FECHA DE EMISIÓN DEL INFORME	Día:	29	Mes:	09	Año:	2023

Proceso:	Gestión de Tecnologías de la Información
Procedimiento:	Componente Modelo de Seguridad y Privacidad de la
Líder de Proceso / Jefe(s) Dependencia(s):	Subgerencia Administrativa y Financiera
Objetivo de la Auditoría:	Verificar los lineamientos definidos por la estrategia de gobierno en línea en el manejo de la seguridad y la privacidad de la información establecidos en el modelo de seguridad y privacidad de la información. Y verificar la accesibilidad a la página web de la Empresa de Desarrollo Urbano y Rural de Dosquebradas, conforme a los criterios de accesibilidad web del anexo 1 de la Resolución 1519 de 2020.
Alcance de la Auditoría:	Evaluar la efectividad de los controles, el nivel de cumplimiento y protección de los principios de seguridad y privacidad de la información y verificar accesibilidad a la página web de la Empresa de Desarrollo Urbano y Rural de Dosquebradas, conforme a los criterios de accesibilidad web del anexo 1 de la resolución 1519 de 2020.
Criterios de la Auditoría:	Se aplica como referente los lineamientos emitidos por el Ministerio de las TIC mediante el Manual para la Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7 Abril de 2019, los lineamientos de la Norma internacional ISO/IEC 27001:2013 y las guías del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea. •Ley 1341 de 2009 min tic "Promover el establecimiento de una cultura de las Tecnologías de la Información y las Comunicaciones en el país, a través de programas y proyectos que favorezcan la apropiación y masificación de las tecnologías, como instrumentos que facilitan el bienestar y el desarrollo personal y social". *Resolución 159 de 2020 con su anexo técnico

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	07	Mes	07	Año	2023	Desde	24/07/20 D / M / A	Hasta	14/08/23 D / M / A	Día	21	Mes	09	Año	23

Representante Alta Dirección	Jefe oficina de Control Interno	Auditor Líder
MARTA CONTRERAS CORREA	LINA MARIA LLANO RAMIREZ	LINA MARIA LLANO R/ ALIRIO SANCHEZ PEREZ

RESUMEN EJECUTIVO

Atendiendo lo estipulado en la normatividad y legislación colombiana, La Oficina de Control Interno en su función de evaluación y seguimiento, establecida en el artículo 2.2.21.5.3 del decreto 1083 de 2015, modificado por el artículo 17 del decreto 648 de 2017 que establece: "/…/ De las oficinas de control interno. Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control. El Departamento Administrativo de la Función Pública determinará los lineamientos para el desarrollo de los citados roles." Realizó la auditoría interna a el procedimiento de Gestión de Tecnologías de la Información, componentes Modelo de Privacidad y Seguridad de la Información y Accesibilidad página web de EDOS.

De conformidad con la Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces del DAFP; de acuerdo con el Rol de enfoque a la prevención, la Oficina Asesora de Control Interno debe desarrollar entre otras actividades la de Asesorar a los líderes de procesos en el establecimiento de planes de mejoramiento.

Así mismo y respecto del Rol de Evaluación y seguimiento establece que éste se desarrolla a través de las auditorías internas y ello conlleva a las siguientes actividades:

Plan de auditorías.

1.1. Planeación de la auditoría.

1.2. Ejecución de la auditoría.

1.3. Comunicación resultados (informes).

1.4. Seguimiento (planes de mejoramiento).

PRINCIPALES SITUACIONES DETECTADAS/ RESULTADOS DE LA AUDITORÍA / RECOMENDACIONES

Para el desarrollo de la auditoría se realizaron reuniones con los ingenieros de sistemas internos que apoyan el proceso de Gestión de Tecnologías de la información, se solicitaron las claves para verificar la ciberseguridad de la página web y se verificó la siguiente información:

El modelo de seguridad y privacidad de la información MSPI, en lo que relaciona levantamiento de información, la madurez y la brecha en la que se encuentra la entidad y donde se miden los riesgos y controles que reflejan el trabajo y compromiso de la herramienta de autodiagnóstico se encuentra en estado de proceso inicial. Ya lo que compete a la página web de la entidad se encuentra desactualizada a lo que relaciona la normatividad del Ministerio de las Tecnologías, información y comunicaciones y el proceso de alimentación de información que debe estar publicada para el servicio de la comunidad.

De la anterior revisión y verificación se desprenden las siguientes observaciones:

Observación N° 1

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona a las herramientas de autodiagnóstico para el MSPI, lo relacionado hace referencia que para el debido proceso se debe realizar un paso a paso que está establecido en un documento maestro y por ende no se está cumpliendo.

Gobierno Digital: articles-5482_G20_Instructivo_instrumento_Evaluacion_MSPI

LEY 1341 DE 2009 (Julio 30)

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

En que componente del ciclo PHVA considera que va?	Planear

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN Lista de información BASICA a solicitar	NOMBRE DEL DOCUMENTO ENTREGADO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)		
2	Misión		
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para		
4	Mapa de Procesos		
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces		
6	Políticas de seguridad de la información formalizada y firmada		
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.		
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de		
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la		
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección		
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)		
12	Procedimientos de control documental del MSPI		
13	Metodología de Gestión de riesgos		
14	Riesgos identificados y valorados de acuerdo a la metodología		
15	Planes de tratamiento de los riesgos		
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información		
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad		
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus		
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información		
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección		
21	Inventario de áreas de procesamiento de información y telecomunicaciones		

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA

Se evidencia muy claro que el instrumento de evaluación no hay un levantamiento de la información para cumplir con su respectivo proceso.

Observación N° 2

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si tienen identificados los controles de riesgo en el MSPI, lo relacionado hace referencia al instrumento de evaluación que requiere de un levantamiento de información para mostrar los resultados esperados y por ende no se está cumpliendo.

Goblerno Digital: articles-5482_G7_Gestion_Riesgos

LEY 1341 DE 2009 (Julio 30)

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

No.	Evaluación de Efectividad de controles DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	15	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	33	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	32	100	REPETIBLE
A.9	CONTROL DE ACCESO	23	100	REPETIBLE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	28	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	26	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	13	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	10	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	37,5	100	REPETIBLE
	PROMEDIO EVALUACIÓN DE CONTROLES	27	100	REPETIBLE

ASPECTOS DE SEGU
INFORMACIÓN DE
DE LA CONTINU
GESTIÓN DE INCIDENT
SEGURIDAD DE LA INFOR
RELACIONES
PROVEED
ADQUISICIÓN, DE
MANTENIMIENTO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA

Se evidencia muy claro que la efectividad de los controles en el instrumento de evaluación no tiene un resultado específico porque no hay un levantamiento de la información correcto para que arrojes los porcentajes esperados.

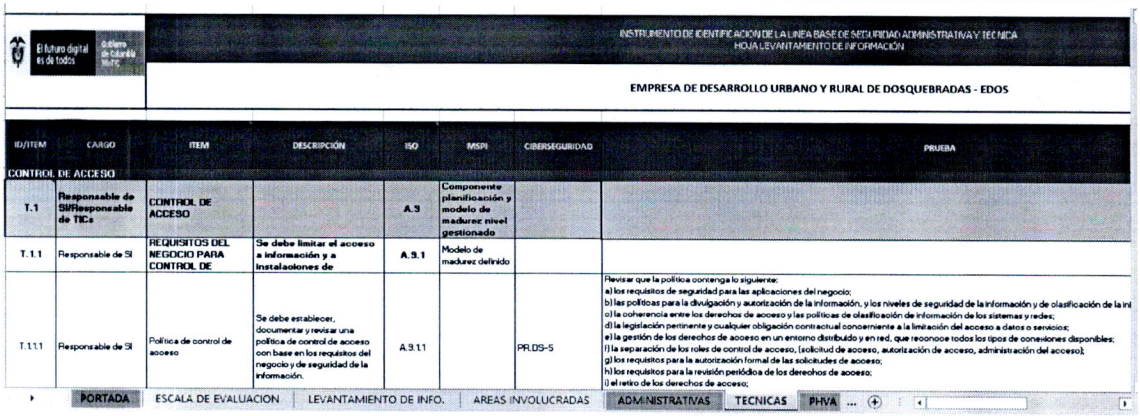
Observación N° 3

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona a las evaluaciones de seguridad técnicas bajo la supervisión de personal autorizado, apoyado en herramientas automáticas y con revisiones manuales MSPI, no se cumple.

Gobierno Digital: articles-5482_G8_Controles_Seguridad

LEY 1341 DE 2009 (Julio 30)

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.



El futuro digital es de todos — Gobierno de Colombia MinTIC

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA DE DESARROLLO URBANO Y RURAL DE DOSQUEBRADAS - EDOS

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA
CONTROL DE ACCESO							
T.1	Responsable de SI/Responsable de TICs	CONTROL DE ACCESO		A.9	Componente planificación y modelo de madurez nivel gestionado		
T.1.1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE	Se debe limitar el acceso a información y a instalaciones de	A.9.1	Modelo de madurez definido		
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la in c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso;

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA

Se evidencia muy claro que las evaluaciones de seguridad técnicas no se establecen correctamente debido a que no están cumpliendo con el paso a paso de la información para que arroje el resultado esperado.

Observación N° 4

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona al cumplimiento con las políticas y normas de seguridad en el MSPI, lo relacionado hace referencia que hay establecidas unas normas y guías con sus respetivas políticas de gobierno digital que se establece en seguridad de la información y por ende no se está cumpliendo.

Nombre

- articles-5482_G1_Metodologia_pruebas_efectividad
- articles-5482_G2_Politica_General
- articles-5482_G3_Procedimiento_de_Seguridad
- articles-5482_G4_Roles_responsabilidades
- articles-5482_G5_Gestion_Clasificacion
- articles-5482_G6_Gestion_Documental
- articles-5482_G7_Gestion_Riesgos
- articles-5482_G8_Controles_Seguridad
- articles-5482_G9_Indicadores_Gestion_Seguridad
- articles-5482_G10_Continuidad_Negocio
- articles-5482_G11_Analisis_Impacto
- articles-5482_G12_Seguridad_Nube
- articles-5482_G14_Plan_comunicacion_sensibilizacion
- articles-5482_G15_Auditoria
- articles-5482_G16_evaluaciondesempeno
- articles-5482_G17_Mejora_continua
- articles-5482_G18_Lineamientos_terminales
- articles-5482_G19_Aseguramiento_protocolo
- articles-5482_G21_Gestion_Incidentes
- articles-5482_Instructivo_instrumento_Evaluacion_MSPI
- articles-5482_Modelo_de_Seguridad_Privacidad

Se evidencia muy claro que las guías del modelo y seguridad de la información muestran efectivamente el cumplimiento del resultado esperado para la entidad, siguiendo las normas establecidas y el documento maestro para su perfecto cumplimiento y resultado de la misma.

Observación N° 5

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona al documento maestro del MSPI para lograr efectivamente el paso a paso del levantamiento de información, lo relacionado hace referencia de que el MSPI tiene una herramienta para su respectivo proceso y resultado de la misma y por ende no se está cumpliendo.

Gobierno Digital: articles-5482_G20_Instructivo_instrumento_Evaluacion_MSPI

LEY 1341 DE 2009 (Julio 30)

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter

transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

TABLA DE CONTENIDO

ANALISIS DEL CONTEXTO N°1

QUE TENEMOS QUE HACER PARA CUMPLIR CON LA CLÁUSULA 4

(ANEXO 4 LINEAMIENTOS PARA LA GESTION DEL RIESGO DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS - GUÍA RIESGOS 2018)

Se trata del punto de partida para desarrollar el SGSI y consiste en determinar o identificar los "problemas" internos y externos a los que se enfrenta la organización.

Explicado de otra forma, el contexto organizacional consiste en considerar las expectativas y necesidades de todas las partes interesadas.

Les resumimos los pasos para poner en marcha este requisito

- Comprender la organización y su contexto
  - Comunicación y Consultas
  - El contexto del SGSI
  - El Contexto de la Gestión de Riesgos
  - Definición de criterios del riesgo
- Comprender las necesidades y expectativas de las partes interesadas
  - En que consiste
  - Ejemplos
- Determinación del Alcance del Sistema de Gestión
  - Propósito del Alcance del SGSI
  - Como definir los límites el SGSI
  - Cuestionario para definir el Alcance del SGSI
  - Ejemplo de Alcance del SGSI
  -

Se evidencia muy claro que el documento maestro nos ilustra cómo se debe elaborar el instrumento de evaluación para que la entidad muestre la evaluación correcta, además todo lo que compete al análisis del contexto.

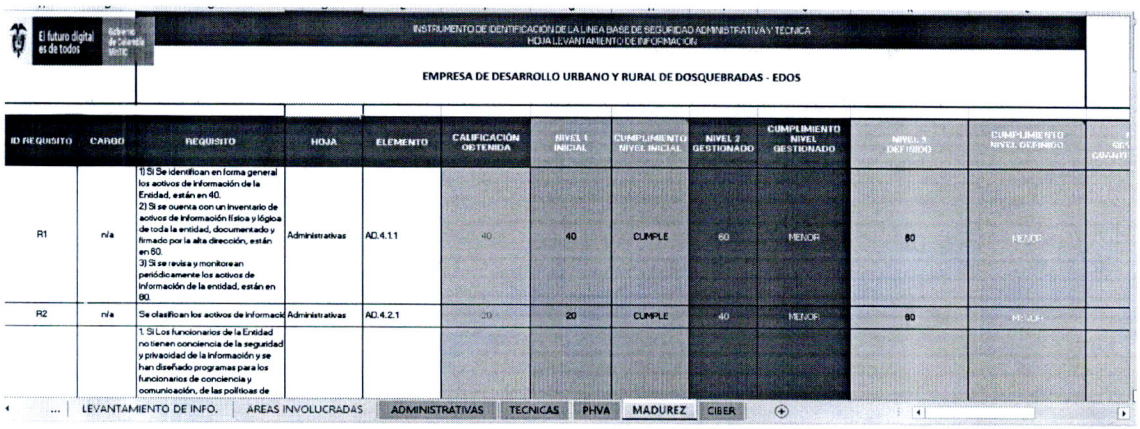
Observación N° 6

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona al nivel de madurez del MSPI la herramienta debe evaluarse con su respectivo paso a paso como está establecido en las guías y en el documento maestro y por ende no se está cumpliendo.

Gobierno Digital: articles-5482_G13_Modelo_de_Seguridad_Privacidad

LEY 1341 DE 2009 (Julio 30)

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.



El futuro digital es de todos — Gobierno de Colombia MINTIC

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA
HOJA LEVANTAMIENTO DE INFORMACION

EMPRESA DE DESARROLLO URBANO Y RURAL DE DOSQUEBRADAS - EDOS

ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 MEDIDO
R1	n/a	1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	Administrativas	AD.4.1.1	40	40	CUMPLE	60	MENOR	80	MENOR	
R2	n/a	Se clasifican los activos de informació	Administrativas	AD.4.2.1	20	20	CUMPLE	40	MENOR	80	MENOR	
		1. SI Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de										

... | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA | MADUREZ | CIBER

Se evidencia que el nivel de madurez en el MSPI no puede arrojar la información esperada ya que no se ha hecho el proceso adecuado como se indica en las guías del modelo y seguridad de la información.

Observación N° 7

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona a la brecha establecida en seguridad y privacidad de la información la herramienta debe evaluarse con su respectivo paso a paso como está establecido en las guías y en el documento maestro y así mismo evidenciar en qué estado se encuentra la entidad y adonde debemos llegar y por ende no se está cumpliendo.

Gobierno Digital: articles-5482_G8_Controles_Seguridad

LEY 1341 DE 2009 (Julio 30)

Artículo 38. Masificación del uso de las TIC y cierre de la brecha digital. El Ministerio de Tecnologías de la Información y las Comunicaciones, revisará, estudiará e implementará estrategias para la masificación de la conectividad, buscando sistemas que permitan llegar a las regiones más apartadas del país y que motiven a todos los ciudadanos a hacer uso de las TIC.

Se evidencia en la gráfica una brecha con un resultado errado ya que su elaboración no es la establecida para su respectivo resultado.

Observación N° 8

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si se adoptan las medidas técnicas y pruebas de efectividad necesarias para proteger la información donde reposan estos datos de la entidad en MSPI, no se está cumpliendo.

Goblerno Digital: articles-5482_G1_Metodologia_pruebas_efectividad

LEY 1341 DE 2009 (Julio 30)

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD

La metodología de pruebas de efectividad es una serie de actividades, que tienen por finalidad comprobar o medir la eficiencia de la implementación del modelo de seguridad en las entidades.

Esta metodología ha sido diseñada para ayudar a las entidades a entender y comprender, la realización de unas pruebas, los objetivos de las mismas y el beneficio que se obtiene al identificar sus etapas y gestionarlas.

Esta metodología es desarrollada en diferentes etapas que permiten concluir que tanto ha avanzado la entidad con la implementación del modelo; de esta manera, a través de la valoración de diferentes aspectos se permitirá identificar vulnerabilidades y amenazas a las cuales está expuesta la entidad, así como también posibles debilidades en los controles implementados.

Al igual que los demás procedimientos planteados en el modelo de seguridad y privacidad de la información, se busca proteger la disponibilidad, integridad y confidencialidad de la información de la entidad.

Un factor externo de mucho impacto, que se alinea con la ejecución de las pruebas de seguridad y privacidad y sus resultados, son los intereses de lo que se denomina Alta Dirección, que para nuestro caso son los directivos de las entidades del estado, estos se ven reflejados en las capacidades de las entidades de llevar a buen término la implementación del modelo de seguridad para dar cumplimiento a la normatividad vigente; así como llevar a la entidad al siguiente nivel de seguridad que permite que sus procesos y atención al ciudadano deje una buena imagen en la sociedad colombiana.

Se evidencia que los procedimientos en sus medidas y pruebas de efectividad permiten identificar todo tipo de inconsistencias en la información.

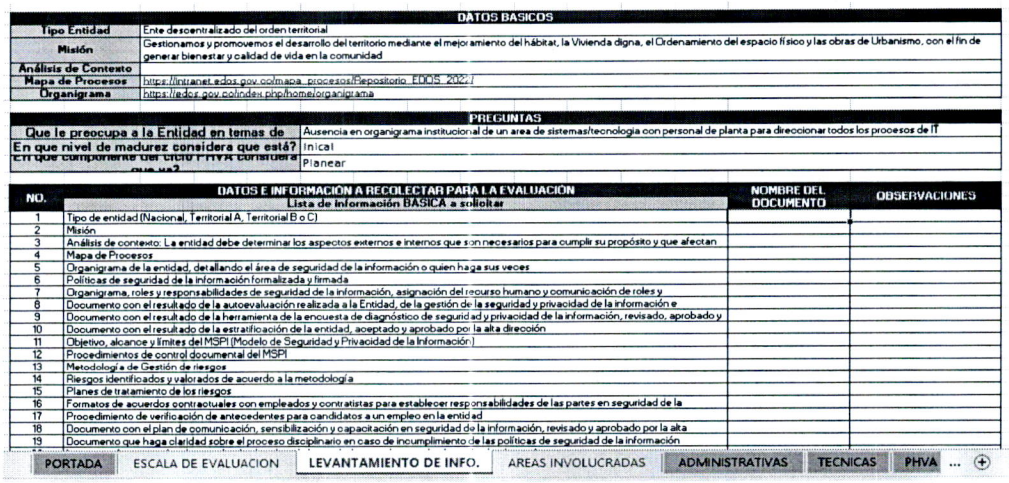
Observación N° 9

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si hay acciones de mejora y cambios en la implementación del modelo de seguridad y privacidad de la información identificados en la herramienta no está establecido porque no se ha realizado el debido proceso como esta en el documento maestro y en las guías de gobierno digital para así lograr identificar las acciones de mejora y por ende no se está cumpliendo.

Gobierno Digital: articles-5482_G11_Analisis_Impacto

LEY 1341 DE 2009 (Julio 30)

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.



DATOS BASICOS	
Tipo Entidad	Ente descentralizado del orden territorial
Misión	Gestionamos y promovemos el desarrollo del territorio mediante el mejoramiento del hábitat, la Vivienda digna, el Ordenamiento del espacio físico y las obras de Urbanismo, con el fin de generar bienestar y calidad de vida en la comunidad
Análisis de Contexto	
Mapa de Procesos	https://intranet.edos.gov.co/mapa_procesos/Repositorio_EDOS_2021/
Organigrama	https://edos.gov.co/index.php/home/organigrama

PREGUNTAS	
Que le preocupa a la Entidad en temas de	Ausencia en organigrama institucional de un area de sistemas/tecnologia con personal de planta para direccionar todos los procesos de IT
En que nivel de madurez considera que está?	Inical
En que componente del ciclo PHVA considera que va?	Planear

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN Lista de información BASICA a solicitar	NOMBRE DEL DOCUMENTO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)		
2	Misión		
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan		
4	Mapa de Procesos		
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces		
6	Políticas de seguridad de la información formalizada y firmada		
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y		
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e		
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y		
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección		
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)		
12	Procedimientos de control documental del MSPI		
13	Metodología de Gestión de riesgos		
14	Riesgos identificados y valorados de acuerdo a la metodología		
15	Planes de tratamiento de los riesgos		
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la		
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad		
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta		
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información		

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA ...

Se evidencia que las acciones de mejora como su implementación no están establecidas porque el instructivo no se ha elaborado como esta en las guías del MSPI.

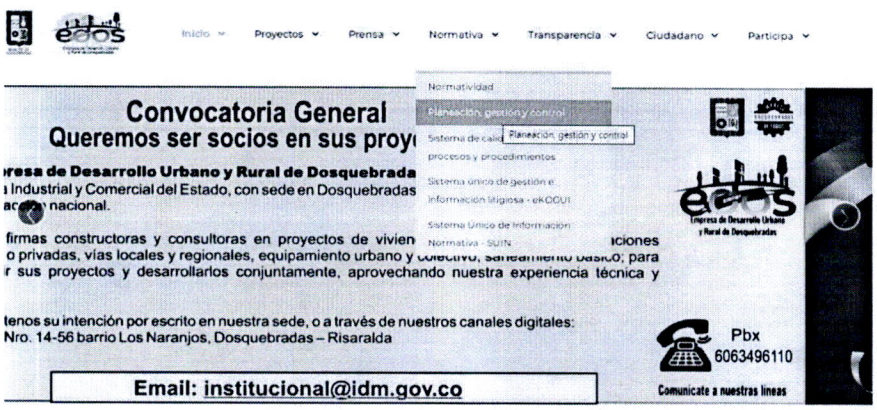
Observación N° 10

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona a la página web de la entidad si maneja lenguaje de señas, lo relacionado hace referencia a que la página web de la entidad en el menú o en las herramientas que tiene no está desarrollado y diseñado el lenguaje de señas para el servicio de la comunidad como lo sugiere la normatividad y por ende no se está cumpliendo.

Goblerno Digital: articles-5482_G4_Roles_responsabilidades

LEY 1341 DE 2009 (Julio 30)

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.



Se evidencia que la página web de la entidad no tiene establecida el lenguaje de señas como lo exige la normatividad donde se requiere de la creatividad y desarrollo de los ingenieros del área de sistemas para dar cumplimiento a esta observación.

Observación N° 11

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona a la página web de la entidad si se puede actualizar de acuerdo a la normatividad de min tic, lo relacionado hace referencia a una serie de normas y requisitos que por ende no se están cumpliendo.

Gobierno Digital: articles-5482_G2_Politica_General

LEY 1341 DE 2009 (Julio 30)

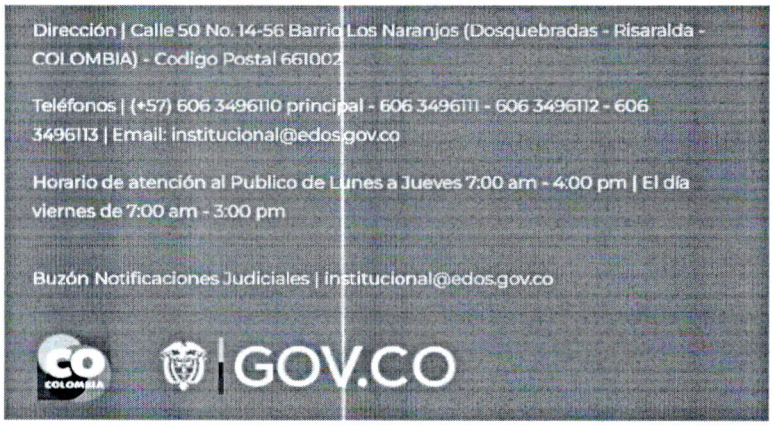
Artículo 53. Régimen jurídico. El régimen jurídico de protección al usuario, en lo que se refiere a servicios de comunicaciones, será el dispuesto en la regulación que en materia de protección al usuario expida la CRC y en el régimen general de protección al consumidor y sus normas complementarias en lo no previsto en aquella.

En todo caso, es de la esencia de los contratos de prestación de servicios de comunicaciones el derecho del usuario a presentar peticiones y/o reclamaciones sobre el servicio ofrecido, y a que estas sean atendidas y resueltas de manera oportuna, expedita y sustentada. De la misma forma, el derecho a recibir atención de forma eficiente y adecuada en concordancia con los parámetros que defina la CRC.

Se reconocerán, al menos, los siguientes derechos a los usuarios:

1. Elegir y cambiar libremente el proveedor y los planes de precios de acuerdo con lo autorizado por la Comisión de Regulación de Comunicaciones, salvo las condiciones pactadas libremente en el contrato, las cuales deben ser explícitas, claras y previamente informadas al usuario.

2. Recibir de los proveedores, información clara, veraz, suficiente y comprobable sobre los servicios ofrecidos, su consumo, así como sobre los precios, de manera tal que se permita un correcto aprovechamiento de los mismos.



Se evidencia perfectamente que la página tiene información desactualizada como números de teléfono, información en carpetas vacías sin brindar a la ciudadanía etc. Por ende, para dar cumplimiento a los requerimientos de la entidad.

Observación N° 12

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona a temas de ciberseguridad la entidad no cuenta con dispositivos de blindaje para la seguridad de información de los equipos de los funcionarios, internet y del software financiero de la entidad, por ende, no se está cumpliendo.

Gobierno Digital: articles-5482_G20_Instructivo_instrumento_Evaluacion_MSPI

Gobierno Digital: articles-5482_G9_Indicadores_Gestion_Seguridad

LEY 1341 DE 2009 (Julio 30)

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.

5.8. HOJA 8 -> CIBERSEGURIDAD:

En esta evaluación se pretende determinar cómo se encuentra la entidad frente a las mejores prácticas en ciberseguridad definidas por el NIST, con miras a ir realizando un diagnóstico frente a los lineamientos de la política de ciberseguridad y ciberdefensa definidos en el documento Conpes 3701 y el Conpes 3854.

Gráfica 60: Marco básico de funciones de Ciberseguridad

Se evidencia perfectamente que la entidad no cuenta con dispositivos como por ejemplo cisco meraki para blindar y proteger la información y la conectividad de los equipos que se conectan a la red y prestan el servicio para temas misionales de la misma.

Observación N° 13

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si tienen DRP como plan de contingencia para la entidad, lo relacionado hace referencia al plan de contingencia e inicio de servicios cuando se requiera y por ende no se está cumpliendo.

Gobierno Digital: articles-5482_G10_Continuidad_Negocio

LEY 1341 DE 2009 (Julio 30)

Artículo 8°. Las telecomunicaciones en casos de emergencia, conmoción o calamidad y prevención para dichos eventos. En casos de atención de emergencia, conmoción interna y externa, desastres, o calamidad pública, los proveedores de redes y servicios de telecomunicaciones deberán poner a disposición de las autoridades de manera gratuita y oportuna, las redes y servicios y darán prelación a dichas autoridades en la transmisión de las comunicaciones que aquellas requieran. En cualquier caso, se dará prelación absoluta a las transmisiones relacionadas con la protección de la vida humana. Igualmente darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables.
Los proveedores de redes y servicios de telecomunicaciones deberán suministrar a las autoridades competentes, sin costo alguno, la información disponible de identificación y de localización del usuario que la entidad solicitante considere útil y relevante para garantizar la atención eficiente en los eventos descritos en el presente artículo.

- Proceso para la administración del riesgo en seguridad de la información

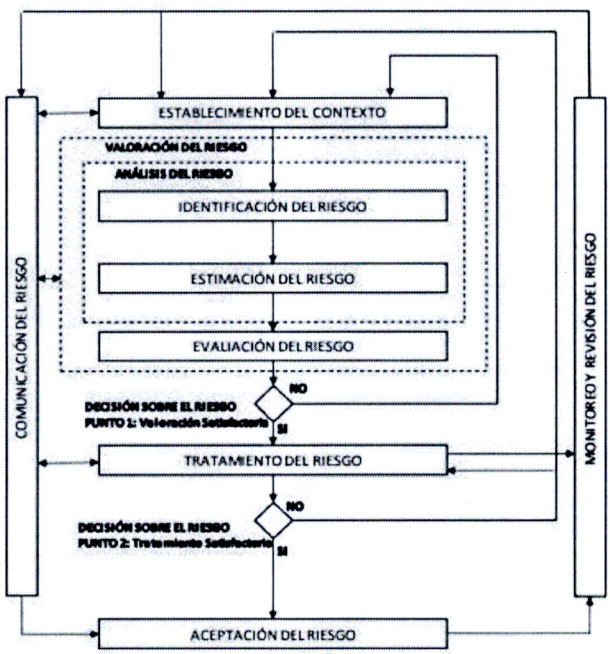


Imagen 2. Tomado de la NTC-ISO/IEC 27005

Se evidencia que para la continuidad del negocio se requiere de dispositivos y equipos que cumplan con los requisitos que requiere la entidad para realizar su debido proceso.

Observación N° 14

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si tienen red cableada como respaldo para la conectividad de los equipos de cómputo, en lo relacionado al cableado hace referencia que la entidad no cuenta con conectividad Ipv4 ni Ipv6 que son temas de infraestructura para intercomunicar los equipos de la entidad y brindar una mayor seguridad en el flujo de información y de los temas misionales que maneja la entidad, por ende, no se está cumpliendo.

Gobierno Digital: articles-5482_G19_Aseguramiento_protocolo

Gobierno Digital: articles-5482_G4_Roles_responsabilidades

LEY 1341 DE 2009 (Julio 30)

Artículo 8°. Las telecomunicaciones en casos de emergencia, conmoción o calamidad y prevención para dichos eventos. En casos de atención de emergencia, conmoción interna y externa, desastres, o calamidad pública, los proveedores de redes y servicios de telecomunicaciones deberán poner a disposición de las autoridades de manera gratuita y oportuna, las redes y servicios y darán prelación a dichas autoridades en la transmisión de las comunicaciones que aquellas requieran. En cualquier caso, se dará prelación absoluta a las transmisiones relacionadas con la protección de la vida humana. Igualmente darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables.

Los proveedores de redes y servicios de telecomunicaciones deberán suministrar a las autoridades competentes, sin costo alguno, la información disponible de identificación y de localización del usuario que la entidad solicitante considere útil y relevante para garantizar la atención eficiente en los eventos descritos en el presente artículo.

MINTIC vive digital TODOS POR UN NUEVO PAÍS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8. LINEAMIENTOS DE SEGURIDAD PARA IPv6

8.1 Lineamientos Generales

- ✓ La fase de implementación del protocolo IPv6 debe ser estructurado con base en los esquemas de seguridad de información, sobre los cuales se tengan contempladas las políticas de confidencialidad, integridad y disponibilidad de las Entidades
- ✓ Se requiere definir un plan de marcha atrás (Plan de Contingencias) para el caso de presentarse inconvenientes de indisponibilidad de los servicios, que atenten contra la seguridad de la información y de las comunicaciones de las Entidades al momento de implementar el protocolo IPv6.
- ✓ En el proceso de transición hacia el nuevo protocolo, revisar la seguridad de información de las infraestructuras de TI, la seguridad de IPv6 y el nivel de impacto de servicios como el Directorio Activo, Sistemas de Nombres de Dominio - DNS, Correo Electrónico, Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC3315 para DHCPv6), Sistemas Proxy, Servicios de aplicaciones, Servicios Web y Sistemas de Gestión y Monitoreo.
- ✓ Se recomienda mantener la utilización de los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6, de tal manera que la resolución de nombres de dominio se de en forma transparente tanto para Ipv4 como en IPv6, se exceptúa de esta regla los ambientes de prueba que se realicen sobre IPv6.
- ✓ De la misma manear que ocurre con IPv4, en Ipv6 se recomienda no usar direcciones IPv6 literales en el desarrollo del software y en el uso de librerías.
- ✓ Generar la documentación necesaria que contemple los aspectos de seguridad del entorno en los sistemas de comunicaciones, sistemas de información y sistemas de almacenamiento, que surjan del desarrollo de la implementación de IPv6.

Se evidencia que la entidad no tiene conectividad IPV4 ni IPV6 para todos los servicios y equipos de los funcionarios de la entidad para lograr efectivamente un servicio de red y establecer una fidelidad en la información compartida de la misma

Observación N° 15

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si la entidad tiene NAS como respaldo y blindaje de la información que utilizan los funcionarios y contratistas de la entidad, lo relacionado hace referencia a la seguridad que debe cumplir la entidad tanto para los funcionarios como contratistas en tener un servicio para proteger la información que maneja la entidad, por ende, no se está cumpliendo.

Gobierno Digital: articles-5482_G3_Procedimiento_de_Seguridad

Gobierno Digital: articles-5482_G4_Roles_responsabilidades

LEY 1341 DE 2009 (Julio 30)

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.

Artículo 41. Aplicación. Las reglas de este capítulo se aplicarán a las actuaciones administrativas de solución de controversias, de fijación de condiciones de acceso, uso e interconexión, y de imposición de servidumbre de acceso, uso e interconexión adelantados de oficio o a solicitud de parte ante la Comisión de Regulación de Comunicaciones.

¿Por qué son importantes los dispositivos NAS?

Las empresas y pequeñas empresas de muchos sectores eligen las soluciones NAS porque ofrecen un almacenamiento eficaz, escalable y de bajo coste. En comparación con otros servidores, los servidores de archivos NAS proporcionan un acceso más rápido a los datos y son más fáciles de configurar y administrar. Pueden admitir diversas aplicaciones empresariales, como sistemas de correo electrónico privados, bases de datos de contabilidad, nóminas, grabación y edición de vídeo, registro de datos y análisis empresarial.

Algunas de las ventajas del NAS son:

Implementación de la nube privada para las organizaciones

Una nube privada es una nube que aloja recursos del propio centro de datos de una organización. Puede basarse en recursos de hardware internos o en una infraestructura separada proporcionada por un tercero. Puede utilizar dispositivos NAS para implementar el almacenamiento en la nube privada en su organización.

Soluciones flexibles de almacenamiento local para pequeñas empresas

Los sistemas NAS se pueden personalizar en función del tamaño y los requisitos de la organización. En el mercado hay disponibles tanto dispositivos de bajo costo y menor almacenamiento, como dispositivos más caros de alta gama.

Se evidencia que la entidad no tiene dispositivos de almacenamiento de alta capacidad conectado a una red que permite a los usuarios y clientes autorizados almacenar y recuperar datos en una ubicación centralizada.

Observación N° 16

Se está incumpliendo la Ley 1341 de 2009 min tic, la norma ISO 27001 de 2013 y las guías del modelo de seguridad y privacidad de la información. En lo que relaciona si la página web de la entidad cuenta con todas las redes sociales disponibles y actualizadas para el servicio de la comunidad, lo relacionado hace referencia a todas las redes sociales como son tiktok, instagram, y que funcionen sin pedir usuarios y contraseñas para visualizar los servicios de realizados por la entidad, por ende, no se está cumpliendo.

Gobierno Digital: articles-5482_G2_Politica_General

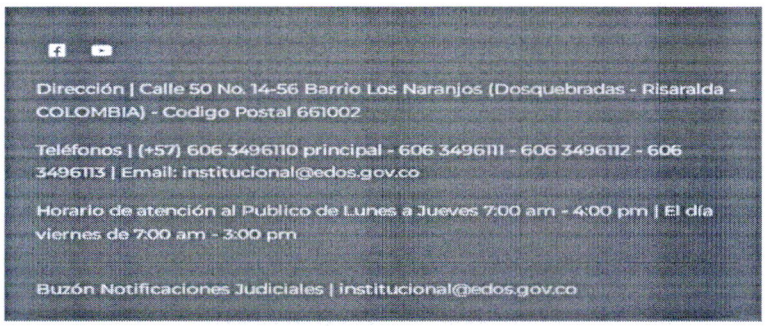
Gobierno Digital: articles-5482_G13_Modelo_de_Seguridad_Privacidad

LEY 1341 DE 2009 (Julio 30)

Artículo 5°. Las entidades del orden nacional y territorial y las Tecnologías de la Información y las Comunicaciones, TIC. Las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones. Para tal efecto, dichas autoridades incentivarán el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y equipos que permitan realmente a los ciudadanos

acceder a las aplicaciones tecnológicas que beneficien a los ciudadanos, en especial a los vulnerables y de zonas marginadas del país.

Artículo 8°. Las telecomunicaciones en casos de emergencia, conmoción o calamidad y prevención para dichos eventos. En casos de atención de emergencia, conmoción interna y externa, desastres, o calamidad pública, los proveedores de redes y servicios de telecomunicaciones deberán poner a disposición de las autoridades de manera gratuita y oportuna, las redes y servicios y darán prelación a dichas autoridades en la transmisión de las comunicaciones que aquellas requieran. En cualquier caso, se dará prelación absoluta a las transmisiones relacionadas con la protección de la vida humana. Igualmente darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables.
Los proveedores de redes y servicios de telecomunicaciones deberán suministrar a las autoridades competentes, sin costo alguno, la información disponible de identificación y de localización del usuario que la entidad solicitante considere útil y relevante para garantizar la atención eficiente en los eventos descritos en el presente artículo.



Se evidencia que la página web de la entidad no tiene configurado para el servicio de la ciudadanía todas las redes sociales que funcionan o todos los medios sociales que hace referencia a las nuevas plataformas y canales de comunicación sociales caracterizadas por la conversación y la interacción entre los usuarios.

FICHA TECNICA
Herramientas Utilizadas: lista de chequeo, papeles de trabajo, herramientas de evaluación, revisión página web, documentos TIC enviados.
Universo: Se verificó la página web con las claves de acceso entregadas, proceso de tecnologías de la información
Población objeto: Proceso, procedimientos, manuales y en general toda la documentación de Tecnologías de la Información
Marco estadístico: NA

INFOGRAFIA

file:///C:/Users/CONTROL%20INTERNO/Mi%20unidad/ASESORIA%20CONTROL%20INTERNO/AUDITORIAS%202023/AUDITORIA%20TIC/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Recomendaciones Control Interno

PROYECTOS

1. Indicadores.

Requerimientos Mantenimiento Preventivo

Requerimientos Seguridad Digital y Redes

Requerimientos Sistemas de gestión crítica

Requerimientos Soporte Técnico y ofimático

Requerimientos Web y comunicaciones

2. Riesgos

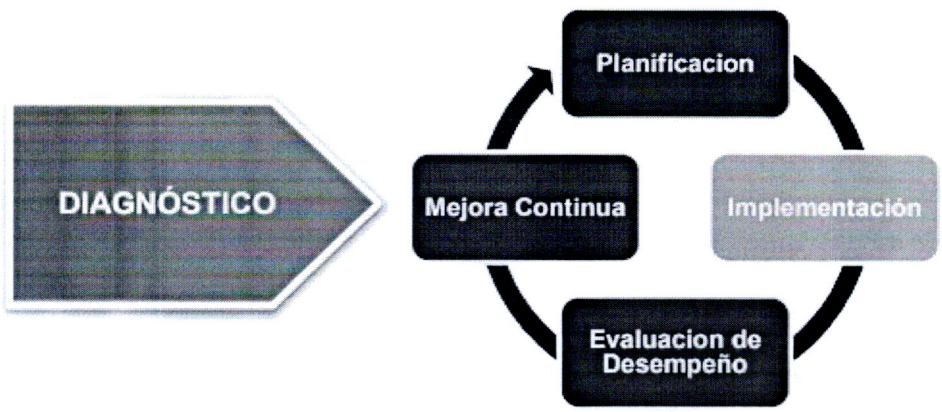
El Mapa de riesgos de tecnologías de la información fue actualizado en el mes de julio de 2023 y tiene cuatro riesgos.

3. Acciones de mejoramiento

No se tienen planes de mejoramiento anteriores, esta es la primera auditoría de seguimiento al modelo de seguridad y privacidad de la información.

CONCLUSIONES DE LA AUDITORÍA

La presente auditoría permite a la empresa concluir que no se cuenta con un MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, en la autoevaluación realizada en abril de 2023 el resultado fue: no cuenta con el nivel inicial del modelo, incumpliendo como se repite en todas las observaciones de la auditoría con la ley 1341 de 2009 del Ministerio de las Tics y la norma ISO 27001 de 2013, haciendo énfasis que el modelo tiene como objetivo la preservación de la confidencialidad, integridad y disponibilidad de la información permitiendo garantizar la privacidad de los datos y la entidad requiere en su planeación estratégica establecer una ruta crítica para ejecutar las diferentes etapas del modelo.



También es necesario que la empresa incorpore el lenguaje de señas en la página web y que sea actualizada de conformidad con la normatividad vigente y se reconozca que esta es una herramienta de interacción permanente con la comunidad para la rendición de cuentas y la participación ciudadana.

Para constancia se firma en Dosquebradas, a los 18 días del mes de octubre del año 2023

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad**	**Firma**
MARTA CONTRERAS CORREA	SUBGERENTA ADMINISTRATIVA Y FINANCIERA /LIDER PROCESO	
ALIRIO SANCHEZ PEREZ	AUDITOR EXTERNO OCI	
LINA MARIA LLANO RAMIREZ	ASESOR OFICINA DE CONTROL INTERNO	

Anexos

A continuación, se describe el estado de los reportes de mejoramiento correspondiente a las vigencias anteriores:

Vigencia	*No. reporte*	*Tipo acción*	*Hallazgo*	*Fuente de la acción*	*Responsable*	*Ultimo seguimiento*