 El futuro es de todos Unidad para la atención y reparación integral a las víctimas	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

FECHA DE EMISIÓN DEL INFORME	Día: 26	Mes: 08	Año: 2020
-------------------------------------	----------------	----------------	------------------


Número de Informe	001
Nombre del Seguimiento	Proceso Gestión para la Asistencia
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 al proceso de Gestión de la Asistencia 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.

 El futuro es de todos	INFORME DE SEGUIMIENTO		Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE		Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES		Fecha: 30/04/2020
			Páginas

“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 prácticas 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
6. Cifrado	4. El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones. 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 una organización internamente o con entidades externas.
10. Adquisición, 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

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


En el anexo a este informe se remite el papel de trabajo en el cual se almacena la información usada de manera 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 por parte del área de gestión de la asistencia 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 si no muestra la brecha que actualmente se tiene frente a una buena práctica, lo que posibilita acciones que corrijan y mejoren la actual situación de la oficina asesora.

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 área de gestión de la asistencia, en la actualidad se conoce la política, su ubicación y la aplicabilidad de esta en el área lo cual se califica según la herramienta de medición del 100%.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

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 área a cargo del proceso de gestión de la asistencia tiene un cumplimiento del 65,00 % en las actividades de control propuestas en la buena práctica. Esta dependencia indica que se requieren proyecciones distintas a las ya establecidas y apoyadas por los lineamientos de la Oficina de Tecnologías de la Información en lo que refiere al cumplimiento de los lineamientos y controles necesarios para contar con un proceso alineado con la seguridad de la información.

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 área cumple los controles propuestos, en un 100% con el talento humano de su área.

GESTIÓN ACTIVOS

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

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


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 crítica 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 oficina asesora tiene un rendimiento del 77.76% 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 de la oficina sobre este ítem es de 87,52%, situación que se evidencia en la prueba de verificación 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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


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 posee 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 la oficina Asesora de comunicaciones desconoce estas políticas, por lo cual su calificación es 50%. Por lo anterior, Control Interno indica la necesidad de que por parte de la oficina de Tecnologías de la Información (OTI), dispongan de acciones, mecanismos, actividades o cualesquiera otras formas de actuar que incremente el conocimiento y la interiorización 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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


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 oficina tiene un rendimiento del 88,90%, 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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

El proceso tiene una efectividad del 100%. Por lo anterior es recomendable enfatizar en continuar la mejora continua para permanecer en este porcentaje y que no se deteriore.

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 un rendimiento del 100%. Se evidencia que el proceso de Gestión de la Asistencia pone un empeño en lo relacionado con el intercambio de información con entes externos

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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


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 oficina asesora tiene un rendimiento del 99,96%. Se evidencia que el 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 esa razón Control Interno recomienda que se exploren actividades que conlleven a difundir y apropiar los controles que permitan integrar en las actividades del proceso de Gestión para la Asistencia en este dominio.

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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


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 83,34% porque la solo manejan un proveedor y en lo indicado por la oficina tienen estrictas relaciones de transmisión de la información.

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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

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 la Oficina Asesora de Comunicaciones tiene un rendimiento del 85,74%. La dependencia está enterada de las acciones a seguir, esto a la comunicación constante del 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, de 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.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

En general, lo que se pretende es que por parte de la Oficina Asesora de Comunicaciones en la ejecución del proceso de Gestión para la Asistencia 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 100.00%. La dependencia tiene conocimiento de los indicado en la política de seguridad de la información, así mismo que lo indicado en el Plan Estratégico de Tecnologías de la Información y considera importante la existencia con la aplicabilidad en el proceso, pero las acciones de ejecución y seguimiento corresponde directamente a la oficina OTI.

CUMPLIMIENTO

Este dominio 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

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

se implementa y opera la seguridad de la información de acuerdo con las políticas y procedimientos organizacionales.


Para este dominio la Oficina Asesora de Comunicaciones tiene un rendimiento del 66,67%. Este resultado implica que se desarrolla en esta área un conocimiento, que permite a los implicados en su proceso el cumplimiento normativo en su conjunto, lo que representa cierra la brecha que existe entre las acciones de control propuestas en la norma técnica y lo que actualmente se ejecuta por parte de la dependencia.

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 cumplimiento establecidos para la Oficina Asesora de Comunicaciones.

Sobre 1400 puntos posibles la oficina asesora alcanzó 195, lo que representa un 86,07% 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 13,94%


El siguiente cuadro muestra el comportamiento de la Oficina Asesora de Comunicación frente a cada uno de los dominios propuestos en la norma técnica que se utilizó como parámetro comparativo:

 <p>El futuro es de todos Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

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	65,00%
3	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	100,00%
4	GESTIÓN DE ACTIVOS	77,76%
5	CONTROL DE ACCESOS	87,52%
6	CIFRADO	50,00%
7	SEGURIDAD FÍSICA Y AMBIENTAL	88,90%
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	83,34%
12	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	85,74%
13	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	100,01%
14	CUMPLIMIENTO	66,67%
PROMEDIO		86,07%

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



 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas


RESULTADOS DE LOS LOGROS DE GESTIÓN

El resultado de la gestión de la Oficina Asesora de Comunicaciones fue objeto de evaluación independiente de Control Interno y en esa oportunidad se evidenció que la gestión obtuvo un logro del 8.10/10.00.

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 por parte de la entidad las posibles debilidades en el proceso, para lo cual se aplica 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 que requieran mayor potencial de gestión en concordancia con los lineamientos de la entidad y la OTI.

Se debe apoyar con mayor vigor la aplicación de los procesos vinculados con la seguridad de la información en lo que refiere a cifrado, aspectos organizativos y cumplimiento. Estos puntos son los de mayor déficit presentando por lo cual, debe ser fortalecidos para su desarrollo, con esto conllevar a la solución de falencias que se logran detectar.

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020 Paginas

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 brechas que se constituyen en potenciales acciones para ser realizadas por la entidad. Si bien esta metodología no es obligatoria y la evaluación es solo de comparación, esta oficina recomienda al proceso de Gestión de la Asistencia determine acciones para cerrar las brechas en temas como son la continuidad del negocio, la adopción de políticas de gestión de la información o cifrado de la información, solo por citarlas como ejemplos.

APROBÓ _____
JEFE OFICINA DE CONTROL INTERNO

 <p>El futuro es de todos</p> <p>Unidad para la atención y reparación integral a las víctimas</p>	INFORME DE SEGUIMIENTO	Código: 150.19.15-10
	PROCESO EVALUACIÓN INDEPENDIENTE	Versión: 04
	ELABORACIÓN DE INFORMES INTERNOS, EXTERNOS POR REQUERIMIENTO LEGAL Y OTROS INFORMES	Fecha: 30/04/2020
		Paginas

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.