Tema	Auditoría Interna al Sistema de Gestión de Seguridad de la Información -SGSI- bajo la norma ISO- 27001:2013									
Tipo de Actividad	Calidad		Gestión		Programada	x	Solicitada			
	Interna	x	Externa		Auditoría	x	Seguimiento			
Ciclo de Auditoría	Año 2021									
Objetivo	• Verificar el cumplimiento de los requisitos establecidos de la norma ISO- 27001:2013. • Determinar si el sistema de gestión de Seguridad de la información- SGSI- cumple con los objetivos organizacionales y se ha implementado eficazmente. • Evaluar las fortalezas y debilidades del sistema de gestión de seguridad de la información- SGSI- y detectar oportunidades para la mejora continua.									
Alcance	Aplica para áreas y/o departamentos definidos dentro del esquema organizacional, que cumplen los procesos definidos dentro del sistema de gestión de seguridad de la información.									
Criterios de Auditoría (Documentos de Referencia)	Requisitos de las normas ISO 27001:2013, procedimientos documentados de la UNGRD, requisitos legales establecidos y vigentes y normatividad aplicable a cada proceso									

Área, dependencia o proceso a auditar	El ciclo de auditoría aplica a los procesos definidos en el sistema de gestión de Seguidad de la Información integrado al SIPLAG: Gestión de Tecnologías de la Información; Gestión Contratación; Gestión de Talento Humano; y Gestión Administrativa; Auditoría presencial y virtual teniendo en consideración las directrices de la norma ISO 19011:2018.
Nombre completo del jefe de área / coordinador	Dr. German Moreno – Jefe de la Oficina de Control Interno de la UNGRD

Auditor líder	Diana Carolina Amortegui Barbosa	
Equipo auditor	David Marcell Bermúdez	José Vicente Casanova – Profesional Especializado OCI
Personas Interesadas	Todos los líderes de los procesos	

NIVEL DE RIESGO				
	CUMPLIMIENTO	GESTIÓN DEL RIESGO	CONTROLES	DESEMPEÑO
Critico	-	-	-	-
Alto	-	-	-	-
Medio	No aplica	Cambios en procesos que no se encuentren	Considerar la información oficial	Alguna de la información documentada del

		debidamente actualizados en la herramienta Neogestión	disponible en Neogestión como criterios de auditoría	sistema de gestión se encuentra en proceso de revisión o aun en proceso de elaboración
Bajo	No aplica	Equipo auditor no cuenta con la competencia colectiva para desarrollar la auditoría interna de forma eficaz	Contratar externamente la ejecución de auditoría interna para la UNGRD	Se contrata con Password SAS, se verifica la competencia del equipo auditor mediante la revisión de sus hojas de vida, soportes asociados con educación, formación, experiencia
Bajo	No aplica	Dificultades en el suministro de información por parte de los auditados	Comunicación previa del plan de auditoría para asegurar que los auditados se encuntren informados y preparados	Se presentan disponibles evidencias requeridas por el equipo auditor, siendo otras suministradas durante el ejercicio de la auditoría interna.

ANTECEDENTES

(Descripción de la actividad que está siendo auditada o una breve explicación del proceso)

En cumplimiento al desarrollo del contrato No. 9677 PPAL001 1171 2021 -2021, suscrito entre la UNGRD y PASSWORD CONSULTING SERVICES SAS, que dentro de sus obligaciones esta previsto llegar cabo los servicios de auditoria de control interno bajo la norma ISO 27001:2013, con el fin de verificar el grado de mantenimiento de sus sistemas de gestión de Seguridad de la Información -SGSI- bajo la norma ISO-27001:2013

Según el cronograma de actividades previsto para el contrato suscrito entre las partes, se realiza plan de auditoría entre la Oficina de Control Interno de la UNGRD y el auditor líder. Para el desarrollo de la auditoría interna se tiene en cuenta todos los procesos publicados en el Sistema Integrado de Planeación y Gestion (SIPLAG) de la UNGRD. Se verifica la planificación, implementación, verificación y mejora de los Sistemas de Gestión de Seguridad de la Información -SGSI- bajo la norma ISO- 27001:2013 y de los requisitos legales aplicables, así como los propios definidos por la UNGRD.

Aunque continua la emergencia sanitaria por temas del Covid-19, se desarrolla esta auditoría interna los días 20 (planeación de la auditoría), y los días en sitio correspondientes a: 22, y 23 de diciembre de 2021, de forma presencial, en la sede principal de la UNGRD y virtual, el medio utilizado para la conexión fue la herramienta *Meet* de Google.

Durante el desarrollo de la auditoría interna no se presentaron situaciones que impidieran el normal desarrollo del plan establecido, por lo cual, se considera que se cumplieron los objetivos de auditoría planteados

FORTALEZAS ENCONTRADAS

(Hace referencia a las capacidades, habilidades, cualidades que posee el área o dependencia y agradecimiento por la cooperación para el desarrollo de la actividad)

Se evidencia nivel de madurez en cuanto a la documentación necesaria para planificar e implementar el Sistema de Gestión de Seguridad de la Información - SGSI, sin embargo, se requiere validar algunos documentos, debido a que se encuentran pendientes de revisión o están en fase de aprobación.

El Sistema de Gestión de Seguridad de la Información, está en su etapa inicial, ya que es la primera vez que cumple con el ciclo de mejora (PHVA).

El líder del proceso atendió la auditoria del Sistema de Gestión de Seguridad de la Información - SGSI.

Cuenta con un Sistema (NeoGestión) para la administración de toda la documentación perteneciente al SGSI.

La auditoría del SGSI se llevó a cabo sin ningún inconveniente, y se contó con la colaboración de todos los procesos y personas involucradas. Esto permitió que el plan de auditoría se cumpliera en su totalidad.

CONTROLES DEFINIDOS POR EL ÁREA O DEPENDENCIA

(Hace referencia al conjunto de métodos y medidas adoptadas por el área o dependencia para promover la eficiencia de su gestión y evitar la materialización de sus riesgos)

Control definidos por el proceso/dependencia/área	Medición de la efectividad del control
Soportes a la gestión documental por medio de Neogestión Mantenimiento del Sistema de Gestión de Seguridad de la Información bajo la norma ISO 27001:2013	

RESULTADOS DE LA AUDITORIA

(Hace referencia a los hallazgos encontrados de acuerdo a los criterios evaluados y siempre deben estar alineados con los objetivos y alcance de la auditoría. Su redacción siempre debe ajustarse a la estructura Condición – criterio – causa – efecto/riesgo)

Criterio de Auditoira evaluado	Aspecto por Mejorar / Observación
ISO 27001:2013 Numeral 5.1	**Gestión de Tecnologías de la Información - OM**: El SGSI en la UNGRD, cuenta con los objetivos de seguridad de la información descritos en el Manual de Políticas (M1101-GTI-05). Se debe validar la herramienta de medición para evidenciar el seguimiento y medición que se le da a los mismos.
ISO 27001:2013 Numeral 5.2	**Gestión de Tecnologías de la Información - OM**: Incluir dentro del plan de socialización el Manual de Políticas y sus respectivas actualizaciones.

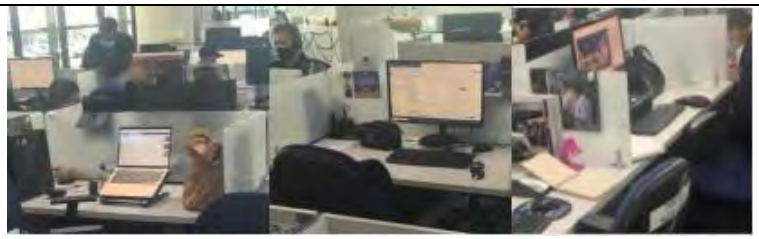
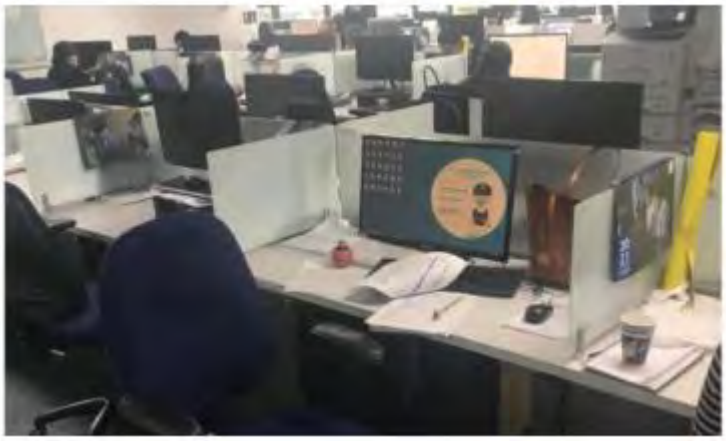
ISO 27001:2013 Numeral 5.3	**Gestión de Tecnologías de la Información - OM**: Documentar la evidencia de evaluación por parte del Comité de Gestión y Desempeño respecto a las funciones y responsabilidades frente a la seguridad de la información
ISO 27001:2013 Numeral 6.1.3	**Gestión de Tecnologías de la Información - OM**: Incluir el control A.12.1.2 Gestión de Cambios. Este control aplica para la gestión de riesgos de la entidad con cualquier cambio que este asociado a los procesos del negocio, instalaciones y sistemas de procesamiento de información. Estos pueden llegar a afectar la seguridad de la información e impactan directamente el SGSI
	Gestión de Tecnologías de la Información - OM: Incluir el control A.6.2.2 Teletrabajo, aunque la UNGRD no contemple esta figura conforme lo establece la Ley 1221 del 2008 y el Decreto 884 del 2012, en la entidad si se realiza trabajo remoto, cuenta con una política de seguridad de trabajo remoto. De atención con la emergencia sanitaria producida el COVID 19 y la Ley 2088 de 2021
ISO 27001:2013 Numeral 7.3	**Gestión de Tecnologías de la Información - OM**: Hacer seguimiento a las jornadas de sensibilización (asistencia del personal), debido a que algunos funcionarios aseguran no poder asistir a las capacitaciones y por lo tanto desconocen el Manual de Políticas de Seguridad de la Información.
ISO 27001:2013 Numeral A.9.2.3	**Gestión de Tecnologías de la Información - OM**: La UNGRD cuenta con el procedimiento de Gestión de Usuarios (PR-11101-GTI-02) y las evidencias de una adecuada gestión. Sin embargo, no hay evidencia del mecanismo que permita la restricción de los usuarios privilegiados.
ISO 27001:2013 Numeral A.9.2.5	**Gestión de Tecnologías de la Información - OM**: Evidenciar el seguimiento de los permisos especiales o de usuario privilegiado.
ISO 27001:2013 Numeral A.9.2.6	**Gestión de Tecnologías de la Información - OM**: Validar las fechas de ingreso y finalización de los contratos, con el fin de hacer coincidir la información de retiro con la deshabilitación de los permisos de acceso
ISO 27001:2013 Numeral A.10.1.2	**Gestión de Tecnologías de la Información - OM**: Actualizar la política de Gestión de Llaves ya que actualmente no se utilizan las llaves criptográficas en la entidad.
ISO 27001:2013 Numeral A.11.1.6	**Gestión de Apoyo Administrativo -OM**: Se recomienda organizar el área del Datacenter y ubicar los demás equipos o elementos que no hagan parte del mismo, en otra área.
ISO 27001:2013 Numeral A.11.2.3	**Gestión de Tecnologías de la Información - OM:** Tener el informe en un repositorio donde se pueda evidenciar la certifiación de los puntos de red (RAE).
ISO 27001:2013 Numeral A.11.2.7	**Gestión de Tecnologías de la Información - OM**: Dar un manejo adecuado a los equipos obsoletos o en desuso (Donaciones, bajas, destrucción, etc.).
ISO 27001:2013 Numeral A.12.1.3	**Gestión de Tecnologías de la Información - OM:** Actualizar y socializar el procedimiento de Gestión de Capacidad con los funcionarios de la entidad.
ISO 27001:2013 Numeral A.12.3.1	**Gestión de Tecnologías de la Información - OM:** Validar e identificar los backups de los funcionarios retirados con el fin de determinar que estén completos y den cumplimiento a la política establecida
ISO 27001:2013 Numeral A.12.5.1	**Gestión de Tecnologías de la Información - OM:** Establecer el procedimiento de Instalación de Software en Sistemas Operativos y socializarlo con las partes interesadas.

ISO 27001:2013 Numerales: A.13.2.2 A.13.2.3	**Gestión de Tecnologías de la Información - OM:** Se recomienda actualizar la firma del correo electrónico, dando cumplimiento a la Ley 527 de 1999, conforme lo establece la política de transferencia de información.
ISO 27001:2013 Numeral A.14.1.1	**Gestión de Tecnologías de la Información - OM:** En la declaración de aplicabilidad, validar la exclusión del control A.14.1.1 Análisis y especificación de requisitos de seguridad de la información, ya que dicho control aplica en especial cuando se requieran mejoras para sistemas de información existentes.
ISO 27001:2013 Numeral A.14.2.2	**Gestión de Tecnologías de la Información - OM:** Validar la exclusión del control de Cambios con el proveedor.
ISO 27001:2013 Numeral A.7.1.2	**Gestión del Talento Humano - OM:** Documentar las cláusulas contractuales sobre cumplimiento de las políticas de seguridad de la información y las responsabilidades frente a la misma con los funcionarios de la entidad. Así como se establece con los contratistas.
ISO 27001:2013 Numeral A.7.3.1	**Gestión del Talento Humano - OM:** Revisar y documentar en el formato “Sin pendientes” las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo.
ISO 27001:2013 Numeral A.15.1.3	**Gestión de Tecnologías de la Información - OM**: Revisar los acuerdos con los proveedores, con el fin de que se incluyan los requisitos de extender los acuerdos de confidencialidad y cumplimiento de políticas de seguridad de la información a toda la cadena de suministro, en caso de que se presente esta situación.
ISO 27001:2013 Numerales: A.15.13 A.15.2.1	**Gestión de Tecnologías de la Información - OM:** Identificar en la matriz de riesgos de los contratos con proveedores, riesgos de seguridad de la información que podrían presentarse de acuerdo al tipo de contrato y hacer seguimiento a los mismos. De igual forma, realizar y evidenciar auditorias regulares a los servicios prestados por los proveedores
ISO 27001:2013 Numerales A.16.1.5 A.16.1.6	**Gestión de Tecnologías de la Información - OM:** Ajustar la matriz de seguimiento a incidentes de seguridad de la información para obtener la información necesaria, mejorar la respuesta a los mismos y documentar las lecciones aprendidas
ISO 27001:2013 Numeral A.16.1.7	**Gestión de Tecnologías de la Información - OM:** Ajustar el procedimiento de Gestión de incidentes de seguridad de la información, respecto a la recolección de evidencia de acuerdo al incidente presentado y la forma de preservar la misma
ISO 27001:2013 Numeral A.17.1.1	**Gestión de Tecnologías de la Información - OM:** Ajustar o actualizar los Planes de Continuidad y el BIA (Análisis de Impacto del Negocio)
ISO 27001:2013 Numeral A.17.1.2	**Gestión de Tecnologías de la Información - OM:** Revisar y ajustar el procedimiento de continuidad de la seguridad de la información, contemplando la revisión de los controles establecidos en los riesgos identificados frente a una situación adversa, a fin de asegurar el nivel de seguridad.
ISO 27001:2013 Numeral A.17.1.3	**Gestión de Tecnologías de la Información - OM:** Realizar pruebas regulares a los escenarios identificados para verificar que los controles de seguridad de la información frente a situaciones de continuidad si responden de acuerdo a los tiempos establecidos y los planes de respuesta definidos por la UNGRD.
ISO 27001:2013 Numeral	**Gestión de Tecnologías de la Información - OM:** Programar y evidenciar los seguimientos periódicos al cumplimiento de políticas de seguridad por parte de

	los funcionarios y contratistas, así como la revisión de cumplimiento técnico a los sistemas de información con los que opera la UNGRD

NO CONFORMIDADES

No.	Criterio de Auditoria evaluado	No conformidad Mayor o Menor	Tipo de No Conformidad
1.	ISO 27001:2013 Numeral A.6.1.2	**Gestión de Tecnologías de la Información - N.C**: Al validar la identificación de roles y responsabilidades del SGSI, no se evidencia un rol responsable de la seguridad de la información, y que estas funciones las desarrolla la Coordinadora de Tecnologías de la Información, por lo que entraría en conflicto en el momento que deba ejecutar cada rol que debe actuar en el Sistema de Gestión de Seguridad de la Información (juez y parte). Lo anterior evidencia el incumplimiento del Control A.6.1.2 del Anexo A de la norma NTC ISO-IEC 27001:2013	**Menor**
2.	ISO 27001:2013 Numeral A.11.1.2	**Gestión de Apoyo Administrativo - N.C:** Se indaga sobre los controles de acceso físicos. A esto, se responde: “el procedimiento y contratos se encuentran en actualización”. Para la recepción y al guarda de seguridad se imparten los lineamientos estipulados; sin embargo, no se verifican los datos registrados (los equipos ni el material que se ingresa). Lo anterior evidencia el incumplimiento del Control A.11.1.2 del Anexo A de la norma NTC ISO-IEC 27001:2013	**Menor**
3.	ISO 27001:2013 Numeral A.11.2.8	**Gestión de Tecnologías de la Información - N.C**: Se tiene documentado el requisito de usuario desatendido inmerso en la política de control de acceso, pero los funcionarios no cumplen con dicha política. Se observa que al levantarse de sus puestos de trabajo, no bloquean los equipos de cómputo:	**Menor**

		 Lo anterior evidencia el incumplimiento del Control A.11.2.8 del Anexo A de la norma NTC ISO-IEC 27001:2013	
4.	ISO 27001:2013 Numeral A.11.2.9	**Gestión de Tecnologías de la Información - N.C.** Se tiene documentada la política de escritorio limpio y pantalla limpia, sin embargo se observa que la mayoría de los funcionarios no cumplen con dicha política, comen en los puestos de trabajo, dejan bebidas cerca de los equipos y documentos con información sensible en sus escritorios.  Lo anterior evidencia el incumplimiento del Control A.11.2.9 del Anexo A de la norma NTC ISO-IEC 27001:2013	**Menor**
5.	ISO 27001:2013 Numeral	**Gestión de Tecnologías de la Información - N.C**.: Al solicitar las pruebas de aceptación para los sistemas de información nuevos, actualizaciones y/o nuevas versiones, la UNGRD indica que se realizan validaciones funcionales, pero no se presentan evidencias de dicho proceso.	**Menor**

		Lo anterior evidencia el incumplimiento del Control A.14.2.9 del Anexo A de la norma NTC ISO-IEC 27001:2013	
6.	ISO 27001:2013 Numeral	**Gestión de Tecnologías de la Información** - N.C.: Al solicitar información sobre la forma en que se seleccionan, protegen y controlan los datos de prueba, la UNGRD indica que se realizan validaciones funcionales; sin embargo, no se presenta evidencia de la implementación del control. Por lo anterior se presenta incumplimiento del Control A.14.3.1 del Anexo A de la norma NTC ISO-IEC 27001:2013	**Menor**

OPORTUNIDADES DE MEJORA

Que oportunidades de mejora identificamos en el desarrollo de la auditoria, que permiten al área o dependencia mejorar o agregar valor a su gestión).
(De acuerdo a las no conformidades identificadas, validar cuales pueden tener una mejora que apunten al cumplimiento de los objetivos del área o dependencia y agreguen valor a la entidad).

Con respecto al cumplimiento de los controles del Anexo A de la NTC ISO-IEC 27001:2013, hay cumplimiento parcial, debido a que es un sistema que entró en operación para esta vigencia, por lo que algunos controles requieren de revisión y ajuste.

Se encontraron 29 oportunidades de mejora en los procesos: Gestión de Apoyo Administrativo, Gestión de Tecnologías de la Información y Gestión de Talento Humano, las cuales deben ser priorizadas, ya que pueden convertirse en una no conformidad.

Es importante continuar con la sensibilización y capacitación para todos los funcionarios de la UNGRD en seguridad de la información

Continuar con la formación de los funcionarios que tienen responsabilidades importantes frente a la seguridad de la información.

Para fortalece el nivel de madurez del SGSI en la UNGRD, es importante dar continuidad a los planes de auditorías internas.

CONCLUSIONES

(Se destacan los puntos más relevantes de la auditoría y siempre alineados con el objetivo de la auditoría o actividad de seguimiento)

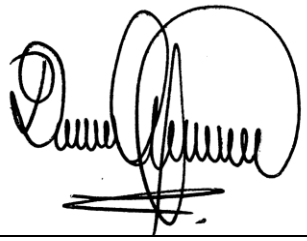
El propósito principal de la auditoría interna fue el determinar el grado de implementación y mantenimiento del sistema de gestión de Seguridad de la Información de la UNGRD bajo las normas ISO 27001-2013, a través del ciclo PHVA (planear, hacer, verificar y actuar) en sus diferentes procesos y actividades, por medio de un muestreo aleatorio que conllevó la revisión de documentos, la ejecución de entrevistas y la visita de campo (al Data Center de 2 y 5 piso de la UNGRD).

Es necesario que el sistema de gestión de seguridad de la Información de la UNGRD se articule de forma dinámica entre los Sistemas de Gestión con que cuenta la UNGRD bajo las las normas ISO 9001-2015, ISO 14001-2015 y ISO 45001-2018 para seguir manteniendo las buenas prácticas aprendidas del modelo de gestión actual, articulando los conocimientos y experiencias de su bien mas preciable, el Talento Humano con el cual cuenta la UNGRD.

El incentivar por parte de la Alta Dirección de la UNGRD la toma de conciencia y el compromiso de sus líderes permitirá sin duda, el fortalecer la comprensión del sistema de gestión de Seguridad de la Información y sus múltiples interacciones.

Ahora bien, es importante anotar que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores o irregularidades que no hayan sido detectadas bajo la ejecución de nuestros procedimientos de auditoría, evaluación o seguimiento, previamente planeados en la muestra seleccionada. La Unidad y las áreas que la componen, son responsables de establecer y mantener un adecuado sistema de control interno y de prevenir posibles irregularidades, de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión para las tres líneas de defensa. Así mismo, es responsabilidad del área la información suministrada, por cualquier medio, para la realización de esta actividad de manera oportuna, completa, integra y actualizada y la de informar en su momento las posibles situaciones relevantes y/o errores que pudieran haber afectado el resultado final de la actividad.

Agradecemos su colaboración y disposición frente al proceso de auditoría ejecutado y esperamos la pronta gestión por parte de todos los líderes de los procesos y sus colaboradores ante los hallazgos encontrados.

Firma Auditor Líder

Nombre **Diana Carolina Amortegui Barbosa**
Cargo Auditor Líder - Password

Miembros del Equipo Auditor			
Nombre:	**David Marcell Bermudez Contreras**	**Nombre:**	**José Vicente Casanova Roa**
Cargo:	Auditor Interno (Apoyo) Password	**Cargo:**	Profesional Especializado Oficina de Control Interno
Nombre:	N.A.	**Nombre:**	N.A.
Cargo:	N.A.	**Cargo:**	N.A.

Elaboró		Revisó		Aprobó	