Tema	Auditoría del Sistema de Gestión de Seguridad De la Información										
Tipo de Actividad	Calidad		Gestión		Programada	X	Solicitada				
	Interna	X	Externa		Auditoría	X	Seguimiento				
Ciclo de Auditoría	2021 y primer bimestre de 2022										
Objetivo	Evaluar el Sistema de Gestión de Seguridad de la Información en la Unidad Nacional para la Gestión de Riesgo de Desastres, en adelante UNGRD										
Alcance	Sistema de Gestión de Seguridad de la Información de la UNGRD										
Criterios de Auditoría (Documentos de Referencia)	Norma Técnica Colombiana NTC-ISO-IEC 27001:2013 Leyes aplicables Documentos de Seguridad de la Información										

Área, dependencia o proceso a auditar	Gestión de Tecnologías de la Información, Planeación Estratégica, Gestión de Talento Humano, Gestión Administrativa y Gestión Contratación, Evaluación y Seguimiento.
Nombre completo del jefe de área / coordinador	Dr. German Moreno – Jefe de la Oficina de Control Interno de la UNGRD

Auditor líder	Ana Rocío Castro Páez	
Equipo auditor	Betty Yaneth Daza Sandoval	
	Claudia Vela – Observador Profesional Especializado – Contratista UNGRD	Jose Casanova – Observador Profesional Especializado UNGRD
Personas Interesadas	Líderes de los procesos, de acuerdo al alcance del Sistema de Gestión de Seguridad de la Información.	

NIVEL DE RIESGO				
	CUMPLIMIENTO	GESTIÓN DEL RIESGO	CONTROLES	DESEMPEÑO
Critico				
Alto				
Medio	No Aplica	Posibilidad que la auditoría no contribuya al logro de los objetivos de la Entidad	Plan general de auditorías internas de UNGRD	Se define el plan general de auditoría al Sistema de Gestión de Seguridad de la Información de la UNGRD, revisada por la

				oficina de Control Interno.
Medio	No aplica	Posibilidad que los resultados del ejercicio de auditoría sean en beneficio propio o de terceros con la manipuación de información	El equipo auditor no pertenece a la UNGRD y hace parte del sector de Presidencia de la República.	Con la socialización de los resultados de la auditoría en reunión de cierre de auditoría y la generación de los documentos relacionados a la auditoría al Sistema de Gestión de Seguridad de la Información de UNGRD.
Bajo	No aplica	Posibilidad que el equipo auditor no tenga las competencias para realizar el proceso de auditoría al Sistema de Gestión de Seguridad de la Información	Solicitud de la documentación que acredita la cerificación del equipo auditor en Seguridad de la Información.	La Oficina de Control Interno de UNGRD realiza la revisión de los documentos solicitados al equipo de auditoría que hace parte del Departamento Administrativo de la Presidencia de la República.

ANTECEDENTES

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

La auditoría al Sistema de Gestión de Seguridad de la Información de la UNGRD, es realizada a partir de la solicitud por parte de UNGRD a la jefatura de la Oficina de Control Interno del Departamento Administrativo de la Presidencia de la República.

De esta forma, se realiza el ejercio de auditoría con la documentación remitida, incluído el Informe de auditoría interna al Sistema de Gestión de Seguridad de la Información – SGSI – bajo la norma ISO 27001:2013, realizada en el mes de Diciembre de 2021 por Password SAS.

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)

- La buena disposición y compromiso del equipo de trabajo que hace parte del proceso de Gestión de Tecnologías de la Información y de los demás procesos involucrados, lo que hizo que se realizara de forma satisfactoria el proceso de auditoría a la seguridad de la información de la Unidad Nacional para la Gestión de Riesgos de Desastres - UNGRD.

- A pesar que el alcance definido que se encuentra descrito en el Manual del Sistema de Gestión de Seguridad de la Información, comprende el proceso de Gestión de Tecnologías de la Información. Se pudo ver que los colaboradores que hacen parte de los demás procesos conocen sobre seguridad de la información.

- El compromiso de la alta dirección hacia el sistema de gestión de seguridad de la información, a partir de las acciones que se han venido tomando en pro de la implementación y mejora continua.

- Se destaca la gestión realizada por el proceso de Gestión de Tecnologías de la Información por el trabajo que ha venido realizando en la mejora continua del Sistema de Gestión de Seguridad de la Información.

- La existencia de un banco de baterías en el centro de datos, permite que la continuidad sea exitosa en caso que haya una interrupción eléctrica.

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
Documentación relacionada al Sistema de Gestión de Seguridad de la Información actualizada acorde a la normatividad vigente y a la Norma NTC-ISO-IEC-27001:2013 Definición de riesgos de Seguridad de la Información.	

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)

No Conformidades

1. Al realizar el recorrido en el Grupo de Infraestructura Tecnológica y el Grupo de Seguridad de Información se evidenció el acceso a puertos USB, permitiendo la copia de archivos, en los equipos de cómputo de: RC11676 Y RC12774.

   No se evidenció autorización por parte del comité de seguridad de la información.
   Incumpliendo el Procedimiento de Gestión de Medios Removibles PR-1101-GTI-1 y con el control "A.8.3.1 Gestión de medios removibles"

2. Al realizar el recorrido por el Grupo de Seguridad de la información se realiza la verificación de acceso a redes Sociales, verificando el acceso a Facebook en los equipos de cómputo: RC11676

y RC12774. Incumpliendo además el numeral 5.13. Política para el uso de internet, del Manual de Políticas de Seguridad de la Información M-1101- GTI-01: "El usuario no puede utilizar redes sociales salvo sean autorizados por el director de la UNGRD." Y con el control "A.9.1.2 Acceso a Redes y servicios de Red"

3. Al revisar el formato CODIGO M-1603 -SIS -01 _Registro Ingreso al Centro de Datos, no se evidencia el registro de entrada y salida, del Auditor Líder de la Empresa PASSWORD CONSULTING SERVICES SAS, en las fechas correspondientes a los días 22 y 23 de diciembre de 2021, fecha en que se realizó la auditoria interna al Sistema de Gestión de Seguridad de la Información.

   Incumpliendo además el numeral 5.17 de la política de Acceso al Centro de Datos, del Manual de Políticas de Seguridad de la Información M-1101- GTI-01 y con el control "A.11.1.2 Controles de Acceso Físico"

4. Al realizar el recorrido por el Centro de Datos Principal, se evidencia que el Rack de datos se encuentra desordenado y sin marquillado, lo que puede ocasionar una mala ventilación de aire y recalentamiento en los servidores, incumpliendo el control "A.11.2.3 Seguridad del Cableado"

5. Al realizar el recorrido en la Coordinación de TI se evidenció que el equipo de cómputo RC 12774 no tiene instalado el antivirus Kaspersky de la UNGRD, incumpliendo el control "A.12.2.1 Controles contra códigos maliciosos"

6. Durante la Auditoría del SGSI realizada en la UNGRD, no se evidenció el formato de confidencialidad para ser firmado por las funcionarias del DAPRE, incumpliendo el control "A.13.2.4 Acuerdo de confidencialidad o de no divulgación"

   Nota: la NCR 6 fué subsanada durante la auditoría, con el diligenciamiento y firma del compromiso de confidencialidad proceso auditor, por parte de Betty Yanteh Daza Sandoval y Ana Rocío Castro Páez, los cuales fueron remitidos a la Oficina de Control Interno de UNGRD.

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).

- Realizar periódicamente pruebas de restauración de los backups de información y llevar control de estas pruebas.

- Revisar los 33 riesgos del SGSI y unificarlos teniendo en cuenta los lineamientos de la Guía de Administración del Riesgo de la Función Pública.

- Llevar control de las capacitaciones del SGSI teniendo en cuenta la asistencia de los funcionarios y contratistas de todas las dependencias.

- Realizar una matriz de asignación de responsabilidades de Seguridad de la Información.

- Se recomienda la inclusión del control “A.6.2.2 Teletrabajo”, de acuerdo a la política existente de teletrabajo y el control de acceso mediante VPN a la plataforma tecnológica.

- Incluir la página web y token en el inventario de los activos de información.

- Incluir el etiquetado de la Clasificación de la Información (información pública, clasificada y reservada) en el aplicativo de Gestión SIGOB.

- Se recomienda la aplicación de controles de acuerdo a la clasificación de la información Clasificada y reservada como el control de encriptación

- Evaluar la configuración de reutilización de las contraseñas, desde la configuración de Directorio Activo.

- Se recomienda la instalación de programa criptográfico para control de información clasificada y reservada.

- Se recomienda validar la configuración de control criptográfico en correo electrónico de usuarios que envían información clasificada y/o reservada.

- Se recomienda realizar auditorías a los servicios prestados por los proveedores.

- Se recomienda realizar documentación del aprendizaje obtenido del incidente que se presente.

- Se recomienda realizar documentación de recolección de evidencia.

CONCLUSIONES

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

Al realizar el ejercicio de auditoría al Sistema de Gestión de Seguridad de la Información, se evidencia que se ha realizado la gestión para la mejora continua del Sistema de Gestión de Seguridad de la Información de la UNGRD, a partir del apoyo por parte de la alta dirección.

Con la aplicación de los controles se busca la protección de la información de la UNGRD.

Firma Auditor Líder

Nombre
Ana Rocío Castro Páez

Cargo
Profesional Especializado
Departamento Administrativo de la Presidencia de la República

Miembros del Equipo Auditor

Nombre:	**Betty Yaneth Daza Sandoval** **Equipo auditor**	**Nombre:**	Claudia Vela Observadora
Cargo:	Asesora Departamento Administrativo de la Presidencia de la República	**Cargo:**	Profesional Especializado – Contratista UNGRD
Nombre:	Jose Casanova Observador	**Nombre:**	No Aplica
Cargo:	Profesional Especializado UNGRD	**Cargo:**	No Aplica

Elaboró	Ana Rocío Castro Páez	Revisó	Dr. German Moreno	Aprobó	Dr. German Moreno