ✓ **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

5. MARCO LEGAL

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

6. CONOCIMIENTO DE LA ENTIDAD.

MISIÓN.

La Misión del Instituto de Desarrollo de Arauca - IDEAR-, consiste en contribuir con el fomento del desarrollo económico y bienestar social del Departamento de Arauca, a través de la ejecución de las actividades financieras y gestión de programas y proyectos de inversión que, en el marco legal vigente, puede desplegar como establecimiento público del orden territorial y su categoría de instituto para el financiamiento y desarrollo territorial -INFIS-.

VISIÓN.

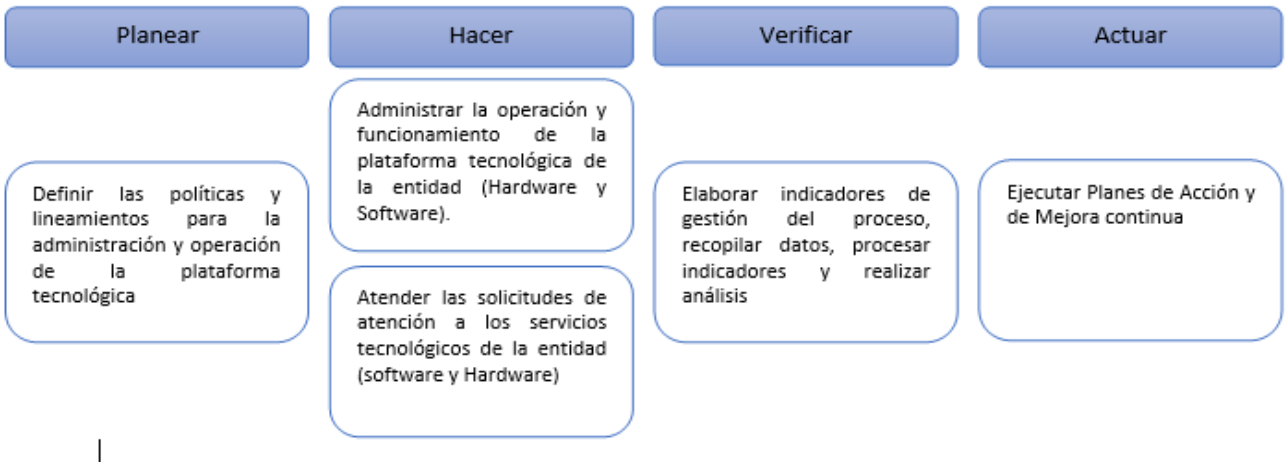
El Instituto de Desarrollo de Arauca - IDEAR- se consolidará como una entidad líder del nivel descentralizado departamental consecuencia de la implementación de su modelo de gestión y financiamiento de proyectos socioeconómicos que promuevan el bienestar de la Región y garanticen su sostenimiento y rentabilidad institucional y social.

7. MODELO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI.

7.1 ANTECEDENTES.

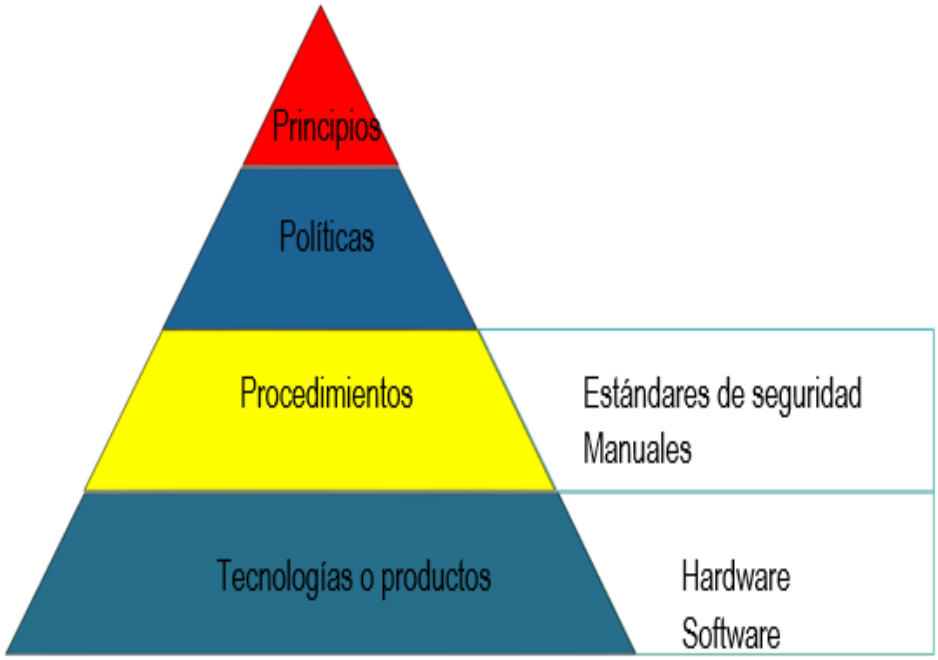
En la actualidad y de acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; el IDEAR trabaja permanentemente en pro de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

En efecto, el modelo del SGSI del IDEAR se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.



7.2 DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo con su importancia, a continuación, se ilustran dichos componentes:



7.3 ALCANCE DEL SGSI

Teniendo en cuenta el análisis del contexto externo, interno y las partes interesadas, el IDEAR define el alcance de SGSI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología, así:

Alcance: "El Plan de Seguridad Informática del IDEAR, busca proteger la información y los elementos clave dentro del instituto (activos, equipos e infraestructura tecnológica), definiendo las responsabilidades que deben asumir cada uno de los funcionarios de la entidad, durante su permanencia en la misma. Esto con el fin de desarrollar operaciones y servicios seguros, basados en normativas y estándares en seguridad de la información, para que sean divulgados y conocidos por todos los funcionarios de la entidad. Igualmente, se contempla la definición de estrategias y actividades que se deben llevar a cabo durante la implementación de este plan y su permanente control, validación y actualización".

8 DESARROLLO

8.1 CONTEXTO

En esta fase inicial del desarrollo del plan de tratamiento de riesgos de seguridad y privacidad de la información, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

- ✓ La misión.
- ✓ La visión.
- ✓ Estructura organizacional.
- ✓ Procesos.
- ✓ Cultura y valores.
- ✓ Normatividad

8.2 SITUACIÓN ACTUAL

Por situación actual se entiende el nivel de madurez que posee en este momento el IDEAR con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina análisis GAP o análisis de brecha. Para poder realizar el plan de tratamiento de riesgos de seguridad y privacidad de la información es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios (ver figura a continuación) con el fin de plantear prioridades sobre su implementación. Para obtener estos resultados, fue indispensable utilizar la herramienta denominada “Instrumento de Evaluación MSPI” diseñada por el MINTIC.

8.2.1 CONTROLES DE SEGURIDAD

Tablas de Controles Estándar ISO/IEC 27001:2013 Vs Dominios a los Pertenece			
Núm.	**Nombre**		**Descripción / Justificación.**
1	Objeto y Campo de Aplicación.	SI	Seleccionar los controles dentro del Sistema de Gestión de Seguridad de la Información – SGSI.
2	Referencias Normativas.	SI	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y Definiciones.	SI	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma.	SI	La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5	**Políticas de Seguridad de la información.**		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información.		**Objetivo:** Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos.
A.5.1.1	Políticas para la seguridad de la información.	SI	**Control:** Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información.	SI	**Control:** Las políticas para la seguridad de la información se debería revisar en intervalos planificados o si ocurren cambios significativos. Para asegurar su convivencia, adecuación y eficacia continuas.
A.6	**Organización de la seguridad de la información.**		
A.6.1	Organización Interna.		**Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y Responsabilidad para la seguridad de la información.	SI	**Control:** Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes.	SI	**Control:** Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las Autoridades.	SI	**Control:** Se deberían mantener los contados apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especiales	SI	**Control:** Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	**Control:** La seguridad de la información se debería tratar en la gestión de provectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos Móviles y Teletrabajo		**Objetivo:** Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles de la entidad.

A.6.2.1	Política para Dispositivos Móviles	SI	**Control:** Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	NO	**Control:** Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	**Seguridad de los Recursos Humanos**		
A.7.1	Antes de asumir el Cargo		**Objetivo:** Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección	SI	**Control:** Las verificaciones de los antecedentes de todos los candidatos a un cargo se deberían llevar a cabo de acuerdo con las leyes reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
A.7.12	Términos y condiciones del Cargo	SI	**Control:** Los acuerdos contractuales con empleados y contratistas deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del Cargo		**Objetivo:** Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la Dirección	SI	**Control:** La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	SI	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso Disciplinario	SI	**Control:** Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo		**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista v se deberían hacer cumplir.
A.8	**Gestión de Activos**		
A.8.1	Responsabilidad por los activos.		**Objetivo:** identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos.	SI	**Control:** Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de

			información, y se debería elaborar v mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	SI	**Control:** Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos.	SI	**Control:** Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	SI	**Control:** Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información		**Objetivo:** Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	SI	**Control:** La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	SI	**Control:** Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	SI	**Control:** Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información ado9tado por la organización.
A.8.3	Gestión de medios		
A.8.3.1	Gestión de medios removibles	SI	**Control:** Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	SI	**Control:** Se debería disponer en forma segura de los medios cuando va no se requieran. utilizando procedimientos formales.
A.8.3.3	Transferencia de medios Físico	SI	**Control:** Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	**Control de Acceso**		
A.9.1	Requisitos del negocio para el control de Acceso		**Objetivo:** Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	SI	**Control:** Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de Red	SI	**Control:** Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		**Objetivo:** Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

A.9.2.1	Registro y cancelación del registro de usuarios	SI	**Control:** Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuario	SI	**Control:** Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	SI	**Control:** Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información autenticación secreta de usuarios	SI	**Control:** La asignación de la información secreta se debería controlar por medio de un proceso de gestión forma.
A.9.2.5	Revisión de los derechos de acceso de usuarios	SI	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidad de los usuarios		**Objetivo:** Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	SI	**Control:** Se debería exigir a los usuarios que cumplan las prácticas de la organización Dara el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones		**Objetivo:** Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso a la información	SI	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	SI	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistemas de gestión de contraseñas	SI	**Control:** Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	SI	**Control:** Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	SI	**Control:** Se debería restringir el acceso a ¡os códigos fuente de los programas.
A.10	**Criptografía**		
A.10.1	Controles criptográficos		**Objetivo:** Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos	NO	**Control:** Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	NO	**Control:** Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

A.11	Seguridad Física y del entorno		
A.11.1	Áreas seguras		**Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización
A.11.1.1	Perímetro de seguridad Física	SI	**Control:** Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles Fiscos de entrada	SI	**Control:** Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a Personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	**Control:** Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenaza externas y ambientales	SI	**Control:** Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en área seguras.	SI	**Control:** Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A11.1.6	Áreas de despacho y carga		**Control:** Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos		Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos	SI	**Control:** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades Dara acceso no autorizado.
A.11.2.2	Servicios de Suministro	SI	**Control:** Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	SI	**Control:** El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de Equipos	SI	**Control:** Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	SI	**Control:** Los equipos. información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	**Control:** Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	SI	**Control:** Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuarios desatendidos	SI	**Control:** Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.

A.11.2.9	Política de escritorio limpio y pantalla limpia	SI	**Control:** Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	**Seguridad de las Operaciones**		
A.12.1	Procedimientos operacionales y responsabilidades		**Objetivo:** Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operaciones documentadas	SI	**Control:** Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten
A.12.1.2	Gestión de cambios	SI	**Control:** Se deberían controlar los cambios en la organización, en los procesos de negocio, en las ¡instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	SI	**Control:** Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	SI	**Control:** Se deberían separar los ambientes de desarrollo. prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos		**Objetivo:** Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	SI	**Control:** Se deberían Implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios. Dara proteger contra códigos maliciosos.
A.12.3	Copias de respaldo		**Objetivo:** Proteger contra la perdida de datos.
A.12.3.1	Respaldo de Información	SI	**Control:** Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y Seguimiento		**Objetivo:** Registrar eventos y generar evidencia.
A.12.4.1	Registro de Eventos	SI	**Control:** Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	SI	**Control:** Las instalaciones y la información de registro se deberían proteger contra alteración Y acceso no autorizado.
A.12.4.3	Registro del administrador y del operador	SI	**Control:** Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	SI	**Control:** Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de Software		**Objetivo:** Asegurar la integridad de los sistemas

			operacionales.
A.12.5.1	Instalación de software en sistemas operativos	SI	**Control:** Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de vulnerabilidad técnica		**Objetivo:** Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	SI	**Control:** Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	SI	**Control:** Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios
A.12.7	Consideraciones sobre auditorias de sistemas de información		**Objetivo:** Minimizar el impacto de las actividades de auditoria sobre los sistemas operacionales
A.12.7.1	información controles de auditoria de sistemas	SI	**Control:** Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	**Seguridad de las comunicaciones**		
A.13.1	Gestión de la seguridad de las redes		**Objetivo:** Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes	SI	**Control:** Las redes se deberían gestionar y controlar para proteger la información en sistemas v aplicaciones.
A.13.1.2	Seguridad de los servicios de red	SI	**Control:** Se deberían identificar los mecanismos de seguridad. los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	SI	**Control:** Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información		**Objetivo:** Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información	SI	**Control:** Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	SI	**Control:** Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas
A.13.2.3	Mensajería electrónica	SI	**Control:** Se debería proteger adecuadamente la información incluida en la mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	**Control:** Se deberían ¡identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		

A.14.1	Requisitos de seguridad de los sistemas de información		**Objetivo:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	**Control**: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	SI	**Control:** La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	**Control:** La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte		**Objetivo:** Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro	SI	**Control:** Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	SI	**Control:** Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	**Control:** Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	SI	**Control:** Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros	SI	**Control:** Se deberían establecer. documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	SI	**Control:** Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	SI	**Control:** La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	SI	**Control:** Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.

A.14.2.9	Prueba de aceptación de sistemas	SI	**Control**: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación v criterios de aceptación relacionados.
A.14.3	Datos de prueba		**Objetivo:** Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba	SI	**Control:** Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15	**Relación con los proveedores**		
A.15.1	Seguridad de la información en las relaciones con los proveedores		**Objetivo:** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	SI	**Control:** Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	SI	**Control:** Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	**Control:** Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información v comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores	SI	**Objetivo:** Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	**Control:** Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	SI	**Control:** Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riegos.
A.16	**Gestión de incidentes de seguridad de la información**		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		**Objetivo:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos	SI	**Control:** Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz v ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	SI	**Control:** Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible

A.16.1.3	Reporte de debilidades de seguridad de la información	SI	**Control:** Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	**Control:** Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información
A.16.1.5	Respuesta a incidentes de seguridad de la información	SI	**Control:** Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la Información	SI	**Control:** El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	SI	**Control**: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**		
A.17.1	Continuidad de seguridad de la información		**Objetivo:** La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	**Control:** La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	**Control:** La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	**Control:** La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias		**Objetivo:** Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	SI	**Control:** Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	**Cumplimiento**		
A.18.1	Cumplimiento de requisitos legales y contractuales		**Objetivo:** Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información. y de cualquier requisito de seguridad.
A.18.1.1	identificación de la legislación aplicable y de los requisitos contractuales	SI	**Control:** Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para

			cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	SI	**Control:** Se deberían ¡implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	SI	**Control:** Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	SI	**Control:** Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	SI	**Control:** Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, ¡legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información	SI	**Control:** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	**Control:** Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas. v cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimento técnica	SI	**Control:** Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

8.2.2 DECLARACION DE APLICABILIDAD.

			RAZON DE LA SELECCION	ESTADO	OBSERVACION
DOMINIO	**A.5**	**Políticas de Seguridad de la información.**			
OBJETIVO	A.5.1	Directrices establecidas por la dirección para la seguridad de la información.	**Objetivo:** Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos.		
CONTROL	A.5.1.1	Políticas para la seguridad de la información.	Generar el documento de la política de seguridad de la información, aprobarla por dirección, publicarla y comunicarla a los empleados y partes externas.	Implementado parcialmente	Se ve la necesidad de definir las políticas para la seguridad de la información y aplicarlas en la entidad.
CONTROL	A.5.1.2	Revisión de las políticas para la seguridad de la información.	La política de seguridad de la información debe ser revisada periódicamente o si hay cambios significativos, para garantizar la conveniencia, adecuación y eficiencia.	No implementado	Se debe realizar la revisión y evaluación de la política de seguridad de la información para identificar los cambios que se deben aplicar, tener una versión final y a su vez poder comunicar a los empleados y partes externas.
DOMINIO	**A.6**	**Organización de la seguridad de la información.**			
OBJETIVO	A.6.1	**Organización Interna.**		**Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	
CONTROL	A.6.1.1	Roles y Responsabilidad para la seguridad de la información.	Se deben definir todas las responsabilidades en cuanto a seguridad de la información.	No implementado	Se requiere definir todas las responsabilidades en cuanto a seguridad de la información para una lograr, una mejor gestión dentro de la entidad.
CONTROL	A.6.1.2	Separación de deberes.	Es necesario separar los deberes y áreas de responsabilidad en conflicto, con el fin de reducir el riesgo de modificación no autorizada o no intencional, o el uso indebido de los activos de la entidad.	No Implementado	Se hace necesario ¡identificar los conflictos que generan riesgo para separar los deberes y áreas de responsabilidad.

CONTROL	A.6.1.3	Contacto con las Autoridades.	Se deben mantener contactos apropiados con las autoridades pertinentes.	Aplica a una fase posterior del MSPI	Es necesario estar en contacto con las autoridades y darle solución a los problemas legales que incumplan las Leyes Colombianas.
CONTROL	A.6.1.4	Contacto con grupos de interés especiales	Se debe contar con asesoría o contactos adecuados con grupos especiales de interés u otros foros especializados de seguridad o asociaciones profesionales	Parcialmente implementado	Se hace necesario para dar mejor eficiencia y cumplimiento, contar con la orientación o asesoría de personas expertas en temas de seguridad de la información.
CONTROL	A.6.1.5	Seguridad de la información en la gestión de proyectos	Se debe tratar la seguridad de la información en la gestión de proyectos independientemente al tipo de proyecto.	No Implementado	Se hace necesario el manejo adecuado de la seguridad de la información en la gestión de proyectos sin tener en cuenta el tipo de proyecto.
OBJETIVO		A.6.2	**Dispositivos Móviles y Teletrabajo**		**Objetivo:** Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles de la entidad.
CONTROL	A.6.2.1	Política para Dispositivos Móviles	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No Implementado	No se tiene definida una política de dispositivos móviles.
CONTROL	A.6.2.2	Teletrabajo	Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No Implementado	Todo trabajo debe ser realizado en las instalaciones de la entidad.
DOMINIO		**A.7**	**Seguridad de los Recursos Humanos**		
OBJETIVO		A.7.1	Antes de asumir el Cargo		**Objetivo:** Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
CONTROL	A.7.1.1	Selección	Se debe hacer verificación de los antecedentes de los candidatos a ser empleados, contratistas o usuarios de acuerdo con las leyes, reglamentos establecidos por la entidad y la ética, deben ser proporcionales a los requisitos del negocio, la clasificación de la información a lo cual se va a tener acceso y a los riesgos percibidos.	implementado	Se debe tener la certeza que el personal o candidatos a vincular en la entidad deben ser idóneo y no haber sido sancionado ni disciplinaria, fiscal, ni judicialmente de acuerdo con las Ley Colombianas.

CONTROL	A.7.12	Términos y condiciones del Cargo	Como parte de su obligación contractual, los empleados y contratistas deben estar de acuerdo, y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la entidad con relación a la seguridad de la información.	implementado	Con la aceptación de los términos y condiciones del empleo, se busca garantizar el cumplimiento del objeto contractual, sus funciones y obligaciones. Lo anterior con el fin de salvaguardar la integridad, disponibilidad y confidencialidad de la seguridad de la información.
CONTROL	A.7.2	Durante la ejecución del Cargo	Los empleados y contratistas de la entidad deben recibir formación adecuada en concientización y actualizaciones sobre la política de seguridad y los procedimientos de la entidad relativa a sus funciones laborales.	Parcialmente implementado	Se hace necesario la sensibilización y concientización a los funcionarios y contratistas en cuanto a la seguridad de la ¡información, con el fin de generar una cultura de seguridad.
CONTROL	A.7.2.1	Responsabilidades de la Dirección	Los Secretarios de Despacho deben exigir que los empleados y contratistas apliquen la seguridad según las políticas y los procedimientos establecidos por la entidad.	Aplica a una fase posterior del MSPI	Los Secretarios de Despacho deben tener un compromiso porque son los representantes de alto nivel de la entidad que le dan viabilidad a la iniciativa requerida para la implementación del Modelo de la Política de Seguridad Pública y a su vez exigir el cumplimento de la misma.
CONTROL	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la entidad y, cuando sea pertinente los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la entidad, según sea pertinente para sus funciones laborales.	Parcialmente implementado	Se hace necesario la sensibilización a los empleados y si es el caso a los contratistas en cuanto a seguridad de la información con el fin de generar una cultura en la entidad de seguridad.
CONTROL	A.7.2.3	Proceso Disciplinario	Se debe establecer un proceso disciplinario formal y darlo a conocer a los empleados, con el fin de emprender acciones en caso de presentarse violación de la seguridad de la información dentro de la entidad.	Parcialmente implementado	Se debe tomar acciones y hacer las respectivas denuncias ya que la Ley así lo exige.
CONTROL		A.7.3	Terminación o cambio de empleo		**Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
CONTROL	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Se deben definir y asignar las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.	Implementado	Se busca garantizar la ejecución y cumplimento de lo contratado.

DOMINIO		**A.8**	**Gestión de Activos**		
OBJETO		A.8.1	Responsabilidad por los activos.	**Objetivo:** identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	
CONTROL	A.8.1.1	Inventario de activos	Todos los activos asociados con la información y las instalaciones de procesamiento de información deben estar identificados e inventariados.	Parcialmente implementado	Es necesario tener un inventario de activos de información para tener una trazabilidad en los recursos, y saber que recuperar en caso de desastres.
CONTROL	A.8.1.2	Propiedad de los activos	Se deben identificar los propietarios de los activos.	Parcialmente implementado	Es necesario tener un inventario de activos de información para tener una trazabilidad en los recursos, y saber que recuperar en caso de desastres.
CONTROL	A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	Parcialmente implementado	Se hace necesario de definir lineamientos que orientan en el uso adecuado de la plataforma tecnológica de la entidad, así como definir recomendaciones para obtener el mayor provecho y evitar el uso indebido de los recursos tecnológicos.
CONTROL	A.8.1.4	Devolución de activos	Todos los empleados y contratistas deben devolver todos los activos pertenecientes a la entidad que estén en su poder al finalizar su contratación laboral. contrato o acuerdo.	implementado	Para manejo de la información y seguimiento a los activos de la información pertenecientes a la entidad.
OBJETO		A.8.2	Clasificación de la información	**Objetivo:** Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.	
CONTROL	A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de los requisitos legales, valor, criticidad, y susceptibilidad a la divulgación o modificación no autorizada.	Parcialmente implementada	La información debe ser clasificada para una mejor trazabilidad y tratamiento de la información.
CONTROL	A.8.2.2	Etiquetado de la información	Debe ser desarrollado e implementado de acuerdo al esquema de clasificación adoptado por la entidad un conjunto adecuado de procedimientos Dara e etiquetado de la información.	No implementado	Para tener un buen conocimiento de la información a tratar.

CONTROL	A.8.2.3	Manejo de activos	Debe ser desarrollado e implementado procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptada por la entidad.	Parcialmente implementado	Para tener un buen conocimiento de la información a tratar.
OBJETO		A.8.3	Gestión de medios		
CONTROL	A.8.3.1	Gestión de medios removibles	Deben existir procedimientos para la gestión de medios removibles	No implementado	Se busca reducir el riesgo de fuga o perdida de información confidencia
CONTROL	A.8.3.2	Disposición de los medios	Los medios deben ser eliminados de manera segura y sin peligros usando procedimientos formales.	No implementado	Se busca dar un adecuado tratamiento a los residuos tecnológicos, para no atentar con el medio ambiente y dar cumplimiento a las entidades de control.
CONTROL	A.8.3.3	Transferencia de medios Físico	Los medios que contienen ¡información se deben proteger con el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte.	No implementado	Se debe garantizar la integridad y confidencialidad de los activos de información cuando estos se transportan fuera de la entidad.
DOMINIO		**A.9**	**Control de Acceso**		
OBJETO		A.9.1	Requisitos del negocio para el control de Acceso	**Objetivo:** Limitar el acceso a información y a instalaciones de procesamiento de información.	
CONTROL	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos de la entidad y de la seguridad para la seguridad de la información.	No implementado	Garantizar la confidencialidad e integridad de la Información.
CONTROL	A.9.1.2	Política sobre el uso de los servicios de Red	Los usuarios que tienen acceso a la red y servicios de la red deben ser únicamente los autorizados por la entidad.	Implementado	Garantizar que únicamente acceda a la información, red y servicios el personal autorizado por la entidad.
OBJETO	A.9.2	Gestión de acceso de usuarios			
CONTROL	A.9.2.1	Registro y cancelación del registro de usuarios	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	Parcialmente implementado	Se llevará un control del personal al que se le brinda acceso y manipulación a la información.

CONTROL	A.9.2.2	Suministro de acceso de usuario	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	Parcialmente implementado	Se llevará un control del personal al que se le brinda acceso y manipulación a la información.
CONTROL	A.9.2.3	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y el uso de privilegios.	implementado	Permite llevar un control del personal al que se le brinda acceso y manipulación a la información.
CONTROL	A.9.2.4	Gestión de información autenticación secreta de usuarios	La asignación de información secreta (contraseñas) se debe controlar a través de un proceso de gestión formal.	implementado	Garantiza la confidencialidad, integridad de la información.
CONTROL	A.9.2.5	Revisión de los derechos de acceso de usuarios	Los reportes y registros de los propietarios de los activos se deben revisar con regularidad y las auditorías se deben llevar a cabo a intervalos regulares.	implementado	Permite llevar un control y seguimiento del servicio prestado.
CONTROL	A.9.2.6	Retiro o ajuste de los derechos de acceso	Los retiros de acceso de todos los empleados y/o contratistas a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	implementado	Permite garantizar la integridad y confidencialidad de la Información.
OBJETO		A.9.3	Responsabilidad de los usuarios		**Objetivo:** Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
CONTROL	A.9.3.1	Uso de la información de autenticación secreta	Se debe erigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseña.	Implementado	Permite disminuir el riesgo de suplantación de identidad por el mal uso de contraseñas.
OBJETO		A.9.4	Control de acceso a sistemas y aplicaciones		**Objetivo:** Evitar el acceso no autorizado a sistemas y aplicaciones.
CONTROL	A.9.4.1	Restricción de acceso a la información	Se debe restringir y controlar la asignación y el uso de privilegios de conformidad con la política de control de acceso.	Implementado	Permite llevar un control del personal al que se le brinda acceso v manipulación a la información.
CONTROL	A.9.4.2	Procedimiento de ingreso seguro	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de ingreso seguro.	Implementado	Garantiza que solo puedan acceder a la red y sus servicios aquellos usuarios debidamente autorizados por la entidad.
CONTROL	A.9.4.3	Sistemas de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Implementado	Se deben generar contraseñas seguras para reducir el riesgo de acceso no autorizado.

CONTROL	A.9.4.4	Uso de programas utilitarios privilegiados	Se deben restringir y controlar estrictamente el uso de programas utilitarios que pueden anular el sistema y los controles de las aplicaciones.	Implementado	Evitar que los programas utilitarios huecos de seguridad en la red y aplicaciones, los cuales pueden ser utilizados para realizar ataques.
CONTROL	A.9.4.5	Control de acceso a códigos fuente de programas	Es necesario que el acceso al código fuente de los programas sea restringido.	implementado	Para evitar alteraciones no permitidas y controladas a las aplicaciones que afecten el funcionamiento de estas.
DOMINIO		**A.10**	**Criptografía**		
OBJETO		A.10.1	Controles criptográficos	**Objetivo:** Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.	
CONTROL	A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar o implementar una política sobre el uso de controles criptográficos para la protección de la información.	No implementado	Garantiza la integridad de la información.
CONTROL	A.10.1.2	Gestión de llaves	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la entidad.	No implementado	Garantiza la confidencialidad e integridad de la información.
DOMINIO		**A.11**	**Seguridad Física y del entorno**		
OBJETO		A.11.1	Áreas seguras	**Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización	
CONTROL	A.11.1.1	Perímetro de seguridad Física	Se debe utilizar un sistema de seguridad (puertas de acceso controladas) para proteger las áreas que contienen información y servicios de procesamiento de información.	Implementado	Es necesario evitar el acceso no autorizado a la información y sabotaje a la misma.
CONTROL	A.11.1.2	Controles Fiscos de entrada	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso al personal autorizado.	Implementado	Es necesario evitar el acceso no autorizado a la información y sabotaje a la misma.
CONTROL	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Implementado	Las oficinas, cuartos e instalaciones se deben asegurar como prevención y contra medidas ante amenazas a los recursos e información confidencial.
CONTROL	A.11.1.4	Protección contra amenaza externas y ambientales	Se deben diseñar y aplicar protecciones fiscas contra daño por incendio, inundación, terremoto, explosión,	Implementado	Las instalaciones, oficinas y cuartos se deben asegurar como prevención y

			manifestaciones sociales y otras formas de desastre natural o artificial.		contramedidas ante amenazas a los recursos e ¡información confidencial.
CONTROL	A.11.1.5	Trabajo en área seguras.	Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	Implementado	El trabajo en áreas seguras se debe realizar por cumplimiento a la normatividad v salud ocupacional.
CONTROL	A11.1.6	Áreas de despacho y carga	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones, se deben controlar y si es posible, aislarse los servicios de procesamiento de información para evitar el acceso no autorizado.	Implementado	Permite evitar daños y destrucción de la información por acceso no autorizado a las áreas restringidas del manejo de la información.
OBJETO	A.11.2	Equipos		Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	
CONTROL	A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.	Implementado	Permite disminuir el riesgo de amenazas a equipos tecnológicos.
CONTROL	A.11.2.2	Servicios de Suministro	Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	Implementado	Permite garantizar la continuidad y la atención del servicio a los usuarios.
CONTROL	A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegidos contra interceptaciones o daños.	Implementado	Permite garantizar que las transferencias de información por las canales de comunicación se realicen de forma segura.
CONTROL	A.11.2.4	Mantenimiento de Equipos	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	Implementado	Para asegurar la continuidad e integridad de los equipos.
CONTROL	A.11.2.5	Retiro de activos	Ningún equipo, información ni software se deben retirar sin autorización previa por el área encargada dentro de la entidad.	Implementado	Para custodiar la información que se encuentre en los equipos y el buen funcionamiento de estos.
CONTROL	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la entidad.	No implementado	Permite garantizar la seguridad de los equipos fuera de la entidad.
CONTROL	A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para	implementado	Permite llevar un control en cuanto a licenciamientos.

			asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación o reutilización.		garantizando la confidencialidad e integridad de la información
CONTROL	A.11.2.8	Equipos de usuarios desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	implementado	Permite que los equipos estén debidamente custodiados.
CONTROL	A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	No implementado	Garantizar la confidencialidad de la información.
DOMINIO		**A.12**	**Seguridad de las Operaciones**		
OBJETO		A.12.1	Procedimientos operacionales y responsabilidades	**Objetivo:** Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	
CONTROL	A.12.1.1	Procedimientos de operaciones documentadas	Se debe documentar y estar disponibles a todos los usuarios que los necesite los procedimientos operación.	Por implementar	Es necesario tener documentados todos sus procesos y registros con su respectiva codificación; esto con la finalidad de mantener controles internos que van a permitir una mejor gestión y desempeño por parte del personal en cada área.
CONTROL	A.12.1.2	Gestión de cambios	Los cambios a las instalaciones para el procesamiento de la información y a los sistemas deben ser controlados.	implementado	Permite llevar un control sobre los cambios en instalaciones para el procesamiento y los sistemas de información.
CONTROL	A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos del sistema capacidad futura para asegurar el desempeño requeridos del sistema.	implementado	Es necesario tener una proyección del crecimiento de los diferentes recursos del sistema, para de esta forma poder gestionar y garantizar los recursos que se requerirán para el adecuado funcionamiento del sistema.
CONTROL	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Los ambientes de desarrollo, pruebas e instalaciones operacionales deben separarse para reducir el riesgo de acceso no autorizado o cambios al sistema operacional.	Por implementar	Se debe contar con ambientes de pruebas o desarrollo independientemente de los ambientes de producción, esto con el fin de reducir el riesgo de cambios o accesos no

					autorizado.
CONTROL		A.12.2	Protección contra códigos maliciosos		**Objetivo:** Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
CONTROL	A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, prevención y recuperación para la protección contra código malicioso y los procedimientos de sensibilización de los usuarios deben ser implementados.	implementado	Se busca reducir el riesgo de pérdida de información, alteración de la información y no disponibilidad de esta.
CONTROL		A.12.3	Copias de respaldo		**Objetivo:** Proteger contra la perdida de datos.
CONTROL	A.12.3.1	Respaldo de Información	Se deben hacer copias de seguridad de la información y del software, y poner a prueba con regularidad de acuerdo a la política de respaldo adoptada.	implementado	Permite que la entidad tenga un respaldo de seguridad de la información ante un evento de daño o sabotaje de la información.
CONTROL		A.12.4	Registro y Seguimiento		**Objetivo:** Registrar eventos y generar evidencia.
CONTROL	A.12.4.1	Registro de Eventos	Se debe hacer seguimiento y revisar regularmente los registros de las actividades, excepciones, falla§ y eventos de la seguridad de la información.	Por implementar	Garantiza que los eventos y debilidades en la seguridad asociados con los sistemas de información se identifiquen de modo que se puedan realizar acciones correctivas oportunas.
CONTROL	A.12.4.2	Protección de la información de registro	Los servicios y la información de la actividad de registro se deben proteger con el acceso no autorizado.	Por implementar	Se busca garantizar la integridad de la informaçión
CONTROL	A.12.4.3	Registro del administrador y del operador	Se debe registrar las actividades tanto del operador como del administrador del sistema, además proteger y revisar con regularidad.	Por implementar	Los registros de las actividades son valiosos para el control de la trazabilidad de la información.
CONTROL	A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la entidad o del dominio de seguridad deben estar sincronizados con una única fuente de tiempo acordada.	implementado	Todos los sistemas manejen el mismo horario para evitar inconsistencias en procesamientos de información y posibles reclamaciones por parte de los usuarios.
CONTROL		A.12.5	Control de Software		**Objetivo:** Asegurar la integridad de los sistemas operacionales.

CONTROL	A.12.5.1	Instalación de software en sistemas operativos	Deben existir procedimientos en funcionamiento para controlar la instalación de software en los sistemas operativos.	implementado	Para conocer el rendimiento y capacidad, y para efectos de licenciamiento del software operativo.
CONTROL		A.12.6	Gestión de vulnerabilidad técnica		**Objetivo:** Prevenir el aprovechamiento de las vulnerabilidades técnicas.
CONTROL	A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la entidad a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	Implementado	Se busca identificar las vulnerabilidades y estar preparados para cuando se presente alguna amenaza.
CONTROL	A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las normas para la instalación de software por parte de los usuarios.	Parcialmente implementado	Permite estandarizar el procedimiento para la instalación de software.
CONTROL		A.12.7	Consideraciones sobre auditorias de sistemas de información		**Objetivo:** Minimizar el impacto de las actividades de auditoria sobre los sistemas operacionales
CONTROL	A.12.7.1	información controles de auditoria de sistemas	Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos de la entidad	Por implementar	Permite minimizar el riesgo de interrupción de los procesos de la entidad garantizando su cumplimiento.
DOMINIO		**A.13**	**Seguridad de las comunicaciones**		
OBJETO		A.13.1	Gestión de la seguridad de las redes		**Objetivo:** Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
CONTROL	A.13.1.1	Controles de redes	Las redes se deben mantener y controlar adecuadamente para proteger las de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red.	Parcialmente implementado	Se busca reducir el riesgo de accesos no autorizados a la red y a la información, así como de posibles ataques a la red.
CONTROL	A.13.1.2	Seguridad de los servicios de red	Se debe identificar e incluir en los acuerdos de servicios de la red los mecanismos, los niveles y los requisitos de todos los servicios de la red, sin importar si los servicios se prestan en la entidad o se contratan.	implementar	Garantizar que los servicios de red funcionen correctamente y de forma segura.

CONTROL	A.13.1.3	Separación en las redes	En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	Por implementar	Permite llevar un control para tener una trazabilidad en las comunicaciones.
OBJETO		A.13.2	Transferencia de información		**Objetivo:** Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
CONTROL	A.13.2.1	Políticas y procedimientos de transferencia de información	Se deben establecer políticas, procedimientos y controles formales de transferencia de información para protegerla mediante el uso de todo tipo de servicios de comunicación.	Por implementar	Se busca garantizar la disponibilidad, integridad y confidencialidad mediante el establecimiento de MSPI.
CONTROL	A.13.2.2	Acuerdos sobre transferencia de información	Se deben establecer acuerdos para el intercambio de la información y del software entre la entidad y partes externas.	Por implementar	Garantizar la confidencialidad entre las partes a transferir información.
CONTROL	A.13.2.3	Mensajería electrónica	La información contenida en la mensajería electrónica debe tener la protección adecuada.	Parcialmente implementado	Se debe garantizar la integridad y confidencialidad de la información cuando es enviada por medios electrónicos.
CONTROL	A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se debe identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la entidad para la protección de la información.	Parcialmente implementado	Es necesario preservar la confidencialidad de la información se deben realizar acuerdos de confidencialidad, que ¡impliquen la no divulgación de la información.
DOMINIO		**A.14**	Adquisición, desarrollo y mantenimientos de sistemas		
OBJETO		A.14.1	Requisitos de seguridad de los sistemas de información		**Objetivo:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
CONTROL	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos de la entidad para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	Parcialmente implementado	Es necesario mantener los niveles de seguridad ante cualquier adquisición o mejoras realizadas a las aplicaciones.
CONTROL	A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas	implementado	Garantizar la seguridad de los datos personales y ofrece confianza al usuario al acceder a las aplicaciones de la

			contractuales y divulgación y modificación no autorizadas.		entidad.
CONTROL	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	implementado	Garantizar la seguridad de las transacciones en ofrecer confianza al usuario al acceder aplicaciones de la entidad.
OBJETO		A.14.2	Seguridad en los procesos de desarrollo y soporte	**Objetivo:** Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	
CONTROL	A.14.2.1	Política de desarrollo seguro	Se debe establecer y aplacar normas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la entidad.	Por implementar	Permite estandarizar los procesos para el desarrollo de software y de sistemas.
CONTROL	A.14.2.2	Procedimientos de control de cambios en sistemas	Se Debe controlar las implementaciones de cambios utilizando procedimientos formales de control de cambios.	Por implementar	Garantizar un control preciso de los cambios efectuados.
CONTROL	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	se cambian los sistemas operativos, las aplicaciones críticas para la entidad se deben revisar y someter aprueba para asegurar que no haya impacto adverso en las operaciones ni en la seguridad de la entidad.	implementado	Garantizar que no haya impacto adverso en las operaciones ni en la seguridad de la entidad, al efectuar cambios en los sistemas operativos.
CONTROL	A.14.2.4	Restricciones en los cambios a los paquetes de software	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	implementado	Permitir tener un control preciso en los cambios efectuados en los paquetes de software.
CONTROL	A.14.2.5	Principios de construcción de sistemas seguros	Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información	implementado	Es necesario elaborar el documento con los principios para la construcción de sistemas seguros
CONTROL	A.14.2.6	Ambiente de desarrollo seguro	La entidad debe identificar y proteger los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas	Por implementar	Permite proteger y asegurar los ambientes de desarrollo durante el ciclo de vida de desarrollo de sistemas.
CONTROL	A.14.2.7	Desarrollo contratado externamente	La entidad debe supervisar y monitorear el desarrollo de software contratado externamente.	implementado	Garantizar que el producto software a desarrollar cumpla con los requerimientos exigidos en seguridad y en funcionamiento.
CONTROL	A.14.2.8	Pruebas de seguridad de sistemas	Se deben llevar a cabo pruebas de funcionalidad de seguridad de la información.	Parcialmente implementado	Garantizar que la información sea protegida y controlada.

CONTROL	A.14.2.9	Prueba de aceptación de sistemas	Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación y puesta en producción.	Parcialmente implementado	Es necesario el protocolo para aceptación de nuevos sistemas, con esto se busca garantizar que los sistemas que se adquieran cumplan con el objetivo para el cual se adquirió.
OBJETIVO		A.14.3	Datos de prueba		**Objetivo:** Asegurar la protección de los datos usados para pruebas.
CONTROL	A.14.3.1	Protección de datos de prueba	Datos de ensayo deben ser seleccionados cuidadosamente, protegidos y controlados.	Parcialmente Implementado	Garantizar la calidad de la información ante posibles amenazas o vulnerabilidades del sistema.
DOMINO		**A.15**	**Relación con los proveedores**		
OBJETIVO		A.15.1	Seguridad de la información en las relaciones con los proveedores		**Objetivo:** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
CONTROL	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Se deben acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad.	Por implementar	Garantizar tener claro entre la entidad y los proveedores los requisitos de seguridad de la información y reducir los riesgos con el acceso de los activos de la entidad.
CONTROL	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	establecer y acordar con el proveedor que tenga acceso, procesar, almacenar, comunicar o suministrar componentes de la infraestructura TI, en cuanto a los requisitos de seguridad de la información.	Por implementar	Garantizar tener claro entre la entidad y los proveedores los requisitos de seguridad de la información y reducir los riesgos en el tratamiento de la información.
CONTROL	A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Se debe incluir en los acuerdos con los proveedores los requisitos de riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología y comunicación.	Parcialmente implementado	Garantizar tener claro entre la entidad y los proveedores los requisitos de seguridad de la información y reducir los riesgos asociados en la cadena de suministro de productos y servicios de tecnología y comunicación.
OBJETIVO		A.15.2	Gestión de la prestación de servicios con los proveedores	SI	**Objetivo:** Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
CONTROL	A.15.2.1	Seguimiento y revisión de los servicios	La entidad debe hacer seguimiento, revisar y auditar	Parcialmente implementado	Permite llevar un control y seguimiento

		de los proveedores	con regularidad la prestación de servicios de los proveedores.		del servicio prestado por proveedor.
CONTROL	A.15.2.2	Gestión de cambios en los servicios de proveedores	Los cambios en la prestación de los servicios' incluyendo mantenimiento y mejora de las políticas exigentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos de la entidad involucrados, así como la reevaluación de los riesgos.	Parcialmente implementado	Garantiza llevar la trazabilidad del MSPI.
DOMINIO		**A.16**	**Gestión de incidentes de seguridad de la información**		
OBJETIVO		A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		**Objetivo:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
CONTROL	A.16.1.1	Responsabilidad y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de la información.	Parcialmente implementado	Garantizar que se aplique un tratamiento adecuado para la gestión de los incidentes en la seguridad de información.
CONTROL	A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de los canales con la dirección tan pronto como sea posible.	Parcialmente implementado	Permite que los eventos y debilidades en la seguridad con los sistemas de información se comuniquen y puedan tomar acciones correctivas oportunas.
CONTROL	A.16.1.3	Reporte de debilidades de seguridad de la información	Todos los funcionarios y contratistas que utilicen los sistemas de información y servicios, se les debe requerir identificar y reportar cualquier debilidad observada o sospechosa.	implementado	Permite identificar las debilidades en cuanto a seguridad de la información.
CONTROL	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información deben ser evaluados y reportados a través de los canales mediante el reporte de incidentes de seguridad.	Parcialmente implementado	Garantizar que los eventos sean evaluados de manera oportuna y se tomen acciones.
CONTROL	A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Parcialmente implementado	Se lleva control y seguimiento a los incidentes o eventos de seguridad de la información
CONTROL	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la Información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	Parcialmente implementado	Garantizar que no se tomen correcciones y medidas para que no se repitan los incidentes de seguridad de la información.

CONTROL	A.16.1.7	Recolección de evidencia	La entidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Parcialmente implementado	Conocer las causas del incidente de seguridad de la información, para poder ejecutar acciones correctivas, preventiva, además presentar pruebas ante las autoridades competentes
DOMINO		**A.17**	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**		
OBJETIVO		A.17.1	Continuidad de seguridad de la información		**Objetivo:** La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
CONTROL	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La entidad debe determinar los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la conformación en situaciones adversas.	Por implementar	Permitir hacer control y seguimiento MSPI dentro de la entidad.
CONTROL	A.17.1.2	Implementación de la continuidad de la seguridad de la información	La entidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Por implementar	Garantizar la implementación, control, seguimiento al MSPI dentro de la entidad.
CONTROL	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	Por implementar	Permite llevar el control y seguimiento del servicio prestado por terceras partes.
CONTROL					
CONTROL	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Por implementar	Garantiza unas instalaciones que cumplan con los requisitos establecidos por la norma.
DOMINIO		**A.18**	**Cumplimiento**		
OBJETIVO		A.18.1	Cumplimiento de requisitos legales y contractuales		**Objetivo:** Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información. y de cualquier requisito de seguridad.
CONTROL	A.18.1.1	identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios reglamentarios, contractuales pertinentes y el enfoque de la entidad,	Por implementar	Garantizar el cumplimiento a ley y normatividad vigente que rige la

			para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información.		seguridad de la información.
CONTROL	A.18.1.2	Derechos de propiedad intelectual	asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	Por implementar	Garantizar el cumplimiento de la legislación, regulaciones y requisitos contractuales para el uso de material con posibles derechos de propiedad intelectual asociados y para el uso de productos software propietario.
CONTROL	A.18.1.3	Protección de registros	Los registros importantes se deben proteger contra destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales para las entidades públicas.	Por implementar	Garantizar la integridad y confidencialidad de los registros de la entidad.
CONTROL	A.18.1.4	Privacidad y protección de datos personales	Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales. cómo se exige en la legislación y la reglamentación pertinentes.	Por implementar	Garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes.
CONTROL	A.18.1.5	Reglamentación de controles criptográficos	Se deben implementar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	Por implementar	Garantizar el cumplimiento de las leyes y reglamentos pertinentes en cuanto a controles criptográficos.
OBJETIVO		A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
CONTROL	A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la entidad la gestión de la seguridad de la información y su implementación (los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Por implementar	Garantizar la implementación, control y seguimiento al MSPI dentro de la entidad.
CONTROL	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	seguridad dentro de sus áreas de responsabilidad se llevan acaso correctamente para lograr el cumplimiento con las políticas y los lineamientos de seguridad.	Por implementar	La administración de la entidad deben tener un compromiso con la continuidad de la política de seguridad porque son los representantes de alto nivel de la entidad.
CONTROL	A.18.2.3	Revisión del cumplimento técnica	Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con los lineamientos de implementación de la seguridad.	Por implementar	Garantizar el cumplimiento de MSPI.

RECOMENDACIÓN

se recomienda después haber realizado el análisis e identificación de los controles de seguridad y privacidad de la información establecer acciones de mejoras, mediante el seguimiento y evaluación de planes de acción, con el fin de dar continuidad y trazabilidad al proceso de Modelo de seguridad y Privacidad de la información (MSPI), además ofrece a la entidad, empleados y contratistas confidencialidad, integridad y disponibilidad de la seguridad de la información ante posibles eventos o incidentes que puedan afectarlos activos de la información.

ELABORÓ	REVISÓ	APROBÓ
Firmado en Original	Firmado en Original	Firmado en Original
PROFESIONAL UNIVERSITARIO REQ.TECNOLOGICOS	**PROFESIONAL UNIVERSITARIO PLANEACION**	**GERENTE**

CONTROL DE CAMBIOS			
FECHA	DESCRIPCION DEL CAMBIO	VERSION	MODIFICADO POR
17 de Enero de 2019	Aprobado por Comité Institucional de Gestión y Desempeño. Acta 01/2019	V1	Profesional Universitario de Requerimientos Tecnológicos.
15 de Marzo de 2021	Aprobado por Comité Institucional de Gestión y Desempeño.	V2	Profesional Universitario de Requerimientos Tecnológicos
22 de Febrero de 2022	Aprobado por Comité Institucional de Gestión y Desempeño.	V3	Profesional Universitario de Requerimientos Tecnológicos
30 de Enero de 2023	Aprobado por Comité Institucional de Gestión y Desempeño.	V4	Profesional Universitario de Requerimientos Tecnológicos