



REPUBLICA DE COLOMBIA
DEPARTAMENTO DE CUNDINAMARCA
ALCALDÍA DE FACATATIVA

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

ALCALDÍA DE FACATATIVA

LUIS CARLOS CASAS ALVARADO
ALCALDE MUNICIPAL

ENERO 2024

Cra. 3 N° 5-68 / PBX: (57+) 843 9101
www.facatativa-cundinamarca.gov.co
Código Postal: 253051



CODIGO:	CIYS-PL-01
VERSIÓN:	1
FECHA:	



CONTENIDO

1.	INTRODUCCION	3
2.	OBJETIVOS	4
2.1.	Objetivo general	4
2.2.	Objetivos específicos	4
3.	ALCANCE	4
4.	MARCO REFERENCIAL	4
4.1.	Políticas de Gestión de Incidentes de Seguridad	4
5.	IDENTIFICACION DE ACTIVOS	5
5.1.	Tipos de activos	5
5.2.	Determinación de controles y gestión de riesgos	6
5.3.	Riesgo neto encontrado en la Alcaldía de Facatativá	7
5.4.	Evaluación del sistema de control interno de la Alcaldía de Facatativá	9
5.5.	Tratamiento de los riesgos	28
5.6.	Resultados	31
6.	CRONOGRAMA	32



1. INTRODUCCION

En la actualidad, la información es el activo más valioso de las organizaciones, pero esto también lo saben los delincuentes informáticos, y por ello las amenazas y riesgos que la información enfrenta son cada día mayores, por lo tanto, las entidades de carácter público y privado deben emplear un marco de trabajo que les permita implementar de una manera sistemática y efectiva un mayor control sobre la seguridad de la información y los activos informáticos, de tal manera que involucre a todo el personal de la empresa. Este marco es conocido como un Sistema de Gestión de la Seguridad de la Información y está basado en estándares, modelos y normas internacionales que a través de una serie de mejores prácticas aseguran una adecuada gestión de la seguridad de la información.

Por tal motivo se ve necesario desarrollar un plan de tratamientos de riesgos de seguridad y privacidad de la información aplicado a la Alcaldía Municipal de Facatativá, utilizando la norma ISO/IEC 27002, y la metodología MAGERIT, lineamientos que son establecidos por MINTIC y que se utilizarán como base para la elaboración del presente documento, con el fin de identificar la situación actual de la entidad, la identificación de riesgos existentes y el plan de tratamiento de riesgos de la seguridad de la información.



2. OBJETIVOS

2.1. Objetivo general:

Proporcionar a la Alcaldía de Facatativá un documento que facilite las pautas necesarias para realizar el adecuado tratamiento de los riesgos a los que se ven expuestos los activos de información de la entidad, el cual permitirá una adecuada toma de decisiones para reducir o evitar las probabilidades de que se presenten amenazas y vulnerabilidades en la entidad.

2.2. Objetivos específicos:

- Establecer una metodología de análisis y gestión del riesgo de los activos de información en la Alcaldía de Facatativá.
- Realizar un cronograma el cual permita establecer las actividades a desarrollar durante el año con el fin de mantener actualizado el plan de tratamiento de riesgos y cumplir con los requerimientos establecidos en el presente documento.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

3. ALCANCE

La gestión y el plan de tratamiento de riesgos de seguridad de la información, podrá ser aplicada sobre cualquier activo de la información de la Alcaldía de Facatativá, con el fin de administrar, reducir y mitigar los riesgos y vulnerabilidades que se presenten en la seguridad de la información, establecer un plan de continuidad y establecer pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

4. MARCO REFERENCIAL

4.1. Políticas de Gestión de Incidentes de Seguridad

La Alcaldía de Facatativá debe asegurarse que todos los colaboradores conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información, para lo cual se establecen las siguientes directrices:

- Se debe establecer los mecanismos para registrar los incidentes con sus pruebas y



evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

- Todos los servidores públicos y contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información.
- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.
- La Alcaldía de Facatativá establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.
- La Alcaldía de Facatativá debe establecer y poner a disposición de los colaboradores el formato o mecanismos de reporte de eventos e incidentes de seguridad y privacidad de la información.
- La Alcaldía de Facatativá debe contar con una bitácora de los incidentes de seguridad de la información reportados y atendidos y el establecimiento de indicadores relacionados a la gestión de los incidentes de seguridad y privacidad de la información

5. IDENTIFICACIÓN DE ACTIVOS

La identificación de Activos debe realizarse teniendo en cuenta las recomendaciones establecidas por MAGERIT.

MAGERIT: “Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno” (Portal administración Electrónica). Está compuesta por tres libros, el libro I, describe el método a seguir para la ejecución del análisis de riesgos. El libro II; catálogo de elementos discriminados en: activos, amenazas, vulnerabilidades, impacto, riesgo y salvaguardas. Y el libro III, es la guía de técnicas para realizar el análisis final y gestión de riesgos, se puede aplicar técnicas cualitativas o cuantitativas.

Los activos son identificados y clasificados tomando como base el libro II de la metodología MAGERIT versión 3.

5.1. Tipos de activos

La tipificación de los activos es tanto una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo. Un activo puede ser simultáneamente de varios tipos. Aunque no son los únicos tipos, mencionaremos los que se identificaron para este caso en particular.

- Activos esenciales - [essential] Activos esenciales



En un sistema de información hay 2 cosas esenciales: la información que se maneja y los servicios que prestan.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si es de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos.

- [S] Servicios

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

- [SW] Software - Aplicaciones informáticas

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

- [HW] Equipamiento informático (hardware)

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesamiento o la transmisión de datos.

- [AUX] Equipamiento auxiliar

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

- [L] Instalaciones

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

5.2. Determinación de controles y gestión de riesgos.



Hallazgos encontrados en la organización.

En la tabla 1 se detalla de acuerdo con la matriz de riesgos, los tipos de activos encontrados, el activo identificado, la amenaza de seguridad de acuerdo con la metodología MAGERIT y las vulnerabilidades asociadas a la Alcaldía de Facatativá. Para luego analizar los riesgos a los que están expuestos los activos y los controles que están implementados con el fin de gestionar los riesgos de la manera óptima posible.

Tabla 1. Hallazgos encontrados en la Alcaldía de Facatativá.

Activos de Información	Nombre del activo de información	Amenazas Metodología MAGERIT	Vulnerabilidades
[HW] EQUIPAMENTO INFORMÁTICO	[FW_UTM] Firewall	[N1] Fuego	Ausencia de dispositivos detectores de humo
[HW] EQUIPAMENTO INFORMÁTICO	[PC] Equipos de cómputo.	[E25] Pérdida de equipos	Los equipos no tienen una medida de seguridad física (guaya, cadena o acceso no restringido a salas).
[S] SERVICIOS	[WWW] Servidor de Sitio Web.	[E24] Caída del sistema por agotamiento de recursos	Poco espacio en disco
[S] SERVICIOS	[INTERNET_EMP] Internet a Empleados.	[A5] Suplantación de la identidad del usuario	Phishing
[AUX] EQUIPAMENTO AUXILIAR	[UPS] Sistema de Alimentación Ininterrumpida.	[I5] Avería de origen físico o lógico	Fallos de circuitos eléctricos internos
[D] DATOS	[D_CONF] datos de configuración	[E18] Destrucción de información	Pérdida de información

5.3. Riesgo neto encontrado en la Alcaldía de Facatativá.

En la tabla 2, Se sigue con el proceso de analizar la matriz de análisis de riesgos con el fin de identificar el riesgo neto que presentan los activos y así decidir de mejor manera cuáles riesgos se van a gestionar (aceptar, evitar, mitigar o transferir). Para ello se toma la valoración del riesgo de los activos y se multiplica por la probabilidad de vulneración, con el fin de



obtener el riesgo neto. Este riesgo neto será usado como criterio para gestionar los riesgos e implementar o mejorar controles de seguridad.

Tabla 2. Obtención del riesgo neto de los activos de la Alcaldía de Facatativá.

Activos de Información	Nombre del activo de Información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología MAGERIT	Vulnerabilidades	Probabilidad de vulneración (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 prácticamente seguro)	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)
[HW] EQUIPAMENTO INFORMÁTICO	[FW_UTM] Firewall	9	[N1] Fuego	Ausencia de dispositivos detectores de humo	3	27
[HW] EQUIPAMENTO INFORMÁTICO	[PC] Equipos de cómputo.	20	[E25] Pérdida de equipos	Los equipos no tienen una medida de seguridad física (guaya, cadena o acceso no restringido a salas).	3	60
[HW] EQUIPAMENTO INFORMÁTICO	[SW_A] Switch Administrable	15	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Equipo Obsoleto	3	45
[S] SERVICIOS	[WWW] Servidor de Sitio Web.	18	[E24] Caída del sistema por agotamiento de	Poco espacio en disco	5	90



Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología MAGERIT	Vulnerabilidades	Probabilidad de vulneración (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 prácticamente seguro)	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)
[S] SERVICIOS	[INTERNET_EMP] Internet a Empleados.	20	[A5] Suplantación de la identidad del usuario	Phishing	2	40
[AUX] EQUIPAMIENTO AUXILIAR	[UPS] Sistema de Alimentación Ininterrumpida.	19	[I5] Avería de origen físico o lógico	Fallos de circuitos eléctricos internos	2	38
[D] DATOS	[D_CONF] datos de configuración	19	[E18] Destrucción de información	Pérdida de información	3	57

5.4. Evaluación del sistema de control interno de la Alcaldía de Facatativá.

Para la evaluación del sistema de control interno la Alcaldía de Facatativá, se calificarán los controles de acuerdo con los criterios expuestos en la tabla 3.

Tabla 3. Criterios de cumplimiento de los controles de seguridad.

Estado	Significado
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. Cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió, pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

Después de establecer el criterio de evaluación de los controles ISO/IEC 27002:2013 se procede con la evaluación de cada control que aplica la Alcaldía de Facatativá, ésta puede ser observada en la tabla 4.



Tabla 4. Evaluación del sistema de control interno.

CONTROLES ISO/IEC 27002:2013			
A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION		ESTADO
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Cumple satisfactoriamente
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	Cumple satisfactoriamente
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION		
A6.1	Organización interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple satisfactoriamente
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Cumple parcialmente
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple satisfactoriamente



A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Cumple parcialmente
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Cumple parcialmente
A6.2	Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Cumple satisfactoriamente
A6.2.2	Teletrabajo	Control: Se deben 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 el trabajo en casa.	Cumple satisfactoriamente
A7	SEGURIDAD DE LOS RECURSOS HUMANOS		
A7.1	Antes de asumir el empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			



A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben 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.	Cumple satisfactoriamente
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Cumple satisfactoriamente
A7.2	Durante la ejecución del empleo		
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Cumple satisfactoriamente
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Cumple satisfactoriamente
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Cumple satisfactoriamente
A7.3	Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			



A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Cumple satisfactoriamente
--------	---	---	---------------------------

A8	GESTION DE ACTIVOS		
A8.1	Responsabilidad por los activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.			
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Cumple parcialmente
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	Cumple satisfactoriamente
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Cumple satisfactoriamente
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple satisfactoriamente
A8.2	Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Cumple satisfactoriamente



A8.2.2	Etiquetado de la información	Control: Se debe 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.	Cumple satisfactoriamente
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Cumple satisfactoriamente
A8.3	Manejo de medios		

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Cumple satisfactoriamente
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Cumple satisfactoriamente
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Cumple satisfactoriamente
A9	CONTROL DE ACCESO		
A9.1	Requisitos del negocio para el control de acceso		
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Cumple satisfactoriamente
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple satisfactoriamente
A9.2	Gestión de acceso de usuarios		



Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Cumple satisfactoriamente
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Cumple satisfactoriamente
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Cumple satisfactoriamente
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Cumple satisfactoriamente
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cumple satisfactoriamente
A9.2.6	Retiro o ajuste de los derechos de acceso	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 deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Cumple satisfactoriamente
A9.3	Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Cumple satisfactoriamente
A9.4	Control de acceso a sistemas y aplicaciones		



Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Cumple parcialmente
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Cumple satisfactoriamente
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Cumple satisfactoriamente
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Cumple satisfactoriamente
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	Cumple satisfactoriamente
A10	CRIPTOGRAFIA		
A10.1	Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información			
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Cumple satisfactoriamente
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Cumple satisfactoriamente
A11	SEGURIDAD FISICA Y DEL ENTORNO		



A11.1	Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Cumple parcialmente
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Cumple parcialmente
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Cumple parcialmente
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Cumple parcialmente
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Cumple satisfactoriamente
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Cumple satisfactoriamente
A11.2	Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Cumple satisfactoriamente



A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Cumple parcialmente
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Cumple parcialmente
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple satisfactoriamente
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Cumple satisfactoriamente
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben 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.	Cumple satisfactoriamente
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	Cumple satisfactoriamente
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Cumple satisfactoriamente
A11.2.9	Política de escritorio y pantalla limpios	Control: Se debe 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.	Cumple satisfactoriamente
A12	SEGURIDAD DE LAS OPERACIONES		
A12.1	Procedimientos operacionales y responsabilidades		





Objetivo: Registrar eventos y generar evidencia			
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Cumple satisfactoriamente
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Cumple satisfactoriamente
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Cumple satisfactoriamente
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Cumple satisfactoriamente
A12.5	Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales			
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Cumple satisfactoriamente
A12.6	Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			

A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe 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.	Cumple satisfactoriamente
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Cumple satisfactoriamente



A12.7	Consideraciones sobre auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos			
A12.7.1	Controles de auditorías de sistemas de de los planificar y acordar interrupciones en	Control: Los requisitos y actividades de auditoría que involucran la verificación sistemas operativos se deben información cuidadosamente para minimizar las los procesos del negocio.	Cumple satisfactoriamente
A13	SEGURIDAD DE LAS COMUNICACIONES		
A13.1	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.			
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Cumple satisfactoriamente
A13.1.2	Seguridad de los servicios de red	Control: Se deben 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 servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Cumple satisfactoriamente
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Cumple satisfactoriamente
A13.2	Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	



A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Cumple satisfactoriamente
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Cumple satisfactoriamente
A13.2.4	Acuerdos de confidencialidad o de no divulgación.	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las de la organización para la protección de la información.	Cumple satisfactoriamente
A14	Adquisición, desarrollo y mantenimiento de sistemas		
A14.1	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 sobre redes.			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Cumple parcialmente
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Cumple satisfactoriamente
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben 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.	Cumple satisfactoriamente
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		



Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Cumple satisfactoriamente
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Cumple satisfactoriamente
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Cumple satisfactoriamente
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Cumple satisfactoriamente
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Cumple satisfactoriamente
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Cumple satisfactoriamente
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Cumple satisfactoriamente
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Cumple satisfactoriamente



A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	
A14.3	Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para pruebas.			
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Cumple satisfactoriamente
A15	RELACIONES CON LOS PROVEEDORES		
A15.1	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.			
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	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 deben acordar con estos y se deben documentar.	Cumple parcialmente
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben 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.	Cumple satisfactoriamente
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben 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 y comunicación.	Cumple satisfactoriamente
A15.2	Gestión de la prestación de servicios de proveedores		



Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Cumple satisfactoriamente
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	
A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		
A16.1	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.			
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Cumple satisfactoriamente
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Cumple satisfactoriamente



A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Cumple satisfactoriamente
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Cumple satisfactoriamente.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Cumple satisfactoriamente
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Cumple satisfactoriamente
A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO		
A17.1	Continuidad de Seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			



A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe 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.	Cumple parcialmente
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización 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.	Cumple parcialmente
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe 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.	Cumple parcialmente
A17.2	Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Cumple satisfactoriamente

A18	CUMPLIMIENTO		
A18.1	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.			
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Cumple satisfactoriamente



A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben 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.	Cumple satisfactoriamente
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Cumple satisfactoriamente
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	Cumple satisfactoriamente
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Cumple satisfactoriamente
A18.2	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.			
A18.2.1	Revisión independiente de la seguridad de la información	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 deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Cumple parcialmente
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben 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, y cualquier otro requisito de seguridad.	Cumple satisfactoriamente



A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Cumple satisfactoriamente
----------------	-----------------------------------	---	---------------------------

5.5. Tratamiento de los riesgos.

Para realizar el tratamiento de los riesgos se usará la matriz de riesgos donde, se identificaron los controles existentes para los activos de acuerdo con las vulnerabilidades y amenazas presentadas y en la que también se identificó un nivel de aceptación del riesgo, lo cual se puede apreciar en la tabla 5. Los riesgos se pueden tratar de 4 maneras posibles, evitándolos, aceptándolos, mitigándolos o transfiriéndolos. Para hallar los resultados, los riesgos cuyo nivel sea aceptable, se van a aceptar, los riesgos cuyo nivel sea moderado e inaceptable se van a gestionar teniendo en cuenta que no tengan un control efectivo y documentado.

Tabla 5. Calificación de gestión, controles aplicados y aceptación del riesgo.

Activos de Información	Nombre del activo de información	Amenazas Metodología MAGERIT	Vulnerabilidades	Calculo del riesgo neto Valoración del riesgo * probabilidad de vulneración	Calificación de Gestión control no existe, 2 existe, pero no efectivo, 3 efectivo, pero no documentado, 4 efectivo y documentado	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Niveles de aceptación del riesgo a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I)
[S] SERVICIOS	[WWW] Servidor de Sitio Web.	[E24] Caída del sistema por agotamiento de recursos	Poco espacio en disco	90	2	Proyecto de reposición de equipos.	I
[S] SERVICIOS	[INTERNET_EMP] Internet a Empleados.	[A5] Suplantación de la identidad del usuario	Phishing	80	1		I
[HW] EQUIPAMIENTO INFORMÁTICO	[PC] Equipos de cómputo.	[E25] Pérdida de equipos	Los equipos no tienen una medida de seguridad física (guaya, cadena o acceso no restringido a salas).	60	1		I



[D] DATOS	[D_CONF] datos de configuración	[E18] Destrucción de información	Perdida de información	57	4	Se restablece la información por medio de la NAS, si el usuario ha guardado la información en la carpeta de documentos importantes que esta sincronizada con la Unidad NAS.	A
[AUX] EQUIPAMENTO AUXILIAR	[UPS] Sistema de Alimentación Ininterrumpida.	[I5] Avería de origen físico o lógico	Fallos de circuitos eléctricos internos	38	3	Se procede a solucionar el incidente reparando o cambiando los circuitos	M
[HW] EQUIPAMENTO INFORMÁTICO	[FW_UTM] Firewall	[N1] Fuego	Ausencia de dispositivos detectores de humo	9	1		M
[S] SERVICIOS	[WWW] Servidor de Sitio Web.	[E24] Caída del sistema por agotamiento de recursos	Poco espacio en disco	90	2	Proyecto de reposición de equipos.	I
[S] SERVICIOS	[INTERNET_EMP] Internet a Empleados.	[A5] Suplantación de la identidad del usuario	Phishing	80	1	Se procede a informar al operador o encargado de solucionar este tipo de incidentes.	I

Se procede entonces con el plan de tratamiento de los riesgos teniendo en cuenta los controles ISO/IEC 27002:2013.

Tabla 6. Plan de tratamiento de los riesgos.



Nombre del activo de información	Amenazas Metodología MAGERIT	Vulnerabilidades	Control aplicado actualmente	Riesgo residual riesgo neto dividido entre la calificación de gestión)	Niveles de aceptación del riesgo a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I)	Plan de Tratamiento			
						Transferir	Aceptar	Mitigar	Control a aplicar a partir de la norma ISO 27001 si el plan es mitigar
[WWW] Servidor de Sitio Web.	[E24] Caída del sistema por agotamiento de recursos	Poco espacio en disco	Proyecto de reposición de equipos.	45	I			X	A11.2.4 Se debe realizar un cambio de equipos para asegurar la confidencialidad, integridad y disponibilidad de la información en todo momento.
[INTERNET_EMP] Internet a Empleados.	[A5] Suplantación de la identidad del usuario	Phishing		80	I			X	A13.1.1 Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

[PC] Equipos de cómputo.	[E25] Pérdida de equipos	Los equipos no tienen una medida de seguridad física (guaya, cadena o acceso no restringido a salas).		60	I			X	A11.1.1 Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
[D_CONF] datos de configuración	[E18] Destrucción de información	Pérdida de información		57	A			X	A12.3.1 Se deben realizar capacitaciones a los usuarios para que manejen la información de una forma correcta y así en caso de pérdida se pueda realizar un backup por medio de la Unidad NAS.



[UPS] Sistema de Alimentación Ininterrumpida.	[I5] Avería de origen físico o lógico	Fallos de circuitos eléctricos internos		38	M				X	A17.1.3	La organización debe 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.
[FW_UTM] Firewall	[N1] Fuego	Ausencia de dispositivos detectores de humo		9	M	X				A15.1.2	Se contratará un seguro que proteja las instalaciones.

5.6. Resultados

- Se debe realizar un cambio de equipos para asegurar la confidencialidad, integridad y disponibilidad de la información en todo momento.
- Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
- Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
- Se deben realizar capacitaciones a los usuarios para que manejen la información de una forma correcta y así en caso de pérdida se pueda realizar un backup por medio de la Unidad NAS.
- La organización debe 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.
- Se debe contratar un seguro que proteja las instalaciones.

6. CRONOGRAMA

Tabla 7. Cronograma año 2021

METODOLOGIA PLAN DE TRATAMIENTO DE RIESGOS	AÑO 2024
	MES



REPUBLICA DE COLOMBIA
DEPARTAMENTO DE CUNDINAMARCA
ALCALDÍA DE FACATATIVA

GESTION	ACTIVIDAD	RESPONSABLE	01	02	03	04	05	06	07	08	09	10	11	12
Gestión de Riesgos	Revisar y/o actualizar el inventario de activos de información	Dirección de informática / Líder de gobierno digital		X	X	X	X							
	Revisar y/o actualizar la identificación de riesgos	Dirección de informática / Líder de gobierno digital			X	X	X	X						
	Revisar y/o actualizar metodología de gestión de riesgos de seguridad de la información	Dirección de informática / Líder de gobierno digital				X	X	X	X					
	Desarrollo y ejecución de Actividades definidas en el plan de tratamiento de riesgos	Dirección de informática / Líder de gobierno digital		X	X	X	X	X	X	X	X	X	X	X
	Valoración y mejoramiento del riesgo residual	Dirección de informática / Líder de gobierno digital										X	X	X
	Informe de riesgos y plan de continuidad	Dirección de informática / Líder de gobierno digital											X	X

CARLOS MAURICIO PINTO MARTÍNEZ
Director Técnico de Informática

Elaboro y proyectó: Cesar Granados – Profesional Universitario
Reviso: Carlos Mauricio Pinto Martínez

