INFORME DE AUDITORIA SOBRE EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL FONDO ROTATORIO DE LA POLICIA.

OSCAR DIAZ

AUDITOR LIDER ISO 27001:2013

2019

Contenido

Fecha	**20/11/2019 – 10/12/2019**
Auditor Líder	Oscar Rolando Diaz Ortiz
Objetivo	Evaluar el cumplimiento del sistema de gestión de seguridad de la información de acuerdo con los requerimientos del estándar ISO/IEC 27001:2013, así los controles establecidos en el Anexo A.
Alcance	El Sistema de Gestión de Seguridad de la Información – SGSI del Fondo Rotatorio de la Policía abarca los procesos misionales de Gestión contractual, Industrial y Créditos y los procesos de soporte de Telemática y Gestión documental conforme a lo establecido en su mapa de procesos los cuales requieren, utilizan, generan o producen la información que se requiere proteger.
Criterios de Auditoría	Procedimientos documentados y establecidos por la organización bajo la NTC ISO/IEC 27001:2013 y su Anexo ISO/IEC 27002:2013

1. ENTREVISTAS REALIZADAS

No.	PROCESOS
1.	**TELEMATICA**
2.	**SEGURIDAD DE LA INFORMACIÓN**
3.	**PLANEACION ESTRATEGICA**
3.	**CONVENIOS**
4.	**GESTIÓN DOCUMENTAL**
5.	**CONTRATOS**
6.	**CONSTRUCCIONES**
7.	**COMERCIO EXTERIOR**
8.	**CREDITOS**
9.	**INSDUSTRIAL**

Toda la información evidenciada durante esta Auditoria es tratada en absoluta confidencialidad y no será revelada a un tercero sin consentimiento escrito del cliente.

Este reporte es confidencial y su distribución es limitada al equipo auditor, al representante del cliente y a la UT Gamma-Identian.

2. POSIBLES RIESGOS DEL PROCESO DE AUDITORÍA.

1.	**Incumplimiento de horarios del plan de auditoria por horarios**
2.	**Disponibilidad de auditados**
3.	**Falta de evidencia de auditoria**
4.	**Indisponibilidad de la sede o lugar de la Auditoria**

3. ASPECTOS RELEVANTES DURANTE LA ENTREVISTA (POSITIVOS).

1.	Disponibilidad de los auditados
2.	Disposición del personal para la atención de la auditoría interna
3.	A nivel tecnológico se ve que se tiene muy claro cuál es la estrategia de seguridad de la información en cuanto a seguridad informática.
4.	A todos los que firman contrato se les realiza una verificación de antecedentes, experiencias y referencias laborales necesarias
5.	Se tiene una herramienta de software para gestión de riesgos, lo cual es muy apropiado para el SGSI y para el efectivo seguimiento a la gestión de riesgos para todos los procesos involucrados.

4. HALLAZGOS.

No.	PROCESO	NC / OM	CONTROL O CLAUSULA AFECTADA	DESCRIPCIÓN
1.	SEGURIDAD DE LA INFORMACIÓN	**OM**	NTC-ISO-IEC-27001/2013 Numeral 4.	SE EVIDENCIA LA MATRIZ DOFA ESTRATEGICA CON VERSION 1, DEL 26/02/2019, SE DEBE PODER TENER CENTRALIZADA LA INFORMACIÓN DE LA MATRIZ DOFA EN UN REPOSITORIO DONDE SEA DE FÁCIL ACCESO Y DE CONOCIMIENTO COMÚN DE LAS PARTES INTERESADAS.
2.	SEGURIDAD DE LA INFORMACIÓN	**OM**	NTC-ISO-IEC-27001/2013 Numeral 4.	SE DEBE ACTUALIZAR LA MATRIZ DOFA CON LOS TEMAS REFERENTES A SEGURIDAD DE LA INFORMACIÓN PARA EL SGSI.
3.	SEGURIDAD DE LA INFORMACIÓN	**OM**	NTC-ISO-IEC-27002/2013 6.2.	PARA LOS OBJETIVOS ESTRATEGICOS DE LA ORGANIZACIÓN, SE DEBERIA VER LA OPORTUNIDAD DE DISEÑAR UN OBJETIVO ESTRATEGICO QUE SE BASE EN EL SGSI Y EN LOS OTROS SISTEMAS DE GESTION QUE SE TIENEN ESTABLECIDOS EN LA ENTIDAD.
4.	SEGURIDAD DE LA INFORMACIÓN	**OM**	NTC-ISO-IEC-27002/2013 **5.2**	EN LA POLITICA DE SEGURIDAD DE LA INFORMACION DOCUMENTADA CON FECHA 2019-06-26, SE DEBE TENER EN CUENTA EL VERSIONAMIENTO DENTRO DEL FORMATO DONDE SE CONSTRUYE LA POLITICA, SEA QUE ESTE EN MEDIO FISICO O DIGITAL.
5.	SEGURIDAD DE LA INFORM ACIÓN	**NC MENOR**	NTC-ISO-IEC-27001/2013 **5.3, 5.1**	SE TIENE DEFINIDO EL CARGO DE QUIEN VA A SER EL OFICIAL DE SEGURIDAD DE LA INFORMACION Y SE TIENEN DEFINIDOS SUS ROLES Y RESPONSABILIDADES DENTRO DEL DOCUMENTO DEFINICION DE ROLES Y RESPONSABILIDADES DEL SGSI, SIN EMBARGO, NO SE TIENE FORMALIZADO EL NOMBRAMIENTO DE ESTA PERSONA Y ESTOS ROLES DENTRO DE SUS FUNCIONES COMO COLABORADOR DE LA ENTIDAD, LO CUAL AFECTA DIRECTAMENTE LO DISPUESTO EN EL NUMERAL 5.3 DE LA NORMA.
6.	SEGURIDAD DE LA INFORMACIÓN	**NC MENOR**	NTC-ISO-IEC-27001/2013	EN LA DEFINICION DE LA COMPETENCIA PARA LAS PERSONAS QUE REALIZAN LA GESTION DE LA

			7.2	SEGURIDAD DE LA INFORMACION EN LA ENTIDAD, NO SE TIENE DEFINIDO UN PERFIL PARA EL OFICIAL DE SEGURIDAD DE LA INFORMACION EN CUANTO A SU FORMACION Y CONOCIMIENTOS PREVIOS Y COMPETENCIA, LO CUAL AFECTA DIRECTAMENTE LO ESTABLECIDO EN EL NUMERAL 6.2 DE LA NORMA.
7.	SEGURIDAD DE LA INFORMACIÓN	**NC MENOR**	NTC-ISO-IEC-27001/2013 **7.5**	EN LA GESTION DE LA INFORMACION DOCUMENTADA Y LOS MARCOS A NIVEL DOCUMENTAL DE LA ENTIDAD, SE EVIDENCIA QUE EXISTE INFORMACION QUE, AUNQUE YA ESTA FINALIZADA NO HA SIDO FORMALIZADA Y SU VERSIONAMIENTO NO ES CLARO, LO CUAL AFECTA DIRECTAMENTE LO DISPUESTO EN EL NUMERAL 5 DE LA NORMA.
8	SEGURIDAD DE LA INFORMACIÓN	**OM**	NTC-ISO-IEC-27001/2013 **9.2**	SE DEBE CONTAR CON PROCEDIMIENTOS DE AUDITORIA ADECUADOS PARA LA MEJORA CONTINUA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION, ASI COMO DEBE EXISTIR PERSONAL EN LA ENTIDAD, A PARTE DE LAS AREAS QUE MANEJAN SEGURIDAD DE LA INFORMACION, QUE PUEDAN EJECUTAR AUDITORIAS SOBRE EL SGSI PARA LA MEJORA CONTINUA.
9	SEGURIDAD DE LA INFORMACIÓN	**OM**	NTC-ISO-IEC-27001/2013 **6.1**	SE DEBE GARANTIZAR QUE TODOS LOS ACTIVOS Y RIESGOS, EVIDENCIADOS EN LA FASE DE GESTION DE ACTIVOS Y EVALUACION Y ANALISIS DE RIESGOS, SE ENCUENTREN DENTRO DE EL SISTEMA SUITE VISION, YA QUE SE EVIDENCIA QUE SOLAMENTE ALGUNOS HAN SIDO CARGADOS AL SISTEMA PERO FALTAN BASTANTES POR SUBIR.
10	CONVENIOS	**OM**	NTC-ISO-IEC-27002/2013 **A 13.2**	SE DEBE REPLANTEAR LA POSIBILIDAD DE RESTRINGIR EL USO DE CORREOS ELECTRONICOS PERSONALES, YA QUE EN ESTE MOMENTO SE EVIDENCIA UNA PROBABILIDAD DE MATERIALIZACION DE RIESGO DE FUGA DE INFORMACION ALTA, POR LA ACEPTACION DEL USO DE CORREOS PERSONALES A LOS FUNCIONARIOS.
11		**OM**	NTC-ISO-IEC-27001:2013	EN EL PROCESO DE INDUCCION DE PERSONAL NUEVO SE DEBEN INCLUIR LOS TEMAS ASOCIADOS A LA GESTION DE LA SEGURIDAD DE LA

	CONVENIOS		**7.3**	INFORMACION, GESTION DE RIESGOS Y GESTION DE INCIDENTES, PARA GARANTIZAR EL CONOCIMIENTO TRANSVERSAL DE LO QUE SE DESARROLLA DESDE EL SGSI EN LA ENTIDAD.
12	CONVENIOS	**OM**	NTC-ISO-IEC-27001:2013 **9.2**	PARA LA CORRECTA GESTION EN EL MONITOREO DE LAS ACTIVIDADES SOSPECHOSAS EN LA RED DE LA ENTIDAD, SE DEBEN EJECUTAR ACTIVIDADES DE AUDITORIA Y REVISION QUE PERMITAN EVIDENCIAR LOS ACCESOS A LA INFORMACION QUE TIENEN LAS PERSONAS Y EL CONTENIDO EN INTERNET AL QUE ACCEDEN.
13	GESTIÓN DOCUMENTAL	**OM**	NTC-ISO-IEC-27001:2013 A 11	EN LA GESTION DE LA SEGURIDAD FISICA Y DE ACCESO A LA INFORMACION DOCUMENTADA DE LOS PROCESOS, SE DEBE GARANTIZAR QUE SE MANTENGAN Y SE USEN LOS CONTROLES DE ACCESO FISICO A LOS ARCHIVOS QUE SE TIENEN EN LAS DIFERENTES AREAS DE FORPO.
14	GESTIÓN DOCUMENTAL	**OM**	NTC-ISO-IEC-27001:2013 A 11	EN LA GESTION DE ACCESO FISICO AL ARCHIVO CENTRAL, SE DEBE TENER EL CONTROL DEL VISITANTE Y EL OBJETIVO DE LA VISITA PARA LLEVAR TRAZABILIDAD DE LAS ENTRADAS Y SALIDAS A LA BODEGA, A PARTE DE LA QUE SE REALIZA EN LA ENTRADA AL PARQUE INDUSTRIAL.
15	GESTIÓN DOCUMENTAL	**OM**	NTC-ISO-IEC-27002:2013 A 17.2	SE TIENE LA COPIA DE LA INFORMACION DOCUMENTAL DEL ARCHIVO CENTRAL EN MICROFILMINAS Y EL ARCHIVO FISICO EN LA MISMA BODEGA, SE DEBE SEPARAR LA INFORMACION QUE SE TIENE EN EL ARCHIVO CENTRAL DE LA INFORMACION DE OTRO MEDIO QUE SERVIRA COMO RESPALDO EN ALGUN EVENTO ADVERSO QUE PUEDA EXPONER LA INFORMACION FISICA DEL ARCHIVO.
16	GESTIÓN DOCUMENTAL	**OM**	NTC-ISO-IEC-27001:2013 7.3	EL PERSONAL DE FUNZA DEBE SENSIBILIZARSE EN CUANTO A SEGURIDAD DE LA INFORMACION, YA QUE SOLO LOS LIDERES HAN ASISTIDO A LAS CAPACITACIONES DADAS EN LA IMPLEMENTACION DEL SGSI.

17	PLANEACIÓN ESTRATEGICA	**OM**	NTC-ISO-IEC-27001:2013 **7.5.3**	SE DEBE GESTIONAR LA ESTRATEGIA DE CERO PAPEL LA CUAL SE DEBE PLANEAR Y EJECUTAR LO MAS PRONTO POSIBLE PARA INICIAR CON EL CAMBIO DE MENTALIDAD DE MANEJO DE INFORMACION, DE FISICO A DIGITAL.
18	PLANEACIÓN ESTRATEGICA	**OM**	NTC-ISO-IEC-27001:2013 9.3 10.2 A 18.2.3	DENTRO DE LA GESTION PARA LA MEDICION DE LA EFECTIVIDAD DEL SGSI SE DEBE GARANTIZAR QUE PERIODICAMENTE SE TENGA LA RESPECTIVA MEDICION DE LOS INDICADORES Y QUE ESTOS RESULTADOS SE PRESENTE A NIVEL GENERAL AL COMITÉ DE SEGURIDAD DE LA INFORMACION DENTRO DE LA GESTION DE IMPLEMENTACION DEL SGSI.
19	CONTRATOS	**OM**	NTC-ISO-IEC-27001:2013	EN LA GESTION PARA EL MANEJO DE ACTIVOS DE INFORMACION DEL PROCESO, SE DEBE GARANTIZAR EL BUEN MANEJO Y EL USO DE LOS ACTIVOS, POR LO CUAL EL ARCHIVO DE CONTRATOS QUE SE TIENEN EN LAS CAJAS APILADAS SOBRE EL SUELO A UN COSTADO DE LA OFICINA DEBERIA ESTAR ORGANIZADO EN UN LUGAR DONDE NO SE PUDIERA ACCEDER TAN FACILMENTE POR CUALQUIER PERSONA.
20	CONTRATOS	**OM**	NTC-ISO-IEC-27001:2013 8.1.3	PARA EL CONTROL DE LA INFORMACION DE LOS CONTRATOS, SE DEBE GARANTIZAR QUE LA INFORMACION QUE SE CONTIENE EN LAS CAJAS ANTES DE FOLIAR, SE CONTROLE EN CUANTO A SU CONTENIDO, YA QUE SOLO SE REALIZA EL CONTROL DESPUES DE FOLIAR.
21	CONTRATOS	**OM**	NTC-ISO-IEC-27001:2013 9	PARA CONTROLAR Y EVITAR LA FUGA DE INFORMACION, SE DEBEN REALIZAR AUDITORIAS PO RPARTE DE SEGURIDAD DE LA INFORMACION HACIA EL AREA, PARA VERIFICAR SI SE ESTA FUGANDO LA INFORMACION DE LOS CONTRATOS A NIVEL FOTOGRAFICO POR MEDIO DE LOS EQUIPOS CELULARES, YA QUE DENTRO DE LAS CARPETAS HAY DOCUMENTOS QUE PODRIAN TENER UN NIVEL DE

				SENSIBILIDAD ALTO POR EJEMPLO COPIAS DE CEDULAS, LICENCIAS, CARNETS, ETC.
22	CONSTRUCCIONES	**OM**	NTC-ISO-IEC-27002:2013 A 13.2.3	EN LA GESTION DE LAS ACTIVIDADES MISMAS DEL PROCESO SE DEBE REVISAR EL ACCESO A LOS CORREOS PERSONALES, YA QUE, AUNQUE NO SE MANEJAN PARA TEMAS CORPORATIVOS SI SE PODRIA DAR PROBABLEMENTE ALGUNA SALIDA DE INFORMACION NO AUTORIZADA.
23	COMERCIO EXTERIOR	**OM**	NTC-ISO-IEC-27001:2013 8.	EN EL MANEJO DE LA INFORMACION DENTRO DEL AREA SE EVIDENCIA QUE SE MANIPULA POR VARIAS PERSONAS Y QUE TRANSITA DENTRO DEL AREA, SE DEBE CONTAR CON SEGURIDAD FISICA DE LOS ARCHIVADORES, YA QUE LAS CARPETAS TIENEN INFORMACION QUE SE PODRIA CONSIDERAR COMO INFORMACION SENSIBLE.
24	COMERCIO EXTERIOR	**OM**	NTC-ISO-IEC-27002:2013 A 11.	SE DEBE CONTAR CON CONTROL DE MONITOREO POR CAMARAS O CCTV EN LAS INSTALACIONES DONDE SE ENCUENTRA EL AREA.
25	COMERCIO EXTERIOR	**OM**	NTC-ISO-IEC-27001:2013 7.3.	DENTRO DE LA GESTION DE SENSIBILIZACION Y CAPACITACION SE DEBE GARANTIZAR Y BUSCAR ESTRATEGIAS PARA QUE LAS PERSONAS ASISTAN Y SE SENSIBILICEN EN LOS TEMAS QUE SE ESTAN IMPLEMENTANDO Y LOS TEMAS RELEVANTES DE SEGURIDAD DE LA INFORMACION.
26	COMERCIO EXTERIOR	**OM**	NTC-ISO-IEC-27001:2013 5.3.	PARA EL GESTOR DE SEGURIDAD DE LA INFORACION DEL PROCESO, SE DEBEN TENER MUY BIEN IDENTIFICADAS SUS RESPONSABILIDADES Y COMO ACTUA PARA EL POYO DEL SGSI DENTRO DE ESTE PROCESO.
27	COMERCIO EXTERIOR	**NC MENOR**	NTC-ISO-IEC-27001:2013	SE EVIDENCIA EL USO DE PAPEL PARA REUSO O RECICLADO, CON INFORMACION DE FIRMAS, DOCUMENTOS, CIFRAS, ESTA INFORMACION PODRIA SER SENSIBLE DENTRO DEL MISMO PROCESO, SE DEBE DAR UN MANEJO ADECUADO AL REUSO DEL PAPEL YA QUE SE EVIDENCIA MUCHA INFORMACION EXPUESTA EN LA “CAJA DE PAPEL RECICLADO”, ESTO AFECTA DIRECTAMENTE A LOS NUMERALES DEL ANEXO A.8.1.3, A.8.2.3.

28	TELEMATICA	**OM**	NTC-ISO-IEC-27001:2013 6.1.2	SE DEBE GARANTIZAR QUE AL SISTEMA SUITE VISION SE CARGUE EL 100% DE LOS RIESGOS IDENTIFICADOS.
29	TELEMATICA	**OM**	NTC-ISO-IEC-27002:2013	SE DEBE REALIZAR UNA REVISION POR PARTE DEL AREA DE SEGURIDAD DE LA INFORMACION, EN CUANTO A LA IMPLEMENTACION EFECTIVA DE LOS CONTROLES TECNICOS DE SEGURIDAD SOBRE LA PLATAFORMA PCSECURE, CON EL FIN DE GARANTIZAR LA IMPLEMENTACION EFECTIVA DE LOS CONTROLES.
30	TELEMATICA	**OM**	NTC-ISO-IEC-27002:2013 16.	DENTRO DE LA GESTION INCIDENTES DE SEGURIDAD DE LA INFORMACION, SE DEBE CAPACITAR A LAS PERSONAS A NIVEL GENERAL EN LA ENTIDAD, EN LA IDENTIFICACION Y REPORTE DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACION DESDE LA HERRAMIENTA DE MESA DE AYUDA.
31	TELEMATICA	**OM**	NTC-ISO-IEC-27002:2013 A 16.	DENTRO DE LA GESTION INCIDENTES DE SEGURIDAD DE LA INFORMACION, SE DEBE SENSIBILIZAR A LAS PERSONAS EN LAS ACCIONES QUE DEBEN LLEVAR A CABO Y EL MANEJO QUE LE DEBEN DAR A LAS SITUACIONES EN LAS QUE SE VEAN ENVUELTOS EN ALGUN INCIDENTE O ALGUN CIBERATAQUE.
32	TELEMATICA	**OM**	NTC-ISO-IEC-27002:2013 A 17.2.1	DENTRO DE LA GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION, SE DEBE TENER LISTO Y EN FUNCIONAMIENTO EL CENTRO DE DATOS ALTERNO PARA EVITAR MATERIALIZACION DE RIESGOS DE PERDIDA DE INFORMACION EN ESTE MOMENTO EN LA ENTIDAD.
33	INDUSTRIAL	**OM**	NTC-ISO-IEC-27001:2013	LA CAPACITACION QUE SE HA VENIDO LLEVANDO A CABO EN LA ENTIDAD Y EN EL PROCESO, SOLAMENTE A TOCADO AL AREA ADMINISTRATIVA, SE DEBERIA EXTENDER EL ALCANCE DE ESTA CAPACITACION EN TEMAS DE SEGURIDAD DE LA INFORMACION A LAS PERSONAS DEL AREA OPERATIVA, YA QUE ELLAS CONOCEN TODO EL PROCESO DESDE LA PARTE DE DISEÑO Y CONSTRUCCION DE LOS PRODUCTOS.

5. CONCLUSIONES.

El Auditor Líder concluye que:

1	La organización muestra una correcta gestión de los marcos normativos basados en la norma ISO 27001:2013, dando un cumplimiento a algunos de los numerales de la norma, por lo cual se debe trabajar en las observaciones, oportunidades de mejora y No conformidades evidenciadas durante la auditoria, se deben cerrar en un lapso muy corto de tiempo o si es posible, de inmediato, por lo cual el riesgo de pérdida de información se podría materializar aprovechando la vulnerabilidad evidenciada y la probabilidad que existe.
2	Desde el área responsable por el SGSI en la compañía, es claro que los esfuerzos que se han tenido hasta el momento en pro de sacar adelante el sistema es evidente, sin embargo se hace necesario que esta área cuente con el apoyo evidente de los gestores de seguridad de la información dentro de los procesos, quienes deben conocer perfectamente sus responsabilidades y como es su gestión dentro del sistema, para que no toda la gestión este centralizada en una única persona como lo es el oficial, sino que este ejerza el liderazgo y el control sobre la gestión de seguridad de la información en la compañía y que se apoye en su equipo en cuanto a la medición de controles, análisis de riesgos y en la gestión misma del sistema, ya que si se deja en el toda la carga y la responsabilidad se podría colapsar a futuro en la gestión, ya que el sistema no es estático sino dinámico y crecerá y madurara con el paso del tiempo.
3	El nivel de implementación del SGSI es optimo para el tiempo que lleva en su gestión, las características y objetivos son claros dentro del alcance que se tiene establecido y se evidencia el trabajo que se ha realizado por las partes encargadas, la alta dirección debe ser consciente que en la madurez del sistema se tendrán que tener nuevos controles que en algunos casos conllevan una inversión económica para poder implementarlos , por lo cual siempre deben estar enterados de lo que se planifico, lo que se desarrolló, lo que se implemento y de lo que se mejoró, siempre serán parte activa dentro del ciclo de Planear, Hacer, Verificar y Actuar.