| **Nombre del informe** |
|---|
| INFORME DE SEGUIMIENTO A LA GESTIÓN DEL RIESGO DE LA SEGURIDAD DIGITAL, PARA EL PERIODO COMPRENDIDO ENTRE OCTUBRE 01 DE 2020 Y ENERO 31 DE 2021. |

| | |
|---|---|
| **Área(s) Auditada(s) - Responsable(s)** | - Subsecretarios.<br>- Jefes de Oficina.<br>- Líderes de proceso. |

## 1. Objetivo

Verificar la gestión del riesgo y la aplicación de la política asociada, en la Secretaría Distrital de Planeación – SDP, en cumplimiento del compromiso establecido para la tercera línea de defensa en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en entidades Públicas, que señaló “Le corresponde a las unidades de control interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad”.

## 2. Alcance

Gestión de los riesgos de la seguridad digital, desde octubre 01 de 2020 a enero 31 de 2021.

## 3. Criterios

- Decreto 124 del 26 de enero de 2016: Plan Anticorrupción y de Atención al Ciudadano.
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, expedida por DAFP en octubre de 2018.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, expedida por DAFP en diciembre de 2020.
- Política de Administración del Riesgo E-LE-030: versión 15, aprobada por acta de mejoramiento 278 de noviembre 07 de 2019 y versión 16, aprobada por acta de mejoramiento 310 de diciembre 24 de 2020.
- Instructivo de Administración del Riesgo E-IN-005: versión 7 aprobada por acta de Mejoramiento 283 de noviembre 19 de 2019.
- Riesgos de seguridad digital.
- Documentos vigentes en el Sistema Integrado de Gestión, relacionados con la gestión de riesgos de la entidad.
- Directrices Generales del Sistema de Control Interno. Tomo 1 Dirección Distrital de Desarrollo Institucional - DDDI, diciembre de 2018, Secretaría General, Alcaldía

Mayor de Bogotá.
- Decreto 1072 de 2015: Decreto único reglamentario del sector trabajo.
- Radicado 3-2021-03869 de febrero 24 de 2021, 3-2021-04565, 3-2021-04748 y 3-2021-05011.
- Decreto 612 de 2018.
- Anexo2.5.2_GestionRiesgosST_Final
- Anexo3.1.1_PlanTratamientoRiesgos
- Anexo4.1.b_PlandeAccionControles2020_Seguimiento
- Anexo4.1.b_PlandeAccionMSPI2020_Seguimiento

## 4. Resultados del informe



### 4.1. INTRODUCCIÓN

El artículo 1° del decreto 612 de 2018 estableció la integración de unos planes, cuya consulta en la entidad se encontró de la siguiente manera:

Tabla 1: Consulta de planes objeto de integración

| Plan | Consulta |
|---|---|
| 1. Plan Institucional de Archivos de la Entidad (PINAR) | A-LE-388 en SIPA |
| 2. Plan Anual de Adquisiciones | SECOP II |
| 3. Plan Anual de Vacantes | |
| 4. Plan de Previsión de Recursos Humanos | A-LE-424 en SIPA |
| 5. Plan Estratégico de Talento Humano | A-LE-423 en SIPA |
| 6. Plan Institucional de Capacitación | A-LE-019 en SIPA |
| 7. Plan de Incentivos Institucionales | A-LE-018 en SIPA |
| 8. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo | A-LE-020 en SIPA |
| 9. Plan Anticorrupción y de Atención al Ciudadano | E-LE-055 en SIPA |
| 10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) | A-LE-015 en SIPA |
| 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información | |
| 12. Plan de Seguridad y Privacidad de la Información. | |

Fuente: Análisis propio.

Como se puede apreciar, los documentos relacionados en su gran mayoría hicieron parte del Sistema de Gestión de la entidad.

En el más reciente informe que presentó la Oficina de Control Interno a la gestión de riesgos de la entidad (radicado 3-2021-03869), no se evaluaron algunos aspectos de la gestión de riesgos de seguridad digital toda vez que esta Oficina no conocía la existencia de los documentos que posteriormente fueron presentados por la Dirección de Sistemas. Se evidenció que dicha información se socializó con la Dirección de Planeación pero es importante que toda la entidad conozca de su existencia y contenido, así como de sus actualizaciones.

La información que quedó pendiente será analizada en el presente informe y complementa lo expuesto en el radicado 3-2021-03869.

Cabe señalar que se trata de un caso excepcional no previsto dentro del Plan Anual de Auditoría, pero que requería ser analizado toda vez que el siguiente informe se producirá hasta octubre de 2021.

### 4.2. DOFA

En el documento “Anexo2.5.2_GestionRiesgosST_Final” presentado por la Dirección de Sistemas se identificaron 8 debilidades, 6 oportunidades, 6 fortalezas y 12 amenazas para los riesgos de la seguridad digital. Seis (6) de las 12 amenazas fueron seleccionadas para la priorización de causas, a saber:

- ASD1_Compromiso de la información - Espionaje remoto
- ASD2_ Acciones no autorizadas - Uso no autorizado del equipo
- ASD3_ Fallas técnicas - Fallas de Equipo
- ASD4_ Acciones no autorizadas - Copia fraudulenta del software
- ASD5_ Fallas técnicas - Mal funcionamiento del software
- ASD6_ Fallas técnicas - Saturación del Sistema de Información
- ASD7_ Fallas técnicas - Incumplimiento en el mantenimiento del sistema de información

### 4.3. Identificación de riesgos

Se identificaron 9 riesgos de la seguridad digital, cuyo contenido se relacionó con pérdida de confidencialidad, disponibilidad e integridad para los activos de información de software, hardware y servicios. Su relación con las amenazas se dio de la siguiente manera:

Tabla 2: Tipología de riesgos

| Riesgo / Amenaza | Pérdida de Confidencialidad | | | Pérdida de Disponibilidad | | | Pérdida de Integridad | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| | Hardware | Software | Servicio | Hardware | Software | Servicio | Hardware | Software | Servicio | |
| | **RSD1** | **RSD4** | **RSD7** | **RSD2** | **RSD5** | **RSD8** | **RSD3** | **RSD6** | **RSD9** | |
| ASD1 | X | X | X | | | | X | X | X | 6 |
| ASD2 | X | | X | X | | X | X | | X | 6 |
| ASD3 | | | | X | | X | | | | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ASD4 | | X | X | | | | | X | | 3 |
| ASD5 | | | | | X | | | | | 1 |
| ASD6 | | | | | | X | | | | 1 |
| ASD7 | | | | | | X | | | | 1 |
| Total | 2 | 2 | 3 | 2 | 1 | 4 | 2 | 2 | 2 | |

Fuente: Datos del anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

Así las cosas, se identificaron como amenazas más representativas las relacionadas con espionaje remoto (ASD1) y uso no autorizado del equipo (ASD2). Y el riesgo para el cual se identificaron el mayor número de amenazas fue la disponibilidad de servicio (RSD8).

## 4.4. Criticidad de los riesgos

La criticidad del riesgo se evaluó por la ubicación dentro del mapa de calor (zona baja, moderada, alta o extrema) resultante de cruzar la probabilidad y el impacto, lo cual con la aplicación de la nueva guía del DAFP, se resume así:

Tabla 3: Criticidad de los riesgos (mapa de calor)

| PROBABILIDAD | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| RIESGO INHERENTE | Muy alta (100%) | | | | | | 0 |
| | Alta (80%) | | | | | | 0 |
| | Media (60%) | | | | | | 0 |
| | Baja (40%) | | | | **RSD7 RSD9** | | 2 |
| | Muy baja (20%) | | **RDS5 RDS6** | **RDS4 RSD8** | **RSD1 RSD2 RSD3** | | 7 |
| | Total | 0 | 2 | 2 | 5 | 0 | 9 |
| RIESGO RESIDUAL | Muy alta (100%) | | | | | | 0 |
| | Alta (80%) | | | | | | 0 |
| | Media (60%) | | | | | | 0 |
| | Baja (40%) | | | | | | 0 |
| | Muy baja (20%) | **RDS5 RDS6** | **RDS4 RSD8** | **RSD1 RSD3 RSD9** | **RSD2** | | 8 |
| | Total | 2 | 2 | 3 | 1 | 0 | 8 |
| | | Leve (20%) | Menor (40%) | Moderado (60%) | Mayor (80%) | Catastrófico (100%) | Total |
| | | **IMPACTO** | | | | | |

| Resumen | Bajo | Moderado | Alto | Extremo |
|---|---|---|---|---|
| Inherente | 2 | 2 | 5 | 0 |
| Residual | 4 | 3 | 1 | 0 |

Fuente: Anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

La única observación al respecto es que el riesgo residual 7 no fue clasificado en la matriz de calor.

## 4.5. Identificación y clasificación de controles

En el anexo4.1.b_PlandeAccionControles2020_Seguimiento entregado por la Dirección de Sistemas se identificaron 114 controles, los cuales fueron codificados como se indica a continuación:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.5.1.1 | A.7.2.3 | A.9.1.2 | A.10.1.1 | A.11.2.6 | A.12.4.4 | A.14.1.2 | A.15.1.2 | A.17.1.3 |
| A.5.1.2 | A.7.3.1 | A.9.2.1 | A.10.1.2 | A.11.2.7 | A.12.5.1 | A.14.1.3 | A.15.1.3 | A.17.2.1 |
| A.6.1.1 | A.8.1.1 | A.9.2.2 | A.11.1.1 | A.11.2.8 | A.12.6.1 | A.14.2.1 | A.15.2.1 | A.18.1.1 |
| A.6.1.2 | A.8.1.2 | A.9.2.3 | A.11.1.2 | A.11.2.9 | A.12.6.2 | A.14.3.1 | A.15.2.2 | A.18.1.2 |
| A.6.1.3 | A.8.1.3 | A.9.2.4 | A.11.1.3 | A.12.1.1 | A.12.7.1 | A.14.2.2 | A.16.1.1 | A.18.1.3 |
| A.6.1.4 | A.8.1.4 | A.9.2.5 | A.11.1.4 | A.12.1.2 | A.13.1.1 | A.14.2.3 | A.16.1.2 | A.18.1.4 |
| A.6.1.5 | A.8.2.1 | A.9.2.6 | A.11.1.5 | A.12.1.3 | A.13.1.2 | A.14.2.4 | A.16.1.3 | A.18.1.5 |
| A.6.2.1 | A.8.2.2 | A.9.3.1 | A.11.1.6 | A.12.1.4 | A.13.1.3 | A.14.2.5 | A.16.1.4 | A.18.2.1 |
| A.6.2.2 | A.8.2.3 | A.9.4.1 | A.11.2.1 | A.12.2.1 | A.13.2.1 | A.14.2.6 | A.16.1.5 | A.18.2.2 |
| A.7.1.1 | A.8.3.1 | A.9.4.2 | A.11.2.2 | A.12.3.1 | A.13.2.2 | A.14.2.7 | A.16.1.6 | A.18.2.3 |
| A.7.1.2 | A.8.3.2 | A.9.4.3 | A.11.2.3 | A.12.4.1 | A.13.2.3 | A.14.2.8 | A.16.1.7 | |
| A.7.2.1 | A.8.3.3 | A.9.4.4 | A.11.2.4 | A.12.4.2 | A.13.2.4 | A.14.2.9 | A.17.1.1 | |
| A.7.2.2 | A.9.1.1 | A.9.4.5 | A.11.2.5 | A.12.4.3 | A.14.1.1 | A.15.1.1 | A.17.1.2 | |

Por su parte, en el anexo 2.5.2 entregado por la misma Dirección se identificaron 51 controles, dentro de los cuales, algunos se repiten porque hacen parte de uno o más riesgos, como se ilustra a continuación:

Tabla 4: Relación de controles y riesgos.

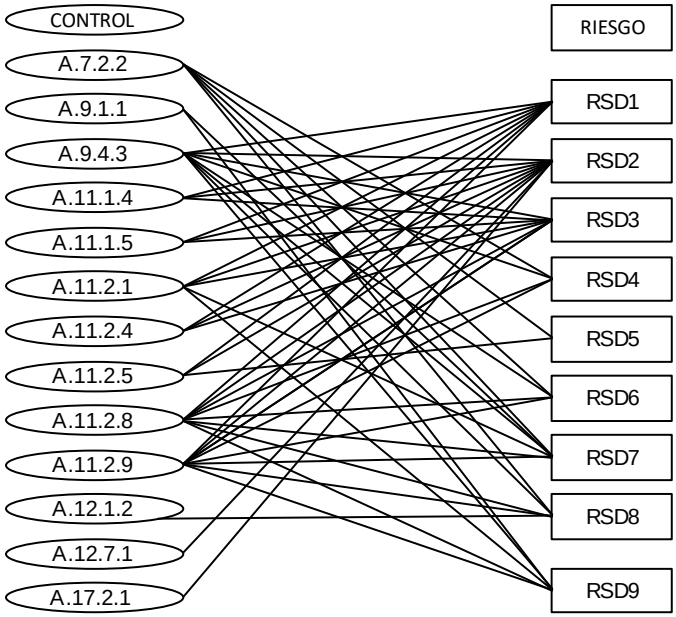
| Riesgo / Control | RSD1 | RSD2 | RSD3 | RSD4 | RSD5 | RSD6 | RSD7 | RSD8 | RSD9 | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|
| A.7.2.2 | | | | X | X | X | X | X | | 5 |
| A.9.1.1 | | | | | | | X | | X | 2 |
| A.9.4.3 | X | X | X | X | | X | X | X | X | 8 |
| A.11.1.4 | X | X | X | | | | | | | 3 |
| A.11.1.5 | X | X | X | | | | | | | 3 |
| A.11.2.1 | X | X | X | | | | X | | X | 5 |
| A.11.2.4 | X | X | X | | | | | | | 3 |
| A.11.2.5 | | X | X | | X | | | | | 3 |
| A.11.2.8 | X | X | X | X | | X | X | X | X | 8 |
| A.11.2.9 | X | X | X | X | | X | X | X | X | 8 |
| A.12.1.2 | | | | | | | | X | | 1 |
| A.12.7.1 | | X | | | | | | | | 1 |
| A.17.2.1 | | X | | | | | | | | 1 |
| TOTAL | 7 | 10 | 8 | 4 | 2 | 4 | 6 | 5 | 5 | 51 |

Fuente: Datos del anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

De los dos anexos se concluye que se contó realmente con 13 controles para gestionar los 9 riesgos. El riesgo 2, relacionado con la pérdida de la disponibilidad de hardware, fue el que más controles tuvo asociados (10). Por su parte, tres de los controles

(A.9.4.3, A.11.2.8 y A.11.2.9) fueron los que se definieron para el mayor número de riesgos. La relación entre riesgos y controles se ilustra de la siguiente manera:

Gráfico 1: Relación de controles y riesgos.




Fuente: Datos del anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

Pese a la intrincada red de relaciones, no hay contradicciones entre los riesgos o sus controles. No obstante, para conocer la efectividad de cada control es necesario hacer la revisión en cada riesgo al que fue asociado.

## 4.6. Calificación de controles

En el paso 8 del documento E-IN-005 se estableció un cuestionario para calificar los controles, que fue aplicado para los riesgos de la seguridad digital, con los siguientes resultados:

Tabla 5: Evaluación de los controles con base en las respuestas dadas a las preguntas del E-IN-005.

| N° | Pregunta (E-IN-005) | Calificación máxima (E-IN-005) | Cantidad | Id del control a revisar |
|---|---|---|---|---|
| 1 | ¿Existe un responsable asignado a la ejecución del control? | • 15 puntos ó 15%: en caso afirmativo.<br>• 0 puntos ó 0%: en caso negativo. | • 51<br>• 0 | No aplica |
| 2 | ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control? | • 15 puntos ó 15%: en caso afirmativo.<br>• 0 puntos ó 0%: en caso negativo. | • 51<br>• 0 | No aplica |
| 3 | ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna? | • 15 puntos ó 15%: en caso afirmativo.<br>• 0 puntos ó 0%: en caso negativo. | • 51<br>• 0 | No aplica |

| N° | Pregunta (E-IN-005) | Calificación máxima (E-IN-005) | Cantidad | Id del control a revisar |
|---|---|---|---|---|
| 4 | ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo verificar, validar, cotejar, comparar, revisar, etc.? | • 15 puntos ó 15%: preventivo.<br>• 10 puntos ó 10%: detectivo.<br>• 0 puntos ó 0%: si no es un control. | • 48<br>• 3<br>• 0 | No aplica |
| 5 | ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo? | • 15 puntos ó 15%: en caso afirmativo.<br>• 0 puntos ó 0%: en caso negativo. | • 50<br>• 1 | A.17.2.1 |
| 6 | ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna? | • 15 puntos ó 15%: en caso afirmativo.<br>• 0 puntos ó 0%: en caso negativo. | • 46<br>• 5 | A.11.2.4<br>A.12.7.1<br>A.17.2.1 |
| 7 | ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión? | • 10 puntos ó 10%: en caso que la evidencia sea completa.<br>• 5 puntos ó 5%: en caso que la evidencia sea incompleta.<br>• 0 puntos o 0%: en caso que no haya evidencia. | • 41<br>• 1<br>• 9 | A.9.4.3<br>A.17.2.1 |
| 8 | ¿El Control se ejecuta de manera consistente por los responsables? | • __: siempre se ejecuta.<br>• __: algunas veces.<br>• __: no se ejecuta. | No evaluado | Todos |

Fuente: documento E-IN-005 administración del riesgo, datos del anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

En dicho esquema la nota máxima que puede obtener un control es de 100 puntos. El número de controles que se registró en cada calificación se resume a continuación:

Tabla 6: Cantidad de controles en cada categoría de calificación.

| Calificación | 60 | 80 | 81 | 90 | 100 | Total |
|---|---|---|---|---|---|---|
| Controles | 1 | 1 | 3 | 8 | 38 | 51 |

Fuente: Datos del anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

La mayoría de los controles fueron evaluados con las máximas calificaciones y hubo consistencia en la calificación de los que se repiten. No obstante, se afirmó que: a) El control A.17.2.1 no tuvo una fuente de información confiable; b) Para los controles A.17.2.1, A.11.2.4 y A.12.7.1 no se revisaron las desviaciones; c) Para los controles A.9.4.3 y A.17.2.1 no se dejó evidencia; d) El control A.17.2.1, relacionado con la disponibilidad de instalaciones de procesamiento de información, fue el más débil en su calificación.

## 4.7. Valoración del diseño de los controles

La Guía del DAFP definió unos aspectos a considerar en los controles, los cuales se cumplieron de la siguiente manera:

Tabla 7. Seguimiento al cumplimiento de los pasos establecidos en la Guía 2020 del DAFP

| N° | Ítem | Definición | Controles que lo incorporaron | Controles que no lo incorporaron |
|---|---|---|---|---|
| 1 | Responsable de ejecutar el control | Identifica el cargo del servidor que ejecuta el control. En caso de que sean controles automáticos se identificará el sistema que realiza la actividad | 0 | 51 |
| 2 | Acción | Se determina mediante verbos que indican la acción que deben realizar como parte del control | 51 | 0 |
| 3 | Complemento | Corresponde a los detalles que permiten identificar claramente el objeto de control | 51 | 0 |

Fuente: Datos del anexo 2.5.2 entregado por la Dirección de Sistemas y análisis propio.

## 4.8. Valoración de la efectividad de los controles

La Dirección de Sistemas reportó evidencias de la ejecución de varios de ellos, no se estableció su relación con los riesgos, salvo los resaltados en la siguiente lista, sobre los cuales ya se hizo referencia en este informe. De los mencionados 13, solo se reportó evidencia para 7 y los otros 6 no se han programado. La totalidad de los controles

La incidencia de los 51 controles (13 en realidad), en la transición que hicieron los riesgos del estado inherente al residual, según el mapa de calor anteriormente presentado, se resume así:

Tabla 8: Cantidad de riesgos en cada zona del mapa de calor

| Zona | Inherente | | Residual | |
|---|---|---|---|---|
| Extrema | 0 | 0% | 0 | 0% |
| Alta | 5 | 56% | 1 | 13% |
| Moderada | 2 | 22% | 3 | 38% |
| Baja | 2 | 22% | 4 | 50% |
| **Total** | 9 | 100% | 8 | 100% |

Fuente: análisis propio.

Como puede apreciarse, la mayoría de los riesgos en su calidad de inherentes ocupaban la zona alta, en tanto que los residuales ocuparon la zona baja. Esto muestra efectividad en los controles. No obstante, la efectividad solo aplicaría a los controles que fueron programados y para los cuales se presentó evidencia de su ejecución.

## 4.9. Acciones

En el anexo 3.1.1., presentado por la Dirección de Sistemas como “plan de tratamiento de riesgos de seguridad de la información[1]” se identificaron 11 acciones que en su mayoría fueron realizadas en 2020 y una en curso para 2021. El monitoreo a las mismas hizo parte del mencionado documento.

# 5. Conclusiones y recomendaciones

[1] No hace parte de los documentos del Sistema de Gestión de la SDP.

## 5.1. Fortalezas

El registro de amenazas, la especificación de las vulnerabilidades y los tratamientos para los Activos de Información que fueron clasificados en criticidad “Alta” pudieron ser verificados en la información suministrada por la Dirección de Sistemas. Por ello con el presente informe se da alcance al radicado 3-2021-03869 de febrero 24 de 2021 y se elimina la situación de mejora que fue consignada en dicho informe con el número 11.

## 5.2. Debilidades

### 5.2.1. Situaciones susceptibles de mejora

| N° | Situación susceptible de mejora | Numeral | Responsable |
|---|---|---|---|
| 1 | Hace falta publicidad y publicación de los documentos relacionados con los riesgos de seguridad digital, por lo cual se recomienda que hagan parte del Sistema de Gestión de la entidad. | 4.1 | Dirección de Sistemas |
| 2 | El riesgo residual 7 no fue clasificado en la matriz de calor. | 4.3 | Dirección de Sistemas |

Aunque la formulación de planes de mejoramiento es opcional para las situaciones de mejora identificadas, dichas situaciones deben ser atendidas en el marco de la gestión propia del área o proceso. La OCI revisará las medidas adoptadas en la próxima auditoría y/o seguimiento.

### 5.2.2. Situaciones críticas

| N° | Condición | Criterio | Causa | Efecto | Numeral | Responsable | Reincidente (si/no) | Tema clave (Max 5) |
|---|---|---|---|---|---|---|---|---|
| | No se encontraron situaciones críticas | | | | | | | |

La formulación de planes de mejoramiento es obligatoria para las situaciones críticas identificadas, y debe hacerse para eliminar de fondo las causas que las originaron, atendiendo lo establecido en los procedimientos S-PD-001 y S-PD-005. En la próxima auditoría y/o seguimiento, la OCI efectuará el análisis y verificación de la efectividad alcanzada.

**Definiciones:**

- **Condición:** Descripción de la situación deficiente encontrada, (lo que es/realidad).
- **Criterio:** Estándar/norma/reglamento contra el cual se ha medido o comparado la condición, (lo que debe o debió ser).
- **Causa:** Razones por las cuales, de acuerdo con lo evidenciado, ocurrió la condición observada. No limita el análisis de causas que debe realizar el responsable de la unidad auditada para la formulación del plan de mejoramiento.
- **Efecto:** Consecuencia real o potencial, cuantitativa o cualitativa de la condición descrita, (la diferencia entre lo que es y debió ser).

| Nombres / Equipo Auditor | | Fecha Inicio | Fecha Fin |
|---|---|---|---|
| **Auditor líder / principal** | Eulalia Porras | Marzo 02 de 2021 | Mayo 03 de 2021 |
| **Auditor(es) interno(s) / acompañante(s)** | No aplica | | |

**JUAN FELIPE RUEDA GARCÍA**
**Jefe Oficina de Control Interno**