FECHA DE EMISIÓN DEL INFORME	**Día:**	30	**Mes:**	08	**Año:**	2020

Número de Informe	001
Nombre del Seguimiento	Proceso Reparación Integral
Objetivo del Seguimiento	Verificar los sistemas de control interno de los procesos se realice atendiendo las políticas aprobadas mediante la aplicación de técnicas de dirección y verificación, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos.
Alcance del Seguimiento	Inicia con la recolección y análisis de la información obtenida por Control Interno de las fuentes identificadas y concluye con el informe final.
Normatividad	el desarrollo de la verificación aplica la norma técnica ISO/IEC 27002 versión 2013, relacionada con la Tecnología de la Información, Técnicas de seguridad, código de practica para la gestión de la seguridad de la información.

A. ANÁLISIS Y OBSERVACIONES.

RESULTADOS OBSERVACIONES ESPECIFICAS EN RELACIÓN CON LA NTC-ISO 27002 2013

Control Interno durante la revisión a la Dirección de Gestión Interinstitucional consideró oportuno y una buena práctica guiarse por lo estipulado en la norma técnica colombiana NTC-ISO 27002 versión 2013, que tiene por objetivo:

"Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

"Los objetivos de control y controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos. Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las practicas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre organizaciones"

El modelo metodológico de la norma utilizada trae 14 dominios, a los cuales les corresponde 35 objetivos de control y 114 actividades de control. Para realizar esta

evaluación Control Interno elaboró un papel de trabajo que recoge cada uno de los dominios, objetivo y actividades así:

Dominios	Objetivo de control
1. Políticas Seguridad	1. Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones
2. Aspectos Organizativos SI	1. El objetivo es el de establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información en la organización.
	2. El objetivo es el de garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.
3. Seguridad Ligada a los recursos humanos	1. El objetivo es el de asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
	2. El objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.
	3. El objetivo es el de proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.
4. Gestión Activos	1. El objetivo es identificar los activos en la organización y definir las responsabilidades para una protección adecuada
	2. El objetivo es el de asegurar que se aplica un nivel de protección adecuado a la información
	3. El objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento
5. Control de Accesos	1. El objetivo es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.
	2. El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.
	3. El objetivo es hacer que los usuarios sean responsables de la protección de la información para su identificación
	4. El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.
6. Cifrado	1. El objetivo es garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
7. Seguridad física y Ambiental	1. El objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información
	2. El objetivo es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización
8. Seguridad en la Operativa	1. El objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.
	2. El objetivo es garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware
	3. El objetivo es alcanzar un grado de protección deseado contra la pérdida de datos.
	4. El objetivo es registrar los eventos relacionados con la seguridad de la información y generar evidencias.
	5. El objetivo es garantizar la integridad de los sistemas operacionales para la organización.
	6. El objetivo es evitar la explotación de vulnerabilidades técnicas
	7. El objetivo es minimizar el impacto de actividades de auditoría en los sistemas operacionales.
9. Seguridad en las Telecomunicaciones	1. El objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.
	2. El objetivo es mantener la seguridad de la información que transfiere un organización internamente o con entidades externas.
10. Aquisición, desarrollo y Mantenimiento de los sistemas de información	1. El objetivo es garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas.
	2. El objetivo es garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.
	3. El objetivo es garantizar la protección de los datos que se utilizan para procesos de pruebas.
11. Relaciones con Suministradores	1. El objetivo es garantizar la protección de los activos de la organización que son accesibles a proveedores.
	2. El objetivo es mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información.
12. Gestión de Incidentes	1. El objetivo es garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.
13. Aspectos de la SI en la Gestión de la Continuidad de Negocio	1. El objetivo es mantener la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la organización.
	2. El objetivo es garantizar la disponibilidad de las instalaciones de procesamiento de información.
14. Cumplimiento	1. El objetivo es evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.
	2. El objetivo es garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales

En el anexo a este informe se remite la matriz completa. Para la evaluación se tiene que por cada dominio se asigna un porcentaje de 100%, el cual se distribuye normalmente entre las actividades de control, así si se cumplen ellas se obtiene el ponderado establecido. Al final se suman los ponderados parciales y se establece el porcentaje definitivo.

La oficina de Control Interno hace relevante el hecho que no es indispensable que el área de Reparación Integral debe cumplir o debiera cumplir con todas las actividades de control y, por ende, el resultado no implica el nivel de gestión de la dependencia sino muestra la brecha que actualmente se tiene frente a una buena práctica, lo que posibilita acciones que corrijan y mejoren la actual situación.

Es en este escenario se dan los resultados de esta evaluación por cada uno de los dominios así:

POLÍTICAS DE SEGURIDAD

La política en un instrumento por medio del cual la entidad dispone de una serie de instrucciones para ser acogidas por los servidores, contratistas y grupos de interés. Su objetivo es dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones. Según lo reportado por el proceso, en la actualidad se conoce la política y la aplicabilidad de esta en el área lo cual se califica según la herramienta de medición del 100%.

ASPECTOS ORGANIZATIVOS DE SISTEMAS DE INFORMACIÓN

Los aspectos organizativos se relacionan con la definición de un ambiente de gestión que permita al menos la aprobación de las políticas de seguridad, la coordinación de su implementación al igual que la asignación de funciones y responsabilidades.

En la actualidad el proceso de Reparación integral cumple en un 100% las actividades de control propuestas en la buena práctica. Esta consecuencia tiene como base el conocimiento sobre las políticas de teletrabajo y uso de dispositivos de movilidad.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

La seguridad es ejecutada por acciones positivas de las personas que acceden o tienen posibilidad de acceder a la información. De lo anterior, todo el talento humano debe desde su vinculación conocer todas las medidas de seguridad y aspectos de confiabilidad. Lo anterior con el propósito de reducir los riesgos, el uso no autorizado de la información y cualquier manifestación de fraudes.

En relación con este dominio del proceso de Participación y Visibilización cumple los controles propuestos, en un 100% con el talento humano de su área. La dependencia considera que por parte del área de talento humano debe trabajar en la aplicación de acciones que permitan la difusión y uso de estos lineamientos.

GESTIÓN ACTIVOS

Considerando que desde ya hace tiempo se ha considerado que la información es el activo más importante que posee una entidad y con mayor razón las entidades públicas que gestionan información en aras de resolver las problemáticas sociales que funcionalmente deben afrontar. En este sentido, los activos de la información se deben clasificar de acuerdo con la sensibilidad y característica critica de la información, lo que determina que su propósito no es otro determinar el tratamiento y protección de la información.

Los objetivos de este dominio son: identificar los activos en la organización y definir las responsabilidades para una protección adecuada; asegurar que se aplica un nivel de protección adecuado a la información y evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento. La dirección tiene un rendimiento del 77.76% para este dominio donde su cumplimiento se afecta por el manejo de los controles de teletrabajo y la eliminación de soportes, ya que en el proceso de Reparación Integral no se tiene estipulado ningún direccionamiento general para el manejo de estos controles.

CONTROL DE ACCESOS

Este dominio tiene cuatro objetivos a saber: controlar los accesos a la información y las instalaciones; garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios; hacer que los usuarios sean responsables de la protección de la información para su identificación e impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

En relación con el rendimiento de la oficina sobre este ítem es de 100%, situación que se evidencia en la prueba de verificación por Control Interno. Por medio de este control se indica el conocimiento de los procedimientos que afectan la gestión de los usuarios, así como buzones de correos institucionales.

CIFRADO

Es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

Este dominio pose como único objetivo garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información. La dirección en este dominio genero una calificación del 100%, esto enfocado a que se conoce la política

SEGURIDAD FÍSICA Y AMBIENTAL

En este escenario lo que se busca es que la información este resguardada de agentes físicos y ambientales que pueda ponerla en peligro de deterioro e incluso perdida.

Los objetivos asociados a este dominio son dos: evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información y el segundo, evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

La dirección tiene un rendimiento del 100%, evidenciando un conocimiento y manejo en la mayoría de los aspectos, la opción a reforzar es establecida por la salida de activos fuera de las dependencias de la entidad.

SEGURIDAD OPERATIVA

Es controlar la existencia de los procedimientos de operaciones, el desarrollo y mantenimiento de documentación actualizada relacionada. Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas, equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes, administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Este dominio posee como una buena práctica siete objetivos así: evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información; garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware; alcanzar un grado de protección deseado contra la pérdida de datos; registrar los eventos relacionados con la seguridad de la información y generar evidencias; garantizar la integridad de los sistemas operacionales para la organización; evitar la explotación de vulnerabilidades técnicas y minimizar el

impacto de actividades de auditoría en los sistemas operacionales. El proceso tiene un rendimiento del 100%, por lo anterior es recomendable hacer un esfuerzo de uso y apropiación en lo indicado para cumplir con lo dispuesto.

SEGURIDAD EN LAS TELECOMUNICACIONES

Es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

Este dominio posee dos objetivos a saber: evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información. El segundo es mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.

La oficina tiene una calificación del 100%. Se evidencia que el proceso de Reparación Integral cuenta con el entendimiento de lo dictado por la Oficina de Tecnologías de la Información para la seguridad de las telecomunicaciones por parte de unidad.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Consiste en asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Este dominio presenta tres objetivos a saber: garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas; garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información y garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.

Para este dominio la dirección genero una calificación del 99.96 %. Por esta razón Control Interno recomienda que se exploren actividades que conduzcan a la aplicación y de los controles del proceso.

RELACIONES CON SUMINISTRADORES

Es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros. La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

Los dos objetivos que se derivan de este dominio son: garantizar la protección de los activos de la organización que son accesibles a proveedores y mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información.

Para Control Interno este aspecto es de los más trabajados institucionalmente en la medida de los múltiples servicios contratados y que requieren de unas claras y transparentes relaciones con los proveedores, el rendimiento de la dependencia es del 100%, se cuentan con controles en el manejo de la información que se entrega a diferentes dependencias.

GESTIÓN DE INCIDENTES

Es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno. Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

El único objetivo asociado a este dominio corresponde a garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.

Para este dominio proceso tiene un rendimiento del 100.00%. El área de Reparación Integral está enterada de las acciones a seguir, frente a lo dictaminado por la OTI para la atención de incidentes.

ASPECTOS DEL SISTEMA DE INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

Es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

En general, lo que se pretende es que por parte del proceso de Reparación Integral y áreas que interfieren en el proceso se apliquen los controles necesarios de acuerdo con su rol. Para este dominio se tiene por parte del proceso un rendimiento del 100.00%.

CUMPLIMIENTO

Este domino es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos. Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Para el efecto se proponen dos objetivos: evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales y garantizar que se implementa y opera la seguridad de la información de acuerdo con las políticas y procedimientos organizacionales. El proceso de Reparación Integral tiene un rendimiento del 100.00%.

RESULTADOS CUANTITATIVOS DE LA MATRIZ DOMINIOS CONTROLES

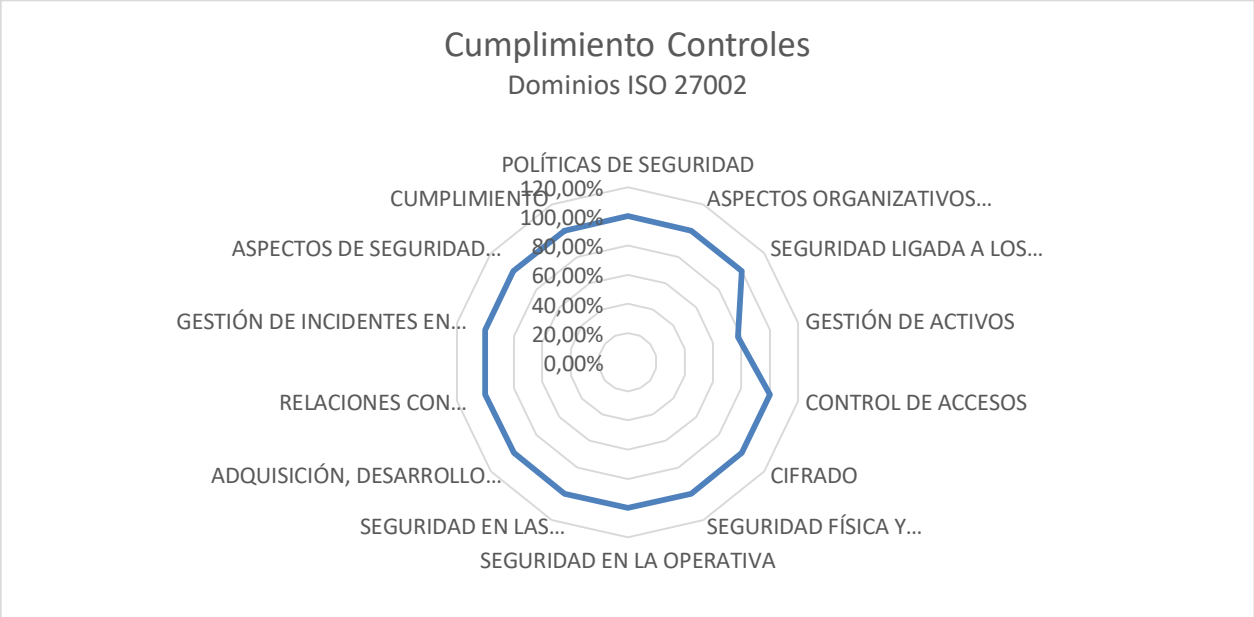
Los resultados que se presentan a continuación son producto de la metodología libre de agregación porcentual y distribución normal. En este escenario la suma total del ejercicio y su distancia con el óptimo de buena práctica se debe tomar como un indicador y parámetro y no como una evaluación obligatoria de cumplimento establecidos para la Oficina Asesora de Comunicaciones.

Sobre 1400 puntos posibles la oficina asesora alcanzó 1378, lo que representa un 98.42% de cumplimiento con los requisitos de validación de la norma, ello significa que en la actualidad y comparado con la buena práctica aplicada (NTC-ISO/IEC 27002) se encuentra en un desfase del 1.58%

El siguiente cuadro muestra el comportamiento del proceso de Reparación Integral frente a cada uno de los dominios propuestos en la norma técnica que se utilizó como parámetro comparativo:

Ítem	Dominio, objetivo de control y actividad de control	Calificación
1	POLÍTICAS DE SEGURIDAD	100,00%
2	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	100,00%
3	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	100,00%
4	GESTIÓN DE ACTIVOS	77,76%
5	CONTROL DE ACCESOS	100,02%
6	CIFRADO	100,00%
7	SEGURIDAD FÍSICA Y AMBIENTAL	100,02%
8	SEGURIDAD EN LA OPERATIVA	100,00%
9	SEGURIDAD EN LAS TELECOMUNICACIONES	100,01%
10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	99,96%
11	RELACIONES CON SUMINISTRADORES	100,01%
12	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	100,03%
13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	100,01%
14	CUMPLIMIENTO	100,01%
PROMEDIO		**98,42%**

Por medio de la gráfica tipo estrella se ejemplifica el modelo y debilidades que se requieren reforzar de acuerdo con los dominios.



B. CONCLUSIONES Y/O RECOMENDACIONES.

La verificación de los controles de seguridad de la información, basado con la buena práctica aplicada (NTC-ISO/IEC 27002) permite evidenciar por parte de la entidad las falencias en cada proceso; aplicar una batería de medición que permita constituirse en fuente de información en tiempo real que contribuya a la toma de decisiones; realizar un seguimiento constante a las variables de gerencia de los procesos y procedimientos que contribuya a una gerencia de cohesión.

Examinada la gestión del área de Reparación Integral y áreas que interfieren en el proceso relacionado con su sistema de control interno se encuentran debilidades que se hace necesario abordar con acciones correctivas.

Las debilidades según lo indicado por el área, la falta de seguimiento en lo que requiere a la eliminación de soportes y los soportes físicos en tránsito afectan directamente la seguridad de activos es una de las principales debilidades. Si bien existe el plan de seguridad de la información, la falta de apropiación de cada punto y la política desarrollada para tal fin genera falencias en la aplicación de estos controles en el proceso.

APROBÓ _____

JEFE OFICINA DE CONTROL INTERNO

ANEXOS Papel de trabajo papel_controles_iso_27 Reparacion Int

Anexo 1 Control de cambios

Versión	Fecha de Cambio	Descripción de la modificación
1	04/08/2014	Creación del formato.
2	09/03/2015	Al revisar el formato se evidencia que la casilla fecha de informe está repetida.
3	02/08/2017	Se modifica formato y se adiciona firma aprobación del Jefe Oficina de Control Interno.
4	30/04/2020	Se actualiza formato, se ajusta la distribución del texto en filas y columnas, las fuentes y fecha de la tabla control de cambios.