FECHA DE EMISIÓN DEL INFORME	**Día:**	30	**Mes:**	6	**Año:**	2020

Número de Informe	Informe verificación de controles de seguridad de la información al proceso de Participación y Visibilización.
Nombre del Seguimiento	Proceso Participación y Visibilización.
Objetivo del Seguimiento	Verificar los sistemas de control interno que el proceso realiza en el contexto del aseguramiento de la información atiendan las políticas aprobadas por la Dirección, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos estén adecuadamente controlados.
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	En el desarrollo de la verificación se 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 al proceso de Participación y Visibilización considera 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 que 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 DE SEGURIDAD

Dominios	Objetivo de control	Actividad 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	Políticas para la seguridad de la información: Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados, así como a todas las partes externas relevantes
		Revisión de las políticas para la seguridad de la información: Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad
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.	Asignación de responsabilidades para la SI: Se debiesen definir y asignar claramente todas las responsabilidades para la seguridad de la información.
	2. El objetivo es el de garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.	Teletrabajo: Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al 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.	Investigación de antecedentes: Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los

		requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
	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.	Cese o cambio de puesto de trabajo: Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.
4. Gestión Activos	1. El objetivo es identificar los activos en la organización y definir las responsabilidades para una protección adecuada	Inventario de activos: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
5. Control de Accesos	1. El objetivo es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.	Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización
	4. El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.	Control de acceso al código fuente de los programas: Se debería restringir el acceso al código fuente de las aplicaciones software

Para la evaluación se tiene que por cada dominio se asigna un porcentaje de 100 que se distribuye normalmente entre las actividades de control, si se cumplen 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 proceso no 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 del proceso que lideran.

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 reportada 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 cumple en un 100% las actividades de control propuestas en la buena práctica. La dependencia está trabajando en instrumentos y acciones que recogen estos lineamientos.

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 el proceso cumple los controles propuestos, en un 100% con el talento humano de su área. No obstante, la rotación de personal puede ser un factor que pueda afectar la apropiación debido a que no se cuenta con un proceso de capacitación o sensibilización de la aplicación de medidas de seguridad de la información que propendan a cumplir con las actividades de control propuestas por la norma técnica.

GESTIÓN ACTIVOS

Desde 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. El proceso tiene un rendimiento del 99.98% para este dominio donde se acerca su cumplimiento general

este se complementa con el proceso que se tiene en la entidad para el manejo los activos de información.

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 el proceso sobre este ítem es de 100%, situación que se evidencia en la prueba de verificación hecha por Control Interno. Por medio de este control se indica el conocimiento de los procedimientos de creación, modificación o actualización y eliminación de 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 Unidad cuenta con una política de encriptación para el tratamiento de los datos enunciado en el numeral 5.5.6. Seguridad de la Información, del Plan Estratégico de Tecnologías de la Información, por medio de la verificación se encuentra que el proceso no conoce adecuadamente estas políticas, por lo cual su calificación es 0%.

Por lo anterior, Control Interno considera necesario que la Oficina de Tecnologías de la Información (OTI) dispongan de acciones, mecanismos, actividades o cualesquiera otras formas de actuar que incremente el conocimiento sobre este dominio.

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.

El proceso tiene un rendimiento del 100%, evidenciando un conocimiento y manejo en la mayoría de los aspectos, la opción a reforzar es establecida por el aseguramiento de los equipos desatendidos 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 control en los sistemas operacionales.

El proceso tiene un rendimiento del 46.43%, específicamente relacionados con los objetivos 1, 2, 3 y 5. Por lo anterior es recomendable hacer un esfuerzo de socialización en lo indicado para para cumplir con lo dispuesto para los objetivos 4, 6 y 7.

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. Según las evidencias aportadas, el proceso tiene un rendimiento del 83.34%.

No obstante, existe espacio para fortalecer este dominio y con el advenimiento de acciones de control asociadas a otros dominios que tienen injerencia en la infraestructura será posible hacerlo.

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 el proceso tiene un rendimiento del 7.40%. Se evidencia que solo se tiene conocimiento de la política de desarrollo seguro de software, los otros puntos de control no son de conocimiento por parte de esta área.

Por ello Control Interno recomienda que se exploren actividades que conlleven a difundir y apropiar los controles que permitan integrar en las actividades 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 el más trabajado 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%.

En este escenario, es recomendable seguir trabajando los temas con los proveedores y definir las políticas que tanto ellos como la entidad aplican en cada uno de los productos adquiridos.

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 el proceso tiene un rendimiento del 100%. La dependencia está enterada de las acciones a seguir amén de la comunicación que se tiene con el oficial de seguridad que tiene la OTI, quien es el personal que se tiene previsto para trabajar sobre estos 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, desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar dentro de los procesos críticos de negocio aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

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 el proceso en la ejecución de sus actividades conozca y aplique los controles necesarios de acuerdo con su rol.

Este dominio posee dos objetivos propuestos: mantener la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la organización y garantizar la disponibilidad de las instalaciones de procesamiento de información.

Para este dominio el proceso tiene un rendimiento del 100%. El proceso tiene conocimiento de lo indicado en la política de seguridad de la información, así mismo que lo establecido en el Plan Estratégico de Tecnologías de la Información.

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.

Para este dominio el proceso tiene un rendimiento del 100%. Este resultado implica que se desarrolla en esta área un conocimiento de los controles.

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 el proceso.

Sobre 1400 puntos posibles la oficina asesora alcanzó 1137,15, lo que representa un 81,23% 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 18,78%

El siguiente cuadro muestra el comportamiento del proceso 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	99,98%
5	Control de Accesos	100,00%
6	Cifrado	0,00%
7	Seguridad Física y Ambiental	100,00%
8	Seguridad en la Operativa	46,43%
9	Seguridad en las Telecomunicaciones	83,34%
10	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	7,40%
11	Relaciones Con Suministradores	100,00%
12	Gestión de Incidentes en la Seguridad de la Información	100,00%
13	Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	100,00%
14	Cumplimiento	100,00%

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

Evaluación Controles Participación y Visibilización

RESULTADOS DE LOS LOGROS DE GESTIÓN

El resultado de la gestión del proceso fue objeto de evaluación independiente de Control Interno es de 8.12/10.00.

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 debilidades en el proceso. Al aplicar una batería de medición que permita constituirse en fuente de información en tiempo real y que contribuya a la toma de decisiones contribuye a una gerencia de cohesión.

Examinada la gestión de la Dirección de Gestión Interinstitucional relacionada con su sistema de control interno se encuentran debilidades que se hace necesario abordar con acciones pertinentes.

La falta de aplicación de determinados controles y manejo del flujo de información en los procesos aplicados frente a la seguridad de la información 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.

Aplicada una metodología de evaluación donde se compara la situación actual de la gestión de la información con buenas prácticas aportadas por la Norma Técnica Colombiana NTC – ISO/ IEC 27002, la Oficina de Control Interno evidencia fortalecimiento en líneas de control,

a lo que se debe tener en cuenta las potenciales brechas que se constituyen acciones para ser realizadas por la entidad.

Si bien esta metodología no es obligatoria y la evaluación es solo de comparación, esta Oficina recomienda a la Oficina de Tecnologías de la Información determine acciones para cerrar las brechas en los temas relacionados con debilidad del proceso de participación y Visibilización.

APROBÓ _____

JEFE OFICINA DE CONTROL INTERNO

ANEXOS

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.