

<b>Líder(es) y/o Responsable del Proceso (3)</b>	CN. (RA) Jorge Alberto Arocha Muñoz - Jefe Oficina de Informática
<b>Proceso y/o Procedimientos, actividad específica auditada y/o evaluada (4)</b>	Gestión Informática Cód.: IM OC OFI PS 001 Rev. 15.
<b>Alcance (5):</b>	Verificación selectiva de las herramientas tecnológicas, gestor documental E-synergy, correo electrónico, seguridad de la información, cumplimiento a los documentos No. 02.290.283 "Directiva transitoria plan de contingencia y continuidad del negocio para enfrentar la Emergencia Sanitaria por causa del COVID-19, No. 02.253.712 - "Directiva transitoria para el apoyo al personal - sus familias y la normalización de la operación en FEXAR" y Documento No.02.266.900 - "CORREO COIMAS ADMINISTRATIVAS EN INDUMIL" - actividad No.10.
<b>Objetivo General (6):</b>	Contribuir al cumplimiento de los objetivos de la Industria Militar a través de la gestión en los roles asignados a la Oficina de Control Interno, adelantando la evaluación independiente, selectiva, sistémica y objetiva, fortaleciendo el mejoramiento continuo del Sistema de Control Interno, teniendo como referente la aplicación de los lineamientos establecidos en el Sistema de Gestión Integral, la legislación y normas vigentes.
<b>Objetivos específicos (7):</b>	<p>Evaluar la funcionalidad y los controles de las herramientas tecnológicas gestor documental E-synergy y Correo Electrónico Microsoft Outlook 2007.</p> <p>Evaluar los controles establecidos del cumplimiento de las políticas para el manejo y seguridad de la información, realización, custodia y recuperación del respaldo de la información.</p> <p>Verificar el cumplimiento del literal G. "Actividades Particulares - Oficina Informática" de la Directiva Transitoria plan de contingencia y continuidad del negocio para enfrentar la Emergencia Sanitaria por causa del COVID-19.</p> <p>Verificar el cumplimiento del literal D. "Misiones Particulares - numeral IX. Oficina Informática" de la Directiva transitoria para el apoyo al personal - sus familias y la normalización de la operación en FEXAR.</p> <p>Verificación de la información suministrada mediante documento No.02.266.900 - "CORREO COIMAS ADMINISTRATIVAS EN INDUMIL" oficio No. 02.266.900 del 11 de febrero de 2020, acerca de presuntos actos de corrupción en la Industria Militar - actividad No. 10.</p>
<b>Documentos de referencia (8): (Criterios)</b>	<p>Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio de Control Interno y organismos del estado y se dictan otras disposiciones."</p> <p>Ley 1474 de 2011 "Por la cual se dictan normas orientadas a</p>

	<p><i>fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y efectividad del control de la Gestión Pública”.</i></p>
	<p>Decreto 2775 de 1997 <i>“Por el cual se aprueba el Acuerdo No. 0393 del 12 de Agosto de 1997 Dictado por la Junta Directiva de la Industria Militar. Por el cual se estable la estructura interna de la Industria Militar y se determinan las funciones de sus dependencias.”</i></p>
	<p>Decreto 1078 de 2015 <i>“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” Artículo 2.2.9.1.2.2. “Los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, ...”.</i></p>
	<p>Decreto 1499 de 2017 <i>“Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”.</i></p>
	<p>Decreto 648 de 2017 <i>“Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública” Artículo 17.</i></p>
	<p>Decreto 612 de 2018 <i>“Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado” Artículo 2.2.22.3.14. “Integración de los planes institucionales y estratégicos al Plan de Acción”.</i></p>
	<p>Resolución 092 de mayo 17 de 2018 <i>“Por el cual se adopta el Modelo integrado de Planeación y Gestión y se crea el comité institucional de Gestión y desempeño en la Industria Militar”.</i></p>
	<p>Norma Técnica Colombiana NTC-ISO-IEC 27001 del 2013-12-11.</p>
	<p>Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 3 - Diciembre de 2019.</p>
	<p>Circular 100.04 del 14 <i>“Cursos virtuales del Modelo Integrado de Planeación y Gestión - MIPG”</i> de Diciembre de 2018.</p>
	<p>Política de Seguridad de la Información para la relación con proveedores Cód: IM OC OFI CP 002 Rev.7.</p>
	<p>Política de Seguridad y Privacidad de la Información Cód: IM OC OFI CP 003 Rev.8.</p>
	<p>Política para el uso de dispositivos móviles Cód: IM OC OFI CP 004 Rev.3.</p>
	<p>Proceso Gestión Informática Cód: IM OC OFI PS 001 Rev.15.</p>
	<p>Procedimiento Seguridad física de la Industria Militar Cód: IM OC DRS PR 001Rev.3.</p>
	<p>Procedimiento para gestionar los roles de la Oficina de Control Interno en la Industria Militar Cód: IM OC OCI PR 002 Rev.5.</p>
	<p>Procedimiento para la administración y gestión de los riesgos y las oportunidades en la Industria Militar Cód: IM OC OFF PR 018 Rev.12.</p>
	<p>Procedimiento Gestión Copias de Respaldo de Información Cód: IM OC OFI PR 006 Rev.10.</p>

CUWA

	Procedimiento para la Administración de Usuarios y Contraseñas Cód: IM OC OFI PR 001 Rev.8.
	Procedimiento Adquisición, Desarrollo y Mantenimiento Software Cód: IM OC OFI PR 002 Rev.6.
	Procedimiento Mantenimiento, Reutilización y Baja de Equipos y Medios Cód: IM OC OFI PR 013 Rev.5.
	Procedimiento Control Versiones de Software Cód: IM OC OFI PR 004 Rev.3.
	Procedimiento Controles Criptográficos. Cód: IM PC OFI PR 014 Rev.5.
	Procedimiento Gestión de Medios e Información en Transito Cód: IM OC OFI PR 005 Rev.6.
	Procedimiento Gestión de Incidentes de Seguridad de la Información Cód: IM OC OFI PR 007 Rev.12.
	Procedimiento Control de Vulnerabilidades Técnicas Cód: IM OC OFI PR 009 Rev.5.
	Procedimiento Gestión del Cambio Cód: IM OC OFI PR 010 Rev.5.
	Procedimiento de Monitoreo y Gestión de Logs Cód: IM OC OFI PR 012 Rev.6.
	Procedimiento Gestión de Riesgos y Oportunidades Seguridad de la Información Cód: IM OC OFI PR 015 Rev.10.
	Procedimiento Control de Software Cód: IM OC OFI PR 017 Rev.4.
	Procedimiento Gestión de la Capacidad Cód: IM OC OFI PR 018 Rev.3.
	Procedimiento Inventario y Clasificación de Activos de Información Cód: IM OC OFI PR 020 Rev.5.
	Procedimiento Control Equipos de Cómputo que se encuentran fuera de red Cód: IM OC OFI PR 019 Rev.3.
	Procedimiento Medición, Satisfacción y Expectativas de las partes interesadas del SGSI Cód: IM OC OFI PR 021 Rev.2.
	Instructivo creación y ejecución de políticas de respaldo para Symantec backup exec Cód: IM OC OFI IN 006 Rev.4.
	Instructivo instalación de agentes de backup DLO Cód: IM OC OFI IN 008 Rev.4.
	Instructivo monitoreo de la ejecución de la Política de Respaldo Cód: IM OC OFI IN 029 Rev.3.
	Instructivo creación y ejecución de políticas de respaldo para Symantec backup exec Cód: IM OC OFI IN 006 Rev.4.
	Instructivo Metodología y Estándares de Desarrollo de Software Cód: IM OC OFI IN 004 Rev.4.
	Documento 02.290.282 - Directiva Transitoria - Plan de Contingencia y Continuidad del Negocio para enfrentar la Emergencia Sanitaria por causa del COVID-19.
	Documento: 02.253.712 - Directiva Transitoria para el apoyo al personal- sus familiar y la normalización de la Operación en FEXAR.
	Documento: 02.266.900 - Correo COIMAS Administrativas en Indumil - actividad No.10.

UVK

<b>Antecedentes (9):</b>	Documento No. 02.246.724 - IM-OC-OCI Informe Auditoría al Proceso Gestión Informática - Adquisición e Implementación Proyectos III Fase de SAP y Módulo CRM SAP.
<b>Documentos Analizados (10):</b>	
<ul style="list-style-type: none"> <li>- Documento No. 02.303.911 - Información para la auditoria al Proceso Gestión informática del 18 de junio de 2020.</li> <li>- II - Comité Seguridad de la Información, 8 junio de 2020.</li> <li>- Anexo Caso 4715 Ampliación buzones servidor Exchange, 31 julio 2020.</li> <li>- Hoja de Vida Indicadores de Gestión - Gestión Informática, 20 febrero 2018.</li> <li>- Inventario equipos fuera de red, 22 septiembre 2020.</li> <li>- Licenciamiento Aranda Metrix, 22 septiembre 2020.</li> <li>- Casos GLPI, 9 de septiembre 2019 al 23 junio 2020.</li> <li>- GLPI - Catalogo Técnicos, 19 junio 2020.</li> <li>- GLPI - Anexo 1. Tabla de referencia, 19 junio 2020.</li> <li>- Informe Mesa de Ayuda – GLPI, 15 septiembre 2020.</li> <li>- Seguimiento Iniciativas Plan de Acción Institucional – PAI, 31 julio 2020.</li> <li>- Auditoria proveedores, vigencia 2017.</li> <li>- Auditoria proveedores, vigencia 2018.</li> <li>- Auditoria proveedores, vigencia 2019.</li> <li>- Programa de Auditoría a Proveedores 2020, 19 junio 2020.</li> <li>- Información Monitoreo capacidad, 31 julio 2020.</li> <li>- Anexo caso 1347 Disponibilidad para máquinas virtuales, 29 noviembre 2019.</li> <li>- Anexo caso 1424 Disponibilidad para máquinas virtuales, 31 diciembre 2019.</li> <li>- Anexo caso 4090 Disponibilidad para máquinas virtuales 30 abril 2019.</li> <li>- Anexo caso 4081 Disponibilidad para máquinas virtuales 31 marzo 2020.</li> <li>- Anexo synergy 02885817 Disponibilidad para máquinas virtuales 8 julio 2019.</li> <li>- Anexo synergy 02844350 Disponibilidad para máquinas virtuales 30 abril 2019.</li> <li>- Anexo synergy 02949788 Disponibilidad para máquinas virtuales 30 septiembre 2019.</li> <li>- Anexo synergy 03004200 Disponibilidad para máquinas virtuales 31 octubre 2019.</li> <li>- Synergy - segregación de funciones enviado por el proveedor, 29 agosto 2020.</li> <li>- Evidencia Matriz Vulnerabilidad synergy, 22 septiembre 2020.</li> <li>- Soporte remoto – Acceso remoto a los computadores, vigencias 2018, 2019 y 2020 hasta el 10 junio 2020.</li> <li>- Imágenes configuración correo electrónico, 19 junio 2020.</li> <li>- Matriz de Riesgos y Oportunidades Primer Cuatrimestre 2020 Gestión Informática, 17 julio 2020.</li> <li>- Cronograma de Actividades Respaldos, mes junio 2020.</li> <li>- Ejecución de respaldos, mes junio 2020.</li> <li>- Estado respaldos sitio alterno – pruebas de restauración de cintas de respaldo de información al 18 junio 2020.</li> <li>- Programación de respaldos diarios e imágenes de servidores, mes de junio y julio 2020.</li> <li>- Resolución No. 070 de abril de 2010 – creación del Comité Seguridad de la Información – CSI – Roles y Responsabilidades del SGSI Oficina de Informática.</li> <li>- Resolución No. 039 del 8 abril de 2011 – creación Comité Técnico de Seguridad de la Información – CTSI.</li> <li>- Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI.</li> <li>- Modelo de Seguridad y Privacidad de la información – MSPI.</li> <li>- Decreto 612 del 4 de abril de 2018 - Decreto 612 del 4 de abril de 2018 "Por medio del cual se fijan directrices para a Integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado" numeral 2.2.22.3.14.</li> </ul>	

WUK

- Documentos Gestión de Respaldos Abril 2020, Respaldos Fexar y Evidencias Ismael Versión del 6 de noviembre de 2020
- Documento No. 02.362.126 Logs de registro y errores Synergy 2019 a 2020 del 11 de noviembre de 2020.

**Resultados de la Auditoria y/o Evaluación (11)****Aspectos positivos (Fortalezas y/o prácticas destacables) (a):****Aplicación de Ethical Hacking y Remediación de las Vulnerabilidades para la vigencia 2020**

El proceso de Gestión Informática realiza la aplicación de los procedimientos de Ethical Hacking para la vigencia 2020 y Remediación de las Vulnerabilidades a través de un proveedor externo, que realizan pruebas de intrusión, pruebas de penetración o pentesting.

Ethical Hacking. Hacking Ético, sirve para explotar las vulnerabilidades existentes en el sistema que se requiere evaluar, valiéndose de un (test) una prueba de intrusión, que permite verificar y evaluar la seguridad física y lógica de sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, entre otros componentes de la infraestructura tecnológica, con la intención de ganar acceso y demostrar que un sistema es vulnerable.

Remediación. Acción que permite minimizar el impacto de las vulnerabilidades en la organización.

**Comentarios Generales y/o especiales (b):****1. APLICACIÓN EXACT E-SYNERGY – GESTIÓN DOCUMENTAL.**

En la auditoría desarrollada se evaluó la funcionalidad y controles del gestor Documental Exact E-Synergy, evidenciando:

- Con documento No. 02.303.911 del 18 de junio de 2020 la Oficina de Informática envía Manuales de usuario y de Administración en el cual informa: "Synergy centraliza sus manuales de configuración, administración y de usuario en línea, para acceder a ellos debemos dar clic sobre el botón ayuda ubicando en la parte superior derecha de cualquier página en la que nos encontremos, dando clic en él nos direccionara a la página del fabricante el cual nos llevara a una detallada descripción de las funcionalidades y servicios", al ingresar al botón ayuda se observa que son archivos de ayuda con los siguientes temas "Overview of workflow and requests, Product Update 254: Error message displayed for bulk action for Service management" donde al consultarlos se encuentra en ingles la descripción general del flujo de trabajo y las solicitudes informadas por el fabricante de la aplicación sin evidenciar los manuales de usuario y técnico apoyo para los usuarios de la aplicación en el aprendizaje y uso de está.
- La aplicación no tiene definido el administrador gestor documental el cual parametriza en la aplicación los documentos y el archivo conforme a las normas del archivo general de la nación, definir las series, sub-series documentales y tablas de retención y gestionar los cambios respectivos en el sistema; lo anterior lo está asumiendo el administrador técnico de la aplicación.

**1.1 Control de Acceso de los usuarios en Exact E-Synergy.** (Información suministrada en correo electrónico del 2 de junio de 2020 por el asesor del departamento comercial JNC – Tic Servicios 360 y documento en pdf "Details on Security Levels (1)").

"La aplicación permite que todos los usuarios tengan un nivel de seguridad en el sistema de Exact E-Synergy, cada usuario solo puede acceder a información con un nivel de seguridad igual o inferior a su propio nivel. Además del nivel de seguridad, cualquier usuario también puede ser miembro de uno o más roles funcionales que le otorgan derechos adicionales a este usuario en una parte específica del

LUX

programa Exact e-Synergy. La siguiente tabla resume el control de acceso a nivel de seguridad:

Nivel	Descripción	Usuarios que pueden acceder a la información
0	Todas	Todos los usuarios, incluidos los usuarios públicos.
1	Clientes	Todos los clientes, todos los socios y todos los recursos.
2	Socios – Socias	Todos los socios y todos los recursos.
3	Cliente (específico)	1. El cliente que es la cuenta vinculada a la información. 2. El revendedor del cliente vinculado a la información. 3. El socio que es la cuenta vinculada a la información. 4. Todos los recursos.
4	Socio (específico)	5. El revendedor del cliente en la solicitud. 6. El socio que es la cuenta en la solicitud 7. Todos los recursos.
5 al 9	Reservado	No utilizado
10 al 98	Interna	1. El creador o propietario de la información. 2. El actor del flujo de trabajo actual de la solicitud. 3. El recurso vinculado a la solicitud. 4. Todos los usuarios con una autorización de nivel de seguridad mayor o igual al nivel de seguridad de la información.
99	Creador	1. El creador de la información. 2. El actor de flujo de trabajo actual de la solicitud.
100	Recurso Especifico	1. El creador o propietario de la información. 2. El recurso vinculado a la información. 3. El gerente del Recurso vinculado a la información. 4. Recursos con Rol 11 - Recursos Humanos o Rol 12 - Asistente de Recursos Humanos basado en la División de Recurso vinculado a la información. 5. Todos los usuarios a los que se les han otorgado los derechos de visualización y / o edición en Ver, Derechos y Editar, derechos respectivamente al crear y / o modificar documentos.
101	Proyecto Especifico	1. El creador o propietario de la información. 2. Miembros del proyecto vinculados a la información. 3. Todos los usuarios a los que se les han otorgado los derechos de visualización y / o edición en Ver, Derechos y Editar, derechos respectivamente al crear y / o modificar documentos.

Los usuarios con el rol de administrador de nivel corporativo pueden ver toda la información independientemente de su nivel de seguridad, con excepción de la solicitud privada.

### Sobre el log.

El informe de registro de datos le permite rastrear todos los detalles de las modificaciones de datos que incluyen lo que se ha modificado, cuándo tuvieron lugar las modificaciones, cómo se modificaron los datos y quién los modificó. Puede definir uno o más criterios para obtener el informe de registro de datos".

### 1.2 Niveles de Seguridad para acceder a la información.

El 5 de agosto de 2020 la Oficina de Informática envió por correo electrónico el archivo llamado "Synergy - Segregación de funciones" generado por el administrador de la aplicación el 31 de julio de 2020 con las rutinas diseñadas en SQL por el proveedor B EXCELLENCE SAS., al realizar el análisis de la información contenida en el archivo, se pudo observar que:

- En la aplicación Exact E-synergy se han definido los siguientes niveles de seguridad:

Nivel de Seguridad en el Aplicativo Exact E-synergy
10
11
15
18
25
50
75
99

CUVA

En el procedimiento "Inventario y Clasificación de Activos de Información" Cód: IM OC OFI PR 020 Rev.5. numeral 4.1.5. *Clasificación de la Información*: "La información estará clasificada en cada documento de acuerdo a los siguientes niveles de seguridad establecidos en el Gestor Documental."

Grupo	Nivel de Seguridad
Todos	0
Cientes	1
Proveedores	2
Ciente Especifico	4
De uso Interno	10
Reservada para jefes de grupo	25
Reservada para jefes de División	50
Reservada para Grupo Gerencia	75
Reservado para la Gerencia General	99

Evidenciando que en la aplicación Exact E-synergy se crearon tres grupos con niveles de seguridad 11, 15 y 18 que no están definidos en el numeral 4.1.5. "Clasificación de la Información", así.

**Nivel de Seguridad No. 11.**

Nombre Completo	Cargo según Exact E-synergy
Leyda Nelcy Aguirre Martínez	Profesional Especializado Of.Informatica
Oriana Milena Ramírez Gallego	Profesional Of.Juridica
Leidy Yuliana Peña Fontecha	Profesional Of.Juridica
John Jenry Ayala Guio	Profesional Especializado Of.Planeación
Jonathan Alfredo Caro Sarmiento	Profesional Of.Juridica
Jhaydy Mileyby Rodriguez Parra	Profesional Of.Juridica

**Nivel de Seguridad No. 15.**

Nombre Completo	Cargo según Exact E-synergy
Gloria Amparo Martín López	Profesional Of.Control Interno
John Jairo Antonio Virgüez Liévano	Profesional Of.Control Interno
Laura Liliana Echeverria Mora	Analista Of.Control Interno

**Nivel de Seguridad No. 18.**

Nombre Completo	Cargo según Exact E-synergy
Yadira Patricia Sánchez Zamudio	Profesional Especializado Of.Informatica
Leonor Cecilia Amado Agón	Secretaria Of.Informatica
Orlando Baquero Parra	Profesional Especializado Of.Informatica
Juan Carlos Consuegra Ballen	Programador Computador Of.Informatica
Jorge Alberto Arocha Muñoz	Jefe de Oficina Of.Informatica
Wilmer Alfonso Bautista Maldonado	Profesional Oficina de informática
Jair Orlando Fajardo Fajardo	Subgerente Financiero
Luisa Fernanda Pulido Paéz	Programador Computador Of.Informatica

LUC

- Teniendo en cuenta los niveles de seguridad establecidos en el Gestor Documental, la clasificación de la información no está de acuerdo a los grupos informados en el numeral 4.1.5. "Clasificación de la Información", así:

**Grupo Información "Reservada para jefes de grupo", nivel de seguridad 25:**

Nombre Completo	Cargo según Exact E-synergy
Bernardo Patino Barrera	Jefe de planta Mantenimiento Industrial
María Dora Morales Gómez	Jefe de división Administrativa Fabrica
Adriana Olaya Valencia	Jefe de Planta Explosivos Militares y Acc.
Hayrlen Hernández Carreño	Jefe de Taller Seg. Industrial - Salud Ocupacional
Yudy Bibiana Alfonso	Jefe de Archivo S.General
Juan Eliseo Sánchez Amaya	Jefe de Grupo Control Calidad Fabrica
Luis Antonio Sierra Castro	Jefe de Planta Exp.Ciales y Nitroderivados
Sergio Alberto Villada Agudelo	Jefe de Grupo

Se generó del sistema SAP / S4 HANA - Nómina el 23 septiembre de 2020 el archivo "Listado de Personal" y se encontró que el cargo de Jefes de Grupo se encuentra conformado por los siguientes funcionarios:

Nombre Completo	Cargo según Módulo de Nómina
Limas Patino Jaime	Jefe Grupo Ingeniería técnica FASAB
Villada Agudelo Sergio A	Jefe Grupo planeación
Sarmiento Roza Carlos Enrique	Jefe Grupo Ingeniería técnica FEXAR
Morales Gómez María Dora	Jefe Grupo relaciones industriales
Romero Granados Lupe Consuelo	Jefe Grupo relaciones industriales
Bernal Bernal Humberto	Jefe Grupo evaluación y control
Ávila Osorio Sandra Milena	Jefe Grupo control calidad
Galvis Murillo Oscar Mauricio	Jefe Grupo Oficina de planeación
Lopez Medina Edward Zamir	Jefe Grupo Ingeniería técnica FAGECOR
Sánchez Amaya Juan Eliseo	Jefe Grupo control calidad
Pinilla Ramírez María Fernanda	Jefe Grupo comercio exterior
Chaparro Ordóñez Mónica Edy	Jefe Oficina jurídica
Rodriguez Garay Natalia	Jefe Grupo contratos
Gaicedo Rocha Etna Margarita	Jefe Grupo control calidad
González Cortes Yuly Mireya	Jefe Grupo seguridad industrial

**Grupo Información "Reservada para jefes de División", nivel de seguridad 50:**

Nombre Completo	Cargo según Exact E-synergy
Luis Alberto Espejo Velandia	Jefe división producción Fabrica
Leonardo Villalobos Alvarado	Jefe de división Administrativa Fabrica
German Isalañas Niño Rodríguez	Jefe división Almacenes Comerciales

CLK

Ronald Jamilton Moreno Samaniego	Jefe de Oficina Of.Planeación
Wilson Ernesto Cucunubo Muñoz	Jefe Oficina Ing. Industrial
Juan Carlos Mosquera Astorquiza	Jefe de división Administrativa Fabrica
Carlos Enrique Sarmiento Rozo	Jefe de Grupo G. Ingeniería Fabrica
Jaime Limas Patino	Jefe de Grupo G. Ingeniería Fabrica
Lupe Consuelo Romero Granados	Jefe de grupo Rel. Industriales Fabrica
Nidia Padilla Valdés	Jefe de Oficina Of.Juridica
Natalia Rodriguez Garay	Jefe Grupo contratos
Martha Cecilia Polania Ipuz	Jefe Oficina De Control Interno
Andrea Del Pilar Corredor Gómez	Jefe división D. Personal
José Wilson Orjuela Avilan	Jefe división D. Adquisiciones
Rubén Darío Sánchez Martínez	Jefe división producción Fabrica
Juan Ángel Palacios Rodriguez	Jefe Div. Operaciones Financieras
Cesar Augusto García Cruz	Jefe Div. Contabilidad
Luis Eduardo Aguirre Garay	Jefe división S. Generales
Raúl Gonzalo Ardila Bellaizan	Jefe división Presupuestos
Edward Zamir Lopez Medina	Jefe de Grupo G. Ingeniería Fabrica

Se generó del sistema SAP / S4 HANA - Nómina el 23 septiembre de 2020 el archivo "Listado de Personal" y se encontró que el cargo de Jefes de División se encuentra conformado por los siguientes funcionarios:

Nombre Completo	Cargo según Módulo de Nómina
Palacios Rodriguez Juan Ángel	Jefe División operaciones financieras
Sánchez Martínez Rubén Darío	Jefe División de producción
Aguirre Garay Luis Eduardo	Jefe División servicios generales
Villalobos Alvarado Leonardo	Jefe División administrativa
Ardila Bellaizan Raúl Gonzalo	Jefe División presupuesto
Espejo Velandia Luis Alberto	Jefe División de producción
Orjuela Avilan José Wilson	Jefe División adquisiciones
Cruz Pulido Jesús David	Jefe División de producción
Mosquera Astorquiza Juan Carlos	Jefe División administrativa
Corredor Gómez Andrea del Pilar	Jefe División administración de personal
Pineda Molina Daniela	Jefe División mercadeo
Lopez Alarcón Juan Carlos	Jefe División Ingeniería industrial
Nino Rodriguez German Isaías	Jefe División almacenes comerciales
Baquero Rodriguez Wilson Fernando	Jefe División de investigación y desarrollo tec.
García Cruz Cesar Augusto	Jefe División de contabilidad
Cortes Rúgeles Juan Carlos	Jefe División administrativa

**Grupo Información "Reservada para Grupo Gerencia", nivel de seguridad 75:**

Nombre Completo	Cargo según Exact E-synergy
Reiber Faner Guzmán Cabrera	Director de Fabrica

LWZ

Rubén Alonso Mogollón Araque	Director de Fabrica
Rodrigo Salazar Echeverri	Subgerente técnico
Heli Rojas Robles	Subgerente Financiero
Nelson Hernando Rojas Rojas	Sub Gerente Comercial
María Del Pilar Serrano Buendía	Subgerente Administrativo
Javier Alfonso Molina Calero	Director de Fabrica

Adicionalmente, se generó del sistema SAP / S4 HANA - Nómina el 23 septiembre de 2020 el archivo "Listado de Personal" y se encontró que el Grupo de Gerencia se encuentra conformado por los siguientes funcionarios:

Nombre Completo	Cargo según Módulo de Nómina
Nidia Padilla Valdés	Jefe Oficina Jurídica
Ronald Jamilton Moreno Samaniego	Jefe Oficina de Planeación
Javier Alfonso Molina Calero	Director FAGECOR
Rubén Alonso Mogollón Araque	Director FASAB
María del Pilar Serrano Buendía	Subgerente Administrativa
Rodrigo Salazar Echeverri	Subgerente Técnico
Reiber Faner Guzmán Cabrera	Director FEXAR
José Leónidas Espitia Duarte	Director Seguridad Física
Nelson Hernando Rojas Rojas	Subgerente Comercial
Hernando Wills Vélez	Gerente General
Jorge Alberto Arocha Muñoz	Jefe Oficina de Informática
Jair Orlando Fajardo Fajardo	Subgerente Financiero
Martha Cecilia Polania Ipuz	Jefe Oficina de Control Interno

Evidenciando inconsistencias en el manejo y control de los activos de información según su nivel de clasificación afectando la integridad, confidencialidad y oportunidad de la información.

### 1.3 Roles funcionales que le otorgan derechos adicionales al usuario.

Realizado el análisis de la información contenida en el archivo "Synergy - Segregación de funciones" suministrado por la Oficina Informática por correo electrónico del 5 agosto de 2020 generado por el administrador de la aplicación el 31 julio de 2020 con las rutinas diseñadas en SQL por parte del proveedor B EXCELLENCE SAS., se pudo observar que se han creado en la aplicación Exact e-synergy ciento un (101) roles funcionales definidos para la Industria Militar, a continuación se relacionan:

ROLES FUNCIONALES			
A Cerrar por (req SAM)	Crea requerimiento creación de códigos Req 9929	Informes Control Interno	Subgerencia Administrativa
Administración de interfaces	Crea Resoluciones Jurídicas	Item management	Subgerencia Comercial
Administrador Synergy Enterprise	Creacion Orden de Reclamo por Calidad	Jefe de Mercadeo	Subgerencia Tecnica
Administrador	Crear Proyectos	Jefe Grupo Control Calidad	Tramita Homologación Dirección
Aprobador Reporte Novedades de Planta y Misión	Customer manager	Jefe Informatica	Tramita Homologación División Producción
Aprobación Noticias a Proveedores	Diligencia vista contables materiales Req 9929	Jefe Inmediato - edición Documentos	Tramita Homologación GIN
Aprobar Entrante con y sin Observación Gdal	Diligencia vista ventas materiales Req 9929	Jefe Jurídica	Tramita Homologación Sub. Técnica
Aprobar Homologación Sub. Técnica	Director Fábrica	Jefe Oficina De Seguridad	Tramita Requisición de Cargo

WUK

Aprobar Noticias	Doc_Convenios	Jefe Servicios Generales	Usar Imprimible
Aprobar Respuesta Homologación	Document approver	Jefe Talento Humano	Usuario Grupos Empleados Públicos
Aprobar Viáticos Administrativa	Edicion documentos SGC	Jefe Técnica	Usuario Synergy
Aprobar Viáticos Recursos Humanos	Edilar Documentos	Junta Directiva Rol	Ver Documentos Archivo
Aprueba Requisición de Cargo	Editar Proyectos	LM - Proceso Gestión Informática	Ver flujo recurso específico
atención A Proveedores	Enabling add-on solutions	Mostrar Boton Estadísticas FT	Ver Oferta Economica
atención Ciudadana	Encuesta Necesidades	Observaciones a Procesos (Req 1000)	Ver todos los documentos entrantes
Audidores Calificados en Calidad	Enl_Doc_Contratación	Oficial de Seguridad de la Información	Verificación Acciones Tomadas
Audidores en Formación en Calidad	Estadigrafo	Oficina Informatica	View administrator
Audidores Líderes en Calidad	Evaluador plan de accion (SAM Creacion)	Production manager	Visualiza evidencias-Plan de Accion SAM
Aut_Doc_Contratación	Finca Raiz	Project administrator	Visualiza Planos
Autorizacion Prorrogas Fecha Actividades SAM	Firma Digital	Prorrogas (Dueños de proceso)	Visualizar Convenios
Cobranzas	Gestor Pruebas Software	Recepción Encuesta	Visualizar Doc. Contratacion
Control - Administración de Software	Grupo Administrador Documentos SGC	Responsable Auditorías	Visualizar Doc. Finales y Acuerdos
Control Interno	Grupo Selección y Contratación	RH Incapacidades	Visualizar Doc. Jurídica
Controller	HR	Secretaría General	
Crea codigo SAP Req 8929	HR assistant	Secretaría Jurídica	
Crea Homologación	Informacion Adquisiciones	Solicitudes a Of Jurídica	

El 23 septiembre de 2020 la Oficina de Informática envió por correo electrónico el archivo llamado "Indumil roles y derechos – Gestor Documental Synergy" generado por el proveedor B EXCELLENCE SAS el 22 de septiembre de 2020 donde relaciona los roles y sus derechos de función (actividades que puede realizar cada Rol), al realizar el análisis selectivo de algunos roles y sus derechos de función de la información contenida en el archivo, se pudo observar que:

- El Rol No. 0 "Administrador" del aplicativo Exact e-synergy se encuentra asignado a cuatro (4) funcionarios con treinta y cuatro (34) derechos de función.

No. Rol/Descripción Rol	Empleado	Cargo
<b>0 / Administrador</b>	Administrador e-Synergy	Gerente
	Juan Pablo Sandoval Ospina	Profesional Secretaria general
	Leonor Cecilia Amado Agón	Secretaria Of.Informatica
	John Jefferson Cante Caicedo	Programador Computador Of.Informatica
<b>Derechos de Funciones</b>		
Mantener repositorio	Permite reparar códigos de factura y selección	
Permite reconstruir el repositorio	Permite reparar las iniciales de los contactos para la división o la base de datos completa	
Mantener el acceso del servidor web al servidor de la base de datos	Permite actualizar la personalización de la tarjeta de cuenta de toda la empresa	
Permite ver todos los elementos (acceso de administrador)	Permite la limpieza por lotes de documentos	
Mantener la configuración de CRM	Mantener la configuración de la división / empresa de oportunidades	
Editar todos los tipos de solicitud	Permite realizar tareas de duplicación de cuentas / contactos	
Permite ejecutar la aplicación de calificación en segundo plano	Mantener sinónimos	
Mantener índices en campos libres	Permitir restablecer el trabajo en segundo plano que falló inesperadamente	
Mantener la configuración de alojamiento de la base de datos	Permitir anclar el espacio de trabajo para otros	

LWZ

Eliminar todas las solicitudes de un tipo específico, junto con la solicitud	Permitir crear, editar y configurar el espacio de trabajo predeterminado de la empresa
Permite modificar el código de cuenta	Acceda a la página Exact Lightweight Integrativo Server Monitor
Edite todas las pruebas y configuraciones de prueba	Permitir crear y editar grupos obligatorios
Mantenga la visibilidad del campo de la cuenta de CRM	Permitir validar números de IVA a granel
Permite personalizar términos	Permitir establecer la propiedad de noticias en un grupo
Mantener los niveles de inventario del almacén	Permitir habilitar secuencias de comandos para insertar widget
Mantener unidades de artículo	Permitir habilitar el envío de formularios a Embed Widget
Mantener las ubicaciones de los almacenes	Permitir ver el registro de licencias

- El Rol No. 11 "HR – Recursos Humanos" del aplicativo Exact e-synergy se encuentra asignado a dos (2) funcionarios con ciento veintisiete (127) derechos de función, se relacionan algunos derechos.

No. Rol/Descripción Rol	Empleado	Cargo
11 / HR	Administrador e-Synergy	Gerente
	Adriana María Chávez Peñaloza	Auxiliar de Oficina S.General

Derechos de Funciones
Cree todos los tipos de solicitud, independientemente del tipo de solicitud definido
Editar todas las solicitudes abiertas
Reabrir todas las solicitudes
Eliminar todas las solicitudes
Cree tipos de solicitud y edite tipos de solicitud sin responsable
Ver tareas (incluido el flujo de trabajo) para empleados específicos
Ver solicitudes de empleado
Permite crear empleados
Mantener roles
Reconstruir el flujo de trabajo de la solicitud
Ver todas las solicitudes de empleados en la división

- El Rol No. 53 "Aprobador de documentos" del aplicativo Exact e-synergy se encuentra asignado a ocho (8) funcionarios con doce (12) derechos de función

No. Rol/Descripción Rol	Empleado	Cargo
53 / Aprobador de Documentos	Adriana María Chávez Peñaloza	Auxiliar de Oficina S.General
	Nubia Maritza Vargas Zarate	Auxiliar de Oficina S.General
	Yudy Bibiana Alfonso	Jefe de Archivo S.General
	John Martin Acevedo Rojas	Supervisor S.General
	Yonathan Jesús Alfonso Guerrero	Auxiliar de Oficina S.General
	Martha E García Cañón	Secretaria Ejecutiva Fabrica
	Sonia Patricia González Ardila	Secretaria Ejecutiva Fabrica
	Cindy Joan Pinzón Rodríguez	Auxiliar de Oficina S.General

Derechos de Funciones
Permite aprobar documentos

CWK

Permite al aprobador de documentos de nivel corporativo aprobar documentos
Permite al aprobador de documentos a nivel de grupo aprobar documentos
Permite archivar documento
Permite rechazar documento
Permite restaurar documento
Permite borrar documento
Permite al aprobador de documentos a nivel de división aprobar documentos
Permite leer documentos - aprobador incluido Joblevel
Mostrar el botón Aprobar en la vista del documento
Ver aprobaciones de documentos
Mantener documento por administrador

- El Rol No. 70 "Administrador de Proyectos" del aplicativo Exact e-synergy se encuentra asignado a un (1) funcionarios con diez (10) derechos de función.

No. Rol/Descripción Rol	Empleado	Cargo
<b>70 / Administrador de Proyectos</b>	Carmen Yaneth Castillo León	Profesional D. Presupuestos
<b>Derechos de Funciones</b>		
Mantenga etiquetas de campos libres y vea el informe de actividad laboral		
Cree, modifique, elimine y copie proyectos cuando se cumpla el criterio de Función Right 603.		
Mantener la configuración del proyecto		
Ver tarjeta de transacciones de proyectos		
Carga XML: Proyecto		
Descarga XML: Proyectos		
Ver documentos específicos del proyecto		
Permite actualizar la personalización de la pantalla de entrada de horas de la empresa		
Ver realizaciones de proyectos		
Solo visible para miembros		

- El Rol No. 1000 "Secretaria General" del aplicativo Exact e-synergy se encuentra asignado a ocho (8) funcionarios con dos (2) derechos de función.

No. Rol/Descripción Rol	Empleado	Cargo
<b>1000 / Secretaria General</b>	Guillermo Laverde Rendon	Secretario General
	Yonathan Jesús Alfonso Guerrero	Auxiliar de Oficina S.General
	Martha E García Cañón	Secretaria Ejecutiva Fabrica
	Adriana María Chávez Peñaloza	Auxiliar de Oficina S.General
	Nubia Maritza Vargas Zarate	Auxiliar de Oficina S.General
	Sonia Patricia González Ardila	Secretaria Ejecutiva Fabrica
	Yudy Bibiana Alfonso	Jefe de Archivo S.General
	John Martin Acevedo Rojas	Supervisor S.General
<b>Derechos de Funciones</b>		
		Permite borrar documento

LUR

Permite al aprobador de documentos a nivel de división aprobar documentos

- El Rol No. 1002 "Aprobar Entrante con y sin Observacion Gcial" del aplicativo Exact e-synergy se encuentra asignado a ocho (3) funcionarios con un (1) derecho de función.

No. Rol/Descripción Rol	Empleado	Cargo
1002 / Aprobar Entrante con y sin Observacion Gcial	Guillermo Laverde Rendon	Secretario General
	Martha E Garcia Cañón	Secretaria Ejecutiva FAGECOR
	Sonia Patricia González Ardila	Secretaria Ejecutiva FEXAR
<b>Derechos de Funciones</b>		
Reabrir todas las solicitudes		

- De los ciento un (101) roles funcionales definidos para la Industria Militar no se pudo identificar los derechos de funciones a ochenta y nueve (89) roles debido a que no se encontraron en el archivo "Indumil roles y derechos - Gestor Documental Synergy" generado por el proveedor B EXCELLENCE SAS el 22 de septiembre de 2020 y entregado por la Oficina de Informatica el 23 septiembre de 2020, a continuación se relacionan:

Nro. Registro	Nro. Rol	Descripción Rol	Nro. Usuarios asignado el Rol
1	92	Usuario Synergy	565
2	93	Habilitación de soluciones complementarias	230
3	210	Responsable Auditorias	1
4	850	Ver administrador	1
5	1001	Aprobar Noticias	1
6	1003	Usar Imprimible	2
7	1004	Editar Documentos	13
8	1005	Ver todos los documentos entrantes	15
9	1006	Usuario Grupos Empleados Públicos	7
10	1007	Administracion de interfases	1
11	1100	Oficina Informatica	16
12	1102	Aprobación Noticias a Proveedores	1
13	1120	Jefe Informatica	1
14	1125	Creacion Orden de Reclamo por Calidad	6
15	1126	Subgerencia Tecnica	1
16	1127	Verificacion Acciones Tomadas	6
17	1128	Subgerencia Comercial	1
18	1129	Jefe Grupo Control Calidad	3
19	1130	Jefe de Mercadeo	1
20	1131	Audidores Lideres en Calidad	21
21	1132	Audidores Calificados en Calidad	14
22	1133	Auditores en Formación en Calidad	40
23	1141	RH Incapacidades	2
24	1150	Edicion documentos SGC	10
25	1151	Grupo Administrador Documentos SGC	13

CWIK

26	1155	Encuesta Necesidades	2
27	1160	Ver Documentos Archivo	3
28	1166	atención Ciudadana	2
29	2500	Secretaría Jurídica	1
30	2600	Solicitudes a Of Jurídica	2
31	2680	Jefe Jurídica	2
32	2690	Firma Digital	93
33	2700	Observaciones a Procesos (Req 1000)	2
34	2710	Control Interno	1
35	2711	Informacion Adquisiciones	1
36	3001	Editar Proyectos	146
37	3002	Ver Oferta Económica	6
38	3003	Visualizar Doc. Contratacion	355
39	3010	Finca Raiz	1
40	3012	Oficial de Seguridad de la Información	1
41	3016	Aprueba Requisición de Cargo	2
42	3017	Tramita Requisición de Cargo	1
43	3021	Crea Homologación	1
44	3022	Tramita Homologación Sub. Técnica	1
45	3023	Tramita Homologación Dirección	3
46	3024	Tramita Homologación División Producción	3
47	3025	Tramita Homologación GIN	3
48	3026	Aprobar Respuesta Homologación	1
49	3028	Aprobar Homologación Sub. Técnica	1
50	3029	Control - Administración de Software	2
51	3033	Aut_Doc_Contratacion	1
52	3034	Ent_Doc_Contratación	1
53	3036	Subgerencia Administrativa	1
54	3038	Jefe Talento Humano	1
55	3040	Administrador Synergy Enterprise	1
56	3050	Jefe Inmediato - Edicion Documentos	5
57	3051	Mostrar Boton Estadísticas FT	4
58	3052	Gestor Pruebas Software	5
59	3053	Visualizar Doc. Finales y Acuerdos	1
60	3054	Aprobar Viáticos Administrativa	1
61	3055	Aprobar Viáticos Recursos Humanos	1
62	3275	Autorizacion Prorrogas Fecha Actividades SAM	5
63	3280	Estadigrafo	5
64	3281	Director Fábrica	3
65	3282	Jefe Técnica	1
66	3283	Visualizar Doc. Jurídica	1
67	3284	Recepción Encuesta	1
68	3300	A Cerrar por (req SAM)	67
69	3301	Evaluador plan de accion (SAM Creacion)	54
70	3302	LM - Proceso Gestión Informática	24

*ivall*

71	3303	atención A Proveedores	1
72	3304	Grupo Selección y Contratación	9
73	3305	Jefe Oficina De Seguridad	1
74	3311	Jefe Servicios Generales	1
75	3312	Crea Resoluciones Jurídicas	3
76	3313	Junta Directiva Rol	2
77	3314	Prorrogas (Dueños de proceso)	14
78	3315	Visualiza Planos	24
79	3316	Cobranzas	4
80	3317	Informes Control Interno	1
81	3318	Doc_Convenios	2
82	3319	Visualizar Convenios	1
83	3320	Ver flujo recurso especifico	2
84	3324	Visualiza evidencias-Plan de Accion SAM	4
85	3325	Crea requerimiento creación de códigos Req 9929	16
86	3326	Diligencia vista ventas materiales Req 9929	2
87	3327	Diligencia vista contables materiales Req 9929	2
88	3328	Crea codigo SAP Req 9929	2
89	3329	Apobador Reporte Novedades de Planta y Misión	2

Evidenciando inconsistencias en la creación de roles y asignación de derechos de funciones en la aplicación Exact E-synergy afectando la integridad, confidencialidad y disponibilidad de la información.

#### 1.4 Seguridad de la información aplicación Exact E-Synergy.

##### 1.4.1 Funcionarios que tienen acceso a editar y/o ver todos los documentos entrantes.

No.	NOMBRE FUNCIONARIO	NIVEL DE SEGURIDAD	CARGO	ROL ASIGNADO
1	Adriana María Chávez Peñaloza	10	Auxiliar de Oficina S.General	Editar y Ver todos los documentos entrantes.
2	Cindy Joan Pinzón Rodriguez	10	Auxiliar de Oficina S.General	Ver todos los documentos entrantes.
3	Diego Alejandro Vargas Duarte	10	Profesional G. Ingeniería Fabrica FEXAR	Editar documentos
4	Guillermo Laverde Rendon	10	Secretario General	Editar y Ver todos los documentos entrantes.
5	Israel Antonio Diaz Macias	10	Profesional Laboratorios Of.Planeación	Editar documentos.
6	Javier Alfonso Molina Calero	75	Director de Fabrica FAGECOR	Ver todos los documentos entrantes.
7	Johnny Moncada Ávila	10	Analista ingeniería del producto Fagecor	Editar documentos.
8	John Martin Acevedo Rojas	10	Supervisor S.General	Editar y Ver todos los documentos entrantes.
9	Jorge Leonardo Rojas Bello	10	Dibujante G. Ingeniería Fabrica FAGECOR	Editar documentos.
10	José Andrés Velásquez Castro	10	Profesional G. Ingeniería Fabrica FEXAR	Editar documentos.
11	Julia Nohelia Téllez Vanegas	10	Profesional División	Ver todos los documentos

LUK

			Administrativa	entrantes.
12	Laura Yesenia Lamus González	10	Auxiliar de Oficina S.General	Ver todos los documentos entrantes.
13	Manuel Antonio Arévalo Betancur	10	Profesional G. Ingeniería Fabrica FEXAR	Editar documentos.
14	María Oliva Rodríguez Parra	10	Secretaria Ejecutiva G. General	Editar documentos.
15	Martha E García Cañón	10	Secretaria Ejecutiva Fabrica Fagecor	Editar documentos.
16	Nubia Maritza Vargas Zarate	10	Auxiliar de Oficina S.General	Editar y Ver todos los documentos entrantes.
17	Reiber Faner Guzmán Cabrera	75	Director de Fabrica	Ver todos los documentos entrantes.
18	Rodrigo Salazar Echeverri	75	Subgerente técnico	Ver todos los documentos entrantes.
19	Sergio Alberto Villada Agudelo	25	Jefe de Grupo Of.Planeación	Editar y Ver todos los documentos entrantes.
20	Sonia Patricia González Ardila	10	Secretaria Ejecutiva Fabrica XXX	Editar y Ver todos los documentos entrantes.
21	Yonathan Jesús Alfonso Guerrero	10	Auxiliar de Oficina S.General	Ver todos los documentos entrantes.
22	Yudy Bibiana Alfonso	25	Jefe de Archivo S.General	Ver todos los documentos entrantes.

**1.4.2 Documentos de la aplicación Exact E-synergy que se pueden ver sin ser observados. Algunos casos son:**

No.	Número Dcto	Asunto	Número Serie Documental / Proyecto	Nombre Funcionario que tiene acceso sin ser observado
1	02.202.957	IRREGULARIDADES DE TIPO ADMINISTRATIVO EN FASAB	56 - Otros	Aura Alicia Acevedo - Analista FASAB. Yolanda Inés Córdoba Guarín - Analista FASAB. Claudia Rosio Flórez - Auxiliar Ingeniera Industrial FASAB.
2	02.203.564	QUEJA EN CONTRA DEL TIPO ADMINISTRATIVO Y MANEJO DE PERSONAL EN FASAB	56 - Otros	Claudia Rosio Flores Boyacá - Auxiliar Ingeniera Industrial FASAB. Fábrica FASAB.
3	02.214.910	IM-OC-OCI Entrega Archivo Magnético - Carpeta Informe de Auditoría al Almacén Comercial D011 Sogamoso No. 02.170.674	Inf.OCI FASAB	Emilce Acero León - Analista Grupo Control Calidad. Claudia Rosio Flórez - Auxiliar Ing. Industrial. Yolanda Inés Córdoba Guarín - Analista FASAB. María Eugenia Zambrano - Analista FASAB.
4	02.331.978	CORREO TRASLADO POR COMPETENCIA	43 - Peticiones, Quejas, Reclamo y Sugerencias	Angelica Diaz Orjuela - Subgerencia Técnica
5	02.331.781	CORREO INICIO PROCESO DE HOMOLOGACIÓN	26 - Homologaciones	Yuli Mireya González Cortes - Subgerencia Técnica - HSE
6	02.329.951	COTIZACIÓN	56 - Otros	Yuli Mireya González Cortes - Subgerencia Técnica - HSE
7	02.256.211	PROYECTO 8749 PÓLIZAS DE	8749 - ADECUACIÓN DE LA OFICINA GIN	Yuli Mireya González Cortes - Subgerencia Técnica - HSE

WVK

		CUMPLIMIENTOS Y RESPONSABILIDAD CIVIL CTO 1-238-2019 HCG CONSTRUCCIONES LTDA	FAGECOR	
8	02.319.868	CORREO PETICIÓN RECONOCIMIENTO BONO PENSIONAL	43 - Peticiones, Quejas, Reclamo y Sugerencias	Lizeth Soto Hernández - Subgerencia Financiera
9	02.331.775	CORREO INICIO PROCESO DE HOMOLOGACIÓN	26 - Homologaciones	Bibiana Andrea Gallego Nieto - Oficina Control Interno
10	02.331.766	CORREO TRASLADO POR COMPETENCIA NOTIFICACIÓN ACCIÓN DE TUTELA	43 - Peticiones, Quejas, Reclamo y Sugerencias	Jonatan Alfredo Caro Sarmiento Auxiliar Oficina Jurídica Bibiana Andrea Gallego Nieto - Analista - Oficina Control Interno
11	02.334.940	CORREO PETICIÓN DE INFORMACIÓN REGISTRO NACIONAL DE OBRAS CIVILES INCONCLUSAS	56 - Otros	Bibiana Andrea Gallego Nieto - Analista - Oficina Control Interno
12	02.332.003	CORREO INFORMACIÓN PAGO DEL 20 AGOSTO 2020 A QUE PERTENECE PARA APLICAR	56 - Otros	Yaneth Tarapues Montenegro - Profesional en Misión - Oficina Control Interno
13	02.331.999	CORREO SOLICITUD DOCUMENTOS	56 - Otros	Yaneth Tarapues Montenegro - Profesional - Oficina Control Interno
14	02.337.561	CORREO AVANCE CON RESPECTO A LAS ACTIVIDADES ENTREGA CAMIONES CONTRATO ARRENDAMIENTO DE CAMIONES (MMU) ORICA COLOMBIA S.A.S. 3 DE JULIO 2019	56 - Otros	Yaneth Tarapues Montenegro - Profesional en Misión - Oficina Control Interno
15	02.256.171	400002380 FACTURA ELECTRÓNICA	828 - Facturas	Yaneth Tarapues Montenegro - Oficina Control Interno
16	02.256.215	PROYECTO 8507 PÓLIZA DE CUMPLIMIENTO Y RESPONSABILIDAD CIVIL O.C 4500005610 CRAING LIMITADA	8507 - Adecuación y mantenimiento de la infraestructura física de l	Yaneth Tarapues Montenegro - Profesional en Misión - Oficina Control Interno
17	02.256.200	PROYECTO 8807 PÓLIZA DE CUMPLIMIENTO O.C 4500005460 Y 4500005461 AS. ELASTOMEROS SAS	807 - TAPAS PARA EMPAQUE ARMAS CORTAS VIG. 2020	Yaneth Tarapues Montenegro - Profesional en Misión - Oficina Control Interno
18	02.331.898	E1354 FACTURA ELECTRÓNICA	828 - Facturas	Gloria Amparo Martín López - Profesional en Misión - Oficina Control Interno
19	02.337.374	CORREO CERTIFICADO DE LA ESTACIÓN DE SERVICIO INDUMIL	56 - Otros	María Alejandra García Dueñas - Profesional en Misión - Oficina Control Interno
20	02.256.175	3748 FACTURA ELECTRÓNICA	828 - Facturas	María Alejandra García Dueñas - Profesional en Misión - Oficina

CUR

				Control Interno
21	02.308.372	CORREO RESPUESTA DOCUMENTO 02.298.395	56 – Otros	Ivis Gálvez Gálvez - Auxiliar División de Mercadeo
22	02.309.673	CORREO SOLICITUD AVANCES EN LA FORMULACIÓN DE LOS PROYECTOS DE INVERSIÓN DE LAS EICE Y SEM - INDUMIL.	56 – Otros	Sebastián Orjuela Valderrama – Profesional División de Producción.
23	02.310.543	CORREO RESPUESTA A OFICIO 02.304.561	56 – Otros	Liliana Acevedo Gutiérrez - operario Seguridad Industrial y Salud Ocupacional.
24	02.310.903	CORREO VIDEOCONFERENCIA BLACKBOARD	56 – Otros	Lina Giselle Ajiaco Song Auxiliar Oficina Secretaria General

**Nota.** Lo informado son algunos casos que selectivamente fueron verificados, la aplicación permite ver los documentos con números serie documental (26 - Homologaciones, 56 – Otros, 828 - Facturas, Proyectos, 43 - Peticiones, Quejas, Reclamo y Sugerencias) sin ser observados.

**1.4.3 Documentos de la aplicación Exact E-synergy que se pueden modificar después de ser tramitados, en prueba realizada permitió que se actualizará documento del año 2014 – soporte llamado “documento No. 01.616.251 del año 2014”**

El 11 de diciembre de 2019 el proveedor de synergy a través de correo electrónico informa que se encontró una alternativa para dar solución (de los documentos creados y observados a otros usuarios, a pesar de ello se pueden realizar cambios), relacionando al administrador del synergy en la Industria Militar los pasos para implementar la solución.

La Oficina de informática genera el caso al gestor de infraestructura, capacidad y disponibilidad en mesa de ayuda con ID 1214 del 16 de diciembre de 2019, solicitando copiar en el servidor de pruebas un archivo. aspx y un script para SQL. Se copia archivo XML indicado a la ubicación Synergy\Docs.

El 16 de enero de 2020 realizan las pruebas en el ambiente de pruebas por parte de la oficina de informática el gestor de servidores, gestor de pruebas y administrador del synergy (esta como programador computadores), el objetivo de esta prueba era comprobar que no se puede modificar un documento una vez se asigna a un flujo de trabajo, como evidencia informática entregó el archivo - Cód. IM OC OFI FO 010, donde se encuentra: 1. Diseño de la prueba, 2. Plan de ejecución y reversión de la prueba, 3. Evaluación de la prueba y anexo de las evidencias con los resultados de los cambios solicitados, cumpliendo con lo establecido en el Procedimiento Adquisición, Desarrollo y Mantenimiento de Software Cod: IM OC OFI PR 002 Rev.6. numeral 4.6 Aceptación de los Sistemas de Información.

En la matriz de vulnerabilidad se identificó la inclusión de la vulnerabilidad para el activo Synergy.

El 2 de septiembre de 2020 en desarrollo de la auditoría se realizó selectivamente pruebas en los años 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019 y 2020 evidenciando que el documento No. 01.616.251 – “Informe resultado de la auditoría a la gestión de copias de respaldo de información en la industria militar” del 13 de noviembre de 2014 el aplicativo Exact E-synergy permitió modificar el documento, como evidencia se envió a la oficina de informática el archivo llamado “evidencia dcto del

WOK

año 2014 que fue actualizado”.

El 14 de octubre de 2020 en desarrollo de la auditoría la oficina de informática en documento No. 02.351.444 *“Informe Avances Plan de Mejoramiento del proceso mes de Septiembre”* informa *“Conforme con la observación a la modificación de los documentos Synergy se evidencia que no estaba habilitado el Flag “Usar seguridad” en la configuración del tipo de documento la cual se ajusta para evitar la modificación de todos los documentos desde su origen, por favor realizar las pruebas correspondientes”*.

Durante el mes de noviembre de 2020 se realizó selectivamente pruebas en los años 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019 y 2020 evidenciando que efectivamente no se puede modificar documentos que tienen requerimiento y han sido observados.

#### **1.4.4 Anulación de anexos de los documentos de la aplicación Exact E-synergy después de ser observado.**

En el proceso implementado para la anulación de los anexos de un documento en la aplicación Exact E-synergy se evidenció:

- Se maneja la opción llamado ID206 – Anulación Documento este debe ser creado por el funcionario que elaboró el documento y el requerimiento.
- Se debe detallar la justificación de la solicitud de la anulación.
- Se debe informar el anexo a anular.
- El anexo es anulado, una vez el jefe inmediato autorice en el flujo de trabajo.
- El documento no es eliminado del sistema, el sistema lo deja como tipo de Documento 494 – *“Control Documentos Anulados”*.
- El 26 de octubre de 2020 se generó de la aplicación Exact E-synergy el listado de los documentos tipo 494 – *“Control de Documentos Anulados”* encontrando 460 anulaciones de anexos en las vigencias 2019 y 2020.

Al verificar la anulación de los anexos del documento 02.355.240 – *“Envío Información Contraloría General de la República”* se evidenció que los documentos que autorizaron cuyo soporte es la autorización del jefe inmediato en el flujo de trabajo del documento, se efectuaron después de observado.

Evidenciando falta de controles en la aplicación Exact E-synergy para el manejo de la información, afectando los principios de integridad, confidencialidad y disponibilidad de la información.

#### **1.5 Ingreso al gestor documental Exact E-synergy mediante el uso de dispositivos móviles y/o portátiles los días sábados, domingos y festivos.**

En desarrollo de la Auditoría con documento No. 02.303.911 del 18 de junio de 2020 la Oficina de Informática informa *“Los funcionarios relacionados en la pestaña (Empleados) tienen ingreso al gestor documental Synergy Externo. (Se entregó la evidencia correspondiente).”*

*Para mitigar la pérdida o fuga de se tienen los siguientes controles:*

*1. Cada usuario tiene configurado en su perfil controles como lo son:*

- Roles.
- Niveles de función.
- Niveles de seguridad.

CWIK

2. Los usuarios firman el acuerdo de confidencialidad en el contrato para el tratamiento de la información.

3. Synergy cuenta con una traza detallada de cada clic que ejecuta el usuario dejando rastro de que documento o requerimiento visualizo, modifiko o elimino, cuantas veces ingreso a cada registro, fecha y hora detallada.

4. La herramienta cuenta con niveles de seguridad en los requerimientos, los cuales garantizan que no se podrá modificar la información contenida.

5. La herramienta cuenta con niveles de seguridad en los documentos, los cuales garantizan que ningún otro usuario podrá ver documentación en la cual no esta observado o asignado, por lo tanto no se podrá modificar la información contenida.

6. Los funcionarios tienen ingreso desde la red de indumil, con acceso y disponibilidad de la aplicación cualquier día de la semana 7x24 servicios establecidos en el documento "Acuerdos Niveles de Servicios" Cód: IM OC OFI IF 004 de lunes a viernes, si el usuario está autorizado para ingresar a las instalaciones de la empresa sábados, domingos o festivos de igual manera podrá acceder.

7. Para el uso de gestor documental E-synergy los días sábados, domingos y festivos el grupo directivo tiene asignados portátiles de propiedad de la Industria Militar y tienen activo fijo asignado.

8. Desde el 19 de marzo de 2020 por la emergencia sanitaria por causa de Coronavirus COVID-19 - los funcionarios de la Industria Militar tienen habilitado el ingreso a la red de Indumil a través de VPN (Virtual Private Network) la cual es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet, con acceso y disponibilidad 7x24 de la aplicación cualquier día de la semana de lunes a domingo."

- Los funcionarios de la Industria Militar firman la cláusula de confidencialidad en el contrato para el tratamiento de los datos.

- La Industria Militar dispone de la Política de Seguridad y Privacidad de la Información Cód: IM OC OFI CP 003. Rev.8.

- La Industria Militar elaboró documento "INDUMIL NO NEGOCIA" entregado al ingresar a la Empresa, en el cual los funcionarios de la Industria Militar se comprometen entre otros, a: Numeral 3. "Se refiere a disponer de información de la empresa o de sus miembros, cualquiera que sea, para uso propio o de terceros y/o divulgación de la misma en las instalaciones de la empresa o fuera de ella, buscando o no un beneficio. En Indumil, las conductas no confidenciales no negociables pueden ser, entre otras: Comentar la información reservada con los compañeros o colaboradores, Publicar información de la Empresa sin autorización de la Gerencia, Hablar sobre asuntos confidenciales en un autobús, en el elevador, o por el teléfono celular estando en público, Hablar con amigos o parientes acerca de la información o suceso críticos de la organización y utilizar la información de la empresa para beneficio propio o de terceros".

- La Industria Militar implementó la "Política para el uso de dispositivos móviles" Cód: IM OC OFI CP 004. Rev.3. cuyo objetivo es "Limitar, establecer y dar a conocer las políticas relacionadas con el control de acceso lógico, dirigido hacia la protección de la información, restricción de acceso a personas no autorizadas a los recursos tecnológicos de INDUMIL, que estén asociados al Proceso GESTIÓN INFORMÁTICA" y establecen "Cualquier incumplimiento de las políticas establecidas en

este documento por parte de los funcionarios de la empresa acarreará las correspondientes sanciones disciplinarias”.

- La oficina de informática implementó el formato “*Relación de Entrada y Salida de Dispositivos Móviles Autorizados a las instalaciones físicas y red de INDUMIL*” IM OC OFI FO 026, el cual se encuentra una copia en las porterías principales de cada Centro Logístico y en centrales debidamente firmado por el jefe de Oficina de Informática.

- Se realizó auditoría al Proceso de Gestión Seguridad Física con documento No. 02.350.638 del 13/10/2020 donde se revisó el cumplimiento de la gestión realizada en las porterías de las fábricas y centrales en el ingreso y la salida de equipos de cómputo y electrónicos, es así como en el informe numeral 16 “*SALIDA Y ENTRADA DE BIENES*” se informa: “*De acuerdo a los documentos soportes enviados por las diferentes unidades de negocio, de manera selectiva se evidenció que se viene dando cumplimiento a lo establecido en el formato IM OC DRS FO 016, en cuanto a la entrada y salida de bienes de la Industria Militar, se evidenció que se viene efectuando control mediante este formato de la entrada y salida de documentación, de acuerdo al numeral 4.1.13 del Instructivo de Seguridad Física de Oficinas Centrales IM OC DRS IN 002 Rev. 3, igualmente se encuentra contemplado en los instructivos de Seguridad Física de cada una de las unidades de Negocio, en los mismos formatos se evidencia registros de entrada y salida equipos de cómputo y electrónicos*”.

#### **1.6 LOG de la aplicación Exact E-synergy**

En desarrollo de la auditoría se solicitó el 12 de junio de 2020 los logs de la aplicación Exact E-Synergy de los años 2019 y 2020. La Oficina de Informática envió el 11 de noviembre de 2020 documento No. 02.362.126 — “*Logs de registro y errores Synergy 2019 a 2020*”, observando:

- Al verificar el cumplimiento al Procedimiento de Monitoreo y Gestión de Logs Cod: IM OC OFI PR 012 Rev.12. numeral 4.1 Condiciones Generales...Análisis de los LOGS. “*Mensualmente o cada vez que las circunstancias lo ameriten, en cada revisión de los logs se registrarán los hechos relevantes encontrados y las acciones sugeridas al respecto con el fin de minimizar los riesgos inherentes. Esta información será registrada en el requerimiento Monitoreo y Gestión de Logs del gestor documental e-Synergy con el fin de que se realicen las acciones correspondientes*”, el administrador de la aplicación informa “*con respecto al análisis del log de errores no se realiza porque no son muy específicos*”.
- Teniendo en cuenta la consulta realizada por el auditor sobre el Log, el asesor del departamento comercial JNC – Tic Servicios 360 en correo electrónico del 2 de junio de 2020 informó: “*El informe de registro de datos le permite rastrear todos los detalles de las modificaciones de datos que incluyen lo que se ha modificado, cuándo tuvieron lugar las modificaciones, cómo se modificaron los datos y quién los modificó. Puede definir uno o más criterios para obtener el informe de registro de datos*” y lo informado en el Procedimiento de Monitoreo y Gestión de Logs Cod: IM OC OFI PR 012 Rev.12. numeral 4.1 Condiciones Generales... Elementos principales de un Log o Registro. “*Un registro o log de software o hardware deberá poseer entre otros, los siguientes campos: fecha del evento, hora del evento, equipo de computó donde se realizó el evento, usuario quien produce el evento, tipo de evento y archivo que se modifica en el evento (cambio de un campo de información, eliminación, creación), especificaciones del evento*” se verificó la configuración de los logs de registros año 2019 y 2020 y logs de errores año 2020 entregados por el administrador de la aplicación y estos no permiten rastrear los detalles de los eventos de las modificaciones de

60/12

datos (que se ha modificado, fechas de las modificaciones, como se modificaron los datos y quien los modifiko).

Evidenciando el no cumplimiento del control definido en el Procedimiento de Monitoreo y Gestión de Logs Cod: IM OC OFI PR 012 Rev.12. afectando los principios de integridad, confidencialidad y disponibilidad de la información.

## 2. MESA DE AYUDA – GLPI

*“La herramienta GLPI es software libre, que facilita la administración de recursos informáticos. GLPI es una aplicación basada en Web escrita en PHP, que permite registrar y administrar los inventarios del hardware y el software de una empresa, optimizando el trabajo de los técnicos gracias a su diseño coherente. GLPI incluye también software de mesa de ayuda para el registro y atención de solicitudes de servicio de soporte técnico, con posibilidades de notificación por correo electrónico a usuarios y al mismo personal de soporte, al inicio, avances o cierre de una solicitud.*

*Las estadísticas son de gran funcionalidad, la confiabilidad de los reportes y búsquedas en general que el aplicativo genera son reales debido a los registros de información almacenados en la base de datos”. (Información obtenida de GLPI: <http://www.glpi-project.org>).*

En desarrollo de la auditoría se solicitó el 8 de junio de 2020 por correo electrónico a la oficina de Informática reporte de servicios con la siguiente información: ID, título, localización, categoría, descripción, tipo, estado, prioridad, solicitante, persona asignada para atender el caso, fecha de apertura, tiempo asignado para resolver el servicio, tiempo de solución, ANS (Acuerdo de nivel de servicio) – ANS (Acuerdo de nivel de servicio) Tiempo de solución, evidencia de aceptación por parte del solicitante, fecha en que se cerró el caso.

El 17 de junio de 2020 la oficina de informática envió por correo electrónico el archivo llamado “GLPI-casos” con 4.484 registros de tickets creados del 18/09/2019 hasta el 23/06/2020, se realizó análisis de este, encontrando:

### 2.1 Eliminación de registros en la base de datos de la herramienta GLPI

En la base de datos de la herramienta GLPI no se encontraron 298 registros. El jefe de la oficina de informática por correo electrónico el 26 de junio de 2020 informa: *“Al respecto de los ID’s de tickets que faltan, son tickets que se han borrado por diferentes causas, por ejemplo: Los que faltan del 1 al 71 fueron los primeros casos que se abrieron y los usamos a nivel solo de la oficina de informática para prácticas y capacitación, teniendo en cuenta que es una plataforma nueva y no teníamos la experiencia, la mesa de ayuda oficialmente se abrió el 01 de octubre de 2019, algunos usuarios crearon casos antes de esa fecha (11 para ser más exactos) los cuales se dejaron y se les ha dado trámite. Hay otros que cuando se implementan nuevas configuraciones se hacen casos de prueba y luego se borran, con el fin de verificar que lo implementado quede funcionando. Finalmente el usuario mismo que crea un caso lo puede borrar”.*

Teniendo en cuenta lo anterior se evidencia que la eliminación física realizada a los datos ocasionó la pérdida de la integridad y disponibilidad de la información de la base de datos de la herramienta GLPI, así como la confiabilidad de los reportes, de las estadísticas y búsquedas que esta herramienta ofrece.

### 2.2 Requerimientos de la aplicación Exact E-Synergy

Se verificó la solución a los requerimientos existentes en la base de datos “GLPI-casos” entregada por

LUCK

la oficina de informática en correo electrónico del 17 de junio de 2020 teniendo en cuenta el documento "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.5 literal b) "Tiempos de solución por proveedor" y la contratación celebrada con el Proveedor B EXCELLENCE S.A.S, encontrando:

La Industria Militar en el 2019 contrato la prestación de servicios para el mantenimiento, soporte y actualización de la aplicación Exact E-Synergy, así:

- El 8 de mayo de 2019 se firmó contrato No. 1-020/219 con la empresa comercial B EXCELLENCE S.A.S. para el servicio de actualización de licenciamiento, mantenimiento, soporte y desarrollo con plazo de ejecución 31 enero de 2020 y cuatro meses de duración única y exclusivamente para la liquidación del contrato.
- El 24 de julio de 2020 se firmó contrato No. 1-042/2020 con la empresa comercial B EXCELLENCE S.A.S. para el servicio de actualización de licenciamiento, mantenimiento, soporte y desarrollos con plazo de ejecución 31 diciembre de 2020.

Evidenciando que la Industria Militar duro aproximadamente seis (6) meses (del 1 de febrero al 23 de julio de 2020) sin contrato de servicios para la actualización de licenciamiento, mantenimiento, soporte y desarrollo de la aplicación Exact E-Synergy, tiempo en el cual la prestación del servicio de soporte no se dio a los usuarios del software, quedando sin resolver las novedades presentadas y afectando la ejecución de sus actividades diarias.

All revisar la Matriz de Riesgos y Oportunidades Primer Cuatrimestre 2020 Cód: IM OC OFP FO 117 Rev.5. del Proceso Gestión Informática no se encontró identificada la situación de la no prestación oportuna del servicio para el mantenimiento, soporte y actualización de los sistemas informáticos.

Teniendo en cuenta lo descrito en el documento Acuerdo Niveles de Servicio Cód: IM OC OFI IF 004. Rev.5 "literal b) *Tiempos de solución por proveedor*" de quinientos noventa y cuatro (594) tickets registrados en la base de datos "GLPI-casos" del 18/09/2019 al 23/06/2020 se encontraron veintitrés (23) pendientes por resolver de la aplicación Exact E-Synergy, a continuación se relacionan:

No. REGISTRO	No. TICKET	FECHA CREACIÓN	PRIORIDAD	ESTADO	No. Días sin resolver
1	1119	10/12/2019	MEDIA	PLANEADO	164
2	2480	12/02/2020	MEDIA	PLANEADO	118
3	2570	17/02/2020	MEDIA	PLANEADO	115
4	4060	8/05/2020	MEDIA	PLANEADO	56
5	4131	13/05/2020	MEDIA	PLANEADO	53
6	4150	14/05/2020	MEDIA	PLANEADO	52
7	4578	5/06/2020	MEDIA	PLANEADO	36
8	4766	18/06/2020	MEDIA	PENDIENTE	27
9	4779	18/06/2020	MEDIA	PENDIENTE	27
10	4781	18/06/2020	MEDIA	PENDIENTE	27
11	4784	18/06/2020	MEDIA	PENDIENTE	27
12	4822	23/06/2020	MEDIA	PENDIENTE	24
13	4825	23/06/2020	MEDIA	PENDIENTE	24
14	4021	6/05/2020	MEDIA	PENDIENTE	58

CLK

15	4746	17/06/2020	MEDIA	PENDIENTE	28
16	4754	17/06/2020	MEDIA	PENDIENTE	28
17	4800	19/06/2020	MEDIA	PENDIENTE	26
18	4811	23/06/2020	MEDIA	PENDIENTE	24
19	4819	23/06/2020	MEDIA	PENDIENTE	24
20	4577	5/06/2020	MEDIA	PENDIENTE	36
21	4752	17/06/2020	MEDIA	PENDIENTE	28
22	4160	15/05/2020	MEDIA	PLANEADO	51
23	4817	23/06/2020	MEDIA	PENDIENTE	24

**2.3 Requerimientos de la aplicación SAP / S4 HANA**

Se verificó la solución a los requerimientos existentes en la base de datos "GLPI-casos" entregada por la oficina de informática en correo electrónico del 17 de junio de 2020 teniendo en cuenta el documento "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.5 literal b) "Tiempos de solución por proveedor" y la contratación celebrada con el Proveedor EPI USE COLOMBIA SAS, encontrando:

La Industria Militar durante los años 2019 y 2020 contrato el servicio para "El soporte, mantenimiento, y actualización de la plataforma SAP, este servicio incluye el mantenimiento correctivo y evolutivo del software por cambios legales, normativos, errores de la aplicación y por nuevas necesidades de desarrollos de la Industria Militar, así mismo prestar el servicio de soporte técnico y funcional a todos los usuarios del software, con el fin de resolver las novedades de operación que puedan presentarse en el sistema", así:

- El 7 de mayo de 2019 se firmó contrato No. 1-014/219 con la empresa EPI USE COLOMBIA SAS para el soporte, mantenimiento, y actualización de la plataforma SAP por valor de \$ 1.857.880.062,5 con plazo de ejecución 20 enero de 2020 y cuatro meses de duración única y exclusivamente para la liquidación del contrato.
- El 20 de enero de 2020 se firmó el primer contrato adicional con la empresa EPI USE COLOMBIA SAS para adicionar en valor y prorrogar el plazo de ejecución del contrato de prestación de servicios No. 1-014/2019. El valor a adicional fue de \$337.796.375 y se prorrogó el plazo de ejecución hasta el 20 de marzo de 2020.
- El 20 de marzo de 2020 se firmó el segundo contrato adicional con la empresa EPI USE COLOMBIA SAS para adicionar en valor y prorrogar el plazo de ejecución del contrato de prestación de servicios No. 1-014/2019. El valor adicional fue de \$168.898.187,5 y se prorrogó el plazo de ejecución hasta el 20 de abril de 2020.

El valor total sumado el contrato principal y las adiciones asciende a \$1.857.880.062,5.

- El 7 de julio de 2020 la Industria Militar inicio la contratación con proyecto No. 9434 – "SERVICIO DE SOPORTE Y MANTENIMIENTO DEL ERP SAP / S4 HANA". "La finalidad del presente proceso es adquirir el SERVICIO DE SOPORTE Y MANTENIMIENTO DEL ERP SAP / S4 HANA, dando continuidad operacional y funcional del sistema de información instalado en la Industria Militar, ERP SAP / S4 HANA." El 30 de septiembre de 2020 se realizó la Legalización de la Orden de Compra No. OC 450006378 EPI USE COLOMBIA SAS. por valor de \$82.110.000 (incluido IVA).

LUK

Evidenciando que la Industria Militar no tiene contrato de servicio soporte y mantenimiento del ERP SAP / S4 HANA, tiempo en el cual la prestación del servicio de soporte no se puede dar a los usuarios del software, quedando sin resolver las novedades presentadas y afectando la ejecución de sus actividades diarias.

Al revisar la Matriz de Riesgos y Oportunidades Primer Cuatrimestre 2020 Cód: IM OC OFF FO 117 Rev.5. del Proceso Gestión Informática no se encontró identificada la situación de la no prestación oportuna del servicio para el mantenimiento, soporte y actualización de los sistemas informáticos.

Teniendo en cuenta lo informado en el documento "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.5 literal b) Tiempo de solución solicitudes ERP SAP S4/HANA" de seiscientos veintidós (622) tickets registrados en la base de datos "GLPI-casos" del 18/09/2019 al 23/06/2020 se encontraron sesenta y ocho (68) pendientes por resolver de la aplicación SAP / S4 HANA, a continuación se relacionan:

No. REGISTRO	No. TICKET	FECHA CREACIÓN	PRIORIDAD	ESTADO	No. Días sin resolver
1	940	28/11/2019	BAJA	PLANEADO	198
2	943	28/11/2019	BAJA	PLANEADO	198
3	946	28/11/2019	BAJA	PLANEADO	198
4	1117	10/12/2019	BAJA	PLANEADO	190
5	1118	10/12/2019	BAJA	PLANEADO	190
6	1277	18/12/2019	BAJA	PLANEADO	184
7	1667	17/01/2020	BAJA	PLANEADO	162
8	1680	17/01/2020	BAJA	PLANEADO	162
9	1800	22/01/2020	BAJA	PLANEADO	159
10	1960	28/01/2020	BAJA	PLANEADO	155
11	2055	29/01/2020	BAJA	PLANEADO	154
12	2098	30/01/2020	BAJA	PLANEADO	153
13	2172	3/02/2020	BAJA	PLANEADO	151
14	2179	3/02/2020	BAJA	PLANEADO	151
15	2329	7/02/2020	BAJA	PLANEADO	147
16	2424	11/02/2020	BAJA	PENDIENTE	145
17	2496	13/02/2020	BAJA	PLANEADO	143
18	2512	13/02/2020	BAJA	PLANEADO	143
19	2723	21/02/2020	BAJA	PLANEADO	137
20	2731	21/02/2020	BAJA	PLANEADO	137
21	2795	24/02/2020	BAJA	PENDIENTE	136
22	2893	27/02/2020	BAJA	PLANEADO	133
23	3011	3/03/2020	BAJA	PENDIENTE	130
24	3166	11/03/2020	BAJA	PLANEADO	124
25	3171	11/03/2020	BAJA	PLANEADO	124
26	3173	11/03/2020	BAJA	PLANEADO	124
27	3175	12/03/2020	BAJA	PLANEADO	123
28	3241	13/03/2020	BAJA	PENDIENTE	122
29	3278	16/03/2020	BAJA	PENDIENTE	121
30	3309	18/03/2020	BAJA	PENDIENTE	119
31	3323	18/03/2020	BAJA	PLANEADO	119
32	3327	18/03/2020	BAJA	PLANEADO	119
33	3538	30/03/2020	BAJA	PENDIENTE	111
34	3617	6/04/2020	BAJA	PENDIENTE	106
35	3626	6/04/2020	BAJA	PLANEADO	106
36	3663	13/04/2020	BAJA	PENDIENTE	101
37	3664	13/04/2020	BAJA	PLANEADO	101
38	3684	14/04/2020	BAJA	PLANEADO	100
39	3699	16/04/2020	BAJA	PLANEADO	98
40	3715	17/04/2020	BAJA	PENDIENTE	97
41	3719	17/04/2020	BAJA	PENDIENTE	97
42	3726	17/04/2020	BAJA	PLANEADO	97
43	3741	20/04/2020	BAJA	PENDIENTE	96

GWR

44	3744	20/04/2020	BAJA	PENDIENTE	96
45	3749	20/04/2020	BAJA	PENDIENTE	96
46	3987	4/05/2020	BAJA	PENDIENTE	86
47	4048	7/05/2020	BAJA	PENDIENTE	83
48	4052	7/05/2020	BAJA	PLANEADO	83
49	4125	12/05/2020	BAJA	PENDIENTE	80
50	4126	12/05/2020	BAJA	PLANEADO	80
51	4136	13/05/2020	BAJA	PLANEADO	79
52	4165	15/05/2020	BAJA	PENDIENTE	77
53	4169	15/05/2020	BAJA	PENDIENTE	77
54	4214	20/05/2020	BAJA	PLANEADO	74
55	4274	26/05/2020	BAJA	PLANEADO	70
56	4294	26/05/2020	BAJA	PLANEADO	70
57	4361	27/05/2020	BAJA	PLANEADO	69
58	4494	2/06/2020	BAJA	PENDIENTE	65
59	4523	3/06/2020	BAJA	PLANEADO	64
60	4576	5/06/2020	BAJA	PENDIENTE	62
61	4587	5/06/2020	BAJA	PENDIENTE	62
62	4623	9/06/2020	BAJA	PENDIENTE	60
63	4640	10/06/2020	BAJA	PENDIENTE	59
64	4650	10/06/2020	BAJA	PENDIENTE	59
65	4696	11/06/2020	BAJA	PLANEADO	58
66	4705	12/06/2020	BAJA	PENDIENTE	57
67	4747	17/06/2020	BAJA	PLANEADO	54
68	4803	19/06/2020	BAJA	PENDIENTE	52

**2.4 Requerimientos Otras categorías**

Se verificó la solución a los requerimientos existentes en la base de datos entregada por la oficina de informática teniendo en cuenta el documento "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.5 literal a) Tiempo de solución, los tiempos de respuesta y solución máximos de las solicitudes para la Oficina de Informática recibidos mediante la herramienta GLP", encontrando requerimientos del 9 de octubre de 2019 al 23 de junio de 2020 pendientes por resolver, a continuación se muestran por categorías:

**2.4.1 Correo Electrónico. (De 165 tickets registrados pendientes por resolver 13).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo (IM OC OFI IF 004)
1	3225	13/03/2020	SIN ASIGNAR	PLANEADO	702	5
2	4156	14/05/2020	SIN ASIGNAR	PENDIENTE	306	5
3	4168	15/05/2020	SIN ASIGNAR	PLANEADO	297	5
4	4407	29/05/2020	SIN ASIGNAR	PENDIENTE	207	5
5	4511	3/06/2020	SIN ASIGNAR	PENDIENTE	180	5
6	4537	3/06/2020	SIN ASIGNAR	PENDIENTE	180	5
7	4584	5/06/2020	MEDIA	PENDIENTE	162	5
8	4601	8/06/2020	MEDIA	PENDIENTE	153	5
9	4642	10/06/2020	ALTA	PENDIENTE	135	5
10	4652	10/06/2020	SIN ASIGNAR	PENDIENTE	135	5
11	4724	13/06/2020	SIN ASIGNAR	PENDIENTE	108	5
12	4750	17/06/2020	SIN ASIGNAR	PENDIENTE	90	5
13	4755	17/06/2020	SIN ASIGNAR	PENDIENTE	90	5

*WUR*

**2.4.2 File server. (De 50 tickets registrados pendientes por resolver 2).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo (IM OC OFI IF 004)
1	4651	10/06/2020	ALTA	PENDIENTE	135	5
2	4816	23/06/2020	ALTA	PENDIENTE	54	5

**2.4.3 Firma Digital. (De 55 tickets registrados pendientes por resolver 30).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo (IM OC OFI IF 004)
1	2139	31/01/2020	BAJA	PLANEADO	972	58
2	3736	20/04/2020	BAJA	PLANEADO	468	58
3	3737	20/04/2020	BAJA	PLANEADO	468	58
4	3738	20/04/2020	BAJA	PLANEADO	468	58
5	3739	20/04/2020	BAJA	PLANEADO	468	58
6	3817	24/04/2020	BAJA	PENDIENTE	432	58
7	3980	4/05/2020	BAJA	PENDIENTE	378	58
8	3997	5/05/2020	BAJA	PLANEADO	369	58
9	3998	5/05/2020	BAJA	PLANEADO	369	58
10	4145	13/05/2020	BAJA	PLANEADO	315	58
11	4188	19/05/2020	BAJA	PLANEADO	279	58
12	4672	11/06/2020	BAJA	PLANEADO	126	58
13	4673	11/06/2020	BAJA	PLANEADO	126	58
14	4674	11/06/2020	BAJA	PLANEADO	126	58
15	4675	11/06/2020	BAJA	PLANEADO	126	58
16	4676	11/06/2020	BAJA	PLANEADO	126	58
17	4677	11/06/2020	BAJA	PLANEADO	126	58
18	4678	11/06/2020	BAJA	PLANEADO	126	58
19	4679	11/06/2020	BAJA	PLANEADO	126	58
20	4680	11/06/2020	BAJA	PLANEADO	126	58
21	4681	11/06/2020	BAJA	PLANEADO	126	58
22	4684	11/06/2020	BAJA	PLANEADO	126	58
23	4685	11/06/2020	BAJA	PLANEADO	126	58
24	4686	11/06/2020	BAJA	PLANEADO	126	58
25	4687	11/06/2020	BAJA	PLANEADO	126	58
26	4688	11/06/2020	BAJA	PLANEADO	126	58
27	4689	11/06/2020	BAJA	PLANEADO	126	58
28	4690	11/06/2020	BAJA	PLANEADO	126	58
29	4691	11/06/2020	BAJA	PLANEADO	126	58
30	4758	17/06/2020	BAJA	PLANEADO	90	58

**2.4.4 Gestión de Usuarios. (De 717 tickets registrados pendientes por resolver 34).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo (IM OC OFI IF 004)
1	442	25/10/2019	BAJA	PLANEADO	1602	3
2	981	2/12/2019	MEDIA	PLANEADO	1368	No se encuentra subcategoría
3	1000	2/12/2019	MEDIA	PLANEADO	1368	3
4	2662	19/02/2020	MEDIA	PENDIENTE	855	3
5	2829	25/02/2020	MEDIA	PLANEADO	819	3
6	3800	24/04/2020	MEDIA	PLANEADO	432	3
7	3820	24/04/2020	MEDIA	PLANEADO	432	3
8	3915	29/04/2020	MEDIA	PLANEADO	405	No se encuentra subcategoría

CWZ

9	3983	4/05/2020	MEDIA	PENDIENTE	378	3
10	4029	6/05/2020	MEDIA	PENDIENTE	360	2
11	4047	7/05/2020	MEDIA	PENDIENTE	351	3
12	4064	8/05/2020	MEDIA	PENDIENTE	342	3
13	4094	11/05/2020	MEDIA	PENDIENTE	333	3
14	4162	15/05/2020	MEDIA	PENDIENTE	297	2
15	4181	18/05/2020	MEDIA	PENDIENTE	288	3
16	4189	19/05/2020	MEDIA	PENDIENTE	279	3
17	4193	19/05/2020	MEDIA	PENDIENTE	279	2
18	4235	21/05/2020	MEDIA	PENDIENTE	261	3
19	4237	21/05/2020	MEDIA	PENDIENTE	261	3
20	4340	27/05/2020	MEDIA	PLANEADO	225	3
21	4427	29/05/2020	MEDIA	PLANEADO	207	3
22	4431	29/05/2020	MEDIA	PLANEADO	207	3
23	4438	29/05/2020	MEDIA	PENDIENTE	207	2
24	4442	29/05/2020	MEDIA	PLANEADO	207	2
25	4538	3/06/2020	MEDIA	PENDIENTE	180	3
26	4549	4/06/2020	MEDIA	PENDIENTE	171	3
27	4572	5/06/2020	MEDIA	PLANEADO	162	3
28	4604	8/06/2020	MEDIA	PENDIENTE	153	3
29	4697	11/06/2020	MEDIA	PLANEADO	126	3
30	4698	11/06/2020	MEDIA	PENDIENTE	126	3
31	4713	12/06/2020	MEDIA	PENDIENTE	117	3
32	4730	16/06/2020	MEDIA	PENDIENTE	99	3
33	4733	16/06/2020	MEDIA	PENDIENTE	99	3
34	4745	16/06/2020	MEDIA	PLANEADO	99	2

**2.4.5 Hardware. (De 427 tickets registrados pendientes por resolver 105).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo (IM OC OFI IF 004)
1	177	7/10/2019	BAJA	PLANEADO	1728	8
2	178	7/10/2019	BAJA	PLANEADO	1728	8
3	181	8/10/2019	BAJA	PLANEADO	1719	8
4	222	9/10/2019	BAJA	PLANEADO	1710	8
5	244	10/10/2019	BAJA	PLANEADO	1701	8
6	300	16/10/2019	BAJA	PLANEADO	1665	8
7	450	25/10/2019	BAJA	PLANEADO	1602	8
8	599	5/11/2019	BAJA	PLANEADO	1539	8
9	615	5/11/2019	BAJA	PLANEADO	1539	8
10	649	7/11/2019	MEDIA	PLANEADO	1521	8
11	696	12/11/2019	MEDIA	PLANEADO	1494	8
12	717	13/11/2019	ALTA	PLANEADO	1485	8
13	834	20/11/2019	ALTA	PLANEADO	1440	8
14	854	21/11/2019	MEDIA	PLANEADO	1431	8
15	982	2/12/2019	MEDIA	PLANEADO	1368	8
16	993	2/12/2019	MEDIA	PLANEADO	1368	8
17	1157	12/12/2019	MEDIA	PLANEADO	1296	8
18	1582	15/01/2020	BAJA	PLANEADO	1080	8
19	1638	16/01/2020	MEDIA	PLANEADO	1071	8
20	1900	27/01/2020	BAJA	PLANEADO	1008	8
21	1941	27/01/2020	SIN ASIGNAR	PLANEADO	1008	8
22	1942	27/01/2020	SIN ASIGNAR	PENDIENTE	1008	8
23	1953	28/01/2020	BAJA	PLANEADO	999	8
24	2002	28/01/2020	MEDIA	PLANEADO	999	8
25	2015	29/01/2020	ALTA	PENDIENTE	990	8
26	2020	29/01/2020	MEDIA	PLANEADO	990	8
27	2193	4/02/2020	SIN ASIGNAR	PLANEADO	954	8
28	2242	5/02/2020	MEDIA	PLANEADO	945	8
29	2497	13/02/2020	ALTA	PLANEADO	891	8
30	2547	14/02/2020	ALTA	PENDIENTE	882	8
31	2606	17/02/2020	MEDIA	PLANEADO	873	8
32	2634	18/02/2020	SIN ASIGNAR	PLANEADO	864	8
33	2686	20/02/2020	BAJA	PLANEADO	846	8

1008

Synergy No (1). 02.373.149

Fecha (2) : 07-dic-2020

34	2698	20/02/2020	MEDIA	PENDIENTE	846	8
35	2718	20/02/2020	SIN ASIGNAR	PLANEADO	846	8
36	2748	21/02/2020	MEDIA	PLANEADO	837	8
37	2793	24/02/2020	BAJA	PLANEADO	828	8
38	2851	26/02/2020	MEDIA	PENDIENTE	810	8
39	2883	27/02/2020	BAJA	PLANEADO	801	8
40	2901	27/02/2020	BAJA	PLANEADO	801	8
41	2910	27/02/2020	MEDIA	PLANEADO	801	8
42	2917	28/02/2020	ALTA	PLANEADO	792	8
43	2918	28/02/2020	MEDIA	PLANEADO	792	8
44	2928	28/02/2020	MEDIA	PLANEADO	792	8
45	2932	28/02/2020	MEDIA	PLANEADO	792	8
46	3007	3/03/2020	ALTA	PLANEADO	774	8
47	3010	3/03/2020	ALTA	PLANEADO	774	8
48	3014	3/03/2020	MEDIA	PLANEADO	774	8
49	3017	3/03/2020	ALTA	PLANEADO	774	8
50	3018	3/03/2020	BAJA	PLANEADO	774	8
51	3031	4/03/2020	MEDIA	PLANEADO	765	8
52	3036	4/03/2020	MEDIA	PLANEADO	765	8
53	3051	4/03/2020	MEDIA	PLANEADO	765	8
54	3114	6/03/2020	MEDIA	PLANEADO	746	8
55	3230	13/03/2020	BAJA	PLANEADO	702	8
56	3281	17/03/2020	MEDIA	PLANEADO	684	8
57	3638	7/04/2020	SIN ASIGNAR	PLANEADO	549	8
58	3656	8/04/2020	SIN ASIGNAR	PLANEADO	540	8
59	3776	22/04/2020	MEDIA	PLANEADO	450	8
60	3792	23/04/2020	BAJA	PLANEADO	441	8
61	3805	24/04/2020	ALTA	PLANEADO	432	8
62	3849	27/04/2020	MEDIA	PLANEADO	423	8
63	3873	28/04/2020	MEDIA	PLANEADO	414	8
64	3892	28/04/2020	SIN ASIGNAR	PLANEADO	414	8
65	3893	28/04/2020	SIN ASIGNAR	PLANEADO	414	8
66	3895	28/04/2020	SIN ASIGNAR	PLANEADO	414	8
67	3967	4/05/2020	MEDIA	PENDIENTE	378	8
68	3994	5/05/2020	MEDIA	PENDIENTE	369	8
69	4012	5/05/2020	SIN ASIGNAR	PENDIENTE	369	8
70	4024	6/05/2020	SIN ASIGNAR	PENDIENTE	360	8
71	4045	7/05/2020	ALTA	PLANEADO	351	8
72	4061	8/05/2020	ALTA	PENDIENTE	342	8
73	4095	11/05/2020	SIN ASIGNAR	PENDIENTE	333	8
74	4110	12/05/2020	ALTA	PENDIENTE	324	8
75	4117	12/05/2020	MEDIA	PENDIENTE	324	8
76	4132	13/05/2020	MEDIA	PENDIENTE	315	8
77	4176	18/05/2020	ALTA	PENDIENTE	288	8
78	4195	19/05/2020	MEDIA	PENDIENTE	279	8
79	4196	19/05/2020	SIN ASIGNAR	PENDIENTE	279	8
80	4197	19/05/2020	SIN ASIGNAR	PENDIENTE	279	8
81	4203	19/05/2020	MEDIA	PLANEADO	279	8
82	4229	21/05/2020	BAJA	PENDIENTE	261	8
83	4232	21/05/2020	MEDIA	PENDIENTE	261	8
84	4252	22/05/2020	ALTA	PENDIENTE	252	8
85	4275	26/05/2020	MEDIA	PENDIENTE	234	8
86	4283	26/05/2020	BAJA	PENDIENTE	234	8
87	4401	28/05/2020	SIN ASIGNAR	PENDIENTE	216	8
88	4463	1/06/2020	ALTA	PENDIENTE	198	8
89	4464	1/06/2020	MEDIA	PENDIENTE	198	8
90	4471	1/06/2020	ALTA	PLANEADO	198	8
91	4535	3/06/2020	ALTA	PENDIENTE	180	8
92	4540	4/06/2020	BAJA	PLANEADO	171	8
93	4582	5/06/2020	MEDIA	PLANEADO	162	8
94	4609	9/06/2020	MEDIA	PENDIENTE	144	8
95	4610	9/06/2020	ALTA	PENDIENTE	144	8
96	4711	12/06/2020	BAJA	PENDIENTE	117	8
97	4717	12/06/2020	ALTA	PENDIENTE	117	8
98	4729	16/06/2020	ALTA	PLANEADO	99	8
99	4732	16/06/2020	MEDIA	PENDIENTE	99	8
100	4743	16/06/2020	SIN ASIGNAR	PENDIENTE	99	8
101	4751	17/06/2020	ALTA	PENDIENTE	90	8

LUK

102	4765	18/06/2020	MEDIA	PENDIENTE	81	8
103	4772	18/06/2020	SIN ASIGNAR	PENDIENTE	81	8
104	4776	18/06/2020	MEDIA	PENDIENTE	81	8
105	4778	18/06/2020	ALTA	PENDIENTE	81	8

**2.4.6 Internet. (De 288 tickets registrados pendientes por resolver 13).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo (IM OC OFI IF 004)
1	4489	2/06/2020	SIN ASIGNAR	PLANEADO	189	2
2	4617	9/06/2020	ALTA	PLANEADO	144	4
3	4637	10/06/2020	MEDIA	PENDIENTE	135	2
4	4669	11/06/2020	ALTA	PENDIENTE	126	4
5	4692	11/06/2020	SIN ASIGNAR	PLANEADO	126	4
6	4699	11/06/2020	ALTA	PLANEADO	126	4
7	4703	12/06/2020	ALTA	PENDIENTE	117	4
8	4738	16/06/2020	MEDIA	PENDIENTE	99	2
9	4741	16/06/2020	MEDIA	PENDIENTE	99	2
10	4742	16/06/2020	MEDIA	PENDIENTE	99	2
11	4744	16/06/2020	MEDIA	PENDIENTE	99	2
12	4789	18/06/2020	MEDIA	PENDIENTE	81	2
13	4801	19/06/2020	MEDIA	PENDIENTE	72	2

**2.4.7 Módulo de Apoyo. (De 448 tickets registrados pendientes por resolver 16).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo - horas (IM OC OFI IF 004)
1	823	19/11/2019	ALTA	PLANEADO	1449	4
2	2690	20/02/2020	ALTA	PLANEADO	846	4
3	3337	19/03/2020	ALTA	PENDIENTE	666	4
4	3389	24/03/2020	ALTA	PENDIENTE	639	4
5	3771	22/04/2020	BAJA	PENDIENTE	450	16
6	3993	5/05/2020	ALTA	PLANEADO	369	4
7	4022	6/05/2020	ALTA	PENDIENTE	360	4
8	4191	19/05/2020	ALTA	PLANEADO	279	4
9	4468	1/06/2020	ALTA	PENDIENTE	198	4
10	4512	3/06/2020	ALTA	PLANEADO	180	4
11	4565	4/06/2020	ALTA	PENDIENTE	171	4
12	4634	10/06/2020	ALTA	PENDIENTE	135	4
13	4659	10/06/2020	ALTA	PENDIENTE	135	4
14	4723	12/06/2020	ALTA	PENDIENTE	117	4
15	4771	18/06/2020	ALTA	PENDIENTE	81	4
16	4804	23/06/2020	ALTA	PENDIENTE	54	4

**2.4.8 Red de Datos. (De 62 tickets registrados pendientes por resolver 8).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo - horas (IM OC OFI IF 004)
1	1854	24/01/2020	MEDIA	PLANEADO	1017	2
2	2027	29/01/2020	BAJA	PLANEADO	990	8
3	3877	28/04/2020	MEDIA	PLANEADO	414	2
4	4396	28/05/2020	MEDIA	PENDIENTE	216	2
5	4649	10/06/2020	MEDIA	PLANEADO	135	2
6	4790	19/06/2020	ALTA	PENDIENTE	72	4
7	4791	19/06/2020	ALTA	PENDIENTE	72	4
8	4823	23/06/2020	ALTA	PENDIENTE	54	4

*Wax*

**2.4.9 Red de Voz. (De 48 tickets registrados pendientes por resolver 8).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo – horas (IM OC OFI IF 004)
1	969	29/11/2019	ALTA	PLANEADO	1337	4
2	2236	5/02/2020	ALTA	PLANEADO	945	4
3	2589	17/02/2020	ALTA	PLANEADO	873	4
4	2941	28/02/2020	ALTA	PLANEADO	792	4
5	4379	28/05/2020	ALTA	PENDIENTE	216	4
6	4391	28/05/2020	ALTA	PENDIENTE	216	4
7	4476	1/06/2020	ALTA	PLANEADO	198	4
8	4612	9/06/2020	SIN ASIGNAR	PENDIENTE	144	4

**2.4.10 Seguridad de la Información. (De 85 tickets registrados pendientes por resolver 5).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo – horas (IM OC OFI IF 004)
1	2822	25/02/2020	BAJA	PLANEADO	819	24
2	3013	3/03/2020	BAJA	PLANEADO	714	24
3	3191	12/03/2020	BAJA	PLANEADO	711	24
4	3331	18/03/2020	BAJA	PLANEADO	675	24
5	4466	1/06/2020	SIN ASIGNAR	PLANEADO	198	8

**2.4.11 Servicio de Apoyo. (De 250 tickets registrados pendientes por resolver 11).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo – horas (IM OC OFI IF 004)
1	3319	18/03/2020	BAJA	PLANEADO	675	8
2	3564	1/04/2020	BAJA	PLANEADO	585	8
3	3601	3/04/2020	BAJA	PLANEADO	567	8
4	4452	1/06/2020	BAJA	PENDIENTE	198	8
5	4704	12/06/2020	BAJA	PENDIENTE	117	8
6	4709	12/06/2020	BAJA	PENDIENTE	117	8
7	4710	12/06/2020	BAJA	PLANEADO	117	8
8	4714	12/06/2020	BAJA	PENDIENTE	117	8
9	4764	18/06/2020	BAJA	PENDIENTE	81	8
10	4785	18/06/2020	BAJA	PENDIENTE	81	8
11	4794	19/06/2020	BAJA	PLANEADO	72	8

**2.4.12 Sitio WEB. (De 300 tickets registrados pendientes por resolver 2).**

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo – horas (IM OC OFI IF 004)
1	4142	13/05/2020	MEDIA	PENDIENTE	315	3
2	4783	18/06/2020	SIN ASIGNAR	PENDIENTE	81	6

**2.4.13 Software. (De 195 tickets registrados pendientes por resolver 28).**

LUK

No. REGISTRO	TICKET	CREACION	PRIORIDAD	ESTADO	Nro. horas sin resolver	Tiempo de solución máximo - horas (IM OC OFI IF 004)
1	303	16/10/2019	BAJA	PLANEADO	1665	6
2	1033	3/12/2019	ALTA	PLANEADO	1359	6
3	2531	14/02/2020	BAJA	PLANEADO	882	6
4	2708	20/02/2020	ALTA	PENDIENTE	846	6
5	2738	21/02/2020	ALTA	PLANEADO	837	6
6	3231	13/03/2020	ALTA	PLANEADO	702	6
7	3252	16/03/2020	ALTA	PLANEADO	693	6
8	3283	17/03/2020	ALTA	PLANEADO	684	6
9	3729	20/04/2020	ALTA	PLANEADO	468	6
10	3973	4/05/2020	ALTA	PLANEADO	378	6
11	4069	8/05/2020	ALTA	PLANEADO	342	6
12	4075	8/05/2020	ALTA	PLANEADO	342	6
13	4522	3/06/2020	ALTA	PLANEADO	180	6
14	4532	3/06/2020	ALTA	PENDIENTE	180	6
15	4542	4/06/2020	ALTA	PENDIENTE	171	6
16	4554	4/06/2020	ALTA	PENDIENTE	171	6
17	4561	4/06/2020	ALTA	PENDIENTE	171	6
18	4595	8/06/2020	ALTA	PENDIENTE	153	6
19	4613	9/06/2020	ALTA	PENDIENTE	144	6
20	4636	10/06/2020	ALTA	PENDIENTE	135	6
21	4656	10/06/2020	ALTA	PENDIENTE	135	6
22	4693	11/06/2020	ALTA	PENDIENTE	126	6
23	4716	12/06/2020	ALTA	PENDIENTE	117	6
24	4721	12/06/2020	BAJA	PLANEADO	117	6
25	4740	16/06/2020	ALTA	PENDIENTE	99	8
26	4809	23/06/2020	ALTA	PENDIENTE	54	6
27	4815	23/06/2020	SIN ASIGNAR	PENDIENTE	54	6
28	4821	23/06/2020	ALTA	PLANEADO	54	6

## 2.5 Requerimientos cerrados sin dar la solución al caso.

Se realizó una verificación selectiva de los requerimientos que tienen en la base de datos estado igual "Cerrado", y se efectuó indagación con las divisiones de personal, operaciones financieras, comercial y oficina control interno, observando que se cierran requerimientos que aún no se le ha dado solución eficaz al caso, a continuación, se detallan:

TICKET	ASUNTO	FECHA CREACIÓN	REQUERIMIENTO AL 30 JUNIO DE 2020 - ESTADO INFORMADO POR LA DEPENDENCIA	DEPENDENCIA
514	ARREGLO UPS	30/10/2019	Se solicitó el arreglo de la UPS ubicada en el Almacén de Valledupar. Lo anterior debido a que este dispositivo se encuentra fuera de servicio desde el mes de mayo de 2019, el cual fue informado con documento No. 02.166.689.	División Almacenes Comerciales
532	IMPRESORA	30/10/2019	Solicitó revisión con carácter urgente la impresora asignada al almacén de Montería, la cual dejó de funcionar después de una baja de energía.	División Almacenes Comerciales
562	SOLICITUD INFORMACIÓN NÓMINA SAP PARA CIERRE FINANCIERO 2019	1/11/2019	A la fecha no se ha recibido el solicitado reporte, adicionalmente las cesantías se encuentran en estado de revisión pues se generaron para los certificados de ingresos y retenciones con algunas que se deben volver a revisar.	División de Personal
699	IMPRESORA	12/11/2019	Solicitó revisión con carácter urgente la impresora asignada al almacén de Montería, la cual dejó de funcionar después de una baja de energía.	División Almacenes Comerciales

WOK

798	SOLICITUD DISTRIBUCIÓN PAGO CONCEPTOS VACACIONES	18/11/2019	Respecto de la revisión de vacaciones a la fecha no se ha recibido el correspondiente ajuste, de tal forma que para este año se creó un nuevo caso para revisar el cálculo por estos conceptos; o anterior teniendo en cuenta la contingencia por la pandemia.	División de Personal
1251	SOLICITUD AJUSTE FACTORES PRIMA NAVIDAD NÓMINA SAP	17/12/2019	Este requerimiento se encuentra pendiente pues a la fecha no se evidencian pruebas realizadas o casos aplicados a algún funcionario.	División de Personal
1255	BASES CÁLCULO PRIMA DE NAVIDAD	18/12/2019	Este requerimiento se encuentra pendiente pues a la fecha no se evidencian pruebas realizadas o casos aplicados a algún funcionario.	División de Personal
1709	SE ACTIVE LA FIRMA DIGITAL PARA LOS ALMACENES	20/01/2020	Con toda atención me permito solicitar se active en todos los Almacenes Comerciales la posibilidad de firmar los documentos electrónicamente , lo anterior teniendo en cuenta que ya ellos cuentan con certicamaras pero a la fecha no ha sido posible que les activen lo que falta para que puedan firmar los documentos digitalmente, tener en cuenta que debemos cerrar un hallazgo de control interno, el cual ya está vencido.	División Almacenes Comerciales
2001	REVISIÓN EL EQUIPO DE COMPUTO	28/01/2020	El almacén de Sogamoso tiene equipo nuevo, pero sin configurar.	División Almacenes Comerciales
2306	SOLICITUD HABILITACIÓN USUARIO NOMINA SAP	6/02/2020	A la fecha se evidencian transacciones a las que no se tiene acceso como es la de emisión de los certificados de ingresos y retenciones.	División de Personal
2403	ENVÍO EQUIPO DE COMPUTO NUEVO	11/02/2020	Estos equipos están en los almacenes de Montería y Corozal pero no están instalados, se requiere se configuren e instalen.	División Almacenes Comerciales
2423	SOLICITUD SISTEMA CHIP	11/02/2020	No se ha dado la solución al caso, por cuanto no ha sido instalado el sistema CHIP en el computador de la funcionaria designada para presentar el informe anual como todos los años se venía realizando.	División de Personal
2548	ERROR INGRESO MATERIAL	14/02/2020	En el mes de febrero e inicio de marzo la oficina de informática informa que no hay contrato con los consultores SAP S4/HANA. Así mismo este fue cerrado, sin corregir la intención de los requerimientos, se vuelven a montar mesa de ayuda el 26 de mayo con el caso # 4274 el cual a la fecha se encuentra en estado planeado sin existir una respuesta.	División Operaciones Financieras
2594	SE ACTIVE LA FIRMA DIGITAL PARA LOS ALMACENES	17/02/2020	Con toda atención me permito solicitar se active en todos los Almacenes Comerciales la posibilidad de firmar los documentos electrónicamente , lo anterior teniendo en cuenta que ya ellos cuentan con certicamaras pero a la fecha no ha sido posible que les activen lo que falta para que puedan firmar los documentos digitalmente, tener en cuenta que debemos cerrar un hallazgo de control interno, el cual ya está vencido.	División Almacenes Comerciales
3135	SOLICITUD AJUSTE CUOTA APOYO DE SOSTEMIENTO APRENDICES PRODUCTIVOS 2020	10/03/2020	A la fecha no se ha cumplido la solicitud, de modo que el proceso se hace manual.	División de Personal

LUCR

3146	SOLICITUD CREACIÓN JUZGADO 41	11/03/2020	Este requerimiento se encuentra pendiente.	División de Personal
3151	SOLICITUD GENERACIÓN DESPRENDIBLES PENSIONADO	11/03/2020	El funcionario a la fecha sigue llamando porque a un no le han creado el usuario y la clave.	División de Personal
4182	APOYO SYNERGY	18/05/2020	Me permito solicitar se preste apoyo a fin de verificar los complementos synergy al usuario ocsba25, con el fin de que pueda realizar trabajo en casa, dado que al querer realizar oficios y le arroja el error que se anexa en adjuntos.	División Almacenes Comerciales
4536	SOLICITUD CONFIGURACIÓN COMPLEMENTOS	3/06/2020	El 5 de agosto se generó otro requerimiento No. 5565 me permito solicitar ser revise el synergy en el almacén de Pereira, el cual lleva más de un mes sin poder elaborar documentos en el gestor documental.	División Almacenes Comerciales
4575	FALLAS SISTEMA E-SYNERGY	5/06/2020	El 15 de julio se generó otro requerimiento No. 5204 el soporte no se realizó	Oficina Control Interno
5046	SOLICITUD REVISIÓN SYNERGY	7/07/2020	Revisión de synergy a los siguientes usuarios almacén Pereira no permite descargar documentos, al usuario OCSBA25 no deja guardar documentos.	División Almacenes Comerciales
5310	SOLICITUD REVISIÓN SYNERGY	22/07/2020	Revisión synergy almacén pasto no le permite observar documentos.	División Almacenes Comerciales

**2.6 Cierre de tickets de SAP S4/HANA pendientes por finalización del contrato soporte.**

Durante el desarrollo de la Auditoría se evidenció que el 9 de julio de 2020 la División de Operaciones Financieras generó el ticket No. 5100 en la mesa de ayuda - GLPI solicitando apoyo para la solución al error que está generando el sistema SAP en el momento de dar ingreso a las facturas de servicio de alimentación del contrato 1-155 de 2019. La Oficina de Informática por correo electrónico del 5 de agosto de 2020 informa al Jefe de la División de Operaciones Financieras "Se cierra el caso por finalización del contrato de soporte y su vez se inicia un nuevo contrato de soporte con la firma EPI USE con modalidad de horas en donde se va a controlar los acuerdos de servicio en donde se va a medir la atención del servicio por lo que prácticamente no se va a tener en cuenta este requerimiento por no estar dentro del alcance de este nuevo soporte. Si no se ha solucionado este caso entonces se requiere crear un nuevo caso con la información completa para ser tenido en cuenta en esta nueva fase de soporte".

Evidenciando que la atención de solicitudes de servicio de soporte técnico no ha sido eficaz afectando la eficacia y oportunidad de la atención a las solicitudes de servicio reportadas por los usuarios de la Industria Militar.

**3. CORREO ELECTRÓNICO**

**3.1. Capacidad del Correo Electrónico.**

En desarrollo de la auditoría la Oficina de Informática en documento No. 02.303.911 - Informe Auditoría Proceso Gestión Informática del 18 de junio de 2020 informa en el numeral 9: "La Industria Militar ha tenido diferentes configuraciones en cuanto a la capacidad del correo electrónico y con base

LWVA

a la recopilación de las encuestas realizadas en el año 2019 se identificó la necesidad de ampliación de los buzones por lo cual el tema fue tratado por el comité técnico de seguridad de la información y aprueba la nueva configuración así: Directivos con capacidad de 500 megas para cada miembro; Jefes de División con capacidad de 200 megas para cada miembro y Funcionarios con capacidad de 75 megas por cada miembro”.

La Oficina de Informática como evidencia de la ampliación entregó archivo en Word con las imágenes de la configuración realizada a las tres bases de datos (Directivos, Jefes de División y Funcionarios).

“Para el año 2020 y teniendo en cuenta los problemas reportados por capacidad del buzón a la Oficina de Informática en el trabajo remoto en casa, en la reunión del Comité de Seguridad de la Información realizada el 8 de junio de 2020 la Oficina de Informática presentó la propuesta para la ampliación de los buzones, y se aprueba la nueva configuración: Directivos 1GB, Jefes de División 500 MB y funcionarios 500 MB. El tamaño de adjuntos para enviar y recibir correos hasta 15 MB por correo realizando la configuración en cada una de las bases”.

La Oficina de Informática como evidencia de la ampliación entregó el archivo en PDF llamado “Anexo\_Caso\_4715\_Ampliación buzones servidor Exchange”.

### 3.2 LOG Correo Electrónico.

En desarrollo de la auditoría la Oficina de Informática en documento No. 02.303.911 – “Informe Auditoría Proceso Gestión Informática” del 18 de junio de 2020 informa en el numeral 11. “La plataforma no cuenta con un monitoreo de log de ser requerido se mostrará la herramienta y el manejo de ella”.

La herramienta adquirida por la Industria Militar es de propiedad de Microsoft, el cual no dispone en su plataforma de un log o registro de eventos con el fin de detectar de las cuentas del correo electrónico actividades de procesamiento no autorizadas sobre la información enviada o recibida.

### 3.3 Acceso al Correo Electrónico Microsoft Exchange.

En desarrollo de la auditoría la Oficina de Informática en documento No. 02.303.911 – “Informe Auditoría Proceso Gestión Informática” del 18 de junio de 2020 informa “Cuando un funcionario requiere acceso al correo electrónico, se realiza la solicitud por la mesa de ayuda por la categoría correo electrónico – subcategoría instalación/configuración requiriendo usuario de dominio y correo.

Los usuarios que conforman el grupo directivo son quienes cuentan con el permiso para el acceso del correo corporativo en dispositivos móviles o IPAD. Los dispositivos móviles o IPAD son de propiedad de la Industria Militar y tienen activo fijo, no se realiza configuración en equipos personales y de verse la necesidad debe ser autorizada por el Comité Técnico de Seguridad de la Información.

El grupo Directivo firman la cláusula de confidencialidad en el contrato para el tratamiento de los datos.”.

La Industria Militar dispone de la Política de Seguridad y Privacidad de la Información Cód: IM OC OFI CP 003. Rev.8.

La Industria Militar implementó la “Política para el uso de dispositivos móviles” Cód: IM OC OFI CP 004. Rev.3. cuyo objetivo es “Limitar, establecer y dar a conocer las políticas relacionadas con el control de acceso lógico, dirigido hacia la protección de la información, restricción de acceso a

1002

personas no autorizadas a los recursos tecnológicos de INDUMIL, que estén asociados al Proceso GESTIÓN INFORMÁTICA" y establecen "Cualquier incumplimiento de las políticas establecidas en este documento por parte de los funcionarios de la empresa acarreará las correspondientes sanciones disciplinarias".

#### **4. GESTIÓN DE RESPALDOS Y PRUEBAS REALIZADAS A LAS COPIAS DE RESPALDO**

Se realizó verificación al cumplimiento descrito en la Norma Técnica NTC-ISO-IEC 27001, numeral A.12.3.1 "Respaldo de la Información" y en el Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006, Rev. 10. numeral 4.4 "Revisión de ejecución y verificación de Backups", evidenciando:

##### **4.1. GESTIÓN DE RESPALDOS.**

En desarrollo de la auditoría la Oficina de Informática en documento No. 02.303.911 del 18 de junio de 2020 informa: "La Industria Militar adquirió la herramienta de Gestión de respaldos de información Symantec Backup Exec – Veritas versión 16.0 por medio de la cual se programan las políticas de respaldo para los sistemas de información de INDUMIL de acuerdo a los lineamientos establecidos en el Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006, Rev. 10 e Instructivo Creación y Ejecución de Políticas de Respaldo para Symantec Backup Exec Cód: IM OC OFI IN 006 Rev.4.

La herramienta de Gestión de respaldos de información Symantec Backup Exec – Veritas versión 16.0 se encuentra instalada en el Data Center (Centrales).

El Gestor de Respaldos de la Oficina de Informática es el administrador de la herramienta Symantec Backup Exec – Veritas en la cual programa, ejecuta y monitorea los respaldos en las cintas.

Se realizan copias de seguridad a los sistemas de operativos, aplicaciones corporativas, dispositivos de red y conectividad, logs de servidores y bases de datos de manera periódica diaria, semanal, mensual y anualmente.

Como soporte la oficina de informática envió archivo en excel llamado Respaldos Abril 2020 – Seguimiento de Respaldos IM OC OFI FO 024 Rev. 2 del mes de abril de 2020 en donde se evidencia la ejecución de las copias de respaldo de acuerdo a la política: Diarias - Respaldos de información de las bases de datos - Lunes a viernes, Semanal - Imágenes - Imagen de los servidores Críticos - Fines de semana - Incluye S.O. Datos , configuración del servidor y Mensual - Imágenes de todos los servidores - Durante el mes + Incluye S.O. Datos , configuración del servidor.

En cuanto a la custodia de los medios magnéticos las copias de respaldo se guardan en Oficinas Centrales (centro de cómputo principal) y en la Fábrica de Explosivos Antonio Ricaurte (centro de cómputo alterno), garantizando la seguridad y confidencialidad de la información, durante la pandemia no se han enviado a la Fábrica de explosivos Antonio Ricaurte (centro de cómputo alterno)".

##### **4.2. PRUEBAS DE RESTAURACIÓN DE CINTAS DE RESPALDOS DE INFORMACIÓN.**

En desarrollo de la auditoría la Oficina de Informática en documento No. 02.303.911 del 18 de junio de 2020 informa en el numeral 18, "Las pruebas de restauración de cintas de respaldos de información se ejecutaban en el Data Center Alterno porque allí contaba con los requerimientos apropiados como es: - espacio físico suficiente, - se dispone de tiempo suficiente del servidor Ismael t y Unidad de Cinta TL200 ya que la carga de trabajos realizados allí es mínima, - no se afecta la calidad de servicio a los

LWR

*usuarios ya que no se hace uso de la red, - no se sobrecarga los procesos de respaldos en Oficinas Centrales.*

*Este proceso no se ha ejecutado por que se presentaron las siguientes novedades que han impedido su realización:*

*En Noviembre de 2018 se procedió a realizar un cambio de política de respaldos DLO que estaba en versión 7.6. al momento de aplicar la nueva política se presentaron errores por lo que se solicitó soporte a Veritas, al revisar el error manifestaron que la política que se estaba implementado no era compatible con la versión del DLO y que además esta versión no tenía soporte por lo que recomendaron actualizar la versión a la 9.3 ya que esta versión corregía el error presentado y si tenía soporte.*

*Se decidió actualizar la versión de DLO a la versión 9.3 y se aprovechó para actualizar la versión de Backup exec que estaba en 16.0 para pasarla a la versión 20.3.*

*Se procedió a realizar la actividad en Data Center principal se realizó la actualización de DLO a la versión 9.3 y Backup exec a la versión 20.3.*

*En Data Center Alterno no se pudo realizar la actualización Backup exec por que el centro de cómputo tenía el inconveniente con el aire acondicionado, servidor Ismael y la unidad de cinta TL200 se encontraban apagados.*

*Una vez solucionado el inconveniente del aire acondicionado se pretendió actualizar la versión de Backup exec pero no se pudo por qué no se contaba con contrato de mantenimiento - soporte de veritas.*

*El 3 de abril de 2020 se procedió a realizar la actualización de versión, pero para esta época las licencias de veritas estaban vencidas y no tenían soporte por lo que dejo instalar únicamente una versión de prueba por 60 días.*

*Pasados los 60 días se empezó a presentar el incidente de no funcionamiento de la herramienta.*

*Se ha tratado de instalar otra versión de prueba, pero no lo permite.*

*Soporte entregado como evidencia es un archivo en Word llamado "Respaldos Fexar" en este se encuentra la imagen del correo electrónico del 5 de junio de 2020 enviado por el Gestor de Respaldos al Jefe Oficina de Informática donde informa que se presentó novedad en FEXAR en los respaldos de información que las licencias de backup exec están vencidas, se anexó en el correo el pantallazo del error".*

*Al revisar la Matriz de Riesgos y Oportunidades Primer Cuatrimestre 2020 Cód: IM OC OFP FO 117 Rev.5. del Proceso Gestión Informática no se encontró identificado la situación de no realizar pruebas de restauración de cintas de respaldo.*

*Al 22 de octubre de 2020 se observa que la Industria Militar se encuentra en proceso de contratación para la adquisición e Instalación de Equipos y Software para la fase II de la Renovación del Centro de Cómputo de la Industria Militar – Solución Hiperconvergente en el cual se tiene contemplado entre otros adquirir para el Data Center Principal (Centrales) y Data Center Alterno (FEXAR) la "Solución de Almacenamiento en Discos para Respaldo" que permite generar backup y restauración en los ambientes virtuales y físicos como los diferentes sistemas de información (Windows, Linux, SQL, S/4HANA, Exchange, entre otros).*

look

Evidenciando incumplimiento al control establecido en el Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006 Rev.10. Numeral 4.4. "Revisión de ejecución y Verificación de Backups" con el riesgo de afectación a los principios de integridad y disponibilidad de la información.

## 5. PROVEEDORES

En desarrollo de la Auditoria la Oficina de Informática con documento No. 02.303.911 – "Informe de Auditoria Proceso Gestión Informática" del 18 de junio de 2020 informa en el numeral 20 "Anualmente se realiza auditorías a los proveedores TI, la persona encargada de esta labor es el OSI (Oficial de Seguridad de la Información), se envía los archivos Auditoria proveedores 2017, Auditoria proveedores 2018, Auditoria proveedores 2019 y Programa de Auditoria proveedores 2020".

Se realizo verificación al cumplimiento a lo dispuesto en la Norma Técnica NTC-ISO-IEC 27001, numeral A.15.2.1 Seguimiento y revisión de los servicios de los proveedores. "Las organizaciones deben hacer seguimiento, revisar y Auditar con regularidad la prestación de servicios de los proveedores", evidenciando:

Se está desarrollando auditorías a todos los proveedores que deben acceder a la información de la Industria Militar, a continuación se muestran por vigencias:

### 5.1 PROVEEDORES INFORMÁTICA – AUDITORÍA A LA VIGENCIA 2017

El proceso de Gestión Informática elaboró contratos que involucran tecnología informática con nueve (9) proveedores, a continuación se relacionan:

No. CONTRATO	NOMBRE PROVEEDOR	OBJETO
175/2017	ORIGIN IT SAS	RENOVACIÓN INFRAESTRUCTURA DE COMUNICACIONES
167/2017	UNION TEMPORAL AVANZA 2018	SERVICIO IMPLEMENTACIÓN TERCERA FASE SAP
165/2017	INTELLIGENT BUSINESSES SAS	ADQUISICIÓN EQUIPOS DE TECNOLOGÍA INFORMÁTICA
160/2017	EPI USE COLOMBIA SAS	SERVICIO SOPORTE ERP-SAP S/4HANA
152/2017	ORIGIN IT SAS	SERVICIO EXTENSIÓN DE GARANTÍA INFRAESTRUCTURA EQUIPOS CENTRO COMPUTO
151/2017	AXEDE SA	SERVICIO DE MANTENIMIENTO, SOPORTE RED DE VOZ, DATOS Y COMUNICACIONES
147/2017	SAP COLOMBIA SAS	ADQUISICIÓN LICENCIAMIENTO SAP
131/2017	SAP COLOMBIA SAS	SERVICIO RENOVACIÓN LICENCIAMIENTO PLATAFORMA SAP
122/2017	UNE EPM TELECOMUNICACIONES SA	SERVICIO ARRENDAMIENTO ENLACES DE COMUNICACIÓN E INTERNET-CONTINGENCIA
121/2017	EMPRESA DE TELECOMUNICACIONES DE BOGOTA ETB SA ESP	SERVICIO ARRENDAMIENTO ENLACES DE COMUNICACIÓN E INTERNET

Al revisar las auditorías ejecutadas por el Proceso de Gestión Informática según programa de auditorías Cód: IM OC OFP FO 024 Rev.6. se programaron realizar dos (2) auditorías a los proveedores UNIÓN TEMPORAL AVANZA 2018 y EPI USE COLOMBIA SAS, que equivalen al 22% de los nueve (9) proveedores que prestaron servicios tecnológicos a INDUMIL.

### 5.2 PROVEEDORES INFORMÁTICA – AUDITORÍA A LA VIGENCIA 2018

LUVK

El proceso de Gestión Informática elaboró contratos que involucran tecnología informática con nueve (7) proveedores, a continuación se relacionan:

No. CONTRATO	NOMBRE PROVEEDOR	OBJETO
132/2018	UPS INGENIERIA LTDA	ADQUISICIÓN EQUIPOS AIRES ACONDICIONADOS Y UPS.
119/2018	SOLUCIONES TECNOLOGIA Y SERVICIOS SA	ADQUISICIÓN SOLUCION DE SEGURIDAD AVANZADA PROXY- FIREWAL.
090/2018	SYSTEM NET INGENIERIA LTDA	SERVICIO DE MANTENIMIENTO, PREVENTIVO CORRECTIVO TECNOLOGIA INFORMATICA.
089/2018	STARCOMPUTO DE COLOMBIA SAS	SERVICIO DE MANTENIMIENTO, PREVENTIVO CORRECTIVO TECNOLOGIA INFORMATICA.
088/2018	ING LTDA	SERVICIO DE MANTENIMIENTO, PREVENTIVO CORRECTIVO TECNOLOGIA INFORMATICA.
087/2018	IIS TECHNOLOGY SOLUTIONS SAS	SERVICIO DE MANTENIMIENTO, PREVENTIVO CORRECTIVO TECNOLOGIA INFORMATICA.
083/2018	ORIGIN IT SAS	ADQUISICION DE EQUIPOS DE TECNOLOGIA INFORMATICA.

Se observa que para la vigencia 2018 los proveedores relacionados para desarrollar sus labores no acceden a la información de la Industria Militar, por lo anterior no se desarrollaron auditorías a estos.

### 5.3 PROVEEDORES INFORMÁTICA – AUDITORÍA A LA VIGENCIA 2019

El proceso de Gestión Informática elaboró contratos que involucran tecnología informática con nueve (11) proveedores, a continuación se relacionan:

No. CONTRATO	NOMBRE PROVEEDOR	OBJETO
197/2019	ORIGIN IT SAS	ADQUISICIÓN DE EQUIPOS DE TECNOLOGIA INFORMATICA E INSTALACION DE SERVER PARA LAS ÁREAS INGENIERIA TÉCNICA.
193/2019	REDCOMPUTO LTDA	ADQUISICIÓN EQUIPOS DE INFORMÁTICA.
176/2019	ENGINEERING SIMULATION AND SCIENTIFIC SOFTWARE COLOMBIA SAS	ADQUISICIÓN DE SOFTWARE PARA LAS ÁREAS INGENIERIA TÉCNICA Y SERVICIO DE IMPLEMENTACIÓN VAULT PROFESIONAL.
175/2019	CIMEX SA	ADQUISICIÓN DE SOFTWARE PARA LAS ÁREAS INGENIERIA TÉCNICA Y SERVICIO DE IMPLEMENTACIÓN VAULT PROFESIONAL.
174/2019	INGENIERIA ASISTIDA POR COMPUTADOR	ADQUISICIÓN DE SOFTWARE PARA LAS ÁREAS INGENIERIA TÉCNICA Y SERVICIO DE IMPLEMENTACIÓN VAULT PROFESIONAL.
154/2019	P C MICROS LTDA.	SERVICIO DE MANTENIMIENTO CORRECTIVO Y SOPORTE ESPECIALIZADO DE HARDWARE Y SOFTWARE DE LA INFRAESTRUCTURA INFORMÁTICA.
153/2019	SOLUCIONES SUMINISTROS CR SAS	SERVICIO DE MANTENIMIENTO CORRECTIVO Y SOPORTE ESPECIALIZADO DE HARDWARE Y SOFTWARE DE LA INFRAESTRUCTURA INFORMÁTICA.
148/2019	GLOBAL TECHNOLOGY SERVICES GTS SA	ADQUISICIÓN E INSTALACIÓN DE (02) AIRES ACONDICIONADOS DE PRECISIÓN Y LA ADECUACIÓN O EL ACONDICIONAMIENTO DE UN SISTEMA CONTAINMENT PARA EL CENTRO DE CÓMPUTO.

*WOK*

131/2019	ORIGIN IT SAS	ADQUISICIÓN E INSTALACION DE EQUIPOS Y SOFTWARE RENOVACIÓN DEL CENTRO DE COMPUTO - SOLUCION HIPERCONVERGENTE.
022/2019	EMPRESA DE TELECOMUNICACIONES DE BOGOTA ETB SA ESP	SERVICIO DE ENLACES DE COMUNICACIÓN E INTERNET.
020/2019	B EXCELLENCE SAS	SERVICIO DE ACTUALIZACIÓN DE LICENCIAMIENTO DEL SOFTWARE SYNERGY MANTENIMIENTO, SOPORTE Y DESARROLLO.
014/2019	EPI USE COLOMBIA SAS	SERVICIO SOPORTE ERP SAP / S4 HANA.

Al revisar las auditorías ejecutadas por el Proceso de Gestión Informática según programa de auditorías Cód: IM OC OFF FO 024 Rev.6. se programó realizar una (1) auditoría al proveedor EPI USE COLOMBIA SAS, que equivale al 8% de los nueve (11) proveedores que prestaron servicios tecnológicos a INDUMIL.

#### 5.4 PROVEEDORES INFORMÁTICA – AUDITORÍA A LA VIGENCIA 2020

En el programa de auditorías Cód. IM OC OFF FO 024 Rev.8. se tienen contempladas tres auditorías a los proveedores que ganen el contrato de soporte en SAP, el proyecto de Ethical y/o remediación y el proceso de Firewall para los meses octubre, noviembre y diciembre de 2020.

Cumpliendo la Política de Seguridad de la Información para la Relación con Proveedores Cód: IM OC OFI CP 002 Rev.7. numeral 3.9. y la norma Técnica Colombiana NTC-ISO-IEC 27001 – 2013-12-11, numeral A.15.2.1 Seguimiento y revisión de los servicios de los proveedores. *“Las organizaciones deben hacer seguimiento, revisar y Auditar con regularidad la prestación de servicios de los proveedores”*.

#### 6. ACCESO REMOTO

Durante el desarrollo de la Auditoría la Oficina de Informática con documento No. 02.303.911 – *“Informe Auditoria Proceso Gestión Informática”* del 18 de junio de 2020 informa en el numeral 16 *“Los ingresos remotos que realiza el personal de la oficina de informática a los equipos TI de la Industria Militar son únicamente para soportes a los servicios de TI y se realizan con autorización verbal del funcionario”*. Se envía archivo llamado *“Soporte remoto”* con el reporte de los soportes remotos realizados desde el año 2018 hasta el 10 de junio de 2020”.

Al verificar la información registrada en el archivo *“Soporte remoto”* se evidenció que contiene 6.197 registros que corresponden a los soportes remotos efectuados desde el 3 de enero de 2018 hasta el 10 de junio de 2020 de los cuales noventa (90) registros se encontraron con tiempos de soporte remoto de más de una hora, sin obtener la evidencia de autorización a la labor desarrollada, así:

Estación Equipo Informática	IP destino	Estación destino Funcionario	Fecha Inicio Soporte	Fecha final soporte	Tiempo Total Soporte Remoto (En horas)
C614YV1	172.17.9.12	8Z13SW1	18/01/2019 15:03	21/01/2019 7:07	51
C614YV1	43NR7V1	43NR7V1	4/09/2019 13:05	5/09/2019 7:32	18
F8JHM22	172.16.8.97	F8GHM22	19/06/2018 13:53	20/06/2018 7:03	17
C614YV1	172.16.5.35	8YZCSW1	17/07/2019 15:08	18/07/2019 7:37	16
F8HVM22	8Z44SW1	8Z44SW1	1/11/2019 20:37	2/11/2019 10:43	14

LWR

Synergy No (1). 02.373.149

Fecha (2) : 07-dic-2020

CHRZM22	1SST8Y1	1SST8Y1	20/04/2020 9:28	20/04/2020 17:02	7:34
CHRZM22	1SSW8Y1	1SSW8Y1	1/06/2020 12:13	1/06/2020 16:00	3:47
F8JHM22	C6S5YV1	C6S5YV1	22/02/2019 12:58	22/02/2019 15:41	2:43
CHRZM22	172.17.9.3	8YYFSW1	1/02/2018 6:30	1/02/2018 9:08	2:38
CHRZM22	172.18.7.7	1V8V8Y1	9/03/2018 12:35	9/03/2018 15:07	2:32
F8JHM22	8YY8SW1	8YY8SW1	2/04/2020 12:26	2/04/2020 14:44	2:18
CHRZM22	172.17.9.6	1RC0182	8/08/2019 10:11	8/08/2019 12:24	2:13
CHPZM22	SALOMON	SALOMON	17/01/2019 6:42	17/01/2019 8:49	2:07
F8JHM22	172.16.7.10	8YZDSW1	15/01/2018 9:44	15/01/2018 11:46	2:02
F8HVM22	1V7T8Y1	1V7T8Y1	28/03/2019 9:52	28/03/2019 11:52	2:00
CHRZM22	172.17.13.4	1T6T8Y1	22/03/2018 7:23	22/03/2018 9:19	1:56
F8HVM22	43GRFZ1	43GRFZ1	1/04/2020 12:00	1/04/2020 13:53	1:53
C614YV1	172.16.6.3	C619YV1	13/04/2020 8:51	13/04/2020 10:43	1:52
CHRZM22	172.17.12.3	8Z4CSW1	26/05/2020 9:41	26/05/2020 11:33	1:52
F8JHM22	8Z29SW1	8Z29SW1	17/07/2019 9:46	17/07/2019 11:38	1:52
F8JHM22	D0VNQ22	D0VNQ22	15/05/2019 8:31	15/05/2019 10:22	1:51
CHRZM22	8YXFSW1	8YXFSW1	30/04/2020 10:28	30/04/2020 12:13	1:45
CHRZM22	8YXFSW1	8YXFSW1	4/05/2020 8:56	4/05/2020 10:35	1:39
CHRZM22	172.18.16.2	1T4V8Y1	17/12/2018 8:30	17/12/2018 10:08	1:38
F8JHM22	CHRTM22	CHRTM22	10/06/2020 11:37	10/06/2020 13:14	1:37
F8JHM22	1T2W8Y1	1T2W8Y1	13/05/2019 8:54	13/05/2019 10:26	1:34
F8HVM22	1VBT8Y1	1VBT8Y1	28/10/2019 19:19	28/10/2019 20:53	1:34
CHRZM22	4D028474H	4D028474H	5/03/2020 10:23	5/03/2020 11:55	1:32
F8JHM22	F8M0N22	F8M0N22	13/05/2019 8:55	13/05/2019 10:26	1:31
F8JHM22	172.16.6.43	F8G1N22	4/06/2020 9:31	4/06/2020 11:02	1:31
F8JHM22	43QH7V1	43QH7V1	18/01/2018 9:01	18/01/2018 10:31	1:30
F8HVM22	43GRFZ1	43GRFZ1	31/03/2020 10:20	31/03/2020 11:50	1:30
CHRZM22	1SST8Y1	1SST8Y1	28/05/2020 11:56	28/05/2020 13:25	1:29
CHRZM22	172.18.13.26	1RBZ082	30/01/2018 9:25	30/01/2018 10:49	1:24
C614YV1	172.16.8.10	8Z02SW1	2/06/2020 10:26	2/06/2020 11:50	1:24
CNU0450T25	C6J6YV1	C6J6YV1	22/01/2018 10:19	22/01/2018 11:41	1:22
CHRZM22	172.17.13.22	D2YCS22	17/06/2019 11:13	17/06/2019 12:34	1:21
F8HVM22	1T1T8Y1	1T1T8Y1	1/03/2019 10:44	1/03/2019 12:04	1:20
CHQZM22	1RD0182	1RD0182	14/05/2019 14:43	14/05/2019 16:02	1:19
CHPZM22	1R6Z082	1R6Z082	21/01/2020 12:19	21/01/2020 13:35	1:16
CHQZM22	F8HVM22	F8HVM22	21/05/2019 8:40	21/05/2019 9:55	1:15
F8JHM22	43PM7V1	43PM7V1	5/03/2019 7:40	5/03/2019 8:55	1:15
F8HVM22	47KH7V1	47KH7V1	20/08/2019 11:20	20/08/2019 12:33	1:13
CHRZM22	172.17.9.22	1V4T8Y1	27/04/2020 9:49	27/04/2020 11:02	1:13
F8JHM22	F8LZM22	F8LZM22	28/11/2019 9:46	28/11/2019 10:57	1:11
D2ZLQ22	17D2QW1	17D2QW1	21/05/2019 14:54	21/05/2019 16:02	1:08
C614YV1	172.16.5.13	C615YV1	12/02/2020 14:32	12/02/2020 15:40	1:08
F8HVM22	172.18.14.2	1V1W8Y1	28/02/2020 12:38	28/02/2020 13:46	1:08
D0WFS22	1SPT8Y1	1SPT8Y1	4/03/2020 14:16	4/03/2020 15:24	1:08
F8JHM22	172.16.8.56	1RK0182	12/05/2020 8:59	12/05/2020 10:07	1:08
CHRZM22	D0YNQ22	D0YNQ22	5/06/2020 7:57	5/06/2020 9:05	1:08
C614YV1	172.20.8.2	C6Q4YV1	9/06/2020 10:31	9/06/2020 11:39	1:08
F8JHM22	172.16.8.15	8Z06SW1	16/01/2018 14:53	16/01/2018 16:00	1:07
F8JHM22	172.50.55.3	C5W5YV1	18/01/2018 9:31	18/01/2018 10:38	1:07
F8JHM22	C629YV1	C629YV1	30/10/2019 15:42	30/10/2019 16:48	1:06

1002

CNU0450T25	2UA3310QKD	2UA3310QKD	9/07/2018 9:09	9/07/2018 10:14	1:05
C614YV1	172.16.6.150	8YZ2SW1	6/05/2019 11:24	6/05/2019 12:28	1:04
CHRZM22	172.17.16.3	43GRFZ1	8/04/2020 11:43	8/04/2020 12:47	1:04
CHRZM22	172.18.9.6	47HH7V1	17/01/2018 11:52	17/01/2018 12:56	1:04
D0WFS22	17M3QW1	17M3QW1	28/04/2020 10:06	28/04/2020 11:10	1:04
C614YV1	172.16.31.73	4D027018H	16/01/2018 16:05	16/01/2018 17:08	1:03
F8HVM22	8YWDSW1	8YWDSW1	20/03/2019 15:00	20/03/2019 16:03	1:03
C614YV1	172.16.6.13	C6B7YV1	17/01/2018 9:08	17/01/2018 10:10	1:02
F8JHM22	172.16.5.26	C6K6YV1	17/01/2018 11:47	17/01/2018 12:49	1:02
1V2W8Y1	172.19.7.7	F8FJM22	5/11/2019 10:34	5/11/2019 11:36	1:02
C614YV1	172.16.13.18	8YZ1SW1	12/07/2019 10:43	12/07/2019 11:45	1:02
C614YV1	172.16.8.8	8Z46SW1	10/02/2020 14:33	10/02/2020 15:35	1:02
CHRZM22	172.17.8.20	433QFZ1	6/02/2018 9:32	6/02/2018 10:33	1:01
CHRZM22	172.16.11.2	CHQZM22	5/03/2018 12:53	5/03/2018 13:54	1:01
C614YV1	172.16.8.195	47LC7V1	22/01/2018 7:36	22/01/2018 8:37	1:01
CHRZM22	172.17.11.8	43BQFZ1	4/03/2019 8:27	4/03/2019 9:28	1:01
F8HVM22	43BPFZ1	43BPFZ1	19/09/2019 8:23	19/09/2019 9:24	1:01
F8HVM22	172.17.8.5	1V1V8Y1	11/03/2020 11:36	11/03/2020 12:37	1:01
C614YV1	172.16.16.11	1SPT8Y1	17/01/2018 10:46	17/01/2018 11:47	1:01
CHRZM22	172.17.13.5	1SST8Y1	6/11/2019 12:56	6/11/2019 13:57	1:01
C614YV1	172.20.8.2	C6Q4YV1	9/06/2020 9:01	9/06/2020 10:02	1:01
CHRZM22	172.17.9.3	8YYFSW1	18/01/2018 11:18	18/01/2018 12:19	1:01
1R20182	C619YV1	C619YV1	16/10/2019 13:33	16/10/2019 14:33	1:00
F8JHM22	42XQFZ1	42XQFZ1	14/11/2019 16:16	14/11/2019 17:16	1:00
F8HVM22	1SLT8Y1	1SLT8Y1	30/03/2020 15:48	30/03/2020 16:48	1:00
1R20182	42WRFZ1	42WRFZ1	19/01/2018 11:14	19/01/2018 12:14	1:00
F8JHM22	172.16.8.52	1RFZ082	26/06/2018 11:30	26/06/2018 12:30	1:00
CHRZM22	172.17.11.8	43BQFZ1	25/02/2019 7:11	25/02/2019 8:11	1:00
F8HVM22	CHWRM22	CHWRM22	28/03/2019 9:51	28/03/2019 10:51	1:00
F8JHM22	172.16.11.33	D0WFS22	30/03/2020 11:14	30/03/2020 12:14	1:00
CHRZM22	172.17.13.5	1SST8Y1	14/05/2020 6:45	14/05/2020 7:45	1:00
CHQZM22	1RD0182	1RD0182	9/05/2019 11:25	9/05/2019 12:25	1:00
D2ZLQ22	17D3QW1	17D3QW1	20/09/2019 8:22	20/09/2019 9:22	1:00
C614YV1	172.16.13.3	8YZ5SW1	24/01/2020 10:33	24/01/2020 11:33	1:00
CHRZM22	172.17.7.9	43MJ7V1	27/04/2020 14:08	27/04/2020 15:08	1:00

Generando posibles riesgos de afectación de la integridad, confidencialidad y oportunidad de la información existente en los equipos de cómputo que se toman por acceso remoto, por no tener establecidos controles que permitan tener la autorización por parte del usuario para desarrollar el soporte correspondiente y la trazabilidad de lo realizado en el equipo.

### 7. SEGREGACIÓN DE FUNCIONES

En el procedimiento Segregación de Funciones Cód: IM OC OFI PR 008 Rev. 4, en el numeral 4.1.1. Creación o Modificación de la Matriz de Segregación de Funciones "La Oficina de Informática es responsable de mantener actualizados los perfiles de usuario y los accesos a las plataformas para el procesamiento de la información, con base en la solicitud efectuada por el jefe de área respectiva generando la Matriz de Segregación de funciones IM OC OFI FO 012" encontrando que la matriz no se encuentra diligenciada.

*WKK*

Evidenciando que no se tiene control de la actualización de usuarios y de los accesos a las plataformas para el procesamiento de la información con el riesgo de uso inadecuado o no autorizado de la Información de la Industria Militar, afectando los principios de integridad, confidencialidad y oportunidad de la información.

## 8. INCIDENTE DE SEGURIDAD

### 8.1. Aires Acondicionados

Durante el desarrollo de la auditoría el auditor solicitó el 9 de junio de 2020 por correo electrónico a la oficina de informática la gestión realizada a los incidentes de seguridad vigencias 2017 al 2020. La Oficina de Informática con documento No. 02.303.911 – “Informe Auditoria Proceso Gestión Informática” del 18 de junio de 2020 envió archivo en excel con la relación de incidentes de seguridad de la información llamado “Resumen Incidentes Seguridad 2017 A 2020” al 12 de junio de 2020.

Al verificar el incidente “Falla del aire del centro de cómputo a causa de los cortes de energía eléctrica” se evidenció: reporte a la mesa de ayuda caso No. 3795 del 7 de marzo de 2020 con la siguiente información: nombre del incidente. “Falla del aire del centro de cómputo a causa de los cortes de energía eléctrica”, descripción del incidente. “Por falla en la energía eléctrica, los equipos de aire acondicionado se aseguraron y no arrancaron cuando se restableció el fluido eléctrico, haciendo que se elevara la temperatura del centro de datos y los equipos se aseguraran por las altas temperaturas”, acciones de mejoramiento implementadas: “1) Se solicitó soporte técnico al proveedor RITTAL, 2) El técnico de RITTAL, realizó la revisión y configuración del sistema de aire acondicionado del centro de cómputo y como lecciones aprendidas: 1) Se debe realizar la revisión y ajuste de las alarmas existentes para el centro de cómputo (Referentes al Aire acondicionado, por ser equipos nuevos), con el fin de minimizar la probabilidad de ocurrencia, 2) Realizar inspección diaria al sistema de aire acondicionado, con el fin de evaluar su desempeño y 3) Se debe programar mantenimientos preventivos”.

El Gestor de Incidentes de la Oficina de Informática envió por correo electrónico del 22 de octubre de 2020 archivo en Word con la información frente al incidente con el aire del centro de cómputo, así:

*“El sábado 7 de marzo de 2020 (madrugada de sábado a domingo) por cortes de energía eléctrica presentadas en el sector, los equipos de aire acondicionado se aseguraron (apagaron) y no arrancaron cuando se restableció el fluido eléctrico, haciendo que se elevará la temperatura del centro de datos y los servidores se asegurarán (apagarán) por las altas temperaturas.*

*En el momento que se presentó los cortes de energía Eléctrica entró a funcionar la UPS, en ese momento la configuración del sistema eléctrico de los nuevos aires acondicionados al recibir la corriente regulada de la UPS no fue suficiente y se aseguraron (apagaron).*

*Los servidores tienen detectores de calor que al sentir altas temperaturas cierran los servicio y se apagan las máquinas.*

*Las acciones de mejora efectuadas y sus soportes de ejecución para minimizar el riesgo del incidente con los aires acondicionados del centro de cómputo fueron:*

- 1) Se solicitó soporte técnico al proveedor RITTAL.

*El técnico de RITTAL, realizó diagnóstico del problema y se instaló un dispositivo tipo Vigilante de Tensión en cada equipo, se entregó como evidencia imagen del informe de servicio y fotos de la instalación de los dispositivos.*

WUC

- 2) Se debe realizar la revisión y ajuste de las alarmas existentes para el centro de cómputo (Referentes al Aire acondicionado, por ser equipos nuevos), con el fin de minimizar la probabilidad de ocurrencia.

Se realizó pruebas de corte eléctrico, simulando un fallo eléctrico, se alimentan nuevamente subiendo las protecciones, el vigilante de tensión se activa 30 segundos después de energizada la línea. Los equipos LCP (paquete de refrigeración líquida) entran en automático después de esa simulación.

- 3) Realizar inspección diaria al sistema de aire acondicionado, con el fin de evaluar su desempeño.

Los equipos instalados en el centro de Cómputo cuentan con alarmas visuales y sonoras, que pueden ser enviados a través de mensajes por correo electrónico, que pueden ser detectados por los Administradores de la infraestructura tecnológica de la Industria Militar.

Los Administradores de Centros de cómputo, deben realizar rutinas diarias, durante su permanencia en las instalaciones físicas, con el fin de detectar alarmas tempranas que puedan dar aviso de posibles eventos de falla en los equipos.

- 4) Se debe programar mantenimientos preventivos.

En la programación Anual de Mantenimiento Preventivo de la Industria Militar, se realizan de dos (02) a tres (03) mantenimientos en el año".

## **8.2 Evento Pérdida de información del Aplicativo Exact e-Synergy**

Al verificar el incidente "Falla del aire del centro de cómputo a causa de los cortes de energía eléctrica" reportado por la Oficina de Informática a la mesa de ayuda caso No. 3795 del 7 de marzo de 2020 no se encontró el reporte del incidente de seguridad por la pérdida de información de la aplicación Exact E-synergy.

**El 4 de noviembre de 2020 por correo electrónico el Gestor de Incidentes de la Oficina de Informática da respuesta a la pérdida de información del aplicativo Exact E-synergy, así:**

"Al restablecer los servicios del centro de cómputo, la aplicación de Gestión Documental Synergy presento error de base de datos de la aplicación, generando interrupción del servicio para toda la Entidad.

Las lecciones aprendidas identificadas fueron:

- 1) Se debe realizar el requerimiento de una nueva herramienta de Gestión de Backup, que permita efectuar de forma más ágil la restauración de copias de seguridad.

2) Se debe realizar seguimiento a la Base de Datos de la aplicación Synergy, con el fin de evaluar la posibilidad de reducir su tamaño, ya que las Bases de Datos SQL Server son demasiado grandes, dificultan su operatividad a la hora de realizar las copias y la restauración de estas.

3) Se debe programar mantenimientos preventivos para el manejo del tamaño de los Log de la base de datos de SQL Server".

**El 13 de noviembre de 2020 por correo electrónico el Gestor de Respaldos de la Oficina de Informática da respuesta a la pérdida de información en el incidente, así:**

*WWE*

*"El proceso de respaldo de servidor Jeremías que contiene a Synergy se ejecuta de la siguiente manera:*

- *El viernes en la noche se programa respaldo completo del aplicativo synergy a las 7:30 PM, este tiene un tamaño aproximado de 1.7 TB y gasta en promedio más de 30 horas en ejecutarse*
- *Los días lunes, martes, miércoles y jueves se ejecuta respaldo incremental programado a las 6 PM, el tamaño aproximado es de 100 GB y gasta en promedio 3 horas*

*Nota: La hora programada para el inicio del respaldo no indica que siempre comience a esa hora ya que se puede presentar represamientos por demoras en las tareas*

*El día 6 de marzo se realizó la actividad: La Industria Militar comunica que el viernes 6 de marzo de 2020 entre las 4 p.m. y 11 p.m. no habrá servicio de red o sistemas de información, ya que en este lapso de tiempo se realizará una prueba de continuidad de TI.*

*Debido a esta actividad se represaron todas las tareas, a las 11:30 pm aún no arrancaba el respaldo de jeremías.*

*Esto indica que cuando se presentó el incidente estaba en proceso el respaldo de Synergy ocasionando el daño en el disco y corrompiendo la tarea de respaldo (envío imágenes de la evidencia del daño del disco - "error generado en proceso a bases de datos no concluyo por error de disco").*

*Cuando se procedió a restaurar de cinta el respaldo se encontró que la última tarea que había terminado satisfactoriamente fue la del 05 de marzo por lo que se tomaron los siguientes respaldos para realizar la tarea Marzo 05, 04,03,02 - incrementales y Marzo 01 - Completa.*

*La tarea que inicio el 06 de marzo no termino satisfactoriamente por lo que no se podía restaurar.*

*Respecto a las demás tareas no presentaron error porque estas son más pequeñas y gastan menos tiempo en ejecutarse".*

*Se evidenció que en la Matriz de Riesgos y Oportunidades Primer Cuatrimestre 2020 del proceso de Gestión Informática se ha identificado el riesgo "No disponibilidad de la información (Afecta la disponibilidad)" y una de las causas identificadas "Pérdida de Información", teniendo en cuenta que este riesgo se materializó por la pérdida de información en la aplicación Exact E-synergy acaecida el 6 de marzo de 2020 no se encontró las acciones de mejora efectuadas y sus soportes de ejecución para minimizar su impacto, incumpliendo lo informado en el Procedimiento "Administración y Gestión de los Riesgos y las Oportunidades en la Industria Militar" Cód: IM OC OFP PR 018 Rev.12. numeral 4.1.13 "Cuando un riesgo se materializa...el Líder de Proceso debe generar informe de materialización de riesgo Cód: IM OC OFP FO 159 - elaborar como plan de mitigación una SAC (solicitud de Acción Correctiva)".*

**9. INDICADORES PROCESO GESTIÓN INFORMÁTICA**

*Durante el desarrollo de la Auditoria se evidenció que en el documento "Proceso Gestión Informática" Cód: IM OC OFI PS 001 Rev.15. se encuentra la Hoja de Vida Indicadores de Gestión del Proceso Cód: IM OC OFP FO 027 el cual tiene definidos diecisiete (17) Indicadores de Gestión, a continuación se relacionan:*

No. / Nombre Indicador	Objetivo del Indicador	Clase Indicador
1. Porcentaje de Atención a Requerimientos	Medir la eficiencia en la atención de requerimientos por parte del personal de la Oficina de Informática.	Eficiencia
2. Nivel de Satisfacción Solución	Medir la satisfacción del cliente interno en cuanto a la	Eficacia

*lwk*

Requerimientos	oportunidad y calidad de la respuesta.	
3. Disponibilidad de Enlaces de Comunicación	Medir el cumplimiento del proveedor en cuanto a la prestación del servicio contratado.	Eficiencia
4. Porcentaje de Cumplimiento de Respaldos por Política	Medir el cumplimiento de ejecución satisfactoria de generación de respaldos en cintas	Eficacia
5. Porcentaje de Vulnerabilidades Tecnológicas	Establecer el porcentaje de vulnerabilidades tecnológicas que deben ser tratadas con prioridad.	Eficacia
6. Porcentaje de Activos que superan el nivel de Riesgo Aceptable	Identificar y gestionar los activos que superan el nivel de riesgo menor aceptado por la Industria Militar.	Eficacia
7. Nivel de concientización de usuarios en seguridad de la información	Evaluar el nivel de concientización y conocimiento del personal con respecto a Seguridad de la Información.	Efectividad
8. Disponibilidad Mensual de Servicios de TI	Medir la disponibilidad de los servicios de TI establecidos en el Informativo IM OC OFI IF 004 en el mes.	Efectividad
9. Gestión de Aspectos e Impactos Ambientales	Establecer el porcentaje de aspectos de impactos ambientales Alto y Medio de las actividades ejecutadas por el proceso.	Ambiental
10. Gestión de Peligros y Riesgos Ocupacionales	Establecer el porcentaje de peligros y riesgos ocupacionales no aceptables de las actividades ejecutadas por el proceso.	S&SO
11. Nivel de Oportunidad en la Atención a Requerimientos Normales	Identificar el tiempo promedio en días que tarda el personal de la Oficina de Informática para cerrar los requerimientos recibidos y clasificados como normales.	Eficiencia
12. Nivel de Oportunidad en la Atención de Requerimientos a largo plazo	Identificar el tiempo promedio en días que tarda el personal de la Oficina de Informática para cerrar los requerimientos recibidos y clasificados a largo plazo.	Eficiencia
13. Nivel de Satisfacción del Usuario	Medir la satisfacción del cliente interno con respecto a los servicios ofrecidos por el personal del área y diferentes servicios de T.I	Efectividad
14. Desempeño prueba de Continuidad	Medir el desempeño de las pruebas de continuidad con respecto a la restauración satisfactoria de los servicios incluidos en el alcance	Efectividad
15. Manejo de Eventos de Seguridad	Medir la cantidad de eventos que aunque fueron tratados se convirtieron en un incidente de seguridad	Efectividad
16. Nivel de oportunidad en la Atención a Requerimientos Urgentes	Identificar el tiempo promedio en días que tarda el personal de la Oficina de Informática para cerrar los requerimientos recibidos y clasificados como urgentes.	Eficiencia
17. Porcentaje de Cumplimiento de los planes de Mejoramiento de las Auditorías de Control Interno	Medir la eficacia de la oportunidad en la atención de planes de mejoramiento de las auditorías de control interno por parte del personal de la Oficina de Informática.	Eficacia

El 15 de septiembre solicite por correo electrónico al Proceso de Gestión Informática la medición y análisis de cada uno de los indicadores que tiene el proceso de Gestión Informática.

Teniendo en cuenta que la creación de los Indicadores de Gestión están orientados principalmente a la medición de efectividad, eficacia y eficiencia de la Seguridad de la Información en la Empresa, es importante para la mejora continua alinear los indicadores que se tienen implementados con los propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC en su documento llamado Modelo de Seguridad y Privacidad de la Información el cual se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL. (Decreto único reglamentario 1078 del 26 de mayo de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones").

### 10. Modelo Integrado de Gestión y Planeación MIPG

#### 2ª. Dimensión: Direccionamiento Estratégico y Planeación

"El propósito de esta dimensión es permitirle a una entidad pública definir la ruta estratégica que guiará su gestión institucional, con miras a garantizar los derechos, satisfacer las necesidades y solucionar los problemas de los ciudadanos destinatarios de sus productos y servicios, así como fortalecer la confianza ciudadana y la legitimidad".

En el numeral 2.2 se describen los aspectos mínimos para la implementación de la segunda dimensión y los lineamientos generales de la implementación dentro de los cuales se informa en:...

✓ En cuarto lugar, se deben formular los planes de acción anual:

*LOWE*

Para la formulación de los planes de acción institucional, las entidades deben tomar en cuenta lo previsto en la Ley 152 de 1994, y en el artículo 74 de la Ley 1474 de 2011, en el que se establece que debe especificar en él los objetivos, las estrategias, los proyectos, las metas, los responsables, los planes generales de compras y la distribución presupuestal de sus proyectos de inversión; así mismo, deber incluir tanto los aspectos relacionados con el componente misional como con los relacionados con los planes de que trata el Decreto 612 de 2018:

**Decreto 612 de 2018**

*"Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.*

*Considerando.*

*Que el Decreto 1078 de 2015 contempló en el artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, ....*

**DECRETA:**

**ARTÍCULO 1.** Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:

*2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:*

...

*10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI".*

El proceso de Gestión de Informática en el Plan de Acción Institucional – PAI creó la Iniciativa estratégica N°. 20. PEI – *"Implementar sistemas de Información y las comunicaciones efectivas, seguras y que cumplan lineamientos del Gobierno"* y programó seis (6) actividades para la construcción del Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI realizarlas en el periodo abril a agosto de 2020:

- 1- Realizar actualización del Plan Estratégico de TI (PETI) organizacional para la vigencia 2020-2022 Fase 1.
- 2- Realizar actualización del Plan Estratégico de TI (PETI) organizacional para la vigencia 2020-2022 Fase 2.
- 3- Realizar actualización del Plan Estratégico de TI (PETI) organizacional para la vigencia 2020-2022 Fase 3.
- 4- Realizar actualización del Plan Estratégico de TI (PETI) organizacional para la vigencia 2020-2022 Fase 4.
- 5- Implementar la Estrategia de Gobierno Digital

Al 31 de Agosto de 2020, están actividades no se han ejecutado.

Se conformo el Comité con documento No. 02.342.159 *"Conformación Comité Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI"*.

WOK

Con documento No. 02.349.628 - *Primera Reunión Comité PETI Fase 1 "Comprender"* del 8 de octubre de 2020 se presentó al comité el cronograma para la construcción "*Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI*" el cual se hará en cuatro fases comprender, analizar, construir, presentar. El cronograma se ejecutará entre los meses de octubre a diciembre de 2020.

## 11. GESTIÓN DE RIESGOS Y OPORTUNIDADES SEGURIDAD DE LA INFORMACIÓN

La gestión de los riesgos de seguridad de la información se encuentra documentado en el Procedimiento "*Gestión de Riesgos y Oportunidades Seguridad de la Información*" Cód: IM OC OFI PR 015 Rev.10., en el cual se establecen y evalúan los riesgos a los cuales están expuestos los activos de información del Proceso de Gestión Informática, con el fin de identificar controles apropiados para mitigar el nivel de riesgo y su impacto.

Durante el desarrollo de la auditoría el Gestor de Riesgos de la Oficina de Informática en correo electrónico del 26 de octubre de 2020, da respuesta a las siguientes preguntas realizadas por el auditor en cuanto a:

### **11.1 la Planilla de Análisis de Riesgos de Información del Proceso de Gestión Informática SGS ISO 27001 (Cód. IM OC OFI FO 017).**

#### **1. Se ha identificado riesgos asociados a la seguridad de información? ¿Cuáles?**

*"No se han identificado nuevos Riesgos asociados a la seguridad de la Información.*

*Se siguen manifestando eventos como Malware (Código malicioso virus - troyanos - Gusanos - Rasonware - etc.), que son detectados por los Firewall por el antivirus.*

*Se toma la decisión de revisar y aumentar la probabilidad a las vulnerabilidades y amenazas para aquellos Activos que se encuentran más expuestos por la modalidad de trabajo remoto de la Industria Militar, de acuerdo con los tipos de Activos clasificados a continuación en la Matriz de Riesgos y Oportunidad de: Aplicaciones Software (Synergy, Adquisiciones, Página Web, Módulos del ERP de SAP, Correo, Herramientas de Colaboración, mesa de Ayuda, entre otras), Comunicaciones (Red Inalámbrica, Sistema de Videoconferencia, enlaces de comunicación, entre otros), Hardware (Firewall, Servidores de Aplicaciones como el de Synergy, ERP de SAP, Página Web, Correo, Adquisiciones, entre otras), Información (Alojamiento de las Bases de Datos de aplicaciones como, Synergy, Adquisiciones, Ventas, ERP de SAP, entre otras), Información Impresa (Licencias, Sobre con las contraseñas, resultados de pruebas de Ethical y Remediación, entre otros), Infraestructura (Centro de Cómputo, UPS, Equipo de Refrigeración Aire Acondicionado, Fibra óptica externa, entre otras), Recursos Humanos (Analista Oficina, Jefe Oficina de Informática, Programador de computadores, Profesional Especializado, Profesional de redes, entre otros), Servicios de Terceros (Servicio de Internet, Consultores o Contratistas de Servicios de Datos, de Voz, Gestión de Recursos Humanos, entre otros)".*

#### **2. Se han definido nuevos controles. ¿cuáles?**

*"No se han incorporado nuevos controles. Se siguen aplicando los controles de acuerdo Anexo A: Norma ISO 27001:2013. Política de la Seguridad de la Información, Organización de la Seguridad de la información, Seguridad de los Recursos Humanos, Gestión de Activos, Control de Acceso,*

6002

*Criptografía, Seguridad Física y del Entorno, Seguridad de las operaciones, Seguridad de las comunicaciones, Relaciones con los Proveedores, Gestión de Incidentes de seguridad de la Información, Seguridad de la Información de la Gestión de la Continuidad de Negocio y Cumplimiento.*

*Se han intensificado los procesos de seguimiento y control de escaneos diarios y periódicos en busca de Vulnerabilidades y Amenazas, apoyados en los procesos de VULNERABILIDAD ETHICAL Y REMEDIACION”.*

**3. En la Gestión del Riesgo, se han incluido riesgos de Trabajo en casa**

*“No se han identificado nuevos Riesgos asociados a la seguridad de la Información. Esto se debe a la debida aplicación de controles en los Procesos de la Industria Militar”.*

**11.2 Matriz de Riesgos y Oportunidades del Proceso de Gestión Informática (Cód. IM OC OFFO 117).**

**1. Se ha identificado riesgos asociados a la seguridad de información? ¿Cuáles?**

No se han identificados nuevos Riesgos asociados a la seguridad Informática. (Pendiente de concertar con el Comité de Seguridad de la Información CTS, dependiendo de los informes de Ethical Hacking y el plan de Remediación que se realizan durante el año).

**2. Se han definido controles, me puede relacionar por riesgo, ¿cuáles?**

No se han definido nuevos controles a los ya aplicados a los Riesgos presentados en la actualización del segundo cuatrimestre del presente año. (Pendiente de concertar con el Comité de Seguridad de la Información CTS, dependiendo de los informes de Ethical Hacking y el plan de Remediación que se realizan durante el año).

Los controles no han sido fortalecidos (Pendiente de concertar con el Comité de Seguridad de la Información CTS, dependiendo de los informes de Ethical Hacking y el plan de Remediación que se realizan durante el año).

**3. ¿De qué Riesgos, los controles han sido fortalecidos y por qué?**

Ninguno, (Pendiente de concertar con el Comité de Seguridad de la Información CTS, dependiendo de los informes de Ethical Hacking y el plan de Remediación que se realizan durante el año).

**12. EQUIPOS FUERA DE RED**

Durante el desarrollo de la Auditoría se evidenció que la Oficina de Informática tiene documentado el control de los equipos fuera de red en el Procedimiento “Control Equipos de Cómputo que se encuentran fuera de Red” Cód: IM OC OFI PR 019 Rev.3., cuyo objetivo es “Establecer las normas e instrucciones a seguir de todos los equipos de cómputo que se encuentran fuera de red en la Industria Militar así como establecer los mecanismos de control con el fin de evitar pérdida o fuga de la información sensible de la Organización”, el cual su última actualización fue el 29 de abril de 2016, incumpliendo lo informado en el procedimiento Gestión de Documentos Cód: IM OC OFFO PR 001 rev.14. numeral 4.2.1. “Descripción de las Etapas. Etapa 1. Identificar necesidades, definir prioridades y consolidar programa de documentos... Los líderes de procesos o subprocesos (LIPRO) deberán dentro de los plazos fijados revisar los documentos que tengan tres (3) o más años de liberados y aquellos que sea necesario crear, actualizar o anular.

1002

En acta No. 21 - "Discusión de documentos" se autorizó eliminar el Procedimiento "Control Equipos de Cómputo que se encuentran fuera de Red" Cód: IM OC OFI PR 019 Rev.3, debido a que se actualizó el documento "Reglas de buen uso de los activos de Información" Cód: IM OC OFI IF 001 Rev. 8. Pendiente que la Oficina de Planeación retire el documento del Gestor Documental.

### 13. HARDWARE ADQUIRIDO PARA MEJORAR LA INFRAESTRUCTURA TECNOLÓGICA DE LA INDUSTRIA INDUSTRIAL

Durante el desarrollo de la Auditoría se evidenció que la Industria Militar inicio el proceso de renovación tecnológica del centro de cómputo, es así que en la primera fase en la vigencia 2019 se adquirieron siete (7) nodos Hiperconvergente, instalándose cuatro (4) en el centro de cómputo principal y los otros tres (3) en su contingencia, equipos críticos e indispensables que soportan algunos procesos que garantizan la disponibilidad, continuidad y el funcionamiento de los sistemas de información, entre otros (SAP, SYNERGY, CORREO ELECTRONICO, etc.).

En la vigencia 2020 la Industria Militar se encuentra en proceso de contratación para la adquisición e Instalación de Equipos y Software para la fase II de la Renovación del Centro de Cómputo de la Industria Militar – Solución Hiperconvergente con el proyecto No. 9039 – Contrato de Compraventa Nacional No. 1-095/2020 – "Adquisición e instalación de equipos y software para la fase II de la renovación de centro de cómputo de la Industria Militar – Solución Hiperconvergente" firmado el 13 de octubre de 2020.

### 14. CONTROLES CRIPTOGRAFICOS

Durante el desarrollo de la Auditoría se evidenció que la Oficina de Informática elaboró el procedimiento Controles Criptográficos Cód: IM PC OFI PR 014 Rev.5. cuyo objetivo y alcance es "Establecer y hacer uso de técnicas y herramientas de cifrado sobre los sistemas de información administrados en el PROCESO INFORMÁTICA de INDUMIL donde se identifique la información que requiera ser protegida con controles criptográficos encaminados a proteger la confidencialidad e integridad de la información dando cumplimiento al Sistema de Gestión Integral".

El 4 de noviembre el auditor solicitó por correo electrónico las técnicas, herramientas de cifrado y controles criptográficos definidos en la Industria Militar encaminados a proteger la confidencialidad e integridad de la información. El 9 de noviembre de 2020 la Oficina de Informática dio respuesta por correo electrónico informando: "Respecto a lo solicitado, la Oficina de Informática bajo el PROCEDIMIENTO CONTROLES CRIPTOGRAFICOS IM OC OFI PR 014, relaciona el control de equipos y llaves Criptográficas (Firmas Digitales). Sin embargo, teniendo en cuenta las recomendaciones de la consultoría para la certificación OEA, este procedimiento se encuentra en proceso de actualización donde se incorporan otros controles que lleva el proceso y no están documentados tales como:

- *Dominio y Correo Electrónico. Con el fin de proteger la comunicación y los diferentes servicios entre los equipos a nivel de red, la Industria militar cuenta con entidad certificadora para la generación de certificados para equipos y servicios de dominio con Microsoft.*
- *Firma Electrónica y/o Llaves Criptográficas. Con el fin de validar la autenticación de origen, no repudio y confirmar que el mensaje enviado no ha sido alterado desde que fue firmado por el emisor originador, se implementa a través de un ente certificador las firmas digitales y llaves criptográficas. Proveedor anterior fue con Certicamaras, no hay contrato en este momento está en proceso el proyecto Nro. 9470 - "Servicio de Renovación y Mantto. Firmas Digitales" fecha de inicio 18 de agosto de 2020.*

1/10/20

- *Acceso desde el exterior con VPN. En la Industria Militar no cuenta con contratos de teletrabajo, pero tenemos habilitados canales de VPN cifrados que garantizan la confidencialidad e integridad de las comunicaciones siguiendo la Política de uso y conexiones externas. Proveedor: STS - Soluciones - Tecnología y Servicios S.A. - Proyecto: 9205, Cto: 1-034/2020.*
- *Certificados WEB. Para garantizar la seguridad, disponibilidad e integridad del sitio web, la Industria Militar cuenta con un certificado web (SSL/TLS). Se entrega evidencia del certificado activo emitido por GlobalSign Extended Validation CA- SHA256 - G3.*
- *Protocolos seguros de comunicaciones. La oficina de informática proporciona a los empleados, herramientas de comunicación que utilizan protocolos criptográficos actualizados con el fin de garantizar la confidencialidad al acceder a nuestros sistemas. Entre otros se incluyen los siguientes protocolos: SSH para el acceso seguro remoto a la administración de equipos; SFTP/FTPS para la transferencia segura de ficheros; Políticas de seguridad para la pyme: uso de técnicas criptográficas y HTTPS para la transferencia segura de datos en servicios web críticos (pagos online, descarga de información sensible).*

*El procedimiento se encuentra en proceso de actualización donde se incorporan los anteriores controles que no están documentados".*

Con respecto al control de la Firma Electrónica y/o Llaves Criptográficas donde la oficina de Informática informa que está en proceso el proyecto Nro. 9470 - "Servicio de Renovación y Mantto. Firmas Digitales" fecha de inicio 18 de agosto de 2020 se evidenció que con documento No. 02.362.914 - IM OC SGA DAD - "Oficio Culminación Proyecto 9470 Proceso 4782020 - SERVICIO DE MANTENIMIENTO Y RENOVACION DE CERTIFICADOS DE FIRMA DIGITAL" la Subgerente Administrativa informa: "Teniendo en cuenta que para el Proyecto 9470 Proceso 478/2020 "SERVICIO DE MANTENIMIENTO Y RENOVACIÓN DE CERTIFICADOS DE FIRMA DIGITAL", no se presentaron ofertas ni hay cumplimiento con la ficha técnica. La Subgerente Administrativa de la Industria Militar, informa que se culmina el proyecto y se realizara apertura nuevamente".

## 15. ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS

La Oficina de Informática desarrollo el Procedimiento para la Administración de Usuarios y Ccntraseñas IM OC OFI PR 001 Rev. 8 con el objetivo de documentar los derechos y permisos de acceso a los sistemas de información, los cuales se encuentran autorizados, controlados y mantenidos de manera apropiada mediante el uso de contraseñas que posee cada uno de los funcionarios de la Industria Militar.

## 16. FORMACIÓN EN LA TOMA DE CONCIENCIA APROPIADA Y ACTUALIZACIONES REGULARES

La Oficina de Informática en la iniciativa estratégica No. 70 PAI dentro de sus actividades programadas han definido la actividad No. 6 "Capacitar y Concientizar al personal de la organización en temas de seguridad de la Información", desarrollada a través de publicaciones de boletines de seguridad.

## 17. CUMPLIMIENTO DEL LITERAL D. "MISIONES PARTICULARES - NUMERAL IX. OFICINA INFORMÁTICA". DOCUMENTO NO. NO. 02.253.712" DIRECTIVA TRANSITORIA PARA EL APOYO AL PERSONAL - SUS FAMILIAS Y LA NORMALIZACIÓN DE LA OPERACIÓN EN FEXAR"

1000

Con documento No. 02.303. 911 del 18 de junio de 2020 el Jefe de la Oficina Informática informa "Se realiza verificación y no hay daños en la infraestructura de TI".

**18. CUMPLIMIENTO DEL LITERAL G. "ACTIVIDADES PARTICULARES - OFICINA INFORMÁTICA". DOCUMENTO NO. 02.290.283 "DIRECTIVA TRANSITORIA PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO PARA ENFRENTAR LA EMERGENCIA SANITARIA POR CAUSA DEL COVID-19".**

**"¿Se establecieron los mecanismos que permitan asegurar el desarrollo de actividades remotas por parte de los funcionarios de la industria Militar?"**

La Oficina de Informática desarrollo las siguientes actividades:

De Apropiación. 135 capacitaciones, 3 Manuales, 3 correos electrónicos, 5 Videos y nueva Intranet.

De soporte Técnico. Equipos Indumil, Equipos personales, Soporte telefónico y remoto vía ZOOM, implementar nueva intranet, módulo de encuestas intranet.

De Alistamiento. Creación y configuración a 395 usuarios de VPN, crear accesos y permisos a los aplicativos seleccionados.

**¿Se realizaron pruebas piloto para realizar trabajo en casa y teletrabajo? (teletrabajo no se maneja)**

En el acta de comité de seguridad de la información del 16 de marzo de 2020 se informa que se autoriza realizar una prueba con un grupo de usuarios significativos de las diferentes áreas, y según el resultado y las disposiciones de la Ley, habilitar el esquema propuesto mediante VPN para habilitar el trabajo remoto en casa.

**¿Se evaluaron y definieron los recursos (hardware y software) requeridos para la implementación de trabajo en casa y teletrabajo en INDUMIL?**

Requerimientos y proyectos para mejorar el trabajo en casa

Adquisición de servicio de Comunicaciones Unificadas:

- Salas de videoconferencia.
- Chat.
- Extensión telefónica.
- Movilidad.
- Suministro de equipos portátiles
- Adquisición de herramienta para administración de seguridad y control de la información.

**¿Se evaluó con base en la gestión de riesgos, los canales utilizados actualmente para la realización de reuniones con los equipos de trabajo?**

Se evaluó concluyendo que se debe realizar la adquisición de servicio de comunicaciones unificadas: salas de videoconferencia, chat, extensión telefónica y Movilidad.

**¿Se ha priorizado el apoyo técnico a los funcionarios, en relación con el acceso a las plataformas para trabajo remoto?**

Se ha dado soporte técnico a equipos Indumil, equipos personales, soporte telefónico y remoto vía

WDR

ZOOM, soporte para implementar nueva intranet, soporte módulo de encuestas intranet.

**¿Se estableció el programa de concientización en lo referente a los riesgos informáticos asociados al trabajo remoto?**

Se socializó las buenas prácticas para el uso de las herramientas de colaboración".

### 19. PLANES DE MEJORAMIENTO

#### Auditorías Internas al Proceso de Gestión Informática

Al 31 de octubre de 2020 el cumplimiento de las acciones definidas en los planes de mejoramiento producto de auditorías al proceso es:

TOTAL HALLAZGO	HALLAZGOS CUMPLIDOS	HALLAZGOS VENCIDOS	HALLAZGOS SIN PLAN DE MEJORAMIENTO	PORCENTAJE CUMPLIMIENTO
17	1	12	2	18%

Para el corte al 30 de noviembre de 2020, los hallazgos Nos. 5 y 7 "Controles que garanticen seguridad para que no se permita realizar modificaciones, luego de tramitados (observados)". de la vigencia 2017 quedan cumplidos.

#### Auditorías Externa realizada a la Industria Militar – Proceso de Gestión de Informática

Al 31 de octubre de 2020 el cumplimiento de las acciones definidas en el plan de mejoramiento producto de la auditoría realizada por la Auditoría de la Contraloría General de la República – Vigencia 2018:

TOTAL HALLAZGOS	HALLAZGOS CUMPLIDOS	HALLAZGOS VENCIDOS	PORCENTAJE CUMPLIMIENTO
11	8	3	73%

Los hallazgos vencidos corresponden a la vigencia 2018, así: Hallazgo No. 6 Control al cumplimiento de los tiempos para atención y solución de solicitudes sistema SAP - VIGENCIA 2018, Hallazgo No. 7 Documentación de los procedimientos de operación y control de TI y sistema de gestión de seguridad de la información - VIGENCIA 2018 y Hallazgo No. 8 Determinación de condiciones de tiempo para desarrollo de actividades en contratos de soporte SAP - VIGENCIA 2018

#### **Oportunidades de Mejora:**

- Estudiar la posibilidad de adquirir una herramienta de administración adicional de LOG o registros de eventos para la plataforma del correo electrónico, permitiría seguimientos, trazabilidad de las cuentas del correo electrónico de la Industria Militar actividades de procesamiento no autorizadas sobre la información enviada o recibida con el fin de asegurar la integridad, confidencialidad y oportunidad de la información.
- Teniendo en cuenta que la creación de los Indicadores de Gestión están orientados principalmente a la medición de efectividad, eficacia y eficiencia de la Seguridad de la Información en la Empresa, es importante para la mejora continua alinear los indicadores que tienen implementados con los propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC en

LOK

su documento llamado Modelo de Seguridad y Privacidad de la Información el cual se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL. (Decreto único reglamentario 1078 del 26 de mayo de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones").

- Actualizar el mapa de riesgos del proceso de Gestión Informática, teniendo en cuenta los eventos negativos que pueden surgir en el ejecución de las tareas del día a día, permitiría a la Industria Militar actuar con oportunidad frente a posibles situaciones como "la no prestación oportuna del servicio para el mantenimiento, soporte de los sistemas informáticos" situación evidenciada en la verificación de los contratos para la prestación de servicios para el mantenimiento, soporte y actualización de las aplicaciones Exact E-Synergy y ERP SAP / S4 HANA y "no realizar pruebas de restauración de cintas de respaldo" situación evidenciada en la verificación al cumplimiento descrito en la Norma Técnica NTC-ISO-IEC 27001, numeral A.12.3.1 "Respaldo de la Información" y en el Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006, Rev. 10. numeral 4.4 "Revisión de ejecución y verificación de Backups", para lo cual la Oficina de Control Interno recomienda evaluar su impacto y gestionarlo a través del mapa de riesgos del proceso teniendo en cuenta los parámetros establecidos en el Procedimiento para la Administración y Gestión de los Riesgos y las Oportunidades en la Industria Militar cód.: IM OC OFP PR 018, revisión No 12.
- La ejecución de acciones inmediatas para dar cumplimiento a las actividades propuestas en los planes de mejoramiento internos y externo, permitirá subsanar los hallazgos que se encuentran vencidos.

**Observaciones de forma subsanadas en desarrollo de la auditoría (d):**

N/A

**Limitantes (e):**

- No se encontraron los manuales de usuario y técnico del aplicativo Exact E-Synergy apoyo para los usuarios y administrador de la aplicación en el aprendizaje y uso de está.
- Desconocimiento en la administración de la Aplicación Exact E-Synergy, lo que dificultó al administrador brindar apoyo oportuno a las solicitudes realizadas en el tiempo de ejecución de la auditoría.
- El Log de errores de la aplicación Exact E-synergy de la vigencia 2019 no fue entregado.
- No fueron suministradas las encuestas realizadas en el año 2019 donde se identificó la necesidad de ampliación de los buzones del correo electrónico Microsoft Exchange.
- No se entregó Acta de Comité Técnico de Seguridad donde se aprobó la ampliación de la capacidad de los buzones del correo electrónico Microsoft Exchange, para la vigencia 2019.

LWV

<b>Hallazgos</b>		
<b>Criterios (a)</b>	<b>Descripción del Hallazgo (b)</b>	<b>Recomendación ©</b>
<p>Artículo 21. Ley General de Archivos. Ley 594 - 2000</p>	<p><b>Aplicación Exact E-synergy. No. 1</b>                      No se encuentra definido en la aplicación Exact e-synergy el rol para el Administrador Gestor Documental, este rol lo está asumiendo el Administrador Técnico de la herramienta sin tener la competencia, generando riesgos en las parametrizaciones por no estar alineadas conforme a las series, sub-series documentales, tablas de retención definidas en la Industria Militar.</p> <p>Lo anterior, incumpliendo Ley 594 – 2000. Título V. Gestión de Documentos. Artículo 21. Programas de Gestión documental. <i>“Las entidades públicas deberán elaborar programas de gestión de documentos, pudiendo contemplar el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivísticos”.</i></p>	<p>Es importante que los procesos de Gestión Informática y Secretaria General establezcan acciones que permitan garantizar el cumplimiento en lo establecido Ley 594 – 2000. Título V. Gestión de Documentos. Artículo 21.</p>
<p>Norma Técnica Colombiana NTC-ISO-IEC 27001 – 2013-12-11.</p> <p>Procedimiento Inventario y Clasificación de Activos de Información de la Industria Militar Cód: IM OC OFI PR 020 Rev.5.</p>	<p>No. 2                      Se evidenciaron inconsistencias en la clasificación de la Información en la aplicación Documental Exact E-Synergy, en atención a:</p> <ul style="list-style-type: none"> <li>- Creación de tres grupos con niveles de seguridad 11, 15 y 18 para el manejo de documentos que no están definidos en el numeral 4.1.5. <i>“Clasificación de la Información”</i> del procedimiento Inventario y Clasificación de Activos de información de la Industria Militar.</li> <li>- Los grupos Información</li> </ul>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Norma Técnica Colombiana NTC-ISO-IEC 27001 – 2013-12-11. Numeral A.8.2.1 y Procedimiento Inventario y Clasificación de Activos de Información de la Industria Militar Cód: IM OC OFI PR 020 Rev.5 numeral 4.1.5.</p>

6/2

	<p><i>"Reservada para jefes de grupo"</i> nivel de seguridad 25, <i>"Reservada para jefes de División"</i> nivel de seguridad 50 y <i>"Reservada para Grupo Gerencia"</i> nivel 75" establecidos en la aplicación no están conformados de acuerdo a los grupos establecidos en el numeral 4.1.5. <i>"Clasificación de la Información"</i> del Procedimiento Inventario y clasificación de activos de la Industria Militar Cód: IM OC OFI PR 020 Rev.5.</p> <p>Afectando la integridad, confidencialidad y oportunidad de la información existente en la aplicación Exact E-synergy.</p> <p>Lo anterior, incumpliendo la Norma Técnica NTC-ISO-IEC Colombiana 27001 – 2013-12-11. Numeral A.8.2.1 <i>"Clasificación de la Información"</i> y el Procedimiento <i>"Inventario y Clasificación de Activos de Información de la Industria Militar"</i> Cód: IM OC OFI PR 020 Rev.5. Numeral 4.1.5 <i>"Clasificación de la Información"</i>.</p>	
<p>Norma Técnica Colombiana NTC-ISO-IEC 27001 – 2013-12-11 numeral A.6.1.1.</p> <p>Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8.</p>	<p>No. 3</p> <p>Se evidenciaron debilidades en la identificación de roles y asignación de derechos de funciones a usuarios para el acceso a la información en la aplicación Exact E-synergy, en atención a:</p> <p>- Definición de roles como <i>"Editar documentos, ver todos los documentos entrantes, creación orden de reclamo por calidad, edición documentos SGC, ver documentos archivos, observaciones a procesos Req1000), visualizar Doc.Contratación,Aut_Doc_C</i></p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Norma Técnica NTC-ISO-IEC Colombiana 27001 – 2013-12-11. Numeral A.6.1.1 y Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. <i>"Cumplir con los principios de seguridad de la información"</i></p>

WOK

	<p><i>ontratación, Mostrar Botón Estadísticas FT, Visualizar Doc. Finales y Crear Resoluciones Jurídicas</i>", los cuales pueden ser derechos de funciones que los usuarios ejecutan de acuerdo con sus roles.</p> <p>- Asignaciones de derechos de funciones como <i>"crear todo tipo de solicitud, editar todas las solicitudes abiertas, reabrir todas las solicitudes, eliminar todas las solicitudes, reconstruir el flujo de trabajo de la solicitud, permite restaurar documento a varios usuarios de la aplicación y permite borrar documento"</i> a diferentes cargos como auxiliares de oficinas y secretarías ejecutivas.</p> <p>Afectando la integridad, confidencialidad y disponibilidad de la información existente en la aplicación Exact E-synergy.</p> <p>Lo anterior, incumpliendo la Norma Técnica NTC-ISO-IEC Colombiana 27001 – 2013-12-11. Numeral A.6.1.1 <i>"Roles y Responsabilidades para la Seguridad de la Información"</i> y la <i>"Política de Seguridad y Privacidad de la Información"</i> Cód. IM OC OFI CP 003 Rev.8. <i>"Cumplir con los principios de seguridad de la información"</i>.</p>	
<p>Norma Técnica Colombiana NTC-ISO-IEC 27001 – 2013-12-11.</p> <p>Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8.</p>	<p>No. 4</p> <p>Se evidenciaron debilidades en cuanto a la Seguridad de la Información residente en la aplicación Exact E-Synergy, en atención a:</p> <p>- Funcionarios que tienen acceso a editar y/o ver los todos documentos entrantes.</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Norma Técnica NTC-ISO-IEC Colombiana 27001 – 2013-12-11. Numeral A.6.1.1 y Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. <i>"Cumplir con los principios de seguridad de la</i></p>

WUR

	<p>- Documentos de la aplicación Exact E-synergy que se pueden ver sin ser observados.</p> <p>- Anulación de anexos de los documentos de la aplicación Exact E-synergy después de ser observado.</p> <p>Ocasionando la pérdida de la integridad, disponibilidad y confidencialidad de la información que se encuentra en la bases de datos de la aplicación Exact E-synergy.</p> <p>Lo anterior, incumpliendo Norma Técnica NTC-ISO-IEC Colombiana 27001 – 2013-12-11. Numeral A.6.1.1 "Roles y Responsabilidades para la Seguridad de la Información" y la "Política de Seguridad y Privacidad de la Información" Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información".</p>	<p>información".</p>
<p>Procedimiento de Monitoreo y Gestión de Logs Cod: IM OC OFI PR 012 Rev.12.</p> <p>Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa"</p>	<p>No. 5                  Se verificó la configuración de los logs de auditoría de registros año 2019 y 2020 y logs de errores año 2020 de la aplicación Exact E-synergy entregados por el administrador de la aplicación y estos no permiten rastrear los detalles de los eventos de las modificaciones de datos (que se ha modificado, fechas de las modificaciones, como se modificaron los datos y quien los modifico). Adicionalmente el Administrador de la aplicación informa "con respecto al análisis del log de errores no se realiza porque no son muy específicos", ocasionando riesgos en la oportuna detección de actividades de procesamiento no autorizadas</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en el Procedimiento de Monitoreo y Gestión de Logs Cod: IM OC OFI PR 012 Rev.12. numeral 4.1 y como primera línea de defensa el "mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol".</p>

WOK

	<p>sobre la información.</p> <p>Lo anterior, incumpliendo el Procedimiento de Monitoreo y Gestión de Logs Cod: IM OC OFI PR 012 Rev.12. numeral 4.1 <u>Elementos principales de un Log o Registro.</u> "Un registro o log de software o hardware deberá poseer entre otros, los siguientes campos: fecha del evento, hora del evento, equipo de cómputo donde se realizó el evento, usuario quien produce el evento, tipo de evento y archivo que se modifica en el evento (cambio de un campo de información, eliminación, creación), especificaciones del evento" y <u>Análisis de los LOGS.</u> "Mensualmente o cada vez que las circunstancias lo ameriten, en cada revisión de los logs se registrarán los hechos relevantes encontrados y las acciones sugeridas al respecto con el fin de minimizar los riesgos inherentes. Esta información será registrada en el requerimiento Monitoreo y Gestión de Logs del gestor documental e-Synergy con el fin de que se realicen las acciones correspondientes" y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: Control Interno al rol principal de la Primera Línea de Defensa, que corresponde al "mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol"", la cual está bajo la responsabilidad, principalmente, de los líderes</p>	
--	--	--

WZR

	<p>de programas, procesos y proyectos y de sus equipos de trabajo.</p>	
<p>Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8.</p> <p>Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa".</p>	<p><b>Mesa de Ayuda – GLPI No. 6</b>                  Al verificar la consistencia de la base de datos de la herramienta GLPI no se encontraron 298 registros que corresponden según lo informado por el jefe de la oficina de informática en correo electrónico del 26 de junio de 2020 a ticket de servicio que se han borrado por ser tickets que se abrieron y los uso la oficina de informática para prácticas, capacitaciones y pruebas y otros corresponden a los usuarios que los abren y los pueden borrar, ocasionando la pérdida de la integridad de la información de la base de datos de la herramienta GLPI, así como la confiabilidad de los reportes, de las estadísticas y búsquedas que esta herramienta ofrece.</p> <p>Lo anterior, incumpliendo la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. en cuanto a: "Cumplir con los principios de seguridad de la información y Proteger la información creada, procesada, transmitida, o resguardada dentro de la infraestructura tecnológica con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta" y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: Control Interno al rol principal de la Primera Línea de</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información y Proteger la información creada, procesada, transmitida, o resguardada dentro de la infraestructura tecnológica con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta" y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa"</p>

LURK

	<p>Defensa, que corresponde al "mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del Autocontrol", la cual está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo.</p>	
<p>Política de Seguridad y Privacidad de la Información              Cód. IM OC OFI CP 003 Rev.8.</p> <p>Acuerdo Niveles de Servicio              Cód: IM OC OFI IF 004. Rev.6</p>	<p>No. 7              La Industria Militar duró seis (6) meses (del 1 de febrero al 24 de julio de 2020) sin contrato de servicios para la actualización de licenciamiento, mantenimiento, soporte y desarrollo de la aplicación Exact E-Synergy, tiempo en el cual la prestación del servicio de soporte no se dio a los usuarios del software, quedando sin resolver veintitrés (23) de 594 soportes de servicios registrados por los usuarios en la herramienta GLPI, afectando los principios de eficacia, eficiencia, efectividad y oportunidad en la prestación del servicio.</p> <p>Lo anterior, incumpliendo la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información y el "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.6 literal b) Tiempos de solución por proveedor".</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información" y el "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.6 literal b) Tiempos de solución por proveedor".</p>
	<p>No. 8              La Industria Militar a la fecha de cierre no tiene contrato de servicio soporte y mantenimiento del ERP SAP / S4 HANA desde el 20 de abril de 2020, tiempo en el cual la</p>	

LUN

<p>Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8.</p> <p>Acuerdo Niveles de Servicio Cód: IM OC OFI IF 004. Rev.6</p>	<p>prestación del servicio de soporte no se ha dado a todos los usuarios, quedando sin resolver sesenta y ocho (68) de 622 soportes de servicios registrados por los usuarios en la herramienta GLPI, afectando los principios de eficacia, eficiencia, efectividad y oportunidad en la prestación del servicio.</p> <p>Lo anterior, incumpliendo la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información" y el "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.6 literal b) Tiempos de solución por proveedor".</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información" y el "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.6 literal b) Tiempos de solución por proveedor".</p>
<p>Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8.</p> <p>Acuerdo Niveles de Servicio Cód: IM OC OFI IF 004. Rev.6</p>	<p>No. 9.          Se verificó los requerimientos de servicios de soporte registrados en el herramienta GLPI encontrando que al 30 de junio de 2020 están pendientes por solucionar (estado pendiente y/o planeado) los siguientes: Correo electrónico trece (13) de 165, File Server dos (2) de 50, Firma Digital treinta (30) de 55, Gestión de usuarios treinta y cuatro (34) de 717, Hardware ciento cinco (105) de 427, Internet trece (13) de 288, Módulo de apoyo dieciséis (16) de 488, Red de Datos ocho (8) de 62, Red de Voz ocho (8) de 48, Seguridad de Información cinco (5) de 85, Servicio de apoyo once (11) de 250, Sitio WEB dos (2) de 300 y Software (28) de 195, afectando la eficacia, eficiencia, efectividad y oportunidad en la prestación del servicio.</p> <p>Así mismo se realizó verificación selectiva de los requerimientos que tienen en la</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido en la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información" y en el "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.6 literal a).</p>

LOWE

	<p>base de datos estado igual "Cerrado", y se efectuó indagación con las divisiones de personal, operaciones financieras, comercial y oficina control interno, encontrando veintidós (22) requerimientos cerrados sin dar solución al caso y uno (1) donde la oficina de informática informa "Se cierra el caso por finalización del contrato de soporte y su vez se inicia un nuevo contrato de soporte con la firma EPI USE con modalidad de horas en donde se va a controlar los acuerdos de servicio en donde se va a medir la atención del servicio por lo que prácticamente no se va a tener en cuenta este requerimiento por no estar dentro del alcance de este nuevo soporte. Si no se ha solucionado este caso entonces se requiere crear un nuevo caso con la información completa para ser tenido en cuenta en esta nueva fase de soporte", afectando la eficacia, eficiencia, efectividad y oportunidad en la prestación del servicio.</p> <p>Lo anterior, incumpliendo la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información" y el "Acuerdo Niveles de Servicio" Cód: IM OC OFI IF 004. Rev.6 literal a) Tiempo de solución, los tiempos de respuesta y solución máximos de las solicitudes para la Oficina de Informática recibidos mediante la herramienta GLPI".</p>	
	<p><b>Pruebas de Restauración de cintas de respaldos de Información</b>                  No. 10                  Se evidenció que desde el mes</p>	

WPA

<p>Norma Técnica Colombiana NTC-ISO-IEC 27001 – 2013-12-11.</p> <p>Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006, Rev. 10.</p>	<p>de febrero de 2019 no se ejecuta las pruebas de restauración de cintas de respaldos de información, afectando la integridad y disponibilidad de la información respaldada.</p> <p>Lo anterior, incumpliendo en la Norma Técnica NTC-ISO-IEC 27001, numeral A.12.3.1 Respaldo de la Información "Se deben hacer copias de respaldo... y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas" y en el Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006, Rev. 10. numeral 4.4 Revisión de ejecución y verificación de Backups "...Para asegurar la confiabilidad de la información almacenada en cinta y que la misma pueda ser recuperada en forma satisfactoria, anualmente se elaborará un cronograma donde se detallarán las fechas y la relación de los servidores a restaurar"</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido Norma Técnica NTC-ISO-IEC 27001, numeral A.12.3.1 "Respaldo de la Información" y en el Procedimiento Gestión de Copias de Respaldo de Información Cód: IM OC OFI PR 006, Rev. 10. numeral 4.4.</p>
<p>Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8.</p> <p>Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa".</p>	<p><b>Acceso Remoto</b>              No. 11              Al revisar el reporte de los soportes remotos realizados desde el año 2018 hasta el 30 de junio de 2020 a los equipos de cómputo de la Industria Militar, se evidencio:</p> <p>- Con documento No. 02.303.911-"Informe Auditoria Proceso Gestión Informática" del 18 de junio de 2020 la Oficina de Informática en el numeral 16 informa "Los ingresos remotos que realiza el personal de la oficina de informática a los equipos TI de la Industria Militar... se</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar el cumplimiento en lo establecido la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. "Cumplir con los principios de seguridad de la información" y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa"</p>

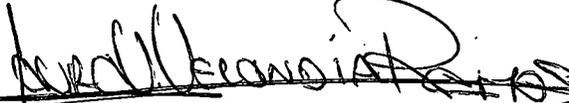
LWC

	<p><i>realizan con autorización verbal del funcionario"</i></p> <p>- Selectivamente se tomaron 90 registros para verificar el tiempo de soporte dado, encontrando tiempos de soporte remoto de más de una hora, sin obtener la evidencia de la labor desarrollada, generando riesgos de afectación de la integridad, confidencialidad y seguridad de la información existente en los equipos de cómputo que se toman por acceso remoto.</p> <p>Lo anterior, incumpliendo la Política de Seguridad y Privacidad de la Información Cód. IM OC OFI CP 003 Rev.8. <i>"Cumplir con los principios de seguridad de la información"</i> y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: Control Interno al rol principal de la Primera Línea de Defensa, que corresponde al <i>"mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del Autocontrol"</i>, la cual está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo.</p>	
	<p><b>Segregación de funciones No. 12</b>                  No se encontró la matriz de Segregación de Funciones Cód. IM OC OFI FO 12 Rev.2., en la cual se deben definir los</p>	

10/12

<p>Procedimiento Segregación de Funciones Cód: IM OC OFI PR 008 Rev.4. numeral 4.1.1.</p> <p>Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa".</p>	<p>roles y responsabilidades de los funcionarios de la Industria Militar que tengan acceso a los sistemas de información de la Entidad, generando el riesgo de uso inadecuado o no autorizado de la Información de la Industria Militar, afectando los principios de integridad, confidencialidad y disponibilidad de la información.</p> <p>Lo anterior, incumpliendo el Procedimiento Segregación de Funciones Cód: IM OC OFI PR 008 Rev.4. numeral 4.1.1. "Creación o Modificación de la Matriz de Segregación de Funciones" y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: Control Interno al rol principal de la Primera Línea de Defensa, que corresponde al "mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del Autocontrol", la cual está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo.</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar en el cumplimiento en lo establecido Procedimiento Segregación de Funciones Cód: IM OC OFI PR 008 Rev.4. numeral 4.1.1 y lo informado en el Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional, versión 3. Séptima Dimensión: "Control Interno al rol principal de la Primera Línea de Defensa"</p>
<p>Procedimiento "Administración y Gestión de los Riesgos y las Oportunidades en la Industria Militar" Cód: IM OC OFF PR 018 Rev.12. numeral 4.1.13</p>	<p><b>Incidente de Seguridad Pérdida de Información 6 de marzo de 2020</b>                  No. 13                  Al verificar el incidente "Falla del aire del centro de cómputo a causa de los cortes de energía eléctrica" reportado por la Oficina de Informática a la mesa de ayuda caso No. 3795 del 7 de marzo de 2020 no se encontró registrado el evento</p>	<p>Es importante para el Proceso Gestión Informática establecer acciones que permitan garantizar en el cumplimiento en lo establecido Procedimiento "Administración y Gestión de los Riesgos y las Oportunidades en la Industria Militar" Cód: IM OC OFF PR 018 Rev.12. numeral 4.1.13.</p>

L00K

	<p>de la pérdida de información en la aplicación Exact E-synergy del día 6 de marzo de 2020 ni las acciones de mejora efectuadas por la materialización del riesgo "No disponibilidad de la información" identificado en la Matriz de Riesgos y Oportunidades Primer Cuatrimestre 2020 del proceso de Gestión Informática, generando el riesgo de la aparición de nuevos eventos por pérdida de información en la aplicación Exact E-synergy, afectando los principios de integridad y disponibilidad de la información.</p> <p>Lo anterior, incumpliendo lo informado en el Procedimiento "Administración y Gestión de los Riesgos y las Oportunidades en la Industria Militar" Cód: IM OC OFP PR 018 Rev.12. numeral 4.1.13 "Cuando un riesgo se materializa...el Líder de Proceso debe generar informe de materialización de riesgo Cód: IM OC OFP FO 159 - elaborar como plan de mitigación una SAC (solicitud de Acción Correctiva)".</p>	
<p><b>Sobre la implementación y efectividad de acciones resultantes de anteriores auditorias y/o evaluaciones (13):</b> No se han dado.</p>		
<p><b>Anexos: (15)</b> N/A</p>		
<p><b>Funcionario(s) Oficina de Control Interno (16)</b></p>	<p><b>Auditados/evaluados (17)</b></p>	
<p>  <b>Ing. Sis. Laura Victoria Velandia Ramos</b>                  Profesional Oficina de Control Interno</p>	<p>  <b>CN. (RA) Jorge Alberto Arocha Muñoz</b>                  Jefe Oficina de Informática</p>	