PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL VIGENCIA 2020

PROYECTÓ	FECHA	REVISÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
	05 05 2020		05 05 2020		05 05 2020		05 05 2020
NOMBRE **Ing. Daris Yaneth Padilla Díaz**		**NOMBRE** **Ing. Yuri Daianny Ruiz Franco**		**NOMBRE** **Ing. César Adolfo González Peña**		**NOMBRE** **Cr. (RA) Sonia Dolly Gutiérrez Carrillo**	
CARGO **Profesional Oficina TICs**		**CARGO** **Coordinadora Grupo de Informática**		**CARGO** **Coordinador Grupo de Redes e Infraestructura Tecnológica**		**CARGO** **Jefe Oficina TICs**	
FIRMA Ing. Daris Yaneth Padilla Díaz Firmado digitalmente por Ing. Daris Yaneth Padilla Díaz Fecha: 2020.05.04 13:18:54 -05'00'		**FIRMA** Yuri Daianny Ruiz Franco Firmado digitalmente por Yuri Daianny Ruiz Franco Fecha: 2020.05.05 16:59:10 -05'00'		**FIRMA** César González Firmado digitalmente por César González Fecha: 2020.05.05 09:43:59 -05'00'		**FIRMA** CR (RA) Sonia Dolly Gutiérrez Carrillo Firmado digitalmente por CR (RA) Sonia Dolly Gutiérrez Carrillo Fecha: 2020.05.05 08:48:58 -05'00'	

TABLA DE CONTENIDO

INTRODUCCIÓN

Gobierno Digital es una de las líneas de MIPG, que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. Esta política es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas.

La información es el principal activo con que cuenta la Agencia Logística de las Fuerzas Militares (en adelante ALFM) para cumplir con sus objetivos misionales y estratégicos; así como establecer relación con los ciudadanos, sus clientes y sus proveedores. Es por ello que resguardar la información de cualquier posibilidad de vulnerabilidad, alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de la Entidad y para salvaguardar el buen nombre de la misma.

OBJETIVOS

El presente plan de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital establece las actividades que se ejecutaran en la vigencia 2020 para mitigar y hacer seguimiento a los riesgos de seguridad y privacidad de la información que se puedan presentar en la ALFM, con el fin de proteger y preservar la información, así como los elementos tecnológicos que la soportan. Este documento es el resultado de la identificación del riesgo y tratamiento, manejo y seguimiento a los controles establecidos en la ALFM para la protección de los activos informáticos.

1. ALCANCE

El Modelo de Seguridad y Privacidad de la Información (MSPI) establece los lineamientos, actividades y responsabilidades que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Agencia Logística de las Fuerzas Militares – ALFM, para el tratamiento, manejo y seguimiento a los riesgos de seguridad y privacidad de la información. En el análisis realizado se tuvieron en cuenta aspectos que involucraron a todos los procesos, y el tratamiento de los riesgos y aplicación de controles se hizo sobre aquellos riesgos que se encuentran en un nivel de criticidad medio y alto. Los riesgos de nivel bajo hacen parte del riesgo residual aceptado por la ALFM dentro de su política de seguridad informática y también hacen parte del tratamiento de riesgos presente en este plan.

Se definirán las actividades a cumplir durante la presente vigencia (2020) para avanzar en la implementación del MSPI aplicando el tratamiento manejo y seguimiento a los riesgos identificados y de acuerdo a los controles establecidos. Para esta labor se involucrarán todos los procesos de la ALFM, los cuales deberán entregar la información que se requiera al grupo encargado de adelantar la gestión de los riesgos identificados.

2. REFERENCIA NORMATIVA

- Ley 1712 de 2014. Congreso de la Republica. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1581 de 2012. Disposiciones Generales para tratamiento de datos personales.
- Ley 1273 de 2009. Congreso de la Republica. Por medio del cual se modifica el código penal, se crea un nuevo bien jurídico tutelado-Denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- DECRETO 1499 DE 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Norma técnica colombiana NTC-ISO-IEC 27001.
- Directiva permanente Ministerio de Defensa No. 018 de 2014. Políticas de seguridad de la información para el Sector Defensa.
- Directiva permanente Ministerio de Defensa No. 03 de 2019. Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional.
- Documento CONPES 3854 de abril 11 de 2016, Política Nacional de Seguridad Digital.
- Directiva Permanente No.03 del 23 01 -2019 Lineamientos para la definición de la política de tratamiento de datos personales en el Ministerio de Defensa Nacional.
- Circular Externa Conjunta No 04 de 09-sep/2019 Tratamiento de datos personales en sistemas de información interoperables.

- Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional - Versión 3 - diciembre de 2019.

- Resolución 27 del 17 de marzo de 2020, por la cual se adoptan medidas preventivas sanitarias, por causa del coronavirus COVID-19 en la Agencia Logística de las Fuerzas Militares, y a través la cual establecen una serie de responsabilidades especial en el Artículo Cuarto Teletrabajo.

3. DEFINICIONES

Para los efectos del presente plan se tendrán en cuenta las siguientes definiciones:

- Activos tecnológicos: Se consideran activos tecnológicos todos los elementos de hardware, software, información y de comunicaciones entregados por la entidad al funcionario con el fin de facilitarle el desempeño de sus funciones. De esta manera, son activos tecnológicos, además de los programas (software aplicativo y de ofimática), los computadores o equipos de cómputo junto con sus periféricos (tarjeta de red, mouse, teclado, monitor, parlantes, unidades externas de almacenamiento, micrófono, entre otros), impresoras, escáneres, etc. También los equipos y elementos de comunicaciones (telefonía, switches, routers, cableado, etc) y la información almacenada en los diversos equipos y bases de datos.

- Análisis de riesgo**:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos. (ISO/IEC 27000).

- Backup (copia de respaldo): Una copia de seguridad o de respaldo es una copia de los datos originales que se realiza fuera de la infraestructura original con el fin de disponer de un medio de recuperación en caso de un desastre o pérdida.

- Base de Datos: Es un "almacén digital" que permite guardar grandes cantidades de información de forma organizada para luego poderla encontrar y utilizar fácilmente. Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada y estructurada. Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulan ese conjunto de datos. En el caso de la Agencia Logística, las bases de datos más utilizadas son Oracle y MySQL.

- Buzón de correo electrónico: Depósito en el que se almacenan los mensajes de correo que llegan a un destinatario determinado.

- Contraseña o password: Es una clave secreta de acceso a un computador, a una cuenta de correo electrónico, a una cuenta de conexión a Internet, a un sistema de información o a una base de datos, que, en aras de maximizar los niveles de seguridad, control y privacidad, sólo debe conocer el usuario. Si se introduce una contraseña incorrecta, no se permitirá la entrada al sistema.

- Correo electrónico o e-mail: Es un servicio mediante el cual un computador permite a los usuarios enviar y recibir mensajes e intercambiar información con otros usuarios (o grupos de usuarios), todo a través de la red.

- Correo electrónico institucional: Es el servicio de correo electrónico que provee y administra directamente la entidad a sus funcionarios como herramienta de apoyo a las funciones y responsabilidades de los mismos. En el caso de la Agencia este correo institucional corresponde al que se accede a través de Outlook o bien mediante el sitio: http://agencia.mail (internamente en la Agencia) o http://mail.agencialogistica.gov.co (equipos con Internet externos a la Agencia).

- Cortafuegos (firewall): Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

- Dirección de correo electrónico o e-mail address: Conjunto de caracteres utilizado para identificar a un usuario de correo electrónico y que permiten la recepción y envío de mensajes. Generalmente está compuesta por el nombre del usuario, el signo @ como divisor entre el usuario y el nombre del proveedor del servicio en el cual se aloja la cuenta de correo (el dominio).

- Equipo de cómputo: Es una máquina electrónica dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, que permiten resolver problemas aritméticos y lógicos, gracias a la utilización de programas instalados en ella. Para efectos de este manual se emplea el término como sinónimo de computador (PC-Computadores personales y portátiles).

- Equipo servidor: Es una máquina electrónica dotada de una alta configuración (velocidad de procesamiento, alta memoria, alta capacidad de almacenamiento. etc.), en donde están almacenados los programas de software aplicativo que operan en red y las bases de datos de la entidad.

- Gobierno Digital: es la política de MIPG que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. La política de Gobierno Digital contribuye a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso te de la tecnología (principalmente tecnologías emergentes y de la Cuarta Revolución Industrial), para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes (Manual Operativo MIPG V3).

- Hardware: Conjunto de componentes físicos (cables, placas, conexiones, partes) que constituyen un computador y sus equipos periféricos. Es la parte física de un computador, lo tangible.

- Ingeniería Social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

- Internet (International Net): Nombre de la mayor red informática del mundo. Red de telecomunicaciones nacida en 1969 en los Estados Unidos a la cual están conectadas centenares de millones de personas, organismos y empresas, en su mayoría ubicadas en los países más desarrollados, y cuyo rápido desarrollo está teniendo importantes efectos sociales, económicos y culturales, convirtiéndose de esta manera en uno de los medios más influyentes de la llamada Sociedad de la Información, siendo conocido en algunos ámbitos con el nombre de la autopista de la información.

- Intranet: Se llaman así a las redes tipo internet pero que son de uso interno o corporativo.

- Medio compartido de información (file share): Ubicación lógica en un servidor donde una dependencia o grupo de personas pueden colocar información (archivos y carpetas) para ser compartida y actualizada por el grupo. Solo las personas pertenecientes al grupo pueden ver y consultar la información.

- Mensaje de correo electrónico o e-mail message: Conjunto de elementos que componen un envío de correo electrónico. Además de los elementos visibles al usuario (campos de: Para: Asunto: CC: cuerpo del mensaje, firma, archivos anexos, etc.), un mensaje de correo electrónico contiene también elementos ocultos, que solo pueden ser "abiertos" por los destinatarios a los que se le remiten.

- Modelo Integrado de Planeación y Gestión (MIPG)**:** Es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio. Es en sí mismo un modelo de gestión de calidad ya que se fundamenta en generar resultados que satisfagan las necesidades y atiendan los problemas de los ciudadanos. Es en torno a estos resultados que deben girar todas sus actuaciones y decisiones (Manual Operativo MIPG V3).

- Modelo de Seguridad y Privacidad de la Información (MSPI): Es un conjunto de mejores prácticas que permiten a la ALFM mejorar sus estándares en seguridad de la información. Conducen a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

- Plan de Tratamiento de Riesgos (PTR): Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Red: Conjunto de computadores o de equipos informáticos conectados entre sí de tal manera que pueden intercambiar información.

- 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).

- 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).Spam: Mensajes que sin ser solicitados llegan al buzón de correo, provenientes de direcciones desconocidas en la mayoría de los casos, muy frecuentemente encaminados a ofrecer productos y servicios. También son conocidos como "correo basura" y algunos de ellos, por ser mensajes que se distribuyen masivamente, son utilizados para transmitir virus informáticos.

- Software: Es un conjunto de instrucciones detalladas que controlan la operación de un sistema computacional. En general, designa los diversos tipos de programas, instrucciones y reglas informáticas para ejecutar distintas tareas en un computador. Dentro de sus funciones están el

administrar los recursos de cómputo, proporcionar las herramientas para optimizar estos recursos y actuar como intermediario entre el usuario y la información almacenada.

- Software del sistema: Es un conjunto de programas que administran y controlan los recursos del computador, como son la unidad central de proceso, dispositivos de comunicaciones y los dispositivos periféricos. Es el denominado Sistema Operativo (Windows, Unix, Linux, Android, IOS entre otros).

- Software aplicativo: Programas que son escritos para realizar una tarea específica mediante el computador y está orientado a dar cubrimiento a un proceso específico. Son los denominados "software de aplicación específica". Este tipo de software está desarrollado sobre los denominados lenguajes de programación (C, Cobol, Developer, .Net, Java, PHP, entre otros), y los de mayor prestación y alto manejo de volúmenes de información están implementados sobre Bases de Datos (Oracle, MySQL, PosgreSql, etc.) en donde reside organizadamente la información que es manejada por intermedio del software aplicativo.

- Software de ofimática: Son programas existentes en el mercado y que basados en un computador, dan cubrimiento a necesidades específicas que se gestionan normalmente en una oficina: procesamiento de textos, hojas de cálculo, diseño de gráficos, resolución de problemas matemáticos, elaboración de presentaciones, entre otras. Tanto el software aplicativo como el de ofimática, deben estar sobre el software del sistema (sistema operativo) para poder operar.

- Software licenciado: Programas o aplicativos que han sido registrados y patentados, sobre los que existen derechos de autor y normas acerca de su uso, distribución, elaboración de copias, etc. Como consecuencia, para su utilización es necesario cumplir las restricciones establecidas por la ley.

- Software no licenciado: Es aquel que aún no ha sido patentado o registrado.

- Software libre: Es aquel que no tiene ningún tipo de restricciones de uso, distribución, modificación o elaboración de copias. Es de denominado software GPL-General Public License, el cual permite a cualquier entidad en el hacer uso de la herramienta, estudiarla, modificarla y re-distribuirla.

- Software pirata: Es una copia ilegal de un software (del sistema, aplicativo, o de ofimática), cuya utilización se está efectuando sin tener la licencia otorgada por el fabricante y proveedor del mismo.

- Tecnologías de la información y las comunicaciones (TIC): Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación,

procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

- Transacción: Es una interacción entre el usuario final del software y el sistema (software y bases de datos), la cual está compuesta por varios procesos internos que se han de aplicar uno después del otro.

- Unidad de almacenamiento fija: Dispositivo(s) no removible(s) por el usuario final que permite(n) registrar y guardar información en un equipo de cómputo. Generalmente conocida como disco duro, tiene una gran capacidad, lo que le permite almacenar una gran cantidad de información, programas y datos.

- Unidad de almacenamiento portátil (CD, DVD, memoria USB): Dispositivo(s) removible(s) por el usuario final, que permite(n) registrar y guardar información, programas y datos para ser utilizados en un computador. Entre los más usados y conocidos están el CD, el DVD y la memoria USB.

- Virus: Programa o rutina de software, cuyo objetivo generalmente es causar daños en un sistema informático. Con tal fin se oculta o se disfraza para no ser detectado. Estos programas son de diferentes tipos y pueden causar problemas de diversa gravedad en los sistemas a los que afectan, desde borrar un tipo de archivos, hasta borrar toda la información contenida en el disco duro. Hoy en día se propagan fundamentalmente mediante el uso del correo electrónico y de medios de almacenamiento de información portátiles infectados como CD, DVD y memorias USB. Se combaten con la instalación de un antivirus que debe ser actualizado periódicamente.

- Vulnerabilidad**:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- Teletrabajo: es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador en la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y puede realizarse a tiempo completo o parcial.

4. ACTIVIDADES A REALIZAR

	ACTIVIDAD	RESPONSABLE	TAREA	ENTREGABLES
1	Sensibilización a usuarios sobre seguridad de la información. Se hará un plan de capacitación y sensibilización a los usuarios sobre temas de seguridad de la información.	Profesional de seguridad de la información de la ALFM y Tec. Seguridad del Grupo de Infraestructura	Elaboración del plan.	**Primer semestre**: Documento con el plan de ca pacitación
			Ejecución del plan.	**Segundo semestre:** Listados de asistencia a las capacitaciones
3	Seguimiento a los reportes generados por WAF (web application firewall).		Realizar seguimiento a los eventos reportados por WAF de la actividad en la web y acciones tomadas.	Entrega **cuatrimestral** de documento con los reportes de seguimiento generados.
5	Seguimiento a la realización periódica de backups.	Grupo de Informática	Realización de Backup Centralizado	Reporte **cuatrimestral** de realización de Backup - reporte de la SAN-NAS
5	Seguimiento a los procesos de Mantenimientos preventivos y correctivos.	Grupo de Redes e Infraestructura Tecnológica	Elaboración de pliegos y contratación del proveedor.	**Primer cuatrimestre**: Contrato adjudicado y firmado.
			Ejecución del contrato por parte del proveedor.	**Segundo y Tercer cuatrimestre**: Informe de avance de acuerdo al cronograma.
			Finalización y cierre del contrato	**Tercer cuatrimestre:** Acta de entrega a satisfacción del objeto contractual

5. GESTION DE RIESGOS

1) Revisión de documentos ante el Comité de MIPG

PANIFICACIÓN		
Metas	**Resultado**	**Instrumento**
Identificación del contexto Interno y Externo	Contexto Interno y Externo	Anexo 4: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas-DAFP Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP
Alcance	Definición del alcance y límites de la Gestión de Riesgos.	
Revisión de la Directiva No. 11 Política de Tratamiento de Riesgos. Revisar roles y responsabilidades Establecer la alineación con el Plan de mitigación de riesgos que gestiona la Oficina Asesora de Planeación e Innovación Institucional	Directiva No.11, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad	

- ✓ **Responsable**: Profesional de seguridad de la información en coordinación con la Oficina Asesora de Planeación e Innovación Institucional

  Plazo: Primer semestre de 2020.
  Evidencia: Acta con las recomendaciones de la revisión de documentos, y adjuntar documentos revisados y ajustados.

2) Identificación de Riesgos

2.1. Valoración

VALORACIÓN		
Metas	**Resultado**	**Instrumento**
• **Identificación** • **Análisis** • **Evaluación**	Lista de todos los riesgos que podrían Crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Identificación de las causas y fuentes de riesgo, consecuencias y probabilidades de ocurrencia; descripción cualitativa y cuantitativa; impacto y aceptación. Identificar los controles existentes, eficacia y eficiencia. Comparación del nivel de riesgo, identificación de la necesidad de tratamiento de riesgos.	Guía No 7 - Gestión de Riesgos. Guía No 8 - Controles de Seguridad. Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP Anexo 4: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas-DAFP

- ✓ **Responsable**: Todos los procesos en coordinación con el Profesional de seguridad de la información de la ALFM

  Plazo: Segundo semestre de 2020.
  Evidencia: Documento de la identificación, análisis y evaluación de riesgos.

2.2. Tratamiento

TRATAMIENTO		
Metas	**Resultado**	**Instrumento**
Preparación e implementación de los Planes de Tratamiento de Riesgos	Razones para la selección de las opciones de tratamiento: Reducción, Retención, Evitar, Transferir; Riesgos residuales Responsables de aprobar e implementar el plan. Acciones propuestas. Cronograma.	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP. Anexo 4: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas- DAFP

- ✓ **Responsable**: Profesional de seguridad de la información en coordinación con la Oficina Asesora de Planeación e Innovación Institucional

  Plazo: Segundo semestre de 2020.
  Evidencia: Documento con el plan de tratamiento de riesgos.

3) Comunicación

Intercambiar y/o compartir información con los responsables para apoyar la gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente con el CSIRT y CCOC.

- ✓ **Responsable**: Oficina TIC.

  Plazo: 31 de diciembre de 2020
  Evidencia: Correos y comunicados.

4) Monitoreo y Revisión.

Con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana, y para mantener una visión general de la perspectiva completa del riesgo. (Valor de los activos, impactos, amenazas, vulnerabilidades, consecuencias, probabilidad de ocurrencia).

- ✓ **Responsable**: Oficina TIC

  Plazo: 31 de diciembre de 2020
  Evidencia: Modelo de Seguridad y Privacidad de la Información

6. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Documento inicial
01	Se actualiza el plan para el año 2020.
02	Actualización de actividades para la vigencia 2020
03	Actualización de actividades para la vigencia Mayo 2020