Auditoría al Proceso Gestión de Servicios Tecnológicos

Informe Final de auditoría interna: AI-29-2024

Fecha de emisión: 19/11/2024

Índice general

Unidad de Planificación Rural Agropecuaria (UPRA)
Calle 28 Nº 13-22, Torre C, piso 3. Edif. Palma Real. Bogotá, Colombia.
+57(601) 552 9820, 245 7307
www.upra.gov.co

1. INTRODUCCIÓN

La Asesoría de Control Interno de la UPRA, en cumplimiento del Plan Anual de Auditoría para la vigencia 2024, aprobado por el Comité Institucional de Coordinación de Control Interno el 22 de enero de 2024, realizó una auditoría a la Oficina TIC en relación con su proceso de Gestión de Servicios Tecnológicos.

Este proceso, cuyo objetivo es gestionar el soporte de los servicios y recursos tecnológicos mediante la administración de la infraestructura de TI, busca asegurar la continuidad, el óptimo desempeño, la operación y la seguridad de los servicios tecnológicos en toda la entidad. La auditoría se realizó tomando como referencia la **caracterización del proceso (GST-PR-001, versión 4 del 20 de mayo de 2024)**. Este documento incluye el plan de seguridad y privacidad de la información, el plan de tratamiento de riesgos, el manual de política de seguridad, la gestión de incidentes de seguridad de la información y los riesgos de seguridad de la información; que les permiten gestionar e implementar buenas prácticas de seguridad de la información asegurando la disponibilidad, confidencialidad e integridad de la información en la Unidad de Planificación Rural y Agropecuaria (UPRA).

Considerando estos elementos, se aplicaron criterios de auditoría relacionados con el Modelo de Seguridad y Privacidad de la Información (MSPI) emitido por MinTIC, así como con las normas técnicas colombianas NTC-ISO/IEC 27001:2013 y NTC-ISO/IEC 27001:2022, que establecen los estándares y mejores prácticas para la gestión de la seguridad de la información.

Es importante destacar que esta auditoría se alinea con la Política de Gobierno Digital, cuyo objetivo es mejorar la calidad de vida de los ciudadanos y la competitividad del país mediante la transformación digital del Estado. Uno de los componentes fundamentales de esta política es la seguridad y privacidad de la información, lo cual hace que la auditoría sea esencial para asegurar la integridad y confidencialidad de los datos, en consonancia con la transversalidad y el cumplimiento de los requisitos normativos. Así, la implementación del MSPI y la norma ISO 27001 contribuye al fortalecimiento de la gobernanza digital, apoyando la innovación pública y la protección de los activos digitales de la entidad.

La auditoría se orientó a evaluar el Control Interno del proceso de Gestión de Servicios Tecnológicos, mediante el análisis de la caracterización del proceso, abarcando actividades de planeación, ejecución y seguimiento. Este ejercicio se llevó a cabo de acuerdo con el procedimiento de Evaluación Independiente y siguiendo buenas prácticas de auditoría, que incluyen la planificación de la auditoría, la ejecución del trabajo, la comunicación de resultados y la elaboración del informe final.

2. METODOLOGÍA

2.1. Identificación

Aspecto evaluable (unidad auditable)	Proceso Gestión de Servicios Tecnológicos
Líder de proceso/jefe(s) de dependencia(s)	Luz Mery Gómez Contreras – Jefe Oficina TIC Andrés Felipe Hernández León – Profesional especializado
Objetivo de la auditoría	Llevar a cabo la evaluación al proceso de Gestión de Servicios Tecnológicos, enfocado en la seguridad de la información y los procedimientos de gestión de la infraestructura tecnológica, conforme a los lineamientos y buenas prácticas impartidas por el MinTIC a través del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta evaluación se llevará a cabo tomando como referencia estándares internacionales y orientando la gestión hacia una implementación adecuada del ciclo de vida de la seguridad de la información: Planeación, Implementación, Evaluación y Mejora Continua.
Alcance de la auditoría	Comprende el periodo entre el segundo semestre de 2023 y el primer semestre de 2024, durante el cual se evaluará la gestión y el control interno en el proceso de Servicios Tecnológicos.
Limitaciones al alcance	Durante la auditoría, no se identificaron limitaciones, ya que el grupo de gestión de servicios tecnológicos y los grupos transversales relacionados proporcionaron oportunamente toda la información solicitada y mostraron total disposición para atender la prueba de recorrido.
Reunión de apertura	Acta de Reunión de Apertura 16 de agosto de 2024. (Radicado SEA # 2024-3-014930)
Ejecución de auditoría	Desde: 16 de agosto de 2024 Hasta: 05 de noviembre de 2024 Memorando presentación de Auditoría (Rad # 2024-3-014318) Presentación de resultados preliminares (29 de octubre de 2024)
Reunión de cierre	05 de noviembre de 2024
Líder de auditoría	Sandra Milena Ruano Reyes Asesora de Control Interno

Auditor	Paola Tatiana Mesa Dávila Contratista Control Interno

2.2 Criterios de auditoría:

- Modelo de Seguridad y Privacidad de la Información – MSPI emitida por MinTIC.
- Norma NTC-ISO/IEC 27001:2022.
- Norma NTC-ISO/IEC 27001:2023.
- Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6. noviembre de 2022.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital. versión 4. octubre de 2018.
- PEC-GU-001 Guía Política de Administración de Riesgos de la UPRA, versión 6 (2024-02-28).
- GST-PR-001 Proceso Gestión de Servicios Tecnológicos.
- Anexo 12. Plan de Seguridad y Privacidad de la Información 2024.
- Anexo 12. Plan de Seguridad y Privacidad de la Información 2023.
- Anexo 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024.
- Anexo 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023.
- Plan de Pruebas de Seguridad y Análisis de Vulnerabilidades Sistema para la Eficiencia Administrativa SEA, portal web upra.gov.co
- GST-IN-002 Instructivo de Metodología de Gestión de Riesgos de Seguridad de la Información.
- Manuales:
    - GST-MA-001 Manual de Catálogo de Servicios de Infraestructura Tecnológica – IT.
    - GST-MA-002 Manual de Política de Seguridad de la Información.
    - GST-MA-003 Manual de Políticas de Infraestructura Tecnológica – IT.
    - GST-MA-004 Manual de Política de Protección de Datos Personales e Información Propiedad o bajo Protección de la UPRA.
    - GST-MA-005 Manual para la Gestión de Cuentas de Usuario – UPRA.
    - GST-MA-006 Manual para la Gestión de Cambios o Actualizaciones de TI.
    - Manual Especifico de Funciones y Competencias Laborales - UPRA.
- Procedimientos:
    - GST-PR-001 Procedimiento de Evaluación Independiente.
    - GST-PD-001 Copias de Seguridad.
    - GST-PD-002 Gestión de Incidentes de Seguridad de la Información.
    - GST-PD-003 Mantenimiento Preventivo y Correctivo de IT.
    - GST-PD-004 Gestión de Infraestructura Tecnológica.
    - GST-PD-005 Soporte Técnico y Actualización de Componentes IT.
    - GST-PD-006 Procedimiento para la Renovación y Aplicación de Certificados SSL.
    - GST-PD-007 Gestión de Cambios de TI.
    - GDR-PD-002 Procedimiento Control Interno Disciplinario.

- Guías:
  - GST-GU-004 Guía de Actualización Infraestructura Tecnológica – IT.
  - GST-GU-005 Guía para la Gestión de Incidentes de Seguridad de la Información.
  - GST-GU-006 Guía Plan de Sensibilización, Comunicación y Entrenamiento en Seguridad de la Información
  - GST-GU-008 Guía para la Gestión de la Capacidad de IT de la UPRA.
  - GST-GU-009 Guía de Clasificación y Rotulación de la Información.
  - GST-GU-010 Guía para el Acuerdo de Nivel de Servicio Infraestructura Tecnológica, Sistemas de Información y Asesoría Comunicaciones.
  - GST-GU-011 Guía para Copias de Respaldo y Restauración
- Mapa de riesgos:
  - GST-RI-001 Mapa de Riesgos del Proceso de Gestión de Servicios Tecnológicos. Versión 4 del 15/08/2024.
- Formatos asociados e indicadores del proceso.
- Normatividad vigente aplicable a la entidad.

2.3 Muestreo y herramientas

- Herramientas utilizadas durante la auditoría:
  - Repositorio One Drive creado por el equipo de Servicios Tecnológicos.
  - Información publicada en el sitio web de la Entidad.
  - Sistema de Eficiencia Administrativa (SEA)
  - Repositorio institucional.
- Relación de plantillas de trabajo utilizadas:
  - 05_Plani1ControlAcceso_20240902
  - 06_Plani2SeguridadOperaciones_20240902
  - 07_Plani3SeguridadComunicaciones_20240902
  - 08_Plani4AdquisicionDesarrolloMatenimientoSistemas_20240902
  - 09_Plani5GestionIncidentes_202400902
  - 10_Plani6SeguridadFisica_20240902
  - 11_Plani7ContinuidadNegocio_20240902
  - 12_Plani8GestionActivos_20240002
  - 13_Plani9RecursoHumano_20240902
  - 14_Plani10ProtecciónDatosPersonales_20240902
  - 15_Plani11Riesgos_20240902
  - 16_Plani12Indicadores_20240902
  - 17_Entrevistas_20241002
  - 18_ListaChequeo_20240902
  - 19_ CálculoMuestra1_20240902
  - 20_ CálculoMuestra2_20240902

1.3. Población

La población objetivo corresponde a los empleados al corte de junio de 2024, identificándose un total de 62 funcionarios y 527 contratistas, ya que es un proceso transversal a la organización.

3. RESULTADOS DE LA AUDITORÍA

3.1 Análisis de Riesgos y Controles

En el ejercicio de esta auditoría se incluyó el análisis de los riesgos y controles del proceso de Gestión de Servicios Tecnológicos (GST-PR-001) el cual cuenta con trece (13) riesgos de gestión todos ellos asociados al alcance de la presente auditoría.

Con el fin de evaluar la ejecución y efectividad de los controles, se tomó como criterio la Guía Política de Administración de Riesgos de la UPRA (PEC-GU-001) versión 6, la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6 - noviembre de 2022 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital, versión 4 - octubre de 2018.

Los resultados finales se presentan de acuerdo con la siguiente matriz de color la cual permite establecer si el control está presente y funcionando, y establecer puntos de mejora:

Clasificación		Observaciones de Control
Mantenimiento de Control		Se encuentra presente y funciona correctamente, por lo tanto, se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa.
Deficiencia de Control (Diseño o Ejecución)		Se encuentra presente y funcionando, pero requiere acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución.
Deficiencias de Control Mayor (Diseño y Ejecución)		No se encuentra presente por lo tanto no está funcionando, lo que hace que se requieran acciones dirigidas a fortalecer su diseño y puesta en marcha. (o no fue posible contar con evidencias para concluir que el control se estuviera ejecutando).

A continuación, se muestran los resultados que fueron revisados por parte de la Asesoría de Control Interno, los cuales están asociados al proceso de Gestión de Servicios Tecnológicos:

Se identificaron deficiencias mayores en el diseño de 16 controles asociados a 8 riesgos, y deficiencias menores en el diseño de 17 controles para 9 riesgos, aunque estos últimos controles se aplican.

En el resultado de la revisión del análisis de controles y riesgos, se destaca la necesidad de revisar y asignar el responsable de cada actividad de control, asegurando que correspondan a los cargos oficialmente definidos por la organización, como podría ser un Profesional Especializado. Además, como parte de este ejercicio práctico, es crucial cuestionar si cada control está efectivamente previniendo las causas identificadas para los riesgos asociados.

Para una información más detallada, consulte el Anexo 1: Análisis de Riesgos y Controles.

3.2 Análisis de Indicadores

Con el fin de poder realizar un análisis a los indicadores del proceso de Gestión de Servicios Tecnológicos, se realiza la revisión de cada una de las cinco (5) fichas correspondientes a las especificaciones técnicas de cada indicador descargadas a través de la plataforma SEA; y los tableros de indicadores relacionados con el III_Cuatrimestre de 2023 y I_Cuatrimestre de 2024 publicados en la página de la UPRA.

Las fichas técnicas revisadas fueron las siguientes:
GST-ID-001 Copias de Respaldo
GST-ID-002 Incidentes de Seguridad
GST-ID-003 Análisis de Vulnerabilidades
GST-ID-005 Mantenimientos de Infraestructura Tecnológica
GST-ID-006 Porcentaje de la Capacidad en la Prestación de Servicios de Tecnología

Se evidencia que no se presentaron desviaciones significativas en los indicadores evaluados para los periodos comprendidos entre el segundo semestre de 2023 y el primer semestre de 2024. Los análisis realizados sobre los indicadores demuestran un desempeño sobresaliente y un alto nivel de cumplimiento en cada área. Esto refleja un adecuado seguimiento de las actividades, así como una gestión efectiva de los recursos tecnológicos, lo que contribuye a la continuidad y seguridad de los servicios en la UPRA. En particular, se destaca la mejora continua en la implementación de soluciones de hiperconvergencia para copias de respaldo, la respuesta eficaz ante incidentes de seguridad y vulnerabilidades, y el cumplimiento del mantenimiento de infraestructura, lo cual asegura la disponibilidad y confiabilidad de los servicios tecnológicos en apoyo a la planificación rural agropecuaria.

3.3 Análisis de la implementación del MSPI y efectividad de los controles de seguridad de la información establecidos por la norma ISO 27001.

En el presente informe, se darán a conocer los resultados de la auditoría realizada para evaluar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, así como la efectividad de los controles de seguridad establecidos conforme a la norma ISO 27001. Este análisis se llevó a cabo con el propósito de verificar que los mecanismos de protección de la información estén alineados con los estándares internacionales y que los controles aplicados sean efectivos en la gestión de riesgos de seguridad de la información.

Los resultados de la auditoría se han organizado en cuatro categorías, de acuerdo con la actualización de la norma ISO 27001:2022, que establece distintos tipos de controles: controles organizacionales, controles de personas, controles físicos y controles tecnológicos. Además, los resultados se presentan en dos componentes: un componente de revisión documental, donde se evaluaron políticas, procedimientos y registros asociados a la seguridad de la información, y un componente evidenciado a través de pruebas de recorrido, que permitió observar en la práctica la implementación y efectividad de dichos controles.

Esta clasificación permite una evaluación detallada de cada área, con especial énfasis en los principios de confidencialidad, integridad y disponibilidad de la información. A través de este análisis, se busca identificar tanto las fortalezas como las oportunidades de mejora en el cumplimiento del MSPI y de los requisitos de la ISO 27001. Esta visión integral sobre el estado actual de la seguridad de la información en la entidad permitirá orientar futuras acciones para fortalecer la seguridad, garantizar la protección de los datos sensibles y asegurar la continuidad operativa.

3.3.1 Controles Organizacionales

Los controles organizacionales en el marco de la norma ISO 27001 están diseñados para establecer políticas, procedimientos y estructuras que respalden la gestión de la seguridad de la información a nivel estratégico y operativo dentro de la organización. Estos controles tienen como objetivo asegurar que la alta dirección se involucre activamente en la protección de los activos de información y que existan mecanismos de gobernanza eficaces para gestionar riesgos, implementar políticas de seguridad y supervisar el cumplimiento de las normativas tanto internas como externas.

Mediante controles organizacionales, tales como la asignación de roles y responsabilidades, la gestión de riesgos, el desarrollo de políticas de seguridad y la creación de comités de supervisión, la norma ISO 27001 promueve un enfoque sistemático y proactivo hacia la seguridad de la información. Estos controles son fundamentales para alinear las prácticas de seguridad con los objetivos estratégicos de la entidad y asegurar que la organización esté preparada para responder de manera efectiva ante incidentes de seguridad.

3.3.1.1 Revisión documental

Durante el ejercicio de auditoría se realizó una exhaustiva revisión documental de los controles organizacionales implementados por la UPRA en conformidad con su política de seguridad de la información (GST-MA-002-Política de Seguridad de la Información) y alineados con la norma ISO 27001. A continuación, se resumen las principales situaciones observadas:

1. **Políticas de Seguridad de la Información**: La UPRA cuenta con políticas de seguridad aprobadas y publicadas por la alta dirección, alineadas con los objetivos organizacionales y revisadas en intervalos planificados. Estas políticas incluyen un compromiso de mejora continua y describen detalladamente los roles y responsabilidades de los distintos niveles de la entidad, desde la alta dirección hasta los usuarios de los activos de información.

2. **Roles y Responsabilidades:** Se han definido claramente los roles y responsabilidades en seguridad de la información, lo que incluye la segregación de deberes para evitar accesos no autorizados, aunque NO se tienen claras las acciones disciplinarias en caso de incumplimiento de las políticas.

3. **Gestión de Incidentes y Contacto con Autoridades**: La entidad ha establecido procedimientos formales para la gestión de incidentes de seguridad, así como un proceso claro para contactar a las autoridades y grupos de interés en caso de incidentes críticos.

4. **Inventario y Clasificación de Activos:** Existe un inventario formal de activos de información, en el que se asigna un responsable para cada activo y se clasifican según su nivel de confidencialidad y criticidad. Este inventario se actualiza anualmente.

5. **Seguridad en la Transferencia y Uso de Activos**: La UPRA ha implementado políticas para la transferencia segura de información y el uso adecuado de los activos. También existen normas claras para el etiquetado y manejo de la información clasificada.

6. **Control de Acceso:** Se han establecido políticas de control de acceso que limitan los permisos de acuerdo con el rol y la necesidad de cada usuario. La UPRA cuenta con procesos formales para la creación, renovación y revocación de permisos de acceso, así como para la gestión de identidades y autenticación segura.

7. **Relaciones con Proveedores y Seguridad en la Cadena de Suministro:** La seguridad de la información se extiende a los acuerdos con proveedores, que incluyen cláusulas específicas en los contratos y la revisión del cumplimiento de los requisitos de seguridad.

8. **Evaluación y Respuesta a Incidentes:** La UPRA cuenta con mecanismos de evaluación de incidentes y recopilación de evidencias, aunque se identificó la necesidad de mejorar el uso de la información de incidentes para implementar medidas preventivas más efectivas.

9. **Seguridad de la información durante la interrupción:** Se verificó que en la sección 17.1 de la Política de Seguridad de la información, donde menciona que: "*La UPRA desarrollará y mantendrá un plan de continuidad del negocio que contempla los requisitos de seguridad de la información necesarios*" y en la sección 17.2 "*se debe establecer un Plan de Recuperación de Desastres Informáticos donde se defina el tratamiento a las fallas e incidentes que interrumpan el acceso a la información soportada por la infraestructura tecnológica*"; durante la prueba de recorrido se evidencia que NO se cuenta con ninguno de los dos planes a los que se hace referencia en la política de Seguridad de la Información.

Estos resultados muestran que la UPRA ha implementado controles organizacionales significativos en alineación con su política de seguridad de la información y la norma ISO 27001. Sin embargo, se recomienda fortalecer los controles relacionados con la seguridad de la información durante las interrupciones. Es necesario revisar y ajustar la política para asegurar el cumplimiento de todas las directrices descritas, ya que actualmente se evidencian algunos incumplimientos. Esto podría afectar la integridad y el cumplimiento de los estándares de seguridad establecidos por la entidad.

3.3.1.2 Pruebas de recorrido

Durante las pruebas de recorrido realizadas los días 2 y 3 de octubre, se evidenciaron los controles relacionados con controles de acceso, gestión de incidentes, continuidad del negocio, gestión de activos y datos personales, las cuales permitieron observar y verificar en campo la implementación y efectividad de estos para gestionar la seguridad de la información, en conformidad con las directrices de la norma ISO 27001 y las políticas internas.

A continuación, se detallan las situaciones observadas durante estas pruebas de recorrido:

1. **Control de Acceso:** La UPRA gestiona los accesos privilegiados mediante Access Control IAM y aplica autenticación de doble factor. El cambio de contraseñas es obligatorio cada 90 días, con un requisito mínimo de 12 caracteres. Existen controles de acceso físicos y monitoreo en el centro de datos, además de restricciones en el acceso al código fuente, limitado al equipo de sistemas de información.

   Se implementa un enfoque de "cero confianza" en la red, desconectando dispositivos no autorizados y limitando el uso de dispositivos personales. Los accesos están definidos por niveles de rol, y se revisan anualmente para asegurar su actualización según cambios de responsabilidad. El acceso a aplicaciones y sistemas se otorga únicamente con aprobación formal y supervisión, asegurando que solo personal autorizado tenga acceso, con cuentas intransferibles.

   Los servicios de red se mantienen seguros y actualizados, y existe un proceso formal para gestionar el ciclo de vida de los accesos en la plataforma SEA. Cada usuario posee una llave única en el directorio activo, fortaleciendo el control de seguridad en el acceso a los sistemas.

2. **Gestión de incidentes:** La UPRA cuenta con un procedimiento formal y documentado para la gestión de incidentes de seguridad de la información, que define claramente las responsabilidades, etapas y acciones para la identificación, respuesta, análisis y seguimiento de los incidentes. Este proceso incluye canales específicos de reporte (SEA, correo electrónico, teléfono y contacto directo con el oficial de seguridad) y garantiza una respuesta oportuna que minimiza el impacto en las operaciones. Adicionalmente, el procedimiento asegura la evaluación adecuada de los eventos reportados para determinar su clasificación como incidentes de seguridad y la recolección de pruebas válidas para futuras investigaciones. Los incidentes son registrados y analizados para identificar patrones y mejorar la respuesta a través del uso de inteligencia de amenazas, fortaleciendo así la seguridad de la organización y cumpliendo con las normativas vigentes.

3. **Continuidad del negocio:** No se pudo evidenciar que la UPRA haya realizado un Análisis de Impacto al Negocio (BIA) ni un perfil de riesgos que identifique vulnerabilidades y el impacto de interrupciones en la seguridad de la información. Tampoco se verificaron servicios de alta disponibilidad para minimizar interrupciones en el acceso a la información. Además, la entidad no cuenta con un plan de continuidad integral ni con un Plan de Recuperación de Desastres Informáticos para gestionar fallas e incidentes de manera eficaz. No se han identificado ni priorizado los activos críticos de información, y no existen pruebas documentadas de servicios críticos ni actualizaciones en el plan de continuidad. Finalmente, el plan actual no contempla cómo los incidentes de seguridad impactan la operación ni ofrece un registro o base de conocimiento para la resolución rápida de problemas.

4. **Gestión de activos:** Se confirmó la existencia de un inventario formal y actualizado de los activos de información, revisado anualmente conforme a los criterios de confidencialidad, integridad y disponibilidad. Se observó que los procesos de eliminación de activos cumplen con los requisitos de seguridad. Sin embargo, algunos empleados no conocen claramente el procedimiento para la devolución de activos al finalizar contratos. Además, cada líder de proceso es responsable de gestionar la clasificación de usuarios autorizados y almacenar la información en las Tablas de Retención Documental (TRD). Aunque las políticas de seguridad establecen directrices claras para actividades no autorizadas, se identificó un incumplimiento en la directriz de deshabilitación de puertos USB durante las pruebas, al encontrarse algunos habilitados sin autorización.

5. **Datos personales:** La UPRA cumple parcialmente con la Ley 1581 de 2012, contando con una política de tratamiento de datos personales documentada y accesible, aunque carece de un protocolo específico para gestionar incidentes relacionados con datos personales y no realiza auditorías internas o externas para verificar el cumplimiento. Se observó que NO se mencionan autorizaciones para el tratamiento de datos de referencias comerciales, ni se ha establecido un programa de capacitación regular en protección de datos para el personal. Aunque la recolección de datos biométricos se realiza adecuadamente para el registro de visitantes, no se abordan temas como la transferencia internacional de datos, ni se designa un oficial de cumplimiento. Tampoco se colocan avisos visibles sobre videovigilancia y no existen medidas específicas para proteger a menores frente a riesgos digitales como el ciberbullying.

La UPRA ha implementado controles de seguridad en gestión de accesos y respuesta a incidentes, incluyendo autenticación de doble factor y un enfoque de "cero confianza". Sin embargo, presenta deficiencias en la continuidad del negocio, al no contar con un Análisis de Impacto al Negocio (BIA), un plan de recuperación ante desastres ni servicios de alta disponibilidad. En gestión de activos, aunque existe un inventario actualizado, hay falta de conocimiento sobre el proceso de devolución y cumplimiento incompleto en deshabilitación de puertos USB. En protección de datos personales, cumple parcialmente con la Ley 1581, pero carece de un protocolo específico para incidentes, auditorías de cumplimiento, y medidas claras para videovigilancia y protección de menores. Estos aspectos representan oportunidades de mejora para fortalecer su postura de seguridad.

3.3.2 Controles de Personas

En la norma ISO 27001, los controles de personas tienen un papel fundamental en la gestión de la seguridad de la información, ya que reconocen que los empleados y contratistas son clave para proteger la confidencialidad, integridad y disponibilidad de la información. Estos controles se enfocan en reducir riesgos derivados de errores humanos, accesos no autorizados o incumplimiento de políticas internas. Incluyen prácticas como la selección adecuada del personal, formación y concienciación continua en seguridad de la información, y procedimientos claros para la gestión de accesos y responsabilidades. Asegurar que todos los individuos entiendan y cumplan con las políticas de seguridad fortalece la cultura organizacional y minimiza los riesgos asociados al factor humano.

3.3.2.1 Revisión documental

Durante el ejercicio de auditoría se realizó una exhaustiva revisión documental de los controles de personas implementados por la UPRA en conformidad con su política de seguridad de la información (GST-MA-002-Política de Seguridad de la Información) y alineados con la norma ISO 27001. A continuación, se resumen las principales situaciones observadas:

1. **Selección**: Se verificó que en la sección 6.3 de la Política de Seguridad de la información, se menciona que "*los antecedentes de los candidatos, incluyendo formación, experiencia, verificaciones de títulos y referencias, deben ser revisados antes de la contratación*"; durante las pruebas se revisa con contratación la verificación de formación y experiencia, confirmando que NO se realiza tal verificación ya que la entidad se acoge al derecho de presunción de buena fe.

2. **Términos y Condiciones de Empleo**: Los contratos de trabajo y de servicios incluyen cláusulas de confidencialidad y compromisos de manejo adecuado de la información, asegurando la obligatoriedad del cumplimiento de las políticas de seguridad por parte de los empleados y contratistas.

3. **Conciencia de Seguridad, Educación y Formación**: La UPRA cuenta con un plan formal de capacitación continua en seguridad de la información dirigido a todo el personal, con el fin de asegurar que comprendan sus responsabilidades en la gestión de la seguridad. Durante la verificación de este control, se realizaron entrevistas al personal, identificando la necesidad de reforzar y mantener los esfuerzos en concientización, educación y formación. Los resultados obtenidos en esta prueba se detallan en el numeral 4.3.2.2 Pruebas de Recorrido.

4. **Proceso Disciplinario**: Se verificó que en la sección 7.2.2 de la política de Seguridad de la Información, se menciona que "*lleva a cabo acciones de revisión del cumplimiento de las políticas de seguridad de la información de la Entidad. Estas acciones establecen un proceso disciplinario formal para los servidores públicos y de sanciones por incumplimiento de obligaciones contractuales a los contratistas que hayan cometido alguna violación a los lineamientos establecidos en el presente manual.";* durante las pruebas de recorrido se hace revisión del procedimiento Control Interno Disciplinario (GDR-PD-002) y NO tiene directrices relacionadas con incumplimientos en temas relacionados con seguridad de la información.

5. **Responsabilidades después de la Terminación o Cambio de Empleo**: La política incluye un procedimiento para revocar accesos, recuperar activos y proteger la información después de la terminación o cambio de empleo, garantizando la seguridad continua de la información.

6. **Acuerdos de Confidencialidad o No Divulgación**: Antes de compartir información con terceros o realizar intercambios de información, se establecen acuerdos de confidencialidad vigentes, protegiendo la información de posibles riesgos; en la verificación del anexo contractual se identifica que NO existen directrices claras con respecto al tratamiento de la información confidencial, prohibición de divulgación a terceros sin consentimiento, notificación en caso de obligación legal de divulgación, responsabilidad y compromiso de indemnización y vigencia de obligaciones de confidencialidad después del contrato.

7. **Trabajo Remoto**: Se aplican medidas de seguridad específicas para el trabajo remoto, que incluyen el uso de conexiones seguras, controles de acceso y la protección de los datos gestionados fuera de las instalaciones de la entidad.

8. **Informes de Eventos de Seguridad de la Información**: Se han implementado canales adecuados para que empleados y contratistas reporten incidentes de seguridad de manera oportuna. Además, se promueve la identificación y notificación de debilidades en la seguridad, permitiendo la comunicación de vulnerabilidades y riesgos detectados.

Este análisis evidenció que la UPRA ha implementado importantes controles de personas en alineación con la política de seguridad de la información y la norma ISO 27001, se recomienda fortalecer ciertos aspectos, como la verificación de antecedentes en la selección de personal, el proceso disciplinario y las directrices en acuerdos de confidencialidad con terceros, para mejorar la efectividad general en la protección de los activos de información. Esto es necesario ya que se evidencian incumplimientos en algunas directrices descritas en la política de seguridad de la información, lo que podría afectar la integridad y cumplimiento de los estándares de seguridad establecidos por la entidad.

3.3.2.2 Pruebas de recorrido

Durante las pruebas de recorrido realizadas los días 2 y 3 de octubre, se evidenciaron los controles relacionados con controles de recurso humano, capacitación y concientización en Seguridad de la Información, los cuales permitieron observar y verificar en campo la implementación y efectividad de estos, para gestionar la seguridad de la información, en conformidad con las directrices de la norma ISO 27001 y las políticas internas.

A continuación, se detallan las situaciones observadas durante estas pruebas de recorrido:

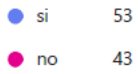
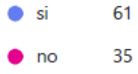
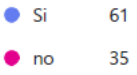
1. **Recurso humano**: En el proceso de selección, se verifica la autorización para el tratamiento de datos personales, aunque no se revisan antecedentes de formación y experiencia debido a la presunción de buena fe. A los nuevos empleados se les asignan accesos y perfiles según sus roles, con restricciones para evitar accesos no autorizados, bajo la supervisión del líder del proceso.

   Las revisiones muestran que, al finalizar la relación laboral, los accesos son retirados de inmediato. También se monitorean y desactivan roles y credenciales de acceso a sistemas e instalaciones. Durante la ejecución contractual, se realizan entregas parciales y se devuelve el equipo al final del contrato con un paz y salvo.

   En el Formato Guía del proceso disciplinario, no se identificaron sanciones específicas por incumplimientos de las políticas de seguridad de la información.

   La UPRA ha implementado un plan regular de capacitaciones en seguridad de la información dirigido a todos los empleados, con una directriz específica en el proceso de inducción que enfatiza la importancia de conocer y adherirse a la política de seguridad. Se realiza un seguimiento continuo de estas actividades y se toman medidas basadas en los resultados obtenidos.

Para evaluar la cultura en seguridad de la información, se aplicaron entrevistas a una muestra representativa de la población total, que incluye 29 funcionarios y 527 contratistas. La muestra seleccionada determinó la realización de entrevistas a 12 funcionarios y 82 contratistas, sumando un total de 94 entrevistas. De estas, 18 se llevaron a cabo de manera presencial los días 2 y 3 de octubre, coincidiendo con las pruebas de recorrido, al personal que se encontraba en la oficina. Las restantes se realizaron mediante un formulario en Google, obteniendo los siguientes resultados:

1. ¿Conoce usted la política de seguridad de la información? 	2. ¿Cuáles son sus responsabilidades y funciones frente a la seguridad de la información? 
3. ¿Conoce que es un activo de información? 	4. ¿Indique 3 activos de información a su cargo? 
5. ¿En caso de que ocurra un incidente de seguridad sabría reportarlo? 	6. ¿Como reportaría un incidente de información y a quién? 

Para las preguntas 2, 4 y 6, el valor reflejado corresponde al número de personas que dieron una respuesta positiva, es decir, que conocían la respuesta a lo que se les consultaba. Este valor debe interpretarse en relación con un total de 94 respuestas posibles.

La revisión de las encuestas de seguridad de la información revela una mezcla en el nivel de conocimiento y preparación del personal de la UPRA. De los encuestados, 53 reconocen estar familiarizados con la política de seguridad de la información, mientras que 43 indican desconocerla. Asimismo, aunque 61 personas mencionan saber cómo reportar un incidente de seguridad, aún hay 35 que no están seguras de los procedimientos de reporte. Esta variabilidad sugiere la necesidad de reforzar el entrenamiento y la concienciación en seguridad de la información, asegurando que todos los empleados y contratistas comprendan sus responsabilidades y sepan actuar adecuadamente en caso de incidentes.

3.3.3 Controles Físicos

Los controles físicos en el contexto de la norma ISO 27001 están diseñados para proteger los activos de información de una organización contra amenazas físicas y ambientales. Estos controles abarcan medidas de seguridad como el control de acceso a instalaciones, sistemas de videovigilancia, protección contra incendios, y otras barreras que aseguran que solo el personal autorizado tenga acceso a áreas sensibles, como centros de datos o archivos confidenciales. Además, incluyen estrategias para mitigar el riesgo de daños por desastres naturales, fallas eléctricas y otras contingencias ambientales. Implementar controles físicos efectivos es fundamental para mantener la confidencialidad, integridad y disponibilidad de la información, reduciendo así el riesgo de accesos no autorizados, pérdidas o interrupciones en la operación.

3.3.3.1 Revisión documental

Durante el ejercicio de auditoría se realizó una exhaustiva revisión documental de los controles de personas implementados por la UPRA en conformidad con su política de seguridad de la información (GST-MA-002-Política de Seguridad de la Información) y alineados con la norma ISO 27001. A continuación, se resumen las principales situaciones observadas:

1. **Perímetros de Seguridad y Entrada Física**: Las áreas críticas que contienen información sensible están protegidas mediante barreras físicas, tales como cerraduras, tarjetas de acceso y sistemas biométricos, limitando el acceso a personal autorizado y protegiendo la integridad de la información.

2. **Protección en Oficinas y Monitoreo de Seguridad:** Existen medidas para asegurar oficinas y estaciones de trabajo, incluyendo políticas de "pantallas limpias" y protectores de pantalla. Además, se cuenta con sistemas de monitoreo como cámaras de vigilancia que permiten una supervisión continua de las áreas seguras.

3. **Protección contra Amenazas Ambientales**: Los activos de información están protegidos contra riesgos físicos y ambientales mediante detectores de humo, sistemas de control de garantizando la continuidad de la operación en caso de emergencia.

4. **Control de Personal en Áreas Seguras**: Se establecen procedimientos para controlar y supervisar las actividades del personal en áreas seguras, verificando la identidad de quienes ingresan y monitoreando sus actividades dentro de estas zonas.

5. **Políticas de "Escritorio y Pantalla Limpios":** La política de "escritorio limpio" exige que los empleados apaguen las pantallas y aseguren sus estaciones de trabajo al ausentarse, además de almacenar documentos sensibles en lugares seguros.

6. **Emplazamiento y Seguridad de Equipos:** Los equipos críticos están protegidos contra condiciones ambientales y accesos no autorizados, con medidas como ubicaciones en áreas seguras, ventilación adecuada y protección contra sobrecargas eléctricas.

7. **Seguridad de Activos Fuera de las Instalaciones:** Los activos utilizados fuera de las instalaciones cuentan con medidas de protección, como cifrado de datos y uso de redes seguras, garantizando la seguridad de la información fuera de la organización.

8. **Manejo y Eliminación Segura de Medios de Almacenamiento**: Existe un manejo cuidadoso de dispositivos extraíbles con requisitos de cifrado. Además, se han establecido procedimientos para la eliminación segura de datos, asegurando que la información no pueda recuperarse después de la disposición o reutilización de equipos.

9. **Control de Equipos que Salen de la Organización**: Los equipos que contienen información sensible están sujetos a un estricto control y autorización antes de salir de las instalaciones, incluyendo el registro de su salida mediante la mesa de ayuda. Durante las pruebas de recorrido se verifico que NO existe ningún control relacionado con la entrada y/o salida de equipo de la organización.

10. **Protección del Cableado y Mantenimiento de Equipos**: Los sistemas de cableado cuentan con protecciones adecuadas contra accesos no autorizados y daños físicos. Asimismo, se realizan mantenimientos preventivos y correctivos a los equipos para asegurar su buen funcionamiento. Durante las pruebas de recorrido se verifico que NO se tiene un con una inspección adecuada al estado y organización del cableado en el Data Center.

Estos resultados muestran la UPRA ha implementado controles físicos sólidos para proteger los activos de información, incluyendo barreras de acceso, sistemas de monitoreo, políticas de "escritorio limpio" y medidas de protección contra amenazas ambientales. Sin embargo, se identificaron áreas de mejora: no existen controles para la entrada y salida de equipos, y el cableado en el Data Center carece de organización y mantenimiento adecuados. Estos aspectos deben fortalecerse para asegurar un cumplimiento efectivo de los estándares de seguridad de la información según la norma ISO 27001.

3.3.3.2 Pruebas de recorrido

Durante las pruebas de recorrido realizadas los días 2 y 3 de octubre, se evidenciaron los controles relacionados con controles físicos, los cuales permitieron observar y verificar en campo la implementación y efectividad de estos, para gestionar la seguridad de la información, en conformidad con las directrices de la norma ISO 27001 y las políticas internas.

A continuación, se detallan las situaciones observadas durante estas pruebas de recorrido:

1. **Controles Físicos:** Durante la auditoría se comprobó que el acceso al Data Center de la UPRA está restringido mediante llaves y verificación biométrica, limitado a tres personas clave, garantizando un control adecuado de seguridad. Aunque los equipos que salen no contienen información sensible, corresponden a dispositivos personales de contratistas, por lo que se sugiere establecer directrices para su protección fuera de las instalaciones.

Los controles de acceso físico en las instalaciones incluyen autenticación por huella dactilar en la entrada principal, pero carecen de un registro formal de entrada y salida de equipos. Además, se identificaron elementos inapropiados almacenados en el área del Data Center, lo que representa un riesgo adicional.

El Data Center se encuentra en un área segura, cuenta con protección ante desastres y dispone de un sistema UPS para garantizar su operatividad ante fallas eléctricas. No obstante, se detectó una falta de organización en el cableado, lo que podría causar interrupciones, por lo que se recomienda una revisión y reordenamiento para asegurar la continuidad operativa.

La auditoría del Data Center de la UPRA confirma controles de acceso adecuados, pero recomienda mejorar la protección de dispositivos personales, reorganizar el cableado y retirar materiales inapropiados para reducir riesgos y asegurar la continuidad operativa.

3.3.4 Controles Tecnológicos

Los controles tecnológicos establecidos en la norma ISO 27001 son fundamentales para proteger la integridad, confidencialidad y disponibilidad de la información en las organizaciones. Estos controles se enfocan en implementar y gestionar tecnologías que protejan los sistemas de información contra amenazas y vulnerabilidades, asegurando un entorno seguro para el procesamiento y almacenamiento de datos.

Entre las principales medidas tecnológicas de seguridad incluidas en la ISO 27001 se encuentran la gestión de accesos, la protección contra software malicioso, el cifrado de información, y el monitoreo continuo de la actividad en la red y los sistemas. La adecuada implementación de estos controles permite detectar y responder eficazmente a incidentes de seguridad, minimizando los riesgos y garantizando la continuidad operativa en un entorno digital cada vez más complejo y desafiante.

3.3.4.1 Revisión documental

Durante el ejercicio de auditoría se realizó una exhaustiva revisión documental de los controles de personas implementados por la UPRA en conformidad con su política de seguridad de la información (GST-MA-002-Política de Seguridad de la Información) y alineados con la norma ISO 27001. A continuación, se resumen las principales situaciones observadas:

1. **Dispositivos de Punto Final de Usuario**: Se aplican medidas de control para dispositivos móviles, incluyendo la restricción de aplicaciones no autorizadas y la implementación de políticas de escritorio limpio para proteger la información cuando los empleados se ausentan de sus puestos.

2. **Acceso y Permisos Especiales:** Se definen procesos específicos para la asignación de permisos de acceso privilegiado, restringiendo los accesos a usuarios que los necesiten para sus funciones, con autorizaciones personales e intransferibles.

3. **Restricción de Acceso y Código Fuente**: Se establecen niveles de acceso según los roles y responsabilidades. El acceso al código fuente de los programas está centralizado, controlado y restringido solo a personal autorizado.

4. **Autenticación y Protección contra Malware**: Se utilizan contraseñas seguras y autenticación de doble factor para el acceso a los sistemas. También se implementan herramientas para detectar y prevenir el software malicioso.

5. **Gestión de Vulnerabilidades y Configuración:** Se realizan pruebas de vulnerabilidades periódicas y se controlan las configuraciones de los sistemas para evitar brechas de seguridad.

6. **Eliminación y Protección de Información**: Existen políticas para la eliminación segura de información sensible, aunque se observa que el enmascaramiento de datos no está detallado.

7. **Respaldo y Redundancia:** La UPRA realiza copias de seguridad periódicas y considera la disponibilidad de sistemas críticos, aunque no se describe un esquema detallado de redundancia.

8. **Control y Registro de Actividades:** Se lleva un registro detallado de eventos, incluyendo intentos de acceso fallidos y exitosos, y se realizan auditorías de seguridad. Los administradores deben generar logs para facilitar la trazabilidad y revisión periódica de actividades.

9. **Control de Cambios y Pruebas de Seguridad:** Existen procedimientos de control de cambios, pruebas de aceptación de sistemas y requisitos para desarrollo seguro. Los cambios en software de terceros se someten a revisión del comité de control de cambios.

La UPRA ha implementado controles tecnológicos sólidos, incluyendo medidas de seguridad para dispositivos móviles, gestión de accesos privilegiados, autenticación segura, y pruebas de vulnerabilidades. También se realizan copias de seguridad y registros de actividades, aunque se sugiere mejorar el enmascaramiento de datos y establecer un esquema de redundancia más detallado para fortalecer la seguridad de la información.

3.3.4.2 Pruebas de Recorrido

Durante las pruebas de recorrido realizadas los días 2 y 3 de octubre, se evidenciaron los controles relacionados con controles de operaciones, comunicaciones y desarrollo seguro, los cuales permitieron observar y verificar en campo la implementación y efectividad de estos, para gestionar la seguridad de la información, en conformidad con las directrices de la norma ISO 27001 y las políticas internas.

A continuación, se detallan las situaciones observadas durante estas pruebas de recorrido:

1. **Controles de operaciones:** La auditoría de la UPRA evidenció un proceso de gestión de cambios documentado y actualizado, con aprobación formal del Comité de Cambios. Se realizan actualizaciones de servidores y controles de vulnerabilidades semestrales, incluyendo un análisis y plan de cierre. Existe un plan de copias de seguridad para 2024, aunque faltan respaldos en algunos sistemas. Se observaron pruebas de restauración en ciertos sistemas, pero no en todos. El desarrollo

de software mantiene una clara separación entre los entornos de desarrollo y pruebas, lo que mejora la seguridad. Los sistemas implementan controles de antivirus y antimalware automáticos mediante Microsoft, junto con restricciones de instalación de software a través de Active Directory, reforzando la seguridad en los dispositivos de la organización.

2. **Controles de comunicaciones:** La auditoría revela que la UPRA implementa medidas de seguridad para la protección de la información. A través de Fortigate, se controlan el tráfico y las comunicaciones, aplicando políticas de integridad y confidencialidad. La red está segmentada para restringir accesos, y Microsoft Defender se utiliza para inteligencia de amenazas, manteniendo el sistema monitoreado contra riesgos. Además, las VPN se configuran para acceso remoto seguro, y se controlan las comunicaciones de mensajería corporativa para fines laborales. Los lineamientos de transferencia y confidencialidad de la información están documentados en políticas, asegurando que los datos sensibles se manejen de acuerdo con las normas establecidas.

3. **Controles de desarrollo seguro**: La auditoría confirma que la UPRA gestiona los cambios en sistemas de información mediante registros formales y aprobaciones del comité de cambios, siguiendo el formato establecido. En el proyecto SIRIIAGRO, se realizaron sesiones formales de derechos patrimoniales, y las migraciones de datos se llevaron a cabo con planes documentados que aseguran una transición segura y responsable. Los entornos de desarrollo y pruebas están separados, y se ejecutan pruebas funcionales, de regresión y de seguridad de acuerdo con los requisitos de seguridad definidos en la TRD. Además, la UPRA implementa controles de desarrollo seguro, usando herramientas de gestión de versiones y enmascaramiento de datos, asegurando que todos los sistemas cumplen con los estándares de calidad y requisitos de seguridad.

La auditoría a la UPRA destaca una gestión robusta en operaciones, comunicaciones y desarrollo seguro de sistemas de información. En operaciones, la gestión de cambios y actualizaciones de servidores están bien documentadas y supervisadas, con controles de vulnerabilidad semestrales y un plan de respaldo que aún requiere ampliar su cobertura. En comunicaciones, se utilizan Fortigate y Microsoft Defender para proteger la información, segmentar redes y monitorizar amenazas, con políticas que aseguran el manejo adecuado de datos sensibles. En desarrollo seguro, la separación de entornos y el uso de herramientas de gestión de versiones y enmascaramiento de datos garantizan que los sistemas cumplan con estándares de seguridad y calidad. Estos controles fortalecen la infraestructura de TI de la UPRA y su alineación con buenas prácticas de seguridad.

3.4 Observaciones

3.4.1 Observación N° 1. Deficiencias en el diseño de los controles asociados a los riesgos del Proceso Gestión de Servicios Tecnológicos.

Durante la auditoría realizada sobre 13 riesgos y 33 controles del proceso de Gestión de Servicios Tecnológicos, de acuerdo con el mapa de riesgos (versión4, publicada en el Sistema de Gestión el 15/08/2023), se evidenció la existencia de deficiencias en el diseño de 16 controles aplicados a 8 riesgos. Cabe destacar que, a pesar de

estas falencias, todos los controles del proceso se están ejecutando. A continuación, se describen los 16 controles con deficiencias identificadas:

Riesgo1: Controles 1 y 2, **Riesgo3:** Controles 1 y 2, **Riesgo4:** Control 2, **Riesgo6**: Controles1, 2 y 3, **Riesgo7**: Controles1, 2 y 3, **Riesgo9**: Control 1, **Riesgo10**: Controles 1 y 2 y para el **Riesgo11:** Controles 1 y 3.

Para información más detallada remitirse al Anexo 1. Análisis de Riesgos y Controles.

Criterio:

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6.- noviembre de 2022.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4. – octubre de 2018.
- Guía Política de Administración de Riesgos de la UPRA, V6 (PEC-GU-001).

Recomendación:

Se recomienda revisar el diseño de los controles objeto de evaluación con respecto a las variables definidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4. – octubre de 2018 para el adecuado diseño de controles y de esta manera subsanar las deficiencias identificadas durante la auditoría y obtener una correcta mitigación del riesgo.

3.4.2 Observación N° 2. Ausencia de Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP) formalizados

Durante la auditoría de la Política de Seguridad de la Información en UPRA, se evidenció la falta de un plan formal de continuidad del negocio (BCP) y un plan de recuperación ante desastres (DRP). Esto compromete la capacidad de la entidad para asegurar la disponibilidad y seguridad de la información. Se identificaron tres deficiencias clave: la ausencia de un Análisis de Impacto en el Negocio (BIA) para priorizar activos críticos, la falta de pruebas periódicas de disponibilidad de servicios esenciales, y la carencia de una priorización de recursos clave. Estas omisiones afectan la preparación y respuesta de UPRA ante incidentes, resaltando la necesidad de un BCP y DRP que aborde recursos físicos, tecnológicos y de infraestructura para fortalecer la resiliencia operativa.

Criterio:

- Política de Gobierno Digital emitida por MinTIC.
- NTC-ISO/IEC 27001:2013 y 2022.
- Modelo de Seguridad y Privacidad de la Información MSPI emitido por MinTIC.
- GST-MA-002-Política de Seguridad de la Información.

Recomendación:

Se recomienda definir, formalizar e implementar un Plan de Continuidad de Negocio y un Plan de Recuperación de Desastres, asegurando pruebas y actualizaciones periódicas para mantener la resiliencia operativa y proteger la integridad, disponibilidad y confidencialidad de la información frente a posibles incidentes y desastres.

3.4.3 Observación N° 3. Ausencia de Documentación para la implementación de la Política de Protección de Datos Personales e Información Propiedad o Bajo Protección de la UPRA

Durante la auditoría a la página web y al Manual de Política de Protección de Datos Personales e Información bajo protección de la UPRA, se evidenció la ausencia de documentación que permita gestionar incidentes relacionados con datos personales, la autorización para el tratamiento de referencias comerciales y personales, y los lineamientos para la transferencia internacional de datos. Implementar estas acciones garantizará el cumplimiento de las normativas vigentes y fortalecerá la efectividad de las medidas de seguridad implementadas.

Criterio:

- Ley 1581 de 2012.
- NTC-ISO/IEC 27001:2013 y 2022.
- GST-MA-004 manual de política de protección de datos personales e información propiedad o bajo protección de la UPRA
- GST-FT-012 Formato autorización para el tratamiento de datos personales

Recomendación:

Se recomienda fortalecer la política de protección de datos mediante el desarrollo y documentación específica para la gestión de incidentes, el manejo de autorizaciones y la transferencia internacional de datos. Adicionalmente, es fundamental contar con un oficial o comité de protección de datos personales que supervise el cumplimiento de estas políticas. También se sugiere establecer un programa de capacitación en protección de datos para el personal y realizar auditorías periódicas, con el fin de garantizar el cumplimiento normativo y la protección integral de los datos personales.

3.4.4 Observación N° 4. Incumplimiento de algunas de las Directrices Definidas en el Manual de Política de Seguridad de la Información.

Durante la auditoría a la Política de Seguridad de la Información, se realizaron entrevistas con base en una muestra de 12 funcionarios y 82 contratistas, de las cuales 18 fueron presenciales durante las pruebas de recorrido y 76 mediante encuestas en Google Forms. Los resultados evidenciaron incumplimientos en algunas directrices de Seguridad de la información: Durante la Interrupción, Selección, Proceso Disciplinario, Acuerdos de Confidencialidad o No Divulgación, Equipos que Salen de la Organización, Cableado, Mantenimiento de Equipos y Dispositivos de Punto Final de Usuario, lo cual afecta la adecuada gestión de procesos críticos,

debilita la efectividad de las políticas y compromete la confidencialidad, integridad y disponibilidad de los recursos de la organización.

Criterio:

- NTC-ISO/IEC 27001:2013 y 2022.
- GST-MA-002-Política de Seguridad de la Información
- Pruebas de recorrido

Recomendación:

Se recomienda asegurar el cumplimiento de las directrices establecidas en el manual de políticas de seguridad de la información mediante la implementación de mecanismos de monitoreo y auditoría regular. Esto incluye reforzar el seguimiento a los procedimientos críticos, garantizando que todas las áreas operen conforme a las políticas definidas.

3.5 Oportunidades de Mejora

3.5.1 Se ha identificado la necesidad de recalificar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) para aquellos controles que actualmente están calificados al 100%, dado que aún requieren mejoras para alcanzar ese nivel. Esta recalificación permitirá una evaluación más precisa permitiendo que los controles se mantengan efectivos y relevantes en la gestión actual de riesgos.

3.5.2 Se recomienda implementar una revisión exhaustiva del cableado y de los elementos presentes en el Data Center para garantizar el cumplimiento de las normas de seguridad y orden en el área. Esto incluye inspeccionar el estado y organización del cableado para evitar riesgos de interferencia, accidentes o daños, así como identificar y remover cualquier equipo o material no esencial para la operación del Data Center. En particular, se debe prestar atención a la presencia de cajas de cartón, que representan un riesgo de incendio y deben ser eliminadas de inmediato.

3.5.3 Establecer un proceso formal para controlar la entrada y salida de equipos, con un registro detallado de cada equipo, roles específicos de supervisión y auditorías periódicas para asegurar cumplimiento. Esto mejorará la seguridad y trazabilidad de los activos.

3.5.4 Definir acciones y articularlas con el procedimiento disciplinario para atender violaciones de seguridad de la información, con medidas según la infracción. Establecer un proceso de investigación de los casos pertinentes y reforzar la capacitación a los empleados. Esta medida fortalecerá la cultura de seguridad y protegerá los activos de información de la organización.

4.5.5 Para fortalecer la confidencialidad y la seguridad de la información en el anexo contractual, se recomienda incorporar las cláusulas relacionadas con: Especificidad en el Tratamiento de Información Confidencial, Prohibición de Divulgación a Terceros sin Consentimiento, Notificación en Caso de Obligación Legal de Divulgación, Responsabilidad y Compromiso de Indemnización y Vigencia de las Obligaciones de Confidencialidad Post-Contrato, asegurando así un mayor control y protección de la información sensible y alineándose mejor con los estándares de seguridad de la información.

4.5.6 Se recomienda implementar un proceso de verificación de antecedentes para el personal que accede a información sensible, alineado con las buenas prácticas de la norma ISO 27001. Aunque actualmente la entidad se rige por el principio de presunción de buena fé, la verificación de antecedentes permite gestionar mejor los riesgos de seguridad de la información, especialmente en roles críticos. Este proceso fortalecerá la protección de los activos de información y garantizará que el personal cumpla con los estándares de confianza necesarios para la seguridad de la entidad.

4.5.7 Se recomienda incluir referencias claras en el Manual de Política de Seguridad de la Información, indicando dónde se puede encontrar el manual, las guías, procedimientos, registros y actas que evidencien la implementación de los requisitos. Además, es importante mantener toda la información relacionada con el proyecto de Seguridad Digital actualizada y centralizada en la TRD.

4. CONCLUSIONES

- La auditoría al proceso de Gestión de Servicios Tecnológicos de la UPRA, basada en la NTC-ISO/IEC 27001 y alineada con el MSPI de MinTIC, identificó fortalezas y áreas de mejora en la seguridad de la información. Aunque se cuenta con una política de seguridad digital integral, es necesario reforzar prácticas de control en todas las etapas del ciclo de vida de la seguridad para mitigar riesgos tecnológicos. La optimización de estos controles permitirá a la UPRA mejorar la gestión de sus activos digitales y consolidar la confianza de los usuarios.

- Es necesario fortalecer la cultura de seguridad de la información en la UPRA, ya que las entrevistas realizadas a los empleados reflejan un alto nivel de desconocimiento en cuanto a las políticas de seguridad y la gestión de incidentes. Este resultado evidencia la importancia de implementar programas de sensibilización y capacitación que aseguren que todos los colaboradores comprendan y apliquen los lineamientos de seguridad, contribuyendo así a una gestión de riesgos más efectiva y a la protección integral de los activos de información de la organización.

- Es pertinente establecer un plan de continuidad es esencial para asegurar la resiliencia y sostenibilidad de los servicios críticos en la organización. La ausencia de este plan aumenta significativamente el riesgo de interrupciones prolongadas en caso de incidentes, comprometiendo la operatividad, seguridad de la información y confianza de las partes interesadas. Un plan de continuidad bien estructurado permite responder de manera eficaz ante eventos adversos, minimizando el impacto en las operaciones y protegiendo la integridad y disponibilidad de los recursos tecnológicos y de información.

- Durante las pruebas de recorrido se constató que los controles relacionados con control de acceso, seguridad de las operaciones y comunicaciones, desarrollo seguro, gestión de incidentes y gestión de activos están correctamente estructurados e implementados. Sin embargo, se recomienda continuar aplicando buenas prácticas y realizar auditorías periódicas para supervisar los controles asociados a los procesos críticos, garantizando así su eficacia y mejora continua.